SANS La référence mondiale en formation, recherche et certification à la sécurité des systèmes d'information

Formations et certifications en CYBERSÉCURITÉ

100+
formateurs certifiés SANS Certified Instructor

40 000+
professionnels formés dans le monde chaque année

Découvrez à l'intérieur nos deux formats en ligne SANS Online Training.
Formez-vous quand vous voulez, où vous voulez.

Découvrez notre
catalogue complet des produits SANS disponibles en Europe, au Moyen-Orient, en Afrique et en Asie-Pacifique

Cursus de formations SANS

Sécurité, inforensique et réponse aux incidents, test d'intrusion, audit informatique, sécurité du cloud, management, systèmes de contrôle industriel (ICS), défense, tactiques *Purple Team*

GIAC CERTIFICATIONS

À propos de SANS

SANS est la référence mondiale de la formation en cybersécurité. Fondé en 1989 et présent dans le monde entier, SANS a déjà formé plus de 200 000 professionnels.

Depuis plus de 30 ans, nous collaborons avec de nombreuses grandes entreprises de renommée mondiale, des institutions militaires et des gouvernements.

La technologie a certes évolué au cours de cette période, mais notre mission première reste la même : protéger les personnes et les actifs par le partage de connaissances et de compétences de pointe en cybersécurité.

Une force humaine
Les formateurs SANS sont avant tout des professionnels de l'industrie, riches d'une expérience acquise sur le terrain ; une expérience qu'ils apportent tout naturellement durant les formations.

Nos formateurs sont nombreux à collaborer avec des organisations influentes. Ils sont responsables ***Red Team***, agents de lutte contre la cybercriminalité, directeurs techniques, RSSI, collaborateurs chercheurs...

Outre un bagage technique respectable, ils ont une expertise certaine dans l'enseignement. Ils savent communiquer leur passion, ce qui facilite l'apprentissage dans les classes SANS.

Une formation de pointe
La cybercriminalité est en évolution constante. SANS prépare ses stagiaires à faire face aux menaces prévalentes et à relever les défis de demain.

Pour ce faire, nos cours et nos supports pédagogiques sont constamment revus et mis à jour. Ce processus est piloté par un comité d'experts qui s'appuie sur le consensus de la communauté mondiale en matière de pratiques exemplaires.

Formation ciblée
La formation SANS vise des activités et des compétences spécifiques. Nous proposons plus de 80 cours qui s'alignent sur les rôles, responsabilités et disciplines majeurs des équipes de sécurité.

Les programmes de formation SANS incluent l'inforensique, l'audit, le management, les tests d'intrusion, les systèmes de contrôle industriel (SCI), le développement de logiciels sécurisés et plus encore (voir les pages 14-19). Chaque programme offre une progression qui conduit les professionnels des bases jusqu'aux spécialisations de haut niveau.

Notre formation est pratique. Les stagiaires, immergés en laboratoire, appliquent leurs nouvelles connaissances et affinent leurs compétences.

La promesse SANS
Notre promesse, au cœur de tout ce que nous entreprenons, est la suivante : faire que les stagiaires puissent déployer immédiatement les compétences qu'ils viennent d'acquérir.

La communauté mondiale
SANS Institute est un acteur majeur dans la communauté internationale de la cybersécurité. Nous sommes aux commandes de l'Internet Storm Center, le système d'alerte précoce d'internet.

SANS développe, met à jour et publie une vaste collection de rapports de recherche sur de nombreux aspects de la sécurité de l'information. Ces rapports sont mis à disposition gratuitement.

L'avantage de la certification GIAC
GIAC valide les compétences des professionnels de la sécurité de l'information, attestant que ceux qui sont certifiés ont les connaissances techniques nécessaires pour travailler dans des domaines clés de la cybersécurité.

Les certifications GIAC sont reconnues dans le monde parce qu'elles mesurent des domaines de compétences et de connaissances spécifiques. GIAC propose les seules certifications en cybersécurité qui couvrent des sujets relevant de domaines techniques très pointus.

À ce jour, il existe plus de 35 certifications spécialisées GIAC. Plusieurs certifications GIAC sont acceptées dans le cadre du programme ANSI/ISO/IEC 17024 de certification du personnel.

De nombreux cours de formation SANS sont alignés sur les certifications GIAC. Une formation SANS est donc idéale pour préparer une certification GIAC.

Ce qui fait de SANS le meilleur des organismes de formation
La formation en immersion de SANS mise sur l'aspect intensif et pratique, et nos exercices sont sans équivalent dans le secteur.

Les formateurs et les concepteurs de cours SANS sont des experts et des professionnels de l'industrie. Leur expérience de terrain enrichit leur enseignement et le contenu des formations SANS.

La formation SANS prépare les stagiaires à passer les certifications GIAC. SANS comme GIAC insistent sur l'importance de l'apprentissage pratique.

Comment s'inscrire à une formation SANS
Les formations SANS peuvent être suivies dans le monde entier à distance et en présentiel. En mode présentiel, les formations intensives durent 5 ou 6 jours. Les cours à distance offrent deux options : SANS OnDemand pour des cours sur 4 mois que vous pouvez adapter à votre rythme ou SANS Live Online pour 1 ou 2 semaines de cours en temps réel avec un formateur. Les cours SANS à distance offrent les mêmes avantages que les cours en présentiel, sans nécessité de se déplacer. Vous pouvez suivre les cours en direct, assurés par un formateur et disponibles sur plusieurs fuseaux horaires, ou vous former à votre rythme, à l'heure et à l'endroit qui vous conviennent, grâce à des sessions préenregistrées.

Choisissez votre cours et les modalités de formation, et vivez pleinement l'expérience de formation SANS.

Les stagiaires doivent s'inscrire en ligne sur www.sans.org

Contacter SANS
Royaume-Uni, Europe continentale et pays nordiques : +44 203 384 3470
Moyen-Orient & Afrique : +971 04 431 0761
Australie : +61 2 6174 4581
Inde : +91 974 1900 324
Japon : +81 3 3242 6276
Singapour : +65 8612 5278 / +65 3165 66 81

Ou par courrier électronique :
emea@sans.org (Europe, y compris le Royaume-Uni),
mea@sans.org (Afrique et Moyen-Orient)
asiapacific@sans.org (Asie-Pacifique)

Table des matières

4 Parcours de formation

Envisagez-vous une formation SANS ou une réorientation professionnelle ? Consultez nos parcours de formation en page 4.

30 SANS Cours

Êtes-vous inscrit à votre premier stage de formation SANS ? Consultez nos guides de formation page 30, puis la description des cours à partir de la page 37.

Training Roadmap

The largest and most trusted source of cyber security training, certification, and research in the world

CORE

New to cyber security?

SEC 301 Intro to Information Security
GISF Certification - Information Security Fundamentals

1A You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques Defend & Maintain

The defence-in-depth techniques taught in SEC401 are essential for every security professional. SEC504 provides additional "offence informs defence" knowledge, teaching defence specialists how attacks occur and how to respond. Students with existing core defence skills could begin their training journey with SEC504.

- **SEC 401** Security Essentials Bootcamp Style - GSEC
- **SEC 504** Hacker Tools, Techniques, Exploits, and Incident Handling - GCIH
- **FOR 308** Digital Forensics Essentials

1B You will be responsible for managing security teams or implementations, but do not require hands-on skills

Security Management

- **MGT 512** SANS Security Leadership Essentials For Managers (with Knowledge Compression™) - GSLC
- **SEC 566** Implementing and Auditing the Critical Security Controls – In-Depth - GCCC

INTERMEDIATE

2 You are experienced in security, preparing for a specialised job role or focus

Security Monitoring & Detection

- **SEC 503** Intrusion Detection In-depth - GCIA
- **SEC 511** Continuous Monitoring and Security Operations - GMON

Penetration Testing and Vulnerability Analysis

- **SEC 460** Enterprise Threat and Vulnerability Assessment - GEVA
- **SEC 542** Web App Penetration Testing and Ethical Hacking - GWAPT
- **SEC 560** Network Penetration Testing and Ethical Hacking - GPEN

Incident Response and Enterprise Forensics

- **FOR 500** Windows Forensics Analysis - GCFE
- **FOR 572** Advanced Network Forensics and Analysis - GNFA
- **FOR 508** Advanced Digital Forensics, Incident Response, and Threat Hunting - GCFA

Security Management

- **MGT 414** SANS Training Program for CISSP® Certification - GISP

ADVANCED/SPECIALISED

3 You are a candidate for specialised or advanced training

SANS' comprehensive curriculum enables professionals to deepen their technical skills in key practice areas. It also directly addresses software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

Cyber Defence Operations

- **SEC450** Blue Team Fundamentals: Security Operations and Analysis
- **SEC487** Open-Source Intelligence Gathering (OSINT) and Analysis - GOSI
- **SEC501** Advanced Security Essentials Enterprise Defender - GCED
- **SEC505** Securing Windows and PowerShell Automation - GCWN
- **SEC530** Defensible Security Architecture - GDSA
- **SEC555** SIEM with Tactical Analytics - GCDA
- **SEC566** Implementing and Auditing the Critical Security Controls - In-Depth - GCCC
- **SEC599** Defeating Advanced Adversaries - Implementing Kill Chain Defences - GDAT

Digital Forensics & Incident Response

- **FOR498** Battlefield Forensics & Data Acquisition - GBFA
- **FOR518** Mac Forensic Analysis
- **FOR526** Memory Forensics In-Depth
- **FOR578** Cyber Threat Intelligence - GCTI
- **FOR585** Advanced Smartphone Forensics - GASF
- **FOR610** Reverse-Engineering Malware: Malware Analysis Tools and Techniques - GREM

Security Management

- **MGT514** IT Security Strategic Planning, Policy and Leadership - GSTRT
- **MGT516** Managing Security Vulnerabilities: Enterprise and Cloud
- **MGT525** IT Project Management, Effective Communication, & PMP® Exam Prep - GCPM

Industrial Control Systems Security

- **ICS410** ICS/SCADA Security Essentials - GICSP
- **ICS456** Essentials for NERC Critical Infrastructure Protection - GCIP
- **ICS515** ICS Active Defence and Incident Response - GRID
- **ICS612** ICS Cyber Security In-Depth

Penetration Testing and Ethical Hacking

- **SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise
- **SEC573** Python for Penetration Testers - GPYC
- **SEC575** Mobile Device Security and Ethical Hacking - GMOB
- **SEC617** Wireless Ethical Hacking, Penetration Testing, and Defences - GAWN
- **SEC642** Advanced Web App Penetration Testing and Ethical Hacking
- **SEC660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking - GXPN
- **SEC699** Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection
- **SEC760** Advanced Exploit Development for Penetration Testers

Cloud Security

- **SEC488** Cloud Security Essentials
- **SEC522** Defending Web Applications Security Essentials - GWEB
- **SEC540** Cloud Security and DevOps Automation - GWEB
- **SEC534** Secure DevOps: A Practical Introduction
- **SEC545** Cloud Security Architecture and Operations
- **SEC588** Cloud Penetration Testing

Audit / Legal

- **AUD507** Auditing & Monitoring Networks, Perimeters & Systems - GSNA
- **LEG523** Law of Data Security & Investigations - GLEG

Formats de formation SANS

Fondé en 1989, SANS est la référence mondiale de la formation en cybersécurité

SANS OnDemand

Les cours SANS OnDemand sont enregistrés par les meilleurs spécialistes dans chaque domaine de la cybersécurité. Vos cours en ligne sont accessibles pendant 4 mois, en tout lieu et à toute heure. Cette formule est idéale pour les stagiaires qui ont besoin d'une très grande flexibilité.
www.sans.org/ondemand

SANS Live Online

La formation SANS Live Online est composée de sessions en direct et interactives, dispensées par des formateurs SANS. Elle comprend des cours dirigés et des labos pratiques, le tout en environnement virtuel. Comme dans les cours en présentiel, vous avez accès à des activités complémentaires telles que les tournois NetWars Tournaments.
www.sans.org/live-online

Conférences SANS Summits et Security Leadership

Ces conférences, qui durent un ou deux jours, se présentent sous forme de discours liminaires et de tables rondes, animés par des leaders d'opinion et des professionnels reconnus de l'industrie.
Une conférence SANS Summit est une source inestimable d'apprentissage ciblé qui se déroule généralement avant ou après un événement de formation SANS, et pour laquelle la participation est proposée à un prix réduit aux personnes inscrites à la formation.

Le SANS CISO Network est réservé aux responsables sécurité les plus chevronnés et met en réseau des professionnels dont l'aspiration et l'autorité font vraiment la différence. Le réseau SANS EMEA CISO Network favorise le partage d'idées et d'expériences dans un grand nombre de secteurs et offre à ses membres une plateforme pour agir sur notre avenir numérique et rendre le monde plus sûr.
www.sans.org/ciso-network

Formation SANS Security Awareness

SANS Security Awareness est une formation de sensibilisation à la sécurité de l'information, dispensée sur ordinateur et adaptée aux utilisateurs finaux, aux ingénieurs et aux développeurs SCI ; elle s'adresse aussi aux secteurs du service public et de la santé. Des modules en format vidéo dispensent une formation pointue et percutante à un grand nombre de salariés, et produisent des résultats quantifiables. La formation va au-delà des questions de conformité et s'attache à changer le comportement.
www.sans.org/security-awareness-training

SANS applique des critères de qualité élevés, quel que soit le format de formation, et toutes nos classes se conforment à la Promesse SANS : transmettre des compétences et des techniques immédiatement applicables dès le retour sur le lieu de travail.

Formation en mode présentiel

Il s'agit de formations dispensées en salle par des formateurs SANS qualifiés. Ces cours sont organisés dans de grandes villes, dans des hôtels de qualité ou des centres d'accueil événementiels de premier ordre.

Les formations SANS en mode présentiel sont particulièrement prisées, car elles permettent d'apprendre et de se constituer un réseau de pairs, de collègues et de personnel SANS. Les frais d'inscription incluent les pauses, le déjeuner et les discours en soirée (le cas échéant). L'hébergement est en sus.

Les événements de formation pour la zone EMEA se déroulent partout en Europe et dans la région du Golfe. Les formations sont dispensées en anglais, en français, en italien et en espagnol.

Reportez-vous à la page **sans.org/cyber-security-training-events/all** pour consulter le calendrier à jour des événements de formation.

SANS Private Training

Ces formations sont dispensées aux équipes de sécurité d'une organisation, en mode présentiel (dans les locaux de l'organisation ou dans des locaux dédiés) ou en mode Live Online réservé. La formation privée est idéale pour les organisations qui ont besoin de former 25 salariés ou plus et/ou qui exigent une confidentialité totale. Elle permet au formateur SANS de se focaliser sur les sujets pertinents pour l'organisation et réduit drastiquement les budgets des trajets, des repas et de l'hébergement.

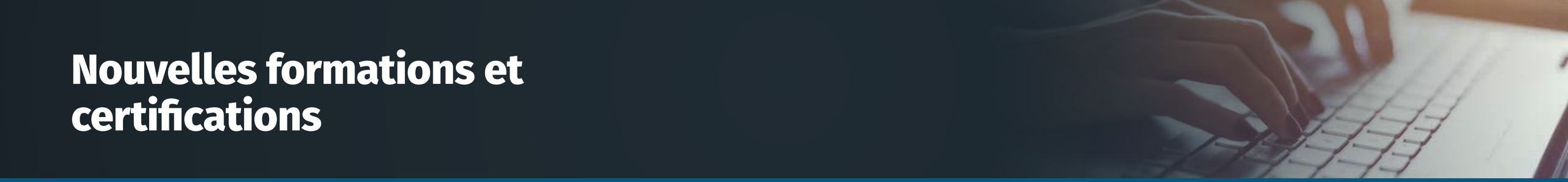
Contactez SANS pour plus d'information : **emea@sans.org** ou **asiapacific@sans.org**

Solutions de formation sur mesure et Cyber Academy

SANS crée des parcours de formation sur mesure pour répondre aux besoins spécifiques des organisations ou encore des États qui souhaitent former la prochaine génération de professionnels cyber. Le contenu de la formation est sélectionné dans la liste des cours SANS, et les programmes incluent généralement des phases d'évaluation à l'aide des outils SANS CyberTalent. SANS Cyber Academy identifie des candidats à fort potentiel pour les former de façon intensive à la certification GIAC avant de les affecter à des postes clés.

Pour plus d'informations sur les partenariats SANS, contactez **emea@sans.org** ou **asiapacific@sans.org**

Nouvelles formations et certifications



SEC488: Cloud Security Essentials
Objet du cours : Plus que jamais, les entreprises déplacent leurs charges de travail stratégiques vers le cloud. Et pas un seul cloud : la plupart des entreprises font appel à différents fournisseurs, jusqu'à cinq selon les études. Le cours SEC488 fournit les outils, techniques et schémas pratiques pour consolider les points faibles d'une organisation.
Concepteurs : Kenneth G. Hartman, Kyle Dickinson et Ryan Nicholson
Nombre de jours : 5
En savoir plus : sans.org/SEC488

SEC588: Cloud Penetration Testing
Objet du cours : La plupart voire toutes les entreprises auront bientôt des charges de travail dans des environnements cloud publics ou autres. Dans ce cours, les stagiaires acquièrent les compétences pour évaluer les infrastructures de cloud privé et public et les services associés.
Concepteur : Moses Frost
Nombre de jours : 6
Suite du cours : SEC488
En savoir plus : sans.org/SEC588

SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection
Objet du cours : Ce cours avancé pour *Purple Team* s'intéresse à l'émulation d'attaquants dans l'objectif de détecter et prévenir les violations de données, notamment à l'émulation de véritables auteurs de menace dans l'environnement d'entreprise et à la simulation et la détection de techniques d'attaques.
Concepteurs : Erik Van Buggenhout et Jim Shewmaker
Nombre de jours : 6
Suite du cours : SEC599
En savoir plus : sans.org/SEC699

SEC403: Secrets to Successful Cybersecurity Presentation – Modules en ligne
Objet du cours : Le cours SEC403 vous donne les clés pour élaborer un briefing de sécurité efficace, susciter l'intérêt et l'adhésion de votre public, et exposer vos présentations avec assurance à différents groupes.
Concepteur : Alan Paller
Nombre de jours : 0,5 (4 crédits CPE)
Suite du cours : SEC402
En savoir plus : sans.org/SEC403

FOR308: Digital Forensics Essentials
Objet du cours : FOR308 est une introduction conçue pour les praticiens de l'inforensique qui veulent devenir virtuoses, les stagiaires non techniques qui débutent dans ce domaine ou les personnes qui veulent en comprendre les tenants et les aboutissants.
Concepteurs : Kathryn Hedley, Jason Jordaan et Phil Moore
Nombre de jours : 6
En savoir plus : sans.org/FOR308

MGT551: Building and Leading Security Operation Centers
Objet du cours : À l'issue de la formation, les participants auront acquis un cadre pour comprendre les grands axes des efforts du SOC, les moyens de suivi et d'organisation des capacités défensives, et le pilotage, la vérification et la communication des améliorations du SOC.
Concepteur : John Hubbard
Nombre de jours : 2
En savoir plus : sans.org/MGT511

SEC552: Bug Bounties & Responsible Disclosure
Objet du cours : Dans ce cours, les experts en test d'intrusion apprennent à découvrir et divulguer en toute responsabilité les défauts des applications logiques et complexes indécelables par les scans automatiques.
Concepteur : Hassan El Hadary
Nombre de jours : 2
En savoir plus : sans.org/SEC552

SEC582: Mastering TShark Packet Analysis
Objet du cours : Ce cours vous apprend à maîtriser l'analyse de paquets avec TShark et à résoudre des problèmes réels via 19 labos, démonstrations et défis. C'est le cours d'analyse de paquets le plus pratique et le plus approfondi qui existe.
Concepteur : Nik Alleyne
Nombre de jours : 2
En savoir plus : sans.org/SEC582

SEC583: Crafting Packets
Objet du cours : La création de paquets est une formidable compétence pour tout analyste sécurité, ingénieur réseau ou administrateur système. Elle sert à tester les politiques de pare-feu, les règles des systèmes de détection et de prévention d'intrusion, les paramètres serveur/hôte, les configurations des applications, etc.
Concepteur : Andy Laman
Nombre de jours : 1
En savoir plus : sans.org/SEC583

SEC584: Defending Cloud Native Infrastructure
Objet du cours : Grâce aux fournisseurs de services et d'infrastructure cloud natifs, les organisations arrivent à construire et livrer des systèmes modernes en des temps record, ce qui peut s'avérer difficile à superviser et à défendre. Les stagiaires acquièrent une expérience pratique en construction, exploration et sécurisation des systèmes actuels.
Concepteur : Andy Martin
Nombre de jours : 3
En savoir plus : sans.org/SEC584

SEC510: Multicloud Security Assessment and Defense
Objet du cours : Ce cours apporte aux professionnels de la sécurité cloud, aux analystes et aux chercheurs une compréhension approfondie des rouages des grands fournisseurs de cloud public, Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).
Concepteurs : Brandon Evans et Eric Johnson
Nombre de jours : 3
En savoir plus : sans.org/SEC510

Nouvelles certifications GIAC

GCSA (SEC540) : Cloud Security Automation
En savoir plus : giac.org/certification/cloud-security-automation-gcsa

GOSI (SEC487) : GIAC Open Source Intelligence Certification
En savoir plus : giac.org/certification/open-source-intelligence-gosi

GBFA (FOR498) : GIAC Battlefield Forensics and Acquisition
En savoir plus : giac.org/certification/battlefield-forensics-acquisition-gbfa

Formations en cours d'élaboration

SEC586: Blue Team Operations – Defensive Powershell. Découvrez les fondamentaux de PowerShell et les techniques de planification éprouvées pour durcir l'infrastructure, automatiser les contrôles et créer un environnement plus défendable.

SEC595: Data Science and Machine Learning for Security Professionals. Apprenez à écrire rapidement des scripts de manipulation et d'analyse des données réseau et sécurité à l'aide des techniques de data science.

FOR608: Enterprise-Class Incident Response & Threat Hunting. Ce cours vise à développer les connaissances approfondies et essentielles à la collecte, l'analyse et la corrélation des artefacts numériques sur les réseaux et serveurs d'entreprise.

SEC587: Advanced Open Source Intelligence Gathering & Analysis (SEC537, 2 jours). Cette formation s'adresse aux personnes qui possèdent déjà un socle solide en renseignement de sources ouvertes (OSINT) et cherchent à approfondir de nombreux aspects de la collecte technique.

SEC556: IoT Pen Testing plonge les stagiaires dans les interfaces couramment utilisées dans les objets connectés et donne un cadre de test et de traitement (IoTA) pour évaluer ces appareils dans de nombreuses couches du modèle OSI.

SEC565: Red Team Operations prépare les opérateurs à émuler professionnellement des attaques et des menaces pour tester dans son ensemble une organisation cible, son personnel, ses processus et sa technologie. Pour réussir ses émulations, cette équipe rouge doit comprendre le fonctionnement des attaquants et des menaces.

FOR710: Reverse-Engineering Malware: Advanced Code Analysis, qui prend la suite de la formation FOR610, aide les stagiaires de niveau intermédiaire en analyse de logiciels malveillants à franchir un cap en rétro-ingénierie.

MGT419: Vendor Risk Management & Data Privacy. Cette formation aborde les principaux facteurs de la fourniture et de la mise en œuvre d'un programme de gestion des risques des fournisseurs et de protection des données.

SEC404: Business Financial Essentials. Peu de sujets sont aussi stratégiques que la bonne administration financière. Ce cours emmène le manager InfoSec à la découverte de l'état financier de son organisation pour mieux le comprendre et s'orienter.

SEC554: Blockchain and Smart Contract Security. Ce cours forme aux interactions avec les blockchains publiques pour en extraire des données, à l'exploitation de plusieurs classes de vulnérabilités des contrats auto-exécutants dits *smart contracts*, au test et à l'exploitation de l'entropie ou du chiffrement faible, à la découverte de clés privées susceptibles d'être recréées, et aux méthodes pour tracer/pister les mouvements dans une blockchain.

SÉCURITÉ CLOUD

SEC388: Intro to Cloud Computing & Sec vous fait découvrir les multiples facettes du cloud, à commencer par la mise en place de votre compte cloud qui vous servira à explorer le fournisseur cloud de votre choix parmi les trois grands, AWS, Azure et Google Cloud Platform, puis se poursuit par l'exploration des services qui facilitent les opérations et la maintenance et renforcent la sécurité.

FOR509: Cloud Forensics & Incident Response. Ce cours donne les clés pour comprendre les données inforensiques dans le cloud, les bonnes pratiques, la conservation des preuves et l'acquisition de la mémoire dans le cloud.

MGT520: Managing Cloud Security Design & Implementation. À l'intention des managers, ce cours apprend à développer leur feuille de route pour réussir la migration des données de l'entreprise vers le cloud, et les superviser et les sécuriser comme il se doit.

SEC557: Security Audit Compliance Automation Essentials (Cloud & Enterprise). À l'intention des auditeurs, ingénieurs et managers, ce cours s'intéresse à l'audit des technologies modernes (méthodes et moyens) dans les environnements entreprise et cloud et à la restitution des informations collectées.

SEC541: Cloud Security Monitoring and Threat Hunting. Ce type de formation a pour objet de présenter aux stagiaires les différentes sources de données natives du cloud AWS qui produisent des données touchant à la sécurité.

Découvrez les avis de nos stagiaires sur SANS Online Training

La plateforme OnDemand ne manque pas d'atouts : 1) Je peux faire une pause pour approfondir les sujets, les commentaires et les notions qui me sont peu familiers. 2) Je peux configurer des outils spécifiques à mon rythme, sans retarder les autres. Et le formateur a rendu le cours très dynamique !

Brian Guzman, AWS

J'aime que OnDemand me permette d'ajuster la cadence à certains moments et de revenir facilement sur les parties où j'ai besoin de clarification. J'apprécie de pouvoir arrêter et reprendre la formation à mon rythme.

Barry Nixon, Airbus

SANS OnDemand est idéal pour moi ! Plus je l'utilise et plus je l'apprécie. Il n'y a pas d'urgence ; je prends mon temps, ce qui élimine toute pression de l'apprentissage.

Shaadie Khoury, Aflac

SANS Live Online valorise très efficacement la technologie. J'adore l'utilisation de Slack. J'ai toutes les informations et les ressources à portée de main.

Peder Muller, Deloitte

Avec SANS, je sais que je suis la meilleure formation à la sécurité de l'information du secteur, et c'est encore le cas avec SANS Live Online !

Harold Stockton, Global Payments, Inc.

Avoir un expert technique comme formateur, riche de son expérience de terrain, facilite grandement la compréhension du cours ; et Live Online est la meilleure plateforme que j'aie jamais utilisée !

Jeremy Swanson, Mantech

Le formateur est très compétent, avec des exemples pertinents et un bon rythme. L'interaction avec les stagiaires est splendide !

John Hoehne, Novetta

Pour lire d'autres témoignages, rendez-vous sur **www.sans.org/customer-reviews**

ONDEMAND

Formation à votre rythme, partout et à tout moment.

« L'espace OnDemand est vraiment pratique. Avec quatre mois pour suivre la formation, j'ai pu trouver un bon équilibre entre vie professionnelle, vie privée et formation. »

— JILL FRASER, JEFFCO

Pourquoi choisir SANS OnDemand

- Accès en ligne à l'ensemble de la formation, des labos virtuels et des questionnaires pendant quatre mois
- Interactions avec des experts techniques certifiés GIAC
- Formation web accessible 24×7 depuis votre ordinateur, votre iPad ou votre tablette Android
- Ni déplacements ni perte de temps de travail
- Avec des vidéos, des labos et des exercices pratiques
- Support de cours numériques en couleur
- Bilans de progression pédagogique
- Plus de 45 cours disponibles, partout et à tout moment
- Mode de préparation idéal à la certification GIAC

Plus de 45 cours en cybersécurité de SANS parmi les plus demandés sont disponibles via OnDemand, notre plateforme de formation privée. En quatre mois d'accès illimité aux contenus numériques, cours, questionnaires, labos, et avec tous les supports imprimés correspondants, vous avez tout le temps et les ressources nécessaires pour en maîtriser le contenu.

Vous n'avez pas de budget de déplacement ou vous appréciez simplement d'avoir accès et soutien sur la durée dans le cadre d'une formation ? Alors SANS OnDemand s'adresse à vous.

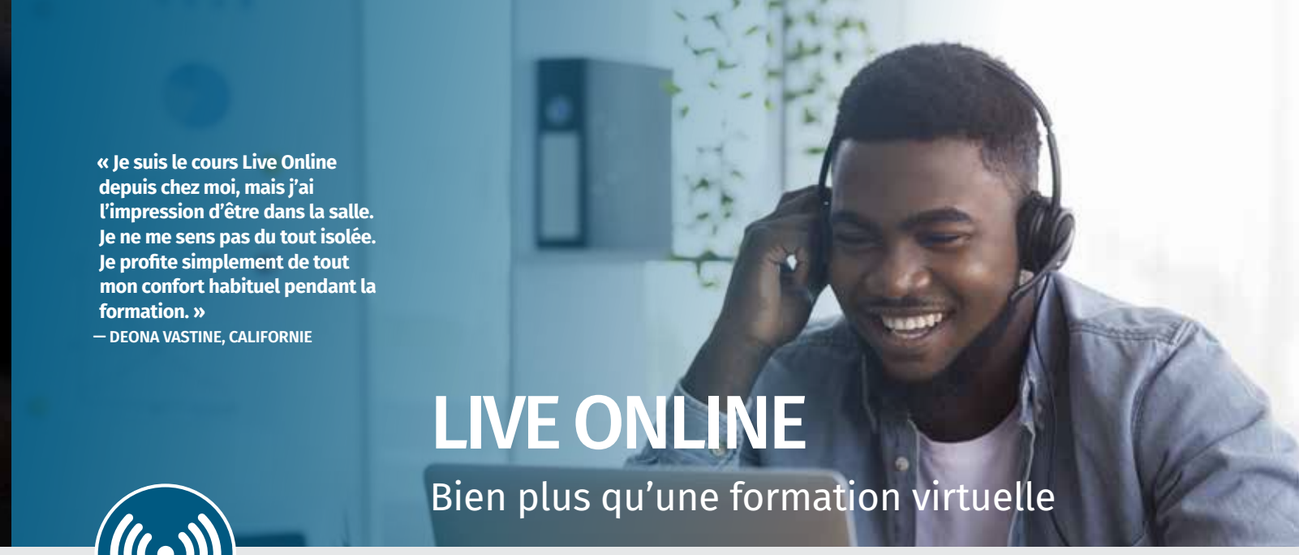
Points forts du mode de formation SANS OnDemand

- La formation est dispensée par ses concepteurs ; vous recevrez la meilleure formation à la cybersécurité qui existe
- La messagerie instantanée avec des experts techniques certifiés GIAC qui répondent rapidement à vos questions et accompagnent votre progression sur les sujets complexes
- Les options de retour en arrière, d'avance rapide et de pause vous donnent la maîtrise totale de votre rythme d'étude
- Le suivi de la progression et les questionnaires vous aident à vous concentrer sur vos objectifs et à valider les acquis
- Des options de recherche, de marque-page et de prise de note pour sélectionner les sections sur lesquelles revenir ou à inclure dans un index de ressources
- L'accès longue durée au cours est idéal pour préparer sa certification GIAC

Nouvelles fonctionnalités dans OnDemand

- Indicateur de maîtrise de la section
- Zoom/panorama vidéo
- Volets ajustables
- Barre de progression pédagogique
- Bouton dynamique Aller à/Retour
- Prendre, exporter et imprimer ses propres notes
- Taille de police ajustable
- Raccourcis clavier et fonctionnalités d'accessibilité améliorés

sans.org/ondemand
emea@sans.org ou **asiapacific@sans.org**



LIVE ONLINE

Bien plus qu'une formation virtuelle

« Je suis le cours Live Online depuis chez moi, mais j'ai l'impression d'être dans la salle. Je ne me sens pas du tout isolée. Je profite simplement de tout mon confort habituel pendant la formation. »

— DEONA VASTINE, CALIFORNIE

Pourquoi choisir SANS Live Online

- La formation en ligne la plus immersive et interactive
- Sans déplacement
- Avec le soutien de spécialistes certifiés GIAC
- L'ensemble des supports de cours et livres sous forme numérique
- Accès en exclusivité aux tournois NetWars Tournament
- Interactions immédiates avec vos pairs dans les canaux Slack dédiés
- Sessions interactives instantanées avec les meilleurs formateurs au monde
- Accès au labo pratique pendant la durée de la formation
- Accès aux enregistrements archivés pendant les 4 mois suivant la formation

Profitez de tout ce que vous aimez des formations SANS en présentiel sans vous déplacer : ces cours d'une à deux semaines sont dispensés par un formateur et disponibles sur plusieurs fuseaux horaires. SANS Live Online représente notre offre de formation en ligne la plus interactive. Les cours sont dispensés par des formateurs SANS chevronnés dans le cadre de sessions participatives en duplex ; et les stagiaires les suivent comme un présentiel : mêmes contenus, même accompagnement en temps réel, mêmes sessions bonus et mêmes bilans d'apprentissage.

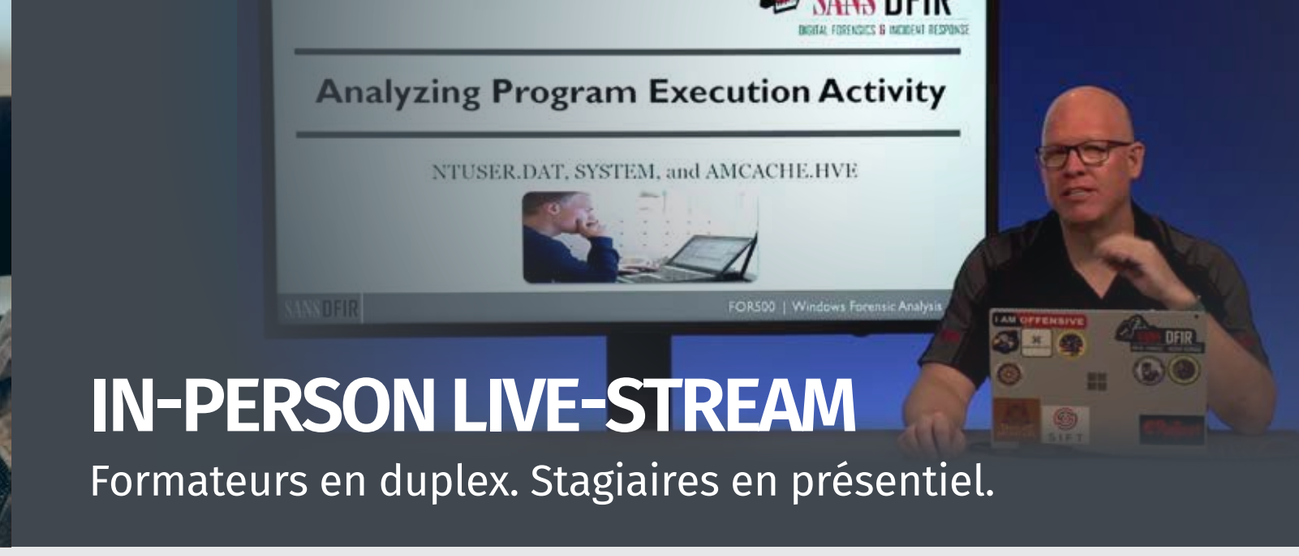
Les stagiaires SANS Live Online profitent aussi pendant 4 mois d'un accès aux enregistrements de leurs cours théoriques. La durée de la période d'étude convient bien au mode d'apprentissage permanent où le stagiaire peut revenir sur les sujets complexes pour mieux les assimiler. Chaque élément d'une formation SANS Live Online est conçu pour vous accompagner dans votre préparation de l'examen de Certification GIAC.

Nous connaissons la diversité des besoins de nos stagiaires et de leurs organisations. Pour répondre à chaque situation, les stagiaires peuvent choisir entre des sessions en direct réparties sur plusieurs semaines ou sur la journée complète.

Bien plus qu'une formation virtuelle, SANS Live Online intègre des fonctionnalités exclusives qui en dynamisent le contenu et vous ouvre un espace d'interaction en ligne qui n'existe nulle part ailleurs. Les stagiaires auront accès à de toutes nouvelles allocutions @MIC, ces exposés de 60 minutes par des experts et intervenants renommés dans le monde entier sur les sujets brûlants en cybersécurité. Ils seront aussi invités à participer à des tournois CFT entre stagiaires, qui mettent l'accent sur le socle commun, l'analyse inforensique et la réponse aux incidents (DFIR), et les NetWars en cyberdéfense. Ils ont également accès à des expériences d'apprentissage gratuites par la pratique, notamment à des minitournois NetWars, au programme Cyber FastTrack et à des événements NetWars Capstone.

Nous savons que, dans une large mesure, la valeur de nos événements de formation dérive des nouveaux liens et contacts créés avec d'autres acteurs du monde de la cybersécurité. C'est pourquoi nous avons développé de nouveaux

sans.org/live-online
emea@sans.org ou **asiapacific@sans.org**



IN-PERSON LIVE-STREAM

Formateurs en duplex. Stagiaires en présentiel.

modes d'interaction en ligne avec les autres stagiaires tels que les canaux de messagerie dédiés et les défis hebdomadaires. Nous connaissons la diversité des besoins de nos stagiaires et de leurs organisations. Pour répondre à chaque situation, les stagiaires peuvent choisir entre des sessions en direct réparties sur plusieurs semaines ou sur la journée complète.

Sessions en journée complète

Plongez-vous en immersion pendant toute une semaine de formation en duplex avec les formateurs SANS. Concentrez-vous pleinement, sans distraction, et restez sur une dynamique d'étude. Les sessions intensives sur des journées complètes permettent aux formateurs de rendre leur sujet plus vivant par des illustrations issues d'expériences personnelles et d'exemples concrets. Elles vous donnent aussi le temps d'appliquer les acquis théoriques. Vous bénéficiez de quatre mois d'accès aux enregistrements vidéo ou audio de vos cours théoriques pour éventuellement reprendre les supports et réviser encore dans le cadre de votre préparation à l'examen de Certification GIAC.

Sessions sur plusieurs semaines

Les fonctionnalités Live Online visent à combiner la puissance des interactions et de l'accompagnement en personne à la commodité du mode en ligne. Partout dans le monde, vous profitez ainsi d'une formation SANS en direct alliant souplesse et efficacité. S'ils optent pour les sessions sur plusieurs semaines, les stagiaires peuvent plus aisément concilier la formation et leurs autres responsabilités, tout en profitant de cours du soir interactifs et stimulants en duplex avec les meilleurs formateurs SANS. La durée de la période d'étude convient bien au mode d'apprentissage permanent où le stagiaire peut étudier à son rythme et revenir sur les sujets complexes pour mieux les assimiler.

Fonctionnalités phares de Live Online

- Sans déplacement
- Assistants-formateurs en soutien
- Accès au labo pratique pendant la durée de la formation
- Accès aux tournois NetWars Tournament
- Canaux Slack dédiés
- Interactions instantanées avec un formateur
- Accès aux enregistrements archivés pendant les 4 mois suivant la formation
- Avec le soutien de spécialistes certifiés GIAC

Témoignages de stagiaires sur Live Online :

« L'expérience d'apprentissage vécue grâce au mode de formation par la plateforme SANS est excellente. »
— Stagiaire SEC301

« J'ai beaucoup apprécié le format en ligne et j'aimerais à nouveau en profiter pour d'autres formations. »
— Stagiaire SEC566

« SANS Live Online prouve encore une fois qu'elle reste une excellente plateforme immersive, stable et accessible pour délivrer des formations de haut vol partout dans le monde ! »
— Stagiaire FOR498

« Le format virtuel m'inquiétait, mais c'est incroyable ! »
— Stagiaire SEC511

« J'étais sceptique sur le format de cours en ligne, je redoutais l'absence d'interaction formateur-stagiaires et d'accompagnement lors des labos. Mon scepticisme s'est envolé dès le premier jour. »
— Stagiaire SEC401

Si les formations SANS à la cybersécurité et aux certifications GIAC vous sont proposées sous plusieurs modes, vous êtes nombreux à souhaiter vous former et étudier en groupe sur une période donnée.

C'est pourquoi nous avons le plaisir de vous présenter nos formations **SANS In-Person Live-Stream (IPLS)** : animées à distance par nos formateurs, elles sont diffusées en direct à un groupe de stagiaires réunis en présentiel.

Les formations IPLS combinent les avantages des cours virtuels en direct SANS Live Online et des formations en présentiel SANS In-Person. Sous cette forme, les stagiaires d'une même région se rendent, si la réglementation les y autorise, à un événement de formation SANS In-Person pour y suivre leur formation Live Online Training dans une salle dédiée qui diffuse en direct le formateur intervenant.

Points forts du mode de formation SANS In-Person Live-Stream :

- **Formation animée en direct :** avec la diffusion en duplex In-Person Live-Stream, nos formateurs réputés animent le cours à distance. Vous pouvez interagir avec eux dans l'instant et poser vos éventuelles questions. Une messagerie instantanée est dédiée au cours. Sauf contrainte matérielle, le formateur apparaîtra sur grand écran dans la salle de cours.
- **Un environnement sûr :** SANS collabore étroitement avec le personnel des lieux de formation partout dans le monde pour garantir l'application des normes d'hygiène et de propreté les plus strictes, conformément aux recommandations des autorités locales et nationales, de l'OMS et du centre de prévention et de contrôle des maladies (CDC).
- **Un modérateur ou assistant présent dans la salle :** si le formateur SANS ne sera pas physiquement présent dans la salle, un modérateur ou assistant-formateur le sera pour vous prêter assistance le cas échéant. L'assistant-modérateur est un formateur SANS en devenir, hautement qualifié et compétent.
- **Une plage de formation dédiée pour mieux se concentrer :** lors d'une formation IPLS, vous réservez une plage horaire et profitez d'une salle de formation hors des murs de votre domicile ou du bureau où les distractions vous guettent.
- **Formation collective :** dans le respect des distances sanitaires, une formation SANS présente toujours un espace privilégié pour interagir avec ses pairs et échanger connaissances, expérience et exemples concrets.
- **Occasion de participer à une Community Talk et à un NetWars Tournament :** vous aurez l'occasion de participer à une discussion Community Talk ou à un tournoi NetWars s'ils se déroulent dans les mêmes locaux que la formation. Ces sessions seront bien sûr réparties en différentes salles dans le respect des règles sanitaires locales et internationales.

> **« Me rendre à une formation SANS en présentiel était primordial pour moi. En effet, je me concentre et j'apprends mieux en salle de cours. »**

emea@sans.org ou **asiapacific@sans.org**

« Les formations SANS sont un excellent moyen de rencontrer des gens qui ont soif des mêmes connaissances. Collaborer avec ses pairs dans un environnement d'étude est tout simplement la recette du succès sur tous les tableaux. »
— CHASE JOHNSON, TDI TECHNOLOGIES

IN-PERSON

Formez-vous en toute sécurité dans une salle de classe pour vivre l'expérience d'apprentissage la plus immersive qui soit

In-Person Training, ce qu'en disent les stagiaires :

« Dans la situation actuelle, je trouve que SANS prend vraiment soin de ses clients. SANS a déployé des efforts palpables pour nous éviter tout risque. À l'hôtel aussi, toutes les mesures d'hygiène nécessaires ont été prises. De plus, j'ai vraiment aimé le nombre réduit de participants qui améliore globalement l'interaction avec le formateur. »

– Tim Tessnow

« J'ai toujours adoré ça. Sauter dans le grand bain avec des formateurs de ce calibre est un rêve qui se concrétise. On n'a pas le temps de réinventer la roue : cette expérience est d'une valeur inestimable. »

– Keith Dunnigan, Best Western Hotels & Resorts

« Tout dans cette expérience est excellent. C'est ardu, mais efficace. »

– *Ryan McAlister, Aegon*

Lors des événements de formation en personne de SANS, nos formateurs animent plusieurs cours dans un même lieu, et une tournée s'arrête dans les grandes villes du monde tout au long de l'année. Ces événements donnent aux stagiaires l'occasion de se former dans un environnement dédié, sans distraction, mais surtout dans une interaction directe avec les formateurs SANS reconnus dans le monde entier.

Ces événements sont un lieu idéal pour établir des liens avec des professionnels de la sécurité qui vous ressemblent. Attendez-vous à une semaine de travail intense émaillée d'activités ludiques comme les NetWars et les présentations SANS@Mic en soirée.

Quelques avantages à suivre votre formation lors d'un événement SANS In-Person Training :

- Une formation dispensée par des experts chevronnés en cybersécurité qui s'appuient sur des exemples tirés de l'expérience
- Des réponses immédiates à vos questions puisque le spécialiste qui vous forme se trouve dans la même salle de cours
- Des occasions de développer votre réseau et de profiter de l'expérience d'autres professionnels de la sécurité
- Des exercices pratiques en labo
- Session bonus sur les derniers développements et techniques cyber
- Préparation idéale pour l'examen de certification GIAC
- Un temps précieux rentabilisé. Consacrez une semaine entière à une formation intensive, puis retournez au bureau avec de nouvelles compétences exploitables immédiatement
- Les cours incluent livres électroniques et labos pratiques
- Découverte d'une nouvelle ville et de son environnement en plus d'une montée en compétence
- Les sessions bonus disponibles varient selon l'événement et le lieu. Consultez la page de l'événement sur notre site pour accéder aux dernières informations

sans.org/in-person-training
emea@sans.org ou **asiapacific@sans.org**

OPTIONS DE FORMATION DE GROUPE SUR MESURE

Grâce aux options de formation sur mesure à la sécurité des informations de SANS, créez votre programme pour un groupe de 25 stagiaires ou plus, partout dans le monde.

Avec nos options adaptées au secteur privé ou public, les formations sur mesure en sécurité de l'information seront conçues selon votre cahier des charges à partir des ressources technologiques et pédagogiques uniques de SANS. Vous profitez en direct des cours et des formateurs qualifiés SANS Certified Instructor sur place, en ligne ou en hybride avec le mode de formation Live Online.

Avantages du SANS Private Training

- Un formateur certifié SANS
- Discussions confidentielles en classe sur les supports de cours et les exemples réels de votre secteur
- Réduction des risques sanitaires et des éventuelles complications associées aux restrictions de déplacement actuelles
- Sujets sensibles. Avec le choix du Private Training, les stagiaires de l'organisation abordent les différents sujets en totale liberté et le formateur peut axer son cours sur des thèmes sensibles ou une violation récente
- Les cours sont offerts partout dans le monde et dispensés dans vos locaux

« Le programme SANS OnSite est intéressant pour notre programme interne de formation à la sécurité. Les "économies" sont astronomiques… Les formateurs ont été excellents et les stagiaires ont apprécié de se retrouver en classe avec leurs collègues qui partagent les mêmes soucis et devoirs sur les projets de sécurité en cours. »

– Tonya Henderson, Département de la Santé et des Services sociaux (États-Unis)

Achat groupé

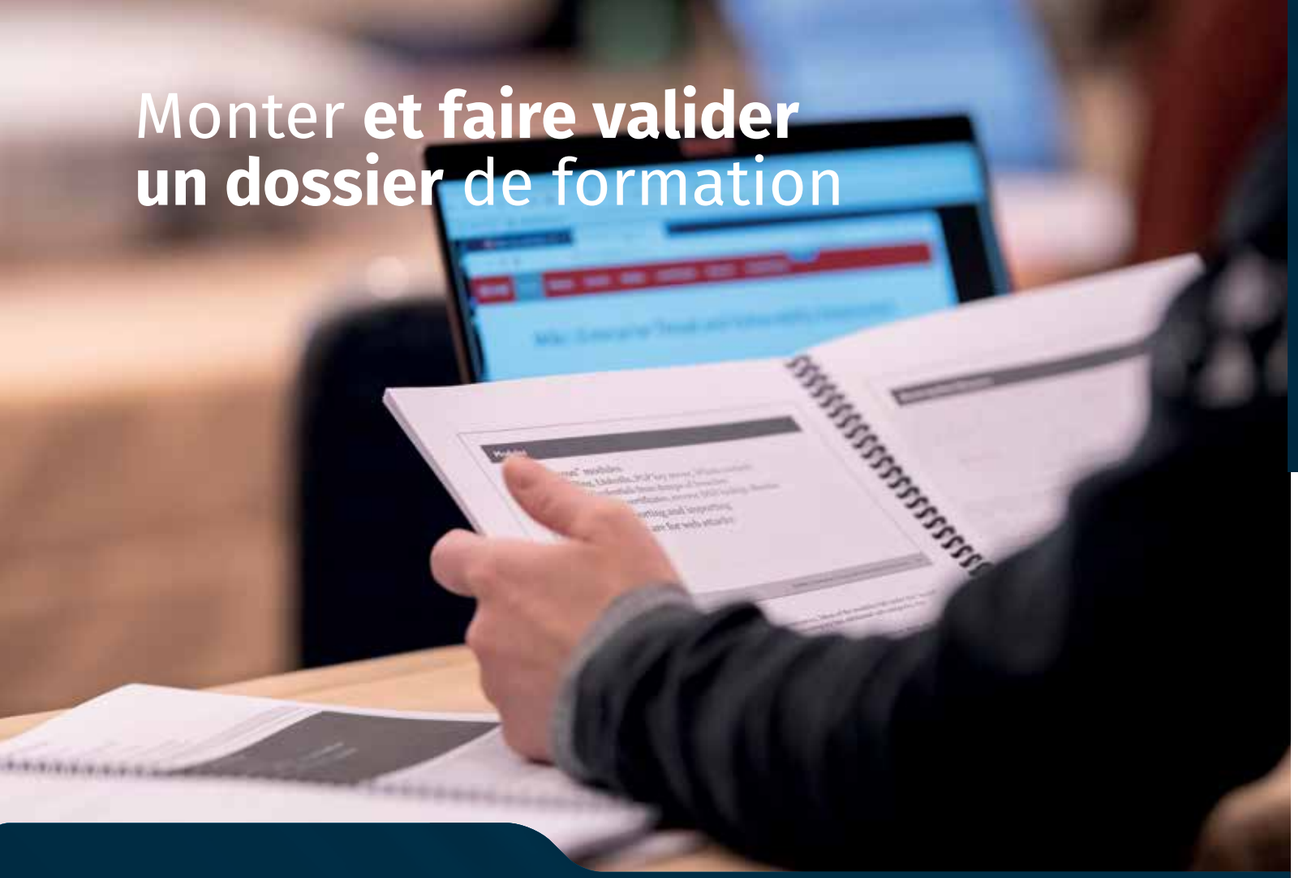
Avec un seul compte Voucher Account, vous gérez le budget formation de votre équipe, vous suivez la progression des stagiaires, vous économisez et vous assurez le suivi.

Dans le cadre du SANS Voucher Program, une organisation n'a qu'un seul compte SANS Voucher Account pour gérer l'ensemble de son budget formation. Une fois son compte ouvert, elle en utilise les fonds pour inscrire ses employés aux formations et certifications SANS dans l'outil en ligne SANS Admin Tool. C'est aussi dans cet outil d'administration que le Program Administrator désigné de l'organisation va approuver les formations et consulter les rapports d'utilisation.

Avec un compte SANS Voucher Account, votre organisation peut :

- Simplifier le processus d'achat avec une facture et un paiement uniques
- Bloquer son budget formation acquis de haute lutte et l'utiliser dans un délai de 12 mois
- Contrôler comment, où et pour qui investir en formation
- Laisser ses employés s'inscrire en formation et centraliser les validations
- Modifier facilement les participants au cours en fonction des aléas

Pour en savoir plus sur le développement et la formation de vos équipes, écrivez-nous à **emea@sans.org** ou **asiapacific@sans.org**



Monter **et faire valider un dossier** de formation

La forme compte aussi

Formulez officiellement une demande de formation

- Une formation constitue un investissement significatif en temps et en argent. Si toutes les organisations fonctionnent différemment, la plupart des demandes validées sont d'abord formulées dans un document (mémo et/ou présentation PowerPoint) qui explique les besoins et les bénéfices escomptés. La majorité des responsables apprécient cet effort.
- Le dossier doit être complet. Mettez toutes les chances de votre côté en ajoutant une présentation de SANS et de ses atouts, le parcours de formation Training Roadmap, la biographie de l'intervenant et les autres avantages de nos événements en présentiel ou en ligne.

Formulez clairement les bénéfices

Soyez spécifique

- En quoi ce cours vous servira-t-il dans le travail qui vous a été confié ? Est-ce qu'il s'agit pour vous d'acquérir des compétences de base ? Ou bien de monter en compétence vers un rôle plus spécialisé ? Pour décider, les responsables doivent comprendre l'objectif et le contexte.
- Mettez l'accent sur ce que vous serez en mesure de faire à l'issue de la formation. Dans la description de chaque cours SANS, vous trouverez une section « Vous apprendrez à… » : pensez à l'inclure dans votre dossier pour clarifier les avantages. Il est important de montrer combien cette formation vous sera utile (voire indispensable) dans votre travail.

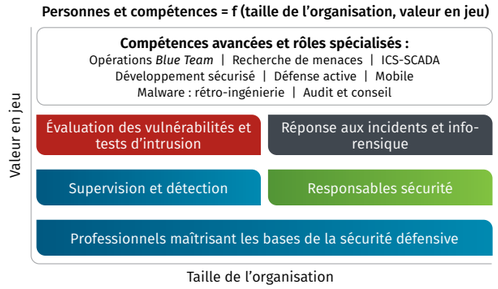
Mettez en perspective

Définissez des objectifs à long terme

- La sécurité de l'information est une spécialisation au sein des métiers de l'informatique qui évolue en fonction des menaces. De ce fait, toute organisation devrait allouer 6 à 10 % de sa masse salariale à l'actualisation et l'amélioration des compétences de ses collaborateurs. La formation dans un domaine aussi dynamique implique des investissements annuels et par personne, car les connaissances évoluent et doivent être mises à jour régulièrement.
- Validez vos acquis par une certification GIAC, dont les employeurs reconnaissent la valeur. Les examens ont été conçus par des experts en psychométrie, de façon à évaluer les capacités d'un individu à réaliser un travail spécifique.
- Réfléchissez à des contreparties éventuelles. Nombre de professionnels accumulent des droits à la formation avant même d'accepter un nouveau poste. Certains s'engagent contractuellement à rester un an en poste à l'issue de la formation.

Construire une organisation de sécurité **ultra performante**

Tout professionnel qui se voit confier des tâches pratiques devrait être formé à un socle commun de savoirs mobilisables pour sécuriser les systèmes, mettre en œuvre une défense en profondeur, comprendre le fonctionnement des attaques et gérer les incidents lorsqu'ils se produisent. Placez haut la barre lorsque vous définissez ce socle commun de compétences essentielles dans votre organisation de sécurité.



Les quatre rôles suivants émergent généralement quand les organisations se développent en taille, risque ou complexité.

- **Professionnels de supervision de la sécurité et de détection :** détecter ce qui se passe dans votre environnement fait appel à un ensemble de compétences et de capacités toujours plus sophistiqué. Bien trop souvent, les formations proposées par les fournisseurs se cantonnent à l'outil lui-même. Elles font l'impasse sur le comment et le pourquoi, et sur le déploiement optimal. Identifier des anomalies de sécurité exige une compréhension fine pour déployer les outils de détection et de supervision, mais aussi pour interpréter les résultats.
- **Analystes de vulnérabilité et experts en tests d'intrusion :** le profil d'un professionnel capable de trouver des points faibles se distingue souvent de l'expert concentré exclusivement sur la construction de défenses. Principe fondamental du déploiement *Red Team*/*Blue Team*, la recherche de vulnérabilité requiert une tournure d'esprit et des outils spécifiques que les défenseurs doivent néanmoins connaître pour renforcer leurs défenses.
- **Analystes inforensiques et chargés de réponse aux incidents :** qu'il s'agisse de suivre une série d'indices dans un système de serveurs/réseaux ou de remonter la piste des menaces avec ce type de méthodes, les grandes organisations ont besoin de spécialistes qui, outre répondre aux incidents, savent analyser une attaque et développer un plan de remédiation et de reprise.
- **Responsables sécurité :** pour gérer les profils techniques toujours plus nombreux et les processus, les organisations doivent s'appuyer sur des responsables compétents. Sans obligatoirement s'atteler eux-mêmes aux tâches techniques, ces managers doivent en savoir assez sur les technologies et infrastructures sous-jacentes pour contribuer à l'élaboration des stratégies, développer des règles appropriées, interagir avec des professionnels compétents et mesurer les résultats.

Dans ces quatre domaines, voire au-delà, les organisations cyber performantes seront amenées à former leurs éléments pour valoriser les compétences avancées de manière globale ou pour répondre à des besoins précis. Avec plus de 30 cours dans tous les domaines de la cybersécurité, de la défense active à celle du cloud en passant par le langage Python pour les tests d'intrusion et la rétro-ingénierie des malwares, nos formations s'adressent à des rôles spécialisés ou traitent des sujets les plus pointus pour répondre à tous les niveaux aux besoins de l'ensemble des professionnels ou presque.

Stratégies pratiques de formation d'un groupe en cybersécurité, d'après nos recherches et nos observations à l'international :

Utilisez des principes d'organisation pratiques dans vos plans et vos efforts. La quasi-totalité des structures les plus complexes se résume à des propositions simples comme : « Construction et maintenance des défenses - Surveillance et détection des intrusions - Auto-évaluation proactive - Réponse aux incidents. »

Hiérarchisez vos efforts dans ces domaines à l'aide des **CIS Critical Controls** à mesure que vous faites évoluer votre organisation.

Déterminez le nombre de personnes et les profils nécessaires aux tâches quotidiennes. **Menez une campagne à long terme** pour développer les compétences et les capacités nécessaires de votre équipe. La cybersécurité est une spécialité de l'informatique qui requiert à ce titre une formation spécialisée.

Découvrez la plateforme SANS Online Training qui vous convient

Fonctionnalités de la plateforme

	ONDEMAND	LIVE ONLINE
Des grands noms de la cybersécurité comme formateurs	●	●
Tous les supports de cours, notamment les médias et les exercices	●	●
Accès flexible en autoformation à la plateforme pendant quatre mois	●	
Cours avec formateur en direct et en ligne sur 1 ou 2 semaines		●
Questionnaires intégrés pour bien acquérir les connaissances	●	
Soutien de spécialistes certifiés GIAC par messagerie instantanée et email	●	
Accès en temps réel aux formateurs		●
Pratique en labo virtuel pour vous préparer à l'examen GIAC	4 mois	Pendant le cours
Enregistrements des cours		4 mois
Aucuns frais de déplacement	●	●
Impact minimal sur votre emploi du temps habituel	●	
Formation SANS flexible et efficace depuis votre propre ordinateur	●	●
Messagerie instantanée avec les autres stagiaires et les formateurs pendant toute la durée de votre formation		●

GIAC CERTIFICATIONS

Validez vos compétences | Restez dans la course | Certifiez-vous GIAC

SANS Online Training est le mode de préparation idéale aux examens de certification GIAC

Revenez en arrière et révisez le contenu, profitez de l'accompagnement de spécialistes pour les questions et sujets complexes tout au long de votre préparation à l'examen GIAC.

38 Certifications spécialisées disponibles

« GIAC exige un niveau de maîtrise et de compétence supérieur pour en obtenir le titre. GIAC se démarque nettement des autres certifications en sécurité. »
— JOSH RINGER, BENEFIS HEALTH SYSTEM

En savoir plus **giac.org**

SANS CISO NETWORK

UNE OCCASION UNIQUE D'ÉCHANGER DES CONNAISSANCES ET DE RENFORCER SON RÉSEAU AVEC DES RESPONSABLES SÉCURITÉ

La contribution de SANS au monde de la cybersécurité comprend la formation, la certification et les programmes de développement de compétences les meilleurs au monde et une large gamme de ressources en accès libre.

Nous avons de plus créé un groupe de réseau de professionnels aguerris de la sécurité.

Nous espérons participer à alléger la pression qui pèse sur ces décideurs en créant un environnement favorable aux échanges d'idées et d'expériences au sein d'un groupe de pairs formé d'influenceurs et de leaders d'opinion.

Ce réseau, ouvert en exclusivité aux responsables sécurité du plus haut niveau, vous connecte à un groupe de professionnels à nul autre pareil qui ont l'envie et l'autorité de faire significativement bouger les choses. En favorisant l'échange d'idées et d'enseignements d'une grande diversité de secteurs, le réseau SANS CISO Network offre à ses membres une tribune pour influencer notre avenir numérique et rendre le monde plus sûr.

Événements SANS CISO Networking

- Écoutez des exposés de formateurs SANS et d'autres experts internationaux
- Participez à des sessions de questions-réponses à huis clos
- Prenez connaissance d'études de cas et des nouveautés du paysage des menaces auprès de praticiens ancrés dans le monde réel
- Rencontrez d'autres RSSI
- Réfléchissez à des thèmes clés et partagez vos connaissances sur les défis des RSSI d'aujourd'hui
- Tenez-vous au courant des initiatives du SANS Institute et restez en contact avec les formateurs SANS
- Accédez en priorité aux nouvelles ressources de SANS

Comité consultatif du SANS CISO Network

James Lyne

James Lyne est DSI au SANS Institute. Il s'est successivement occupé dans diverses organisations de stratégie de sécurité et de la gestion de plusieurs incidents graves. On fait souvent appel à lui comme conseiller en sécurité. Formateur qualifié SANS Certified Instructor, il figure souvent parmi les intervenants de marque des conférences du secteur.

Frank Kim

Frank Kim est le fondateur de ThinkSec, cabinet de conseil sécurité et RSSI. Ancien RSSI au SANS Institute, il a incarné la fonction de risque de l'information pour la référence mondiale de la formation et de la certification en sécurité informatique. Il continue d'encadrer les programmes de sécurité cloud et RSSI auprès du SANS Institute. Il participe de fait à la formation de la nouvelle génération de leaders en cybersécurité.

Rejoignez le SANS CISO Network

Demandez dès aujourd'hui à rejoindre notre réseau exclusif et découvrez les événements prévus à l'adresse sans.org/ciso-network

Partenariats et solutions

SANS collabore avec des entreprises et des gouvernements pour élaborer des solutions de formation et de développement sur mesure, adaptées à des exigences opérationnelles spécifiques.

Nous travaillons avec les organisations pour élaborer un plan de développement des compétences adapté à leurs besoins. Nous consultons, conseillons, puis proposons des solutions forfaitaires adaptées aux entreprises et aux institutions d'État qui cherchent à améliorer leur cybersécurité. Nous fournissons aussi des outils et des solutions permettant aux entreprises de répliquer ces solutions uniques et d'en mesurer l'efficacité.

Avec son expérience et son savoir-faire, SANS est en mesure d'apporter des solutions dans divers domaines : évaluation du personnel, sélection des candidats à l'embauche, développement d'équipe, formation technique intensive.

« Nous collaborons avec des gouvernements et des entreprises sur plusieurs continents, et nous nous adaptons à leur culture, explique Jan-Pieter Spaans, Managing Director Mainland Europe. Nos services incluent des solutions directes, telles que des formations SANS privées. »

Toutes les formations en cybersécurité SANS peuvent être dispensées en intra, sur le site d'une entreprise ou encore dans ses locaux dédiés à la formation. Les formations privées sont dispensées par un formateur SANS qualifié, dans la plus grande discrétion. SANS peut aussi, bien sûr, déléguer des formateurs titulaires d'une habilitation de sécurité, si nécessaire.

« Nos services vont bien au-delà de la formation. Nous aidons aussi les responsables de la sécurité pour que les compétences de leurs équipes soient régulièrement actualisées, explique Jan-Pieter Spaans. Nous pouvons élaborer et déployer des programmes pour développer les compétences individuelles qui, dans la durée, contribuent à retenir les talents. Nous évaluons les besoins d'une entreprise, puis nous proposons des solutions sur mesure que ce soit pour le recrutement, l'intégration ou la formation. »

Pour en parler avec SANS

Pour un premier entretien avec un Directeur de SANS Institute, contactez SANS à l'adresse emea@sans.org ou au +44 203 384 3470. Vous pouvez également contacter :

Stephen M Jones
Directeur général Royaume-Uni et pays nordiques
sjones@sans.org

Ned Baltagi
Directeur général Moyen-Orient et CCG
nbaltagi@sans.org

Jan Pieter Spaans
Directeur général, Europe continentale
jspaans@sans.org

Suresh Mustapha
Directeur général, Asie et Pacifique
smustapha@sans.org

HMG Cyber Schools Programme

Sélectionné pour concevoir et diriger le premier programme d'activité parascolaire en cybersécurité au Royaume-Uni, SANS a élaboré Cyber Discovery. Ce parcours de sensibilisation s'appuie sur un outil d'évaluation et une plateforme d'apprentissage ludique, tous deux développés par SANS, et des initiatives en ligne et en face à face pour améliorer les compétences et les connaissances en cybersécurité du jeune public.

Stephen Jones, Directeur général SANS pour le Royaume-Uni et les pays nordiques : « Nous sommes fiers d'être les acteurs de ce programme vital de formation dans le cadre de la stratégie nationale de cybersécurité du Royaume-Uni et ravis d'éveiller l'intérêt de la jeune génération pour les carrières de la cybersécurité. Par nos actions d'évaluation, de sélection et de formation de jeunes avec un talent naturel pour la cyber, nous espérons contribuer à combler la pénurie actuelle de compétences à travers le monde. »

Le programme britannique à la cybersécurité HMG Cyber Schools Programme lancé à l'automne 2017 s'inscrit dans l'initiative publique CyberFirst.

SANS y apporte son expérience acquise au cours de programmes similaires dans d'autres pays.

Des formations sur mesure

Pour former une équipe en interne à un cours SANS précis, Private Training est le mode de formation idéal. Dans les faits, toutefois, l'organisation doit souvent mettre en place un programme sur mesure regroupant plusieurs de nos cours.

Chez SANS, nous collaborons étroitement avec les organisations pour comprendre leurs besoins spécifiques. Dans le cadre de notre démarche de conseil, nous combinons des cours de notre offre de formation SANS Cyber Security et d'autres complémentaires en une solution sur mesure.

Notre position unique nous permet de vous conseiller, puis d'assurer les formations nous-mêmes.

Évaluation et sélection de candidats

SANS accompagne régulièrement les entreprises dans la rationalisation de leurs processus et procédures de recrutement.

« Le tri des C.V. est le mode de sélection classique des candidats, explique Ned Baltagi, Directeur SANS Moyen-Orient et CCG. Les organisations se plaignent souvent de cette méthode chronophage, aux résultats décevants et peu fiables pour recruter les équipes de cybersécurité de première ligne. »

SANS CyberTalent est un instrument de sélection. Cette suite d'outils d'évaluation améliore l'efficacité du processus de sélection et de recrutement en cybersécurité.

Tests psychométriques et de compétences à l'appui, les produits SANS CyberTalent évaluent l'aptitude et les qualités des candidats en fonction des rôles. Les évaluations en ligne mettent à profit l'expérience de SANS en formation à la cybersécurité et à la certification GIAC pour valider les compétences et les connaissances techniques.

Avec CyberTalent, les équipes RH et les responsables acquièrent une compréhension plus fine des compétences techniques et conceptuelles des candidats.

Forces et faiblesses de l'équipe

SANS CyberTalent et les autres solutions sur mesure vont au-delà de la simple sélection de candidats. Chez SANS, nous accompagnons le développement et l'évolution des équipes de sécurité de nombreuses organisations.

« Les équipes de sécurité doivent changer et s'adapter. Des vecteurs d'attaque émergent, les technologies évoluent et les entreprises elles-mêmes doivent changer, déclare Jan Pieter Spaans. La formation est partie intégrante de cette évolution... mais les besoins en formation varient d'une personne à l'autre. Dans ce domaine, il n'y a pas de solution universelle. »

Pour aider les responsables à développer et accompagner leurs équipes, SANS propose SANS NetWars, SANS CyberCity, SANS CyberTalent et des produits d'évaluation qui offrent aux responsables sécurité et RH une vision claire des forces et des faiblesses de leurs équipes et des besoins en formation.

SANS élabore ensuite un programme de formation unique, axé sur les besoins de l'équipe ou de la personne.

La montée en compétence contribue également à stabiliser le personnel et à conserver toute son efficacité à l'équipe sécurité. Forte de son vaste programme de formations, SANS aide les employeurs à créer des plans de formation sur mesure.

Dans le cadre de notre prestation de conseil, nous proposons des programmes en accord avec les besoins de l'entreprise et un parcours d'évolution professionnelle à ses collaborateurs.

Programmes de formation

SANS a acquis une solide expérience de la conception de programmes de formation en interne pour tout type d'organisations (administrations, entreprises, agences militaires), y compris transnationales et dans des cultures économiques différentes.

Conçus pour répondre précisément aux besoins d'un client, ces programmes varient de par leur taille et leurs axes. SANS Cyber Academy est un de ces programmes déclinables.

« Les programmes de la Cyber Academy détectent et forment de nouveaux talents de la cybersécurité pour les affecter à des postes clés. Au Royaume-Uni, la Cyber Academy, via le programme public de reconversion HMG Cyber Retraining Academy, a formé de nouveaux professionnels de la sécurité, qualifiés et certifiés GIAC, preuve de notre savoir-faire dans la conception de formations sur mesure, déclare Stephen Jones, Directeur général SANS pour le Royaume-Uni et les pays nordiques. La Cyber Retraining Academy est le fruit d'une collaboration avec l'Administration britannique dans le cadre de la stratégie nationale de cybersécurité. »

« SANS commence par identifier des forts potentiels dans le domaine de la cybersécurité. Les candidats sont ensuite évalués à l'aide de SANS CyberTalent. »

« Les candidats retenus s'inscrivent ensuite à la Cyber Academy pour un stage de formation intensive à la cybersécurité avec des modules tirés des programmes de SANS. »

Comme pour la Cyber Academy de 2015, les diplômés en reconversion de la Cyber Retraining Academy s'insèrent rapidement dans des postes en cybersécurité.

SANS | CyberTalent

Recruter, développer et retenir l'équipe cyber ultime !

Évaluations des compétences et des aptitudes

Des informations et des éclairages pour améliorer les performances de l'équipe : SANS dispose de huit outils web d'évaluation qui donnent aux responsables de la cybersécurité des informations et des données utiles pour mieux gérer les compétences et les performances de leur équipe, améliorer le recrutement et mieux rentabiliser les investissements en formation. Si vous êtes un responsable intéressé par l'évaluation des cybertalents, pour votre équipe ou dans le cadre du recrutement, demandez-nous un extrait de cinq questions de nos CyberTalent Assessments.

Nos huit tests d'évaluation couvrent tout le spectre de la cybersécurité. À vous de choisir parmi eux le domaine qui correspond au besoin de votre organisation. Vous pouvez aussi choisir des tests Talent Pipeline : plus larges et aux thèmes variés, ils permettent de bien appréhender les compétences en sécurité des candidats.

Pour en savoir plus sur ces solutions, écrivez-nous à emea@sans.org ou asiapacific@sans.org

« Les CyberTalent Assessments nous servent aussi bien au recrutement que pour évaluer et déterminer les axes de progression de nos employés. Dans le cadre du recrutement, ces évaluations ont fortement contribué à appréhender le degré de compétences des candidats. »

- Jake Dorval, RSA® NetWitness®

SANS Cyber Ranges

Un continuum d'activités pour se former par la pratique

SANS propose un ensemble complet d'entraînements cyber au travers de scénarios interactifs et riches en enseignement. Affûtez les compétences cyber de vos collaborateurs, aiguisez leur attention et développez l'esprit d'équipe avec des expériences hors du commun.

Pourquoi les SANS Cyber Ranges ?

- SANS est la référence reconnue du secteur de la cybersécurité.
- Nos formateurs SANS renommés dans le monde entier créent des entraînements pour tous les niveaux de compétence.
- Les entraînements SANS cyber ranges vous aident, vous et vos équipes, à acquérir des compétences pratiques et à simuler des scénarios réels.
- Les joueurs pourront appliquer les connaissances acquises dans les SANS Cyber Ranges dès leur retour au bureau.
- Chez SANS, vous trouverez un cyber range pour chaque type de compétences, du novice à l'expert.

L'offre Cyber Range

	Évaluation	Événement/compétition	Simulation		
Basic • Socle de compétences • Axé sur le collaborateur	**BootUp CTF** • Niveau débutant à intermédiaire • Large spectre des disciplines de la cybersécurité • Exercices en solo ou en équipe • Rythme individuel • 1 à 2 jours annoncés une semaine à l'avance • Tableau de résultats dynamique	**NetWars** • Défis sophistiqués • Trame narrative convaincante • Avec des formateurs et des assistants-formateurs SANS • Exercices en solo ou en équipe • Plusieurs versions : Core, DFIR, Cyber Defense, ICS et Power Grid • 1 ou 2 jours, ou 4 mois, événements annoncés un mois à l'avance • Tableau de résultats dynamique • Trophées ou médailles avec une invitation au tournoi annuel des champions			
Intermediate • Connaissances plus poussées • Scénarios de terrain • Axé sur le collaborateur			**Cyber City** • Ville miniaturisée à l'échelle 1:87 • Véritables actifs d'ICS qui contrôlent des éléments physiques • Simule les secteurs de l'énergie résidentielle/industrielle, des transports, de l'eau et de la défense • Exercices en solo ou en équipe • 1 à 5 jours annoncés un mois à l'avance		
Expert • Simulation d'événements à fort impact sur l'entreprise • Attaques et défense sophistiquées • Axé sur les compétences d'équipe				**Jupiter Rockets** • Simulation fidèle de l'environnement d'entreprise • Développement des compétences offensives et en tests d'intrusion de niveau Expert • Exercices en solo ou en équipe • Rythme individuel • 1 à 2 jours annoncés un mois à l'avance • Tableau de résultats dynamique	**Cyber STX** • *Red Team* contre *Blue Team* : exercice d'intrusion APT • Protéger l'infrastructure IT et OT cible d'une attaque active • Équipes de 25 à plus de 100 personnes • 1 semaine, mais modulable • Préparation longue de la simulation, à prévoir 6 mois à l'avance
Pro • Environnements authentiques, dynamiques et complexes • Simulation d'attaques sophistiquées et défenses ciblées *best-of-breed* • Axé sur les compétences d'équipe					

« Si vous n'avez encore jamais participé à un événement NetWars CTF, vous ratez une occasion d'affûter vos compétences en vous amusant. Ces événements sont des modes d'apprentissage d'une efficacité redoutable », selon Ed Skodis, formateur SANS, qui sait bien de quoi il parle puisqu'il pratique ces CTF depuis 25 ans.
« J'apprécie particulièrement les CTF de SANS, car ils intègrent un système d'indices : si on est bloqué, on peut demander un coup de pouce, ce qui fait qu'on apprend et qu'on se forme au fur et à mesure. »

Programme Voucher

Le programme SANS Voucher est un système qui vise à gérer la formation de votre personnel chargé de la cybersécurité et qui vous permet de répondre aux besoins en formation de votre entreprise.

En tant que participant au programme SANS Voucher, vous pourrez ainsi :

- Offrir à votre équipe une formation de qualité et la certification correspondante
- Donner à vos employés une solution simple pour sélectionner et suivre la formation dont ils ont besoin quand ils en ont besoin
- Approuver et gérer facilement les inscriptions
- Suivre la progression et les évaluations des employés afin de valider l'acquisition des connaissances
- Vérifier les investissements, les débits et les soldes de comptes pour élaborer un budget optimal

Les crédits Voucher Funds peuvent être dépensés pour toute formation SANS en présentiel comme en distanciel, ainsi que pour tous les événements SANS Summit, les certifications GIAC ou les renouvellements de la certification*. Ils doivent être utilisés dans une période de 12 mois suivant l'achat, extensible par des investissements supplémentaires.

Lancez-vous

Rendez-vous sur www.sans.org/vouchers pour y remplir le formulaire de contact. Un représentant de SANS vous contactera par message électronique ou par téléphone dans les 24 heures ouvrables. Vos équipes pourront commencer à se former dans la semaine qui suit.

*Sont actuellement exclus du programme SANS Voucher : le programme Partnership, la sensibilisation Security Awareness et les ateliers SANS qui se tiennent lors d'événements organisés par d'autres organisations.

www.sans.org/vouchers

Live Online

Profitez de tout ce que vous aimez des formations SANS en présentiel, y compris leur dynamisme, mais sans vous déplacer.

SANS Live Online représente notre offre de formation en ligne la plus interactive. Les cours sont dispensés par des formateurs SANS chevronnés dans le cadre de sessions participatives en duplex ; et les stagiaires les suivent comme un présentiel : mêmes contenus, même accompagnement en temps réel, mêmes sessions bonus et mêmes bilans d'apprentissage.

Nous connaissons la diversité des besoins de nos stagiaires et de leurs organisations. Pour répondre à chaque situation, les stagiaires peuvent choisir entre des sessions en direct réparties sur plusieurs semaines ou sur la journée complète.

Formations et certifications
Apprenez les toutes dernières techniques des meilleurs formateurs au monde.

Sessions Bonus
En plus de la formation en groupe, vous avez accès à des mini-sessions privées avec le formateur.

Cyber Ranges
Mettez vos compétences en pratique lors des événements NetWars, tournois et compétitions de capture du drapeau (CTF).

Réseau
Messagerie instantanée avec vos pairs et les formateurs.

Pour en savoir plus : **sans.org/live-online**

cyberstart

Un ensemble de défis, d'outils et de jeux pour initier les enfants et les jeunes adultes à la cybersécurité.

Du fait de l'évolution des technologies en ligne et de la menace grandissante que posent les cybercriminels, la cybersécurité est désormais une priorité pour tous. Pour se protéger contre les cybermenaces, les gouvernements et les entreprises doivent pouvoir s'appuyer sur un vivier de professionnels compétents.

Problème : la pénurie de talents sévit dans le monde entier, en partie parce que les jeunes sont peu nombreux à s'engager dans la sécurité informatique et l'IT.

C'est précisément pour cela que le SANS Institute a créé CyberStart : un ensemble innovant de défis, d'outils et de jeux pour initier les enfants et les adolescents à la cybersécurité.

Avec CyberStart, SANS bouscule les idées reçues sur la cybersécurité en la présentant comme une orientation professionnelle attrayante, passionnante et accessible, tout en aidant les organisations gouvernementales à développer leurs capacités nationales en cybersécurité.

L'OFFRE CYBERSTART

Il est possible d'adapter l'offre CyberStart aux besoins et spécificités des organisations. Parmi les éléments que SANS propose :

CyberStart Assess pour l'évaluation

Conçu pour repérer les individus présentant un talent et des aptitudes innés pour la cybersécurité, CyberStart Assess est un outil d'évaluation en ligne qui rassemble toute une gamme de petits défis.

CyberStart Game pour les défis en ligne

Avec CyberStart Game, les jeunes endossent le rôle d'un agent de sécurité et doivent rassembler des informations, décrypter des codes, trouver des failles de sécurité et suivre les pistes numériques de criminels. Les jeunes découvrent Linux, le chiffrement et la programmation sur un mode ludique.

CyberStart Essentials pour la théorie

CyberStart Essentials est une suite de labos interactifs, de vidéos, d'examens et de quizz pour acquérir les connaissances théoriques qui sous-tendent des thèmes pointus comme les tests d'intrusion et les réseaux.

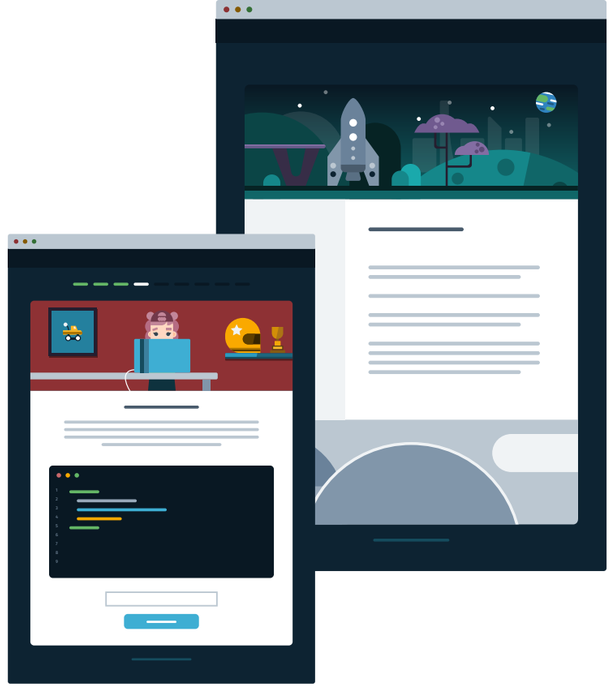
CyberStart Elite pour s'affronter en équipe

Les événements CyberStart Elite permettent aux jeunes de se rencontrer et de s'affronter dans des compétitions de capture du drapeau (CTF). En équipe, les jeunes utilisent leurs nouvelles compétences en cybersécurité pour relever des défis en temps limité.

QU'EST-CE QUI DISTINGUE CYBERSTART ?

On n'enseigne pas aux jeunes comme aux adultes. Ce serait risquer de les repousser. CyberStart joue plutôt la carte ludique et se déploie en une plateforme attractive spécifiquement conçue pour les jeunes.

Ne nécessitant aucune connaissance préalable en cybersécurité et couvrant différentes tranches d'âge et niveaux de compétence et de difficulté, CyberStart a déjà converti des milliers de jeunes dans le monde entier.



COMMENT SE LANCER

Le programme CyberStart et ses composants offrent une certaine souplesse et peuvent s'adapter aux besoins de chaque organisation. L'équipe dédiée de SANS collabore avec les organisations pour prendre en compte leurs spécificités et garantir qu'elles tirent le plein potentiel de CyberStart.

Qu'il s'agisse pour une organisation de sensibiliser davantage à la cybersécurité ou d'inspirer la prochaine génération de cyberexperts, CyberStart sait s'y prendre.

LA PÉNURIE DE COMPÉTENCES EN CYBERSÉCURITÉ

Le manque de compétences en cybersécurité est l'un des principaux enjeux actuels du secteur. SANS s'efforce de trouver des solutions, et CyberStart en fait partie.

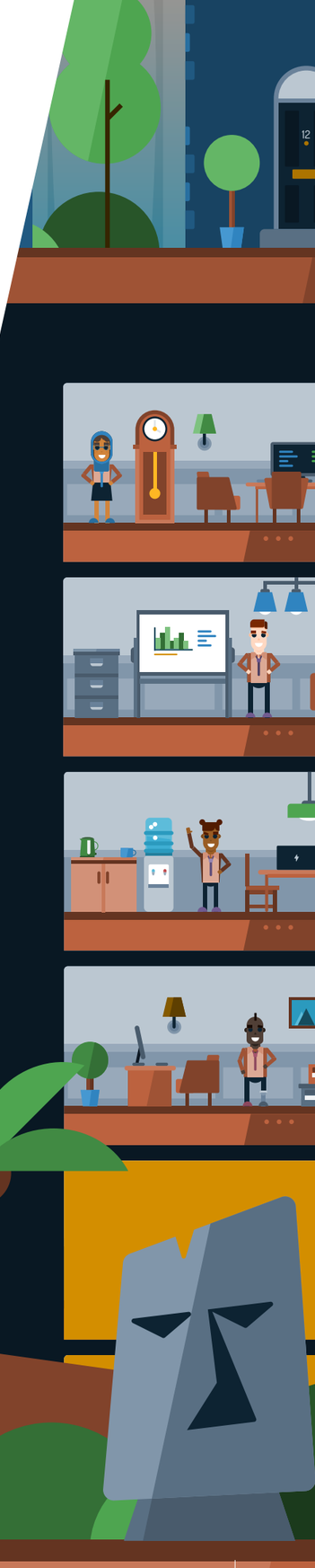
Pour essayer CyberStart, rendez-vous sur go.cyberstart.com.

Pour jouer ou en savoir plus sur la cybersécurité, vous et vos enfants pouvez vous inscrire sur www.cyberstart.com

Pour toute question, demande d'information ou pour vous inscrire à SANS CyberStart, veuillez envoyer un email à : emea@sans.org ou asiapacific@sans.org

« J'ai pu explorer la facilité avec laquelle des cybercriminels arrivent à accéder à nos données et les techniques qu'ils utilisent. J'ai acquis des compétences précieuses, bien plus approfondies que ce que j'ai pu apprendre au lycée. »

Participant au CyberStart Game



Cyberdéfense - Fondamentaux

Tous les professionnels qui se voient confier des tâches pratiques de cybersécurité devraient acquérir un socle commun de compétences sur le fonctionnement des attaques, la mise en œuvre d'une défense en profondeur et la réponse aux incidents afin de réduire les risques et de sécuriser correctement les systèmes.

La sécurité dicte de placer haut la barre lorsque vous définissez ce socle de compétences dans votre organisation. À l'issue d'une formation SANS Cyber Defence Essentials, vous saurez :

- Adopter des techniques axées sur les problèmes de sécurité prioritaires dans votre organisation
- Établir un socle solide de politiques et pratiques fondamentales pour exercer votre équipe de sécurité à la réponse aux incidents
- Déployer une panoplie de stratégies et techniques pour défendre une entreprise sous tous ses angles
- Identifier les vecteurs d'attaque les plus récents et mettre en œuvre des contrôles pour les prévenir et les détecter
- Utiliser des stratégies et des outils pour détecter les attaques
- Développer des indicateurs de sécurité pertinents formant la base d'un guide opérationnel à implémenter par l'équipe IT, à valider par les auditeurs et compréhensible par la direction
- Mettre en œuvre un programme exhaustif de sécurité axé sur la prévention et la détection des attaques et la réponse à y apporter
- Développer une feuille de route de sécurité interne évolutive pour répondre aux besoins d'aujourd'hui et de demain

Fonctions de cyberdéfense :
- Analyste sécurité
- Ingénieur sécurité
- Responsable technique
- Auditeur

« Cette formation dresse le panorama de la sécurité… La manne d'informations vous servira à déterminer des problèmes de sécurité que vous n'aviez même pas envisagés. »

— Frank Perrilli, **IESO**

Tests d'intrusion

Dans une organisation, les tests d'intrusion servent à déceler et comprendre les vulnérabilités d'un système afin de trouver une parade aux problèmes connus avant qu'une attaque ne survienne.

Les adversaires évoluent et les attaques se sophistiquent : les experts en intrusion doivent reproduire les techniques d'attaque qui existent sur le terrain, découvrir les problèmes et formellement documenter leurs constatations pour apporter toute leur valeur à l'équipe sécurité.

À l'issue d'une formation SANS Penetration Testing, vous saurez :

- Reproduire les attaques actuelles les plus puissantes et les plus courantes
- Découvrir des vulnérabilités dans des systèmes cibles
- Exploiter ces vulnérabilités dans un environnement contrôlé
- Mettre en œuvre votre expertise technique pour déterminer et documenter les risques et leur impact commercial potentiel
- Mener des tests sûrs et dans les règles de l'art, conformément au périmètre et aux règles d'engagement précisément définis
- Aider une organisation à hiérarchiser ses ressources par priorité

Fonctions en tests d'intrusion :
- Expert en tests d'intrusion système/réseau
- Expert en tests d'intrusion applicatifs
- Chargé de réponse aux incidents
- Spécialiste dans la recherche de vulnérabilités
- Développeur d'exploits

« En une semaine, le formateur nous a fait passer de l'analyse classique des vulnérabilités à l'art véritable des tests d'intrusion. Merci SANS d'avoir renforcé mes capacités en sécurité de l'information et celles de mon entreprise ! »

— Mike Dozier, **Savannah River Nuclear Solutions**

Fonctions en réponse aux incidents, threat hunting et inforensique

Quelle que soit sa taille, une organisation a besoin de personnel qui maîtrise les techniques de réponse aux incidents pour identifier les systèmes compromis, circonscrire efficacement la violation et remédier rapidement à l'incident.

De même, les organismes publics et les forces de l'ordre sont en demande de personnels compétents pour exploiter les supports informatiques et récupérer les éléments de preuve sur les appareils et systèmes ennemis. Une formation SANS Incident Response Threat Hunting and Digital Forensics vous apprend à :

- Traquer l'adversaire avant et pendant un incident dans toute l'entreprise
- Acquérir des connaissances inforensiques approfondies sur les systèmes d'exploitation Microsoft Windows et Apple OSX
- Examiner smartphones et dispositifs mobiles à la recherche de malwares et d'artefacts forensiques
- Intégrer l'inforensique réseau à vos enquêtes pour obtenir plus rapidement de meilleurs résultats
- Ne négliger aucun détail en intégrant l'analyse des mémoires dans vos enquêtes
- Comprendre les capacités des malwares pour en tirer des renseignements sur les menaces, réagir aux incidents de cybersécurité et fortifier les défenses
- Identifier, extraire, hiérarchiser et exploiter le renseignement sur les cybermenaces provenant d'intrusions persistantes et avancées (APT)
- Apprécier qu'un chargé de réponse aux incidents bien formé peut s'avérer le seul rempart de l'entreprise en cas de compromission
- Identifier, collecter, préserver les données et répondre à un incident sur une large gamme de dispositifs de stockage en garantissant l'intégrité incontestable des éléments de preuves

« Cette formation est indispensable ! Les outils et les compétences qu'on y acquiert sont juste excellents ! »

— James Tayler, **Context Information Security**

Gestion de la sécurité, aspects juridiques et audit

Dans un monde où le paysage des menaces ne cesse d'évoluer, la cybersécurité s'avère plus précieuse que jamais en entreprise. Les acteurs économiques comprennent désormais l'importance de sécuriser les actifs informationnels de valeur et les risques non négligeables que font courir les atteintes ou attaques.

Les organisations ont donc besoin de directeurs et de responsables cyber sachant allier leurs connaissances techniques aux indispensables compétences managériales, pour mener efficacement leurs projets, équipes et initiatives en soutien des objectifs de l'entreprise.

L'axe gestion de la sécurité, aspects juridiques et audit propose des approches pratiques et valides de gestion du risque cyber. Cette séquence de cours interactifs et pratiques aide les managers actuels ou en devenir à mettre leurs compétences managériales au niveau de leurs connaissances techniques.

Dans les formations Management et audit, vous apprendrez à :

- Développer vos compétences en gestion et en leadership
- Comprendre et analyser le risque
- Créer une stratégie efficace de cybersécurité
- Élaborer un programme de gestion des vulnérabilités
- Développer des plans stratégiques de sécurité en fonction des objectifs opérationnels et organisationnels
- Interagir et communiquer efficacement avec les principaux intéressés en responsabilité
- Mesurer les effets de votre programme de sécurité
- Sensibiliser tous les acteurs aux enjeux de la cybersécurité et aux moyens de protéger l'organisation contre les menaces

« Cette formation touche tous les aspects de mon travail, de la gestion du réseau à la gestion de projet. »

— David Chaulk, **Enbridge**

Sécurité cloud

Contre les menaces croissantes qui pèsent sur le cloud, la Sécurité cloud mobilise les précieuses ressources de SANS sous toutes leurs formes (formation, certification, recherche, efforts collectifs), avec l'objectif d'aider les professionnels à construire, déployer et gérer de manière sécurisée leur infrastructure, leurs plateformes et leurs applications en cloud.

Intensives et en immersion, les formations à la cybersécurité cloud du programme Sécurité cloud de SANS vous apprennent, à vous et vos équipes, à maîtriser les étapes concrètes de défense des systèmes et applications cloud contre les menaces les plus dangereuses. Les cours regorgent de techniques utiles et immédiatement exploitables que vous pourrez appliquer dès votre retour au bureau. Issu d'un processus de consensus regroupant les meilleurs ingénieurs, architectes, administrateurs, développeurs, responsables sécurité et professionnels de la sécurité de l'information, ce programme traite les scénarios de cloud public, multicloud et de cloud hybride pour l'entreprise comme pour les organisations en croissance.

« Magistral ! Si vous êtes un architecte en sécurité classique qui touche un peu à DevOps, suivez SEC540 : ce cours vous guide dans les profondeurs de DevSecOps et vous prépare à l'avenir ! »

— Jatin Sachdeva, **CISCO**

Systèmes de contrôle industriel

Le paysage actuel présente un panorama chaotique et varié des menaces qui planent sur les systèmes de contrôle industriel, leurs propriétaires et leurs opérateurs.

Il ne s'agit plus de théorie ni de spéculation : les attaques causent des dommages matériels et affectent des processus physiques. Nous sommes témoins d'incidents où des intrusions malveillantes endommagent les systèmes et perturbent les opérations grâce à des malwares adaptés aux ICS. Nous devons nous tenir prêts à défendre nos systèmes de contrôle contre des adversaires toujours plus sophistiqués. Les formations SANS sur les systèmes de contrôle industriel vous apprendront à :

- Comprendre les systèmes de contrôle industriel notamment les composants, les objectifs, les déploiements, les enjeux et les contraintes
- Identifier les actifs des systèmes de contrôle industriel et leurs topologies réseau, et superviser les points chauds de ces systèmes pour y détecter anomalies et menaces
- Comprendre les approches qui régissent les architectures et techniques de défense des réseaux et systèmes
- Mener une réponse à incident ICS axée sur les opérations de sécurité avec la sûreté et la fiabilité des opérations pour priorité
- Mettre en œuvre efficacement des contrôles d'accès physiques et numériques

« Après une introduction théorique, la formation se focalise rapidement et complètement sur la pratique avec les différents éléments. Une expérience rare. »

– Bassem Hemida, **Deloitte**

SANS OnDemand

Les cours SANS OnDemand s'adressent particulièrement aux stagiaires qui veulent allier l'exhaustivité du contenu à un mode de formation souple, sans déplacement ni absence professionnelle. Le rythme d'apprentissage à la carte convient à tous les styles. Dispensées par les meilleurs formateurs SANS, nos formations OnDemand, accessibles sur ordinateur, iPad et tablette, vous laissent étudier en mobilité ou confortablement installé chez vous.

Un choix de **plus de 50 formations SANS** avec :

Contenu accessible 24h/24 pendant quatre mois

Vous pourrez accéder au contenu de votre cours pendant toute la durée de votre formation : vous avancez à votre rythme et maîtrisez votre environnement comme votre emploi du temps. L'option OnDemand vous donne la liberté de vous former où bon vous semble et lorsque vous le décidez.

Cours magistral, quizz, exercices pratiques et labos virtuels

En plus des supports de cours accessibles 24h/24, vous pouvez consulter tous les enregistrements de vos cours, les exercices en classe et les labos virtuels associés à chaque module. Cette possibilité de revenir sur les sujets complexes pour les réviser vous donne amplement le temps de vous en approprier le contenu et de renforcer les acquis issus des exercices concrets et pratiques.

Experts techniques

À tout moment de la formation, les experts techniques SANS Subject-Matter Experts (SME) sont à votre disposition pour répondre à vos questions et vous aider à appréhender les sujets les plus complexes. Joignables par la messagerie instantanée, nos SME sont là pour accompagner votre réussite et vous aider à vous approprier le contenu.

Jeu complet de livres, supports de cours et bilans de progression pédagogique

Vos cours contiennent tout ce qu'il vous faut pour réussir votre formation. Les livrets de formation sont envoyés à votre adresse postale à l'inscription ; les autres supports (enregistrements des cours, labos virtuels et exercices pratiques) sont accessibles en ligne pendant toute la formation ; et les bilans de progression vous aident à maintenir le cap, à reprendre où vous en étiez et à planifier votre calendrier de formation en conséquence.

Préparation GIAC

Les cours OnDemand sont aussi un excellent moyen de vous préparer à une certification GIAC. L'accès plein et entier au contenu vous donne amplement le temps de réviser le cours, de maîtriser les notions et d'étudier en toute sérénité pour l'examen.

Rendez-vous sur **sans.org/ondemand** pour trouver le cours qu'il vous faut, découvrir nos offres spéciales et vous inscrire dès aujourd'hui !

SEC 301

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

Introduction to Cyber Security

Pour déterminer si le cours SANS SEC301 est adapté à vos besoins, répondez aux cinq questions suivantes :

- Êtes-vous novice en cybersécurité, à la recherche d'une initiation aux fondamentaux de la sécurité ?
- Êtes-vous bombardé de termes techniques complexes dont la signification vous échappe ?
- Avez-vous besoin de vous familiariser avec les concepts élémentaires, les principes et le jargon de la sécurité, sans pour autant vouloir entrer dans les détails ?
- Avez-vous décidé de réorienter votre carrière vers le marché porteur de la cybersécurité, ce qui nécessite une formation et une certification ?
- Êtes-vous un cadre dirigeant angoissé à l'idée que votre entreprise pourrait être victime d'un piratage massif et fasse la une des journaux ?

Si vous avez répondu oui à l'une de ces questions, le cours SEC301: Introduction to Cyber Security est adapté à vos besoins. Nos connaissances et notre enseignement dispensé par de véritables experts de la sécurité reconnus mondialement, sur des sujets fondamentaux pour la cybersécurité, vous donneront une longueur d'avance.

Ce cours complet de cinq jours couvre un large éventail de sujets, de la terminologie aux bases de l'informatique et des réseaux jusqu'aux technologies de sécurité : politiques de sécurité, gestion des risques, nouveautés en matière de mots de passe, principes de la cryptographie, attaques réseau et malwares, sécurité sans fil, pare-feu, sécurité du web et des navigateurs, sauvegardes, machines virtuelles, cloud computing... Tous les sujets sont abordés simplement, sous l'angle de l'initiation.

Ce cours s'adresse aux stagiaires qui ont une connaissance élémentaire des ordinateurs et de la technologie, et n'ont jamais abordé le sujet de la cybersécurité. Notre approche pédagogique, pragmatique et graduelle, vous permettra de comprendre toutes les informations présentées, même si certains sujets sont nouveaux pour vous. L'enseignement concret des principes de la cybersécurité formera un socle solide de connaissances et de compétences pour les années à venir.

Conçu par un professionnel de la cybersécurité fort de plus de 35 ans d'expérience dans les secteurs public et privé, le cours SEC301 est concret et objectif, du début à la fin. Il vous prépare au test de certification GIAC Information Security Fundamentals (GISF) et à votre prochaine formation. Et, bien sûr, il est fidèle à la promesse SANS : « Vous pourrez utiliser les connaissances et compétences acquises dans le cours SEC301 dès votre retour au bureau. »

« J'apprécie vraiment l'enthousiasme des formateurs. Ils maîtrisent leur sujet et partagent leurs connaissances de façon concrète et efficace. La formation SANS est bien plus profitable qu'une certification sur la confidentialité. »

Ron Hoffman,
MUTUAL OF OMAHA

CERT. GIAC :GISF
30 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GISF

Public visé :

- Tout novice en cybersécurité qui cherche une initiation aux fondamentaux de la sécurité
- Toute personne démunie face à une avalanche de termes techniques complexes dont la signification lui échappe
- Responsables sécurité non informaticiens qui traitent des problèmes techniques, qui les comprennent et qui refusent que leur entreprise soit connue comme la dernière victime en date d'un piratage massif
- Professionnels ayant des connaissances informatiques et techniques élémentaires qui ont besoin de se familiariser avec les concepts, principes et jargons généraux, sans pour autant vouloir entrer dans les détails
- Professionnels qui décident de réorienter leur carrière vers le marché porteur de la cybersécurité et ont besoin d'une formation et d'une certification reconnues

Vous apprendrez à...

- Communiquer avec confiance sur divers sujets concernant la sécurité de l'information, les termes et les concepts
- Comprendre et appliquer les principes de moindre privilège
- Comprendre et appliquer la triade CIA (Confidentiality, Integrity, Availability)
- Construire des mots de passe plus sécurisés, et plus faciles à retenir
- Acquérir les principes de la cryptographie, les processus, procédures et applications
- Comprendre les fondamentaux des réseaux informatiques
- Maîtriser les acronymes réseau : TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP et DNS
- Utiliser les outils intégrés de Windows pour voir vos paramètres réseau

SEC 401

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Security Essentials Bootcamp Style

Ce cours aborde les méthodes les plus efficaces pour prévenir une attaque et détecter les intrusions avec des techniques exploitables que vous pourrez utiliser dès votre retour au bureau. Des experts vous donneront conseils et astuces pour remporter le combat contre des cyberassaillants de toute sorte qui cherchent à endommager votre environnement.

PRENEZ LE TEMPS de vous demander :

- Est-ce que vous comprenez réellement pourquoi certaines organisations sont compromises et d'autres non ?
- Pouvez-vous garantir que vous savez trouver les systèmes compromis dans votre réseau s'il y en a ?
- Connaissez-vous l'efficacité de chaque appareil de sécurité et pouvez-vous garantir que tous sont configurés correctement ?
- Est-ce que des indicateurs de sécurité adaptés ont été définis et communiqués à vos responsables pour les aider à prendre les bonnes décisions en matière de sécurité ?

Si vous n'avez pas la réponse à ces questions, alors SEC401 vous apportera toutes les connaissances en sécurité des informations dont vous avez besoin. Cette formation est dispensée dans un format d'entraînement de style bootcamp et est renforcée avec des exercices pratiques.

Le cours SEC401: Security Essentials Bootcamp Style vise à vous enseigner les compétences et techniques fondamentales de sécurité des informations dont vous avez besoin pour protéger et sécuriser les actifs informationnels clés et les systèmes métier de votre organisation. Et bien sûr, notre formation vous montrera comment éviter à votre entreprise de faire partie des victimes de la cyberguerre !

La prévention est idéale, mais la détection est un must.

Les menaces persistantes et avancées sont en constante progression et de ce fait, les organisations finiront tôt ou tard par être prises pour cible. L'efficacité des défenses d'une organisation est le principal critère qui va déterminer la réussite ou l'échec d'une intrusion sur le réseau. Repousser les cyberattaques est un défi permanent, avec de nouvelles menaces qui font sans cesse leur apparition et même de nouveaux types d'attaques. Les organisations doivent comprendre quelles sont les méthodes de lutte efficaces. La bonne vieille recette consiste à adopter une approche basée sur le risque. Il convient de répondre à trois questions avant de consacrer un budget, du temps ou des ressources à la cybersécurité :

- Quels sont les risques ?
- Est-ce qu'il s'agit d'un risque à priorité maximale ?
- Quel est le moyen le plus rentable de réduire ce risque ?

La sécurité commence avant tout par s'assurer d'intervenir au bon endroit. Avec le cours SEC401, vous apprendrez le langage et la théorie de fonctionnement à l'origine de l'informatique et de la cybersécurité. Vous acquerrez les connaissances fondamentales et efficaces pour sécuriser les systèmes ou organisations de votre responsabilité. Ce cours tient nos deux promesses SANS : (1) Vous y apprendrez des compétences actualisées exploitables dès votre retour au bureau. (2) Les intervenants font partie des meilleurs formateurs en sécurité.

CERT. GIAC : GSEC
46 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GSEC

Public visé :

- Professionnels de la sécurité qui veulent combler des lacunes dans leur compréhension de la sécurité des systèmes d'information
- Responsables qui veulent acquérir une compréhension de la sécurité au-delà des concepts et de la terminologie de base
- Personnel opérationnel pour lequel la sécurité n'est pas une responsabilité primordiale, mais qui a néanmoins besoin de comprendre la sécurité informatique pour être efficace
- Ingénieurs IT et superviseurs qui doivent savoir construire un réseau défendable
- Administrateurs chargés de la construction et de l'entretien des systèmes ciblés par des attaquants
- Spécialistes de l'inforensique, experts en tests d'intrusion et auditeurs qui doivent connaître les bases de la sécurité pour être performants
- Toute personne novice en sécurité informatique avec une expérience des systèmes d'information et des réseaux

Vous apprendrez à...

- Concevoir et construire une architecture de réseau avec VLAN, NAC et 802.1x en fonction d'un indicateur de compromission APT
- Exécuter des outils de ligne de commande Windows pour repérer les éléments à risque élevé dans le système
- Exécuter des outils de ligne de commande (ps, ls, netscat, etc.), et du script basique pour automatiser le fonctionnement de programmes afin de superviser en continu divers outils
- Installer VMWare pour créer un laboratoire virtuel où tester et évaluer les outils et la sécurité des systèmes
- Créer une politique efficace applicable au sein d'une organisation et préparer une liste de validation de la sécurité, avec des indicateurs chiffrés pour faire le lien avec les actions de formation et de sensibilisation

SEC 450

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

Blue Team Fundamentals: Security Operations and Analysis NOUVEAU

Vous cherchez à intégrer vite et bien vos nouveaux effectifs d'analystes, d'ingénieurs et d'architectes en cybersécurité dans l'organisation ? Vos responsables du centre des opérations de sécurité (SOC) ont-ils besoin d'acquérir une perspective technique pour améliorer la qualité de leur analyse, réduire le taux de renouvellement du personnel et diriger un SOC efficace ?

La formation intensive SEC450 est un tremplin conçu pour les nouvelles recrues des équipes de cyberdéfense et les responsables SOC. Elle présente aux stagiaires les outils courants dans l'environnement de travail en cyberdéfense et inclut toutes les explications nécessaires sur les outils, les processus et les flux de données que tout membre d'une *Blue Team* doit connaître.

Les stagiaires découvrent les différentes étapes des opérations de sécurité : la collecte de données, les emplacements de la collecte, et le repérage de menaces dans ces données. Le cours s'intéresse en profondeur aux tactiques de tri et d'investigation des événements identifiés comme malveillants, ainsi qu'aux erreurs courantes à éviter et au maintien d'une haute qualité de l'analyse. Les stagiaires découvrent les rouages internes des protocoles les plus courants et les moyens de repérer les fichiers piégés ainsi que les attaques au sein des hôtes et données de leur réseau.

Le cours s'appuie sur un enseignement et des exercices pratiques dans un environnement SOC simulé intégrant l'ensemble des outils professionnels, notamment :

- Un système de gestion des informations et des événements de sécurité (SIEM)
- Un système de gestion et de suivi des incidents
- Une plateforme de renseignement sur les menaces
- Des outils de capture et d'analyse de paquets
- Des outils d'automatisation

Une carrière en cyberdéfense est souvent passionnante et exigeante : de nombreux SOC souffrent d'un fort taux de roulement. Pour agir en amont, le cours présente les conclusions d'études sur la prévention de l'épuisement professionnel et sur le maintien de la motivation par le développement continu, l'automatisation et la réduction des faux positifs. À l'issue de la formation, les stagiaires ont une vue exhaustive du fonctionnement de la collecte et de la détection, de l'utilisation et de la complémentarité des outils SOC, et de l'opérationnalité à long terme de leur SOC.

« Examiner les journaux et comprendre leur remontée vers le SIEM est super utile, surtout pour quelqu'un sur le point de devenir admin SIEM. La partie sur l'analyse des logiciels malveillants est fantastique pour les analystes à tous points de vue. »
Tony Dinkel
Aires

36 CRÉDITS CPE/CMU

Public visé :

- Analystes sécurité
- Spécialistes en investigation d'incident
- Ingénieurs et architectes sécurité
- Responsables sécurité technique
- Responsables de centres des opérations de sécurité (SOC) qui cherchent à acquérir une perspective technique pour améliorer la qualité de leur analyse, réduire le taux de renouvellement du personnel et diriger un SOC efficace
- Quiconque aspirant à une carrière en défense (*Blue Team*)

SEC 487

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Open-Source Intelligence Gathering and Analysis

Les sites internet, les applications et les plateformes des réseaux sociaux que nous utilisons et actualisons au quotidien accumulent des quantités incroyables de données personnelles et potentiellement incriminantes. Les personnes, les pouvoirs publics et les entreprises, avec l'aide d'un spécialiste, peuvent se servir de ces informations pour résoudre des problèmes financiers, voire des conflits au travail ou des affaires criminelles.

Le coursSEC487 enseigne aux stagiaires des moyens licites et efficaces de trouver, rassembler et analyser ces données. Vous découvrirez les emplacements privilégiés où recueillir ces données par divers méthodes et outils manuels ou automatiques. Une fois les données rassemblées, nous vous montrerons comment les analyser, garantir leur fiabilité et les exploiter dans vos investigations.

Ce cours est un socle de formation sur le renseignement de sources ouvertes (Open Source Intelligence, OSINT en anglais) où vous aborderez rapidement de nombreux domaines. Vous y découvrirez les compétences, techniques et outils modernes que les forces de l'ordre, les détectives, les pirates informatiques et les cyberdéfenseurs utilisent sur le terrain pour rassembler des quantités phénoménales d'informations sur internet, en analyser les résultats, et exploiter certains renseignements pour rebondir vers de nouvelles pistes. Notre objectif est de vous fournir un socle de connaissances en OSINT pour réussir dans ce domaine, que vous soyez professionnel de la cyberdéfense, analyste renseignements et menaces, enquêteur privé, enquêteur spécialisé en assurance, analyste renseignements, personnel des forces de l'ordre ou simple curieux en la matière.

Tout au long de la semaine, les stagiaires se familiariseront avec les outils et techniques de base de la collecte de données libres sur internet dans le cadre de vingt laboratoires pratiques qui les emmèneront aussi bien sur internet que dans les profondeurs du darknet pour gagner en assurance. À l'issue de ce cours, en plus de maîtriser les fonctions de recherche sur un site web, vous connaîtrez la totalité des scénarios et leurs critères ainsi que les techniques OSINT de recueil des données OSINT qui vous intéressent vraiment.

Public visé :

- Chargés de réponse aux cyberincidents
- Analystes inforensiques et chargés de réponse aux incidents (DFIR)
- Experts en tests d'intrusion
- Ingénieurs sociaux
- Forces de l'ordre
- Personnel des services de renseignement
- Recruteurs/Sources
- Enquêteurs privés
- Inspecteurs-enquêteurs d'assurances
- Personnel des ressources humaines
- Chercheurs

Vous apprendrez à...

- Créer un processus OSINT
- Mener des investigations OSINT pour une grande diversité de clients
- Comprendre le cycle de vie de la collecte de données
- Créer une plateforme sécurisée de collecte de données
- Analyser les critères de collecte du client
- Capturer et enregistrer des données
- Créer des comptes leurres
- Créer votre propre processus OSINT
- Collecter des données internet
- Effectuer des recherches pour le compte d'autrui
- Accéder aux données des réseaux sociaux
- Évaluer à distance un lieu à l'aide de caméras et de cartes en ligne
- Examiner les données de géolocalisation sur les réseaux sociaux
- Vous renseigner sur des sociétés
- Utiliser les données fournies par l'Administration
- Collecter des données sur le darknet
- Exploiter des sites et outils du monde entier

GIAC CERT: GOSI
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GOSI

SEC 501

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Security Essentials – Enterprise Defender

Une cybersécurité efficace s'avère plus importante que jamais dans la mesure où les attaques se font de plus en plus discrètes, ont un impact financier de plus en plus important et nuisent à la réputation.

Le cours SEC501: Advanced Security Essentials – Enterprise Defender procure une base solide de règles et de pratiques fondamentales qui permet au personnel de sécurité de défendre correctement son entreprise.

Dans l'univers de la sécurité, on dit que « la prévention est l'idéal, la détection est une nécessité ».Mais détecter sans réagir ne sert à rien. La sécurité réseau doit faire l'objet d'une amélioration constante de façon à prévenir autant d'attaques que possible, mais aussi pour détecter rapidement les brèches de sécurité et y répondre de manière appropriée. Cette stratégie PRÉVENIR - DÉTECTER - RÉAGIR doit être mise en place aussi bien en interne qu'en externe. Les données devenant de plus en plus mobiles et les réseaux de plus en plus poreux entraînent un besoin ciblé de protection des données. La sécurité des informations critiques doit être préservée, quel que soit leur emplacement (serveur, architecture réseau solide, appareil mobile...).

Mais tous les efforts du monde ne peuvent garantir une défense et une protection absolues. Partant de cette réalité, les organisations doivent être en mesure de détecter des attaques de manière précoce. Il s'agit ici de comprendre le trafic qui circule sur vos réseaux et de veiller aux signes d'attaques, mais aussi de faire effectuer des tests d'intrusion et des analyses de vulnérabilité afin d'identifier les problèmes et les failles avant que les données de votre entreprise ne soient compromises.

Et dès lors qu'une attaque est détectée, il est indispensable de réagir rapidement et de réaliser des expertises numériques en conséquence. Comprendre les agissements d'un attaquant permet de tirer des leçons utiles pour renforcer les mesures de défense, de prévention et de détection, et compléter ainsi le cycle de la sécurité.

« C'est de loin le meilleur cours auquel j'ai assisté. Chaque jour, j'ai appris des choses applicables au travail. »
- Stuart Long,
BANK OF ENGLAND

« Excellent cours, très intéressant et complet. »
- John O'Brien,
AIRBUS DEFENCE & SPACE

Public visé :

- Experts en tests d'intrusion et personnes chargées de répondre aux incidents
- Analystes et ingénieurs des centres opérationnels
- Professionnels de la sécurité des réseaux
- Toute personne qui cherche à acquérir des connaissances techniques approfondies pour implémenter des solutions de sécurité globales

Vous apprendrez à...

- Identifier les menaces de réseau contre les infrastructures et construire des réseaux défendables pour minimiser l'impact des attaques
- Accéder aux outils qui peuvent être utilisés pour analyser un réseau, prévenir les attaques et détecter l'adversaire
- Décoder et analyser des paquets de données à l'aide d'outils divers pour identifier des anomalies et améliorer les défenses de réseau
- Comprendre les méthodes de l'adversaire pour compromettre les systèmes et répondre aux attaques
- Effectuer des tests d'intrusion contre une organisation afin de déterminer les vulnérabilités et les points de compromission
- Appliquer le processus en six étapes de gestion des incidents
- Utiliser divers outils pour identifier les malwares dans toute l'organisation et y remédier
- Créer un programme de classification des données et déployer des solutions pour prévenir la perte de données tant au niveau de l'hôte qu'au niveau du réseau

CERT. GIAC : GCED
38 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCED

SEC 503

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

Intrusion Detection In-Depth

Les cas de grandes organisations piratées dont la réputation est irrémédiablement compromise font désormais partie du quotidien. Comment faire pour que votre entreprise ne soit pas la prochaine victime d'une cyberattaque de grande ampleur ?

Préserver la sécurité des organisations est plus complexe que jamais dans un monde où la cybermenace est omniprésente. Le paysage de la sécurité évolue constamment, et l'époque du simple périmètre de protection est révolue. Désormais, il faut protéger des systèmes exposés et des appareils mobiles, des cibles connectées presque en permanence et parfois vulnérables. C'est là qu'entre en jeu un personnel de sécurité en mesure de détecter et d'empêcher les intrusions. Notre objectif avec le cours SEC503: Intrusion Detection In-Depth est de vous permettre d'acquérir les connaissances, les outils et les techniques indispensables pour défendre votre réseau en connaissance de cause. Cette formation vous prépare à utiliser immédiatement vos nouvelles compétences et connaissances.

Pour reprendre Mark Twain : « Il est plus facile de tromper les gens que de les convaincre qu'ils ont été trompés. » Bien souvent, les solutions de détection/prévention des intrusions (IDS/IPS) se contentent de proposer une évaluation du trafic de type rouge/vert ou bon/mauvais, que les analystes non formés acceptent sans contester. Ce cours vise à faire comprendre qu'un analyste averti exploitera une alerte IDS comme point de départ d'un examen du trafic, et non comme une évaluation définitive. Le module SEC503 repose sur le principe qu'un analyste doit pouvoir examiner les alertes pour les comprendre et les mettre en contexte.Vous apprendrez à analyser et à reconstruire une activité pour déterminer s'il s'agit d'une indication légitime ou non.

Le cours SEC503:Intrusion Detection In-Depth dispense les connaissances techniques et la formation pratique dont vous avez besoin pour défendre sereinement votre réseau. Vous découvrirez la théorie sous-jacente des protocoles les plus utilisés (TCP/IP, DNS, HTTP, etc.) de façon à pouvoir examiner le trafic réseau en quête de signes d'intrusion. Vous aurez tout le loisir d'apprendre à maîtriser différents outils open source, comme tcpdump, Wireshark, Snort, Bro, tshark et SiLK. Des exercices pratiques et quotidiens adaptés à tous les niveaux d'expérience viendront renforcer le matériel pédagogique pour vous permettre d'appliquer immédiatement vos acquis. Les exercices les plus simples incluent des astuces fonctionnelles tandis que les options avancées offrent un défi plus important pour les stagiaires qui connaissent déjà le contenu du cours ou qui l'ont rapidement maîtrisé.

« Pour défendre un réseau, il faut comprendre comment il fonctionne. Ce cours est aussi agréable qu'exigeant. »
- Holly C,
MOD UK

Public visé :

- Analystes en détection d'intrusion (tous niveaux), système et sécurité
- Ingénieurs/administrateurs réseau
- Responsables sécurité opérationnelle

Vous apprendrez à...

- Configurer et exécuter l'IDS open source Snort et écrire des signatures Snort
- Configurer et exécuter l'IDS open source Bro pour fournir un cadre d'analyse de trafic hybride
- Comprendre les composants des couches TCP/IP pour identifier le trafic normal et anormal
- Utiliser les outils d'analyse de trafic open source pour identifier les signes d'une intrusion
- Comprendre la nécessité de faire appel à l'inforensique réseau pour enquêter sur le trafic, identifier et enquêter sur une possible intrusion
- Utiliser Wireshark pour exclure des pièces jointes suspectes
- Écrire des filtres tcpdump pour examiner de manière sélective un caractère particulier du trafic
- Créer des paquets avec Scapy
- Utiliser l'outil open source de flux de réseau SiLK pour trouver des anomalies de comportement sur le réseau
- Utiliser votre connaissance de l'architecture et du matériel réseau pour personnaliser l'emplacement des capteurs IDS et analyser le trafic réseau

CERT. GIAC : GCIA
46 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCIA

SEC 504

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Hacker Tools, Techniques, Exploits, and Incident Handling

Internet regorge d'outils de piratage puissants et de personnes malintentionnées prêtes à s'en servir. Si votre organisation est connectée à internet et qu'un ou deux employés sont mécontents (et il y en a toujours), votre système informatique finira par être attaqué. Les hackeurs qui s'en prennent à vos systèmes ne manquent ni d'astuce ni de discrétion : sondes quotidiennes par cinq, dix voire cent contre votre infrastructure informatique ou personne malveillante en interne qui avance lentement, mais sûrement dans vos actifs informationnels vitaux n'en sont que quelques exemples. En tant que défenseurs, il est indispensable de bien nous familiariser avec ces outils et techniques de piratage.

Ce cours vous permettra de retourner la situation contre les attaquants en vous aidant à comprendre leurs tactiques et leurs stratégies. Vous apprendrez par la pratique à découvrir des points de vulnérabilité et des intrusions, et vous développerez un plan complet de gestion des incidents. Vous aborderez les vecteurs d'attaque les plus récents et les plus insidieux, les « bonnes vieilles attaques » qui marchent toujours et toutes les autres formes de piratage entre les deux. Plutôt que d'enseigner simplement quelques astuces d'attaquant, ce cours apporte un processus éprouvé et pas à pas de réponse aux incidents informatiques. Il fournit également une description détaillée des méthodes des hackeurs pour affaiblir un système, afin de vous y préparer ou, le cas échéant, de les détecter et de réagir. Vous explorerez en outre l'aspect légal de la réponse aux attaques informatiques, avec entre autres la surveillance des employés, la collaboration avec les forces de l'ordre et la gestion des preuves. Pour finir, vous participerez à des ateliers pratiques sur l'analyse, l'exploitation et la défense des systèmes. Ce cours vous permettra de découvrir les failles dans votre système avant vos adversaires !

Il conviendra tout particulièrement aux responsables ou aux membres d'une équipe de gestion des incidents. Les professionnels de la sécurité générale, les administrateurs système et les architectes sécurité y gagneront des connaissances approfondies de la conception, de l'élaboration et du fonctionnement de leurs systèmes afin de prévenir, détecter et répondre aux attaques.

« Formation structurée et bien préparée. Intéressant et passionnant pour les novices comme pour les professionnels chevronnés. »
- Ewa Konkolska
PRUDENTIAL

Public visé :

- Chargés de réponse aux incidents
- Chef d'équipe de gestion des incidents
- Administrateurs système en première ligne pour défendre leurs systèmes et répondre aux attaques
- Tout autre personnel de sécurité intervenant en premier lieu en cas d'attaque d'un système

Vous apprendrez à...

- Appliquer des procédures exhaustives de gestion des incidents (de la préparation à la récupération en passant par l'identification, le confinement et l'éradication) pour protéger les environnements d'entreprise
- Analyser la structure des techniques d'attaque courantes pour évaluer l'emprise de l'attaquant sur un système ou réseau, anticiper et éviter d'autres attaques
- Utiliser des outils et des indices pour déterminer le type de malware utilisé dans une attaque (rootkits, portes dérobées, chevaux de Troie) et choisir selon le cas les modes de défense et les tactiques de réponse appropriés
- Utiliser des outils en ligne de commande intégrés (tasklist, wmic et reg pour Windows, ainsi que netstat, ps et lsof pour Linux) pour détecter la présence d'un assaillant sur une machine
- Analyser les tables ARP du routeur et du système ainsi que les tables CAM des commutateurs pour suivre les activités d'un assaillant sur un réseau et identifier un suspect
- Utiliser des fichiers de vidage mémoire et l'outil Volatility pour identifier les activités d'un assaillant sur une machine, le malware installé et les autres machines utilisées pour rebondir à travers le réseau

CERT. GIAC : GCIH
38 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCIH

SEC 505

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Securing Windows and PowerShell Automation

NOUVEAU

- Créer des scripts PowerShell pour l'automatisation de la sécurité Windows et Active Directory
- Exécuter en toute sécurité les scripts PowerShell sur des milliers d'hôtes sur le réseau
- Se défendre contre les malwares PowerShell, tels que les ransomwares
- Renforcer Windows Server et Windows 10 contre les attaquants accomplis.

Nous utiliserons notamment PowerShell pour sécuriser Windows contre un grand nombre d'attaques décrites dans le framework MITRE ATT&CK, telles que vol d'informations d'identification d'administration, ransomware, déplacement latéral des pirates dans le LAN, protocoles Windows peu sécurisés comme Remote Desktop Protocol (RDP) et Server Message Block (SMB).

À la fin de ce cours, vous saurez écrire des scripts PowerShell personnalisés pour sécuriser votre environnement Windows. On trouve facilement des checklists de sécurité Windows, mais pas comment automatiser ces modifications sur des milliers de machines. Comment exécuter des scripts en toute sécurité sur plusieurs postes distants ? Ce cours traite non seulement de la sécurité Windows et Active Directory, mais aussi de la gestion de la sécurité avec PowerShell.

IL NE SUFFIT PAS DE CONNAÎTRE LA SYNTAXE POWERSHELL, IL FAUT SAVOIR UTILISER POWERSHELL COMME UN MULTIPLICATEUR DE FORCE POUR LA SÉCURITÉ WINDOWS

Voulez-vous connaître une autre raison du succès de PowerShell ? Il est tout simplement ludique ! Vous allez être surpris par le nombre de tâches que vous pouvez réaliser en peu de temps avec PowerShell. C'est bien plus qu'un langage de script, et nul besoin d'être un maître du codage pour démarrer.

Maîtriser PowerShell s'avère également utile à un autre type de sécurité : la sécurité de l'emploi. Les informaticiens qui maîtrisent ces compétences sont activement recherchés. Nul besoin d'avoir des connaissances en PowerShell pour suivre ce cours : nous verrons tout cela dans les labos.

Bien sûr, vous pouvez vous former tout seul sur YouTube, mais le cours SEC505 va au-delà de la syntaxe élémentaire. Vous y apprendrez à utiliser PowerShell comme plateforme de gestion de la sécurité, comme « multiplicateur de force » pour la *Blue Team*, et comme accélérateur pour votre carrière en informatique Windows.

NOUS ALLONS ÉCRIRE UN SCRIPT DE RANSOMWARE POWERSHELL ET NOUS EN PROTÉGER

Malheureusement, pirates et auteurs de logiciels malveillants se sont emparés de la puissance de PowerShell. Le dernier jour du cours, nous créerons un script de ransomware pour apprendre à nous défendre de ce type de scripts.

« J'ai suivi d'autres formations Windows, mais aucune n'était axée sur la sécurité. C'était une véritable révélation. J'espère participer à d'autres événements de ce type à l'avenir. »

- Dewayne Wasson, *KELLOGG COMPANY*

Public visé :

- Ingénieurs SecOps
- Administrateurs de points de terminaison et de serveurs Windows
- Toute personne souhaitant apprendre l'automatisation PowerShell
- Toute personne chargée de l'implémentation des 10 principales stratégies d'atténuation de la NSA
- Toute personne chargée de l'implémentation des contrôles de sécurité critiques du CIS
- Personnes chargées de déployer ou de gérer une PKI ou des cartes à puce
- Toute personne cherchant à réduire le nombre d'infections dues à des malwares

Vous apprendrez à...

- Créer des scripts PowerShell pour automatiser la sécurité
- Exécuter des scripts PowerShell sur des systèmes distants
- Renforcer PowerShell contre les abus et activer l'enregistrement de la transcription pour votre SIEM
- Accéder au service WMI via PowerShell pour l'exécution de commandes distantes, la recherche de journaux d'événements, la reconnaissance, etc.
- Utiliser Group Policy et PowerShell pour accorder des privilèges d'administration de manière à réduire les dommages en cas d'attaque réussie (principe assumé de brèche)
- Bloquer le déplacement latéral des pirates et les ransomwares au moyen de Pare-feu Windows, d'IPsec, des puits (*sinkholes*) DNS, des protections d'informations d'identification d'administration, etc.
- Empêcher l'exploitation en utilisant AppLocker et d'autres techniques de renforcement de l'OS Windows de façon évolutive avec PowerShell
- Configurer PowerShell à distance pour utiliser les règles JEA (Just Enough Admin) afin de créer une version Windows de Linux sudo et setuid root

CERT. GIAC : GCWN
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCWN

SEC 511

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Continuous Monitoring and Security Operations

Nous sous-estimons en permanence la ténacité de nos adversaires ! Les organisations investissent grandement en temps, en argent et en ressources humaines pour combattre les cybermenaces et prévenir les cyberattaques. En dépit de tous leurs efforts, certaines subiront des brèches et des intrusions. L'approche traditionnelle de l'architecture de sécurité, axée sur le périmètre de sécurité et la prévention, ne suffit en effet pas toujours à prévenir ces attaques. Aucun réseau n'est impénétrable. Cette réalité, les responsables et professionnels de la sécurité doivent l'accepter. La prévention est cruciale, mais nous ne devons pas en faire notre seule et unique stratégie de défense. Il est aujourd'hui nécessaire d'adopter une approche proactive de la sécurité pour permettre aux organisations de détecter les menaces qui passeront tôt ou tard à travers les mailles du filet.

Quant aux organisations victimes d'une attaque, elles sont confrontées en filigrane à un autre défi : la détection des incidents en temps opportun. Les données disponibles suggèrent que la plupart des brèches de sécurité passent inaperçues pendant sept mois en moyenne. Pour la majorité des organisations, les intrus n'ont pas besoin de développer une stratégie allant au-delà de la simple intrusion, car ils savent que le manque de visibilité et les contrôles de sécurité en interne ne représentent pas de danger. Une fois à l'intérieur, ils peuvent tranquillement et méthodiquement mener à bien leur mission.

Ce cours aborde l'architecture de sécurité défendable, la supervision de sécurité réseau (NSM), les diagnostics et atténuations en continu (CDM) et la supervision continue de la sécurité (CSM). Ces notions permettront à votre organisation ou à votre centre des opérations de sécurité (SOC) d'analyser les menaces et de détecter les anomalies suggérant un comportement cybercriminel. Grâce à cette nouvelle approche proactive, vous serez en mesure de détecter une intrusion de manière précoce, voire de contrecarrer les attaques. L'agence gouvernementale américaine de normalisation NIST (National Institute of Standards and Technology) a développé des directives, formalisées dans le document NIST SP 800-137, pour la supervision continue. Notre cours vous permettra d'approfondir votre compréhension et vos compétences dans ce domaine en utilisant le référentiel du NIST.

SEC511 vous ouvrira virtuellement de nouveaux horizons. Nous commencerons par explorer une architecture de sécurité traditionnelle pour en déterminer l'état courant et les attaques qu'elle subit. Nous aborderons ensuite la conception moderne de la sécurité, qui constitue une approche nouvelle et proactive d'une telle architecture, facilement compréhensible et défendable. Nous passerons ensuite à la construction effective du réseau et de la sécurité des terminaux avant d'évoluer dans les courants de l'automatisation et des NSM/CDM/CSM. Pour détecter de potentielles intrusions en temps opportun, le réseau et les systèmes doivent être supervisés en continu et de façon proactive. Le moindre changement dans la sécurité est en effet susceptible d'augmenter les chances de réussite d'une attaque.

Une épreuve finale vous attend pour parachever le cours SEC511 ! Le sixième et dernier jour, vous participerez à une compétition de capture du drapeau (CTF) qui vous demandera d'appliquer les compétences et les techniques que vous avez acquises. Vous serez mis au défi de détecter et de défendre l'architecture moderne de sécurité qui aura été élaborée au cours de cette formation. Les concepteurs de ce cours, Eric Conrad et Seth Misenar, ont voulu cette compétition amusante, attrayante, complète et stimulante. Vous ne serez pas déçu !

Public visé :

- Architectes sécurité
- Ingénieurs sécurité séniors
- Responsables sécurité technique
- Responsables, ingénieurs et analystes SOC
- Analystes défense réseau CND
- Toute personne impliquée dans la mise en œuvre des diagnostics et atténuations en continu (CDM), de la supervision continue de la sécurité (CSM) ou de la supervision de sécurité réseau (NSM)

Vous apprendrez à...

- Analyser une architecture de sécurité pour mettre au jour les failles
- Appliquer les principes appris en cours pour concevoir une architecture de sécurité défendable
- Comprendre l'importance d'une architecture de sécurité axée sur la détection et les centres des opérations de sécurité (SOC)
- Identifier les composants clés de la supervision de sécurité réseau (NSM)/des diagnostics et atténuations en continu (CDM)/de la supervision en continu (CM)
- Déterminer les besoins précis en supervision de sécurité pour des organisations de toutes tailles
- Appliquer une supervision NSM/CSM robuste
- Utiliser les outils pour mettre en œuvre la supervision continue conformément aux directives NIST SP800-137
- Déterminer les capacités de supervision requises pour un environnement SOC
- Déterminer les capacités requises pour prendre en charge la supervision continue des principaux contrôles de sécurité critiques

CERT. GIAC : GMON
48 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GMON

SEC 530

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Defensible Security Architecture and Engineering

REMARQUE : La définition du terme « architecture » varie selon l'organisation ou la région du monde. Ce cours s'intéresse aux cas d'usage et aux applications techniques et stratégiques, notamment à la mise en œuvre et aux ajustements des différents composants de l'infrastructure et techniques de cyberdéfense. Ce cours ne s'adresse pas à vous si vous cherchez une formation axée exclusivement sur les cas d'usage et les solutions stratégiques.

SEC530: Defensible Security Architecture and Engineering vise à apporter aux stagiaires une approche globale et par couche de la sécurité. Pour être efficace, la sécurité doit atteindre un équilibre entre les capacités de détection, de prévention et de réponse aux incidents. Un tel équilibre passe par la mise en œuvre de contrôles sur le réseau, directement aux points d'extrémité, et dans les environnements cloud. Par des actions de placement, d'implémentation et d'ajustement stratégiques, les forces d'une solution viennent compléter les faiblesses d'une autre et réciproquement.

Dans cet esprit, le cours s'attache à combiner les concepts stratégiques d'implantation d'infrastructure et d'outils et s'intéresse à leur application technique. Nous discuterons des solutions, recenserons celles disponibles et nous intéresserons à leur bonne application. Mieux encore, nous évaluerons les différentes solutions, notamment leurs forces et faiblesses, et comment les combiner logiquement en couches successives dans le cadre d'une défense en profondeur.

En pleine mutation, le panorama des menaces impose de changer d'état d'esprit et de modifier la destination de nombreux appareils. Que deviennent dès lors les dispositifs classiques de défense du périmètre comme le pare-feu ? Quelles sont les ramifications de l'état d'esprit du « tout chiffrer » pour des appareils comme les systèmes de détection d'intrusion réseau ?

Dans ce cours, les stagiaires apprendront les fondamentaux de l'architecture sécurité défendable d'aujourd'hui et de sa conception. L'accent sera en particulier mis sur la valorisation de l'infrastructure actuelle (et des investissements), notamment les commutateurs, routeurs et pare-feu. Les stagiaires apprendront à reconfigurer ces appareils pour renforcer considérablement les capacités préventives de leur organisation dans l'environnement de menaces actuel en pleine mutation. Le cours explorera aussi les dernières technologies et leurs capacités, leurs forces et leurs faiblesses. Vous en retirerez des recommandations et des suggestions précieuses pour élaborer une infrastructure de sécurité robuste.

Ce cours ne traite pas de supervision. En revanche, ses enseignements combinés à la supervision continue de la sécurité serviront à mettre en œuvre une architecture de sécurité au rôle non plus simplement préventif, mais aussi capable de transmettre les logs critiques au système de gestion des informations et des événements de sécurité (SIEM) du Centre des opérations de sécurité.

De nombreux exercices pratiques en laboratoire renforceront l'acquisition des points clés du cours et développeront les compétences opérationnelles des stagiaires qui seront en mesure de les exploiter dès leur retour au bureau.

CERT. GIAC : GDSA
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GDSA

Public visé :

- Architectes sécurité
- Ingénieurs réseau
- Architectes réseau
- Analystes sécurité
- Ingénieurs sécurité séniors
- Administrateurs système
- Responsables sécurité technique
- Analystes défense réseau CND
- Spécialistes en supervision de la sécurité
- Spécialistes en investigation numérique

Vous apprendrez à...

- Analyser une architecture de sécurité pour mettre au jour les failles
- Appliquer les principes appris en cours pour concevoir une architecture de sécurité défendable
- Déterminer les besoins précis en supervision de sécurité pour des organisations de toutes tailles
- Valoriser les investissements en architecture de sécurité en reconfigurant les ressources
- Déterminer les capacités requises pour prendre en charge la supervision continue des principaux contrôles de sécurité critiques
- Configurer la journalisation (log) et la supervision appropriées pour la prise en charge du Centre des opérations de sécurité et du programme de supervision continue

SEC 540

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

Cloud Security and DevOps Automation

SEC540 propose aux développeurs, aux opérationnels et aux professionnels de la sécurité une méthodologie pour concevoir et livrer des logiciels et infrastructures sécurisés à l'aide de DevOps et des services cloud. Les stagiaires explorent comment valoriser les principes, pratiques et outils DevOps pour renforcer la fiabilité, l'intégrité et la sécurité des applications sur site et cloud.

Axés sur les déploiements sur site, les deux premiers jours sont consacrés à la méthodologie DevOps et sa mise en œuvre au travers de leçons tirées de programmes de sécurité DevOps qui ont fait leurs preuves. Vous acquerrez une expérience pratique en utilisant des outils open source courants comme Puppet, Jenkins, GitLab, Vault, Grafana et Docker pour automatiser la gestion de la configuration (infrastructure programmable ou *Infrastructure as Code*), l'intégration continue (CI), la livraison continue (CD), la conteneurisation, la microsegmentation et la conformité automatisée (conformité inscrite dans le code ou *Compliance as Code*) et la supervision continue. Les exercices en laboratoire commencent par un projet CI/CD qui, de manière automatique, conçoit, teste et déploie des infrastructures et des applications. Les stagiaires s'appuient sur la chaîne d'outils Secure DevOps pour réaliser une série de labos de sécurisation de projets CI/CD avec des outils, protocoles et techniques de sécurité variés.

Une fois posées les fondations DevSecOps, les trois jours qui suivent abordent la migration des charges de travail DevOps vers le cloud, la construction d'infrastructures cloud sécurisées et la livraison de logiciels sécurisés. DEV540 procure une analyse approfondie de la chaîne d'outils d'AWS (Amazon Web Services) et aborde rapidement les services équivalents de Microsoft Azure. Grâce aux chaînes d'outils CI/CD, les stagiaires développent une infrastructure cloud capable d'héberger des applications et microservices conteneurisés. Suivent des exercices pratiques d'analyse et de correction des vulnérabilités des applications et de l'infrastructure cloud grâce à des services et outils de sécurité – passerelle API, gestion des identités et des accès (IAM), URL signées de CloudFront, service d'émission de jetons de sécurité (STS), service de gestion de clés (KMS), des services de pare-feu d'applications Web (WAF) gérés, des fonctions sans serveur, CloudFormation, AWS Security Benchmark et bien d'autres.

> **« SEC540 m'a amené à repenser les opérations et la sécurité comme jamais depuis SEC401: Security Essentials. »**
> - Todd Anderson
> *OBE*

Public visé :

- Quiconque travaille dans un environnement cloud public ou s'y prépare
- Quiconque travaille dans un environnement DevOps ou s'y prépare
- Quiconque cherche à savoir placer des contrôles, tests de sécurité et autres sur le cloud et sur des projets DevOps à livraison continue
- Quiconque souhaite apprendre à migrer des charges de travail DevOps vers le cloud, notamment vers AWS
- Quiconque souhaite savoir exploiter les services de sécurité applicative cloud proposés par AWS
- Développeurs
- Architectes logiciels
- Ingénieurs opérationnels
- Administrateurs système
- Analystes sécurité
- Ingénieurs sécurité
- Auditeurs
- Gestionnaires de risques
- Consultants en sécurité

Vous apprendrez à...

- Comprendre les principes et modèles fondamentaux qui sous-tendent DevOps
- Localiser les endroits où ajouter des contrôles de sécurité et autres dans la livraison continue et le développement continu
- Sécuriser les opérations de production
- Créer un plan de sécurisation ou d'amélioration de la sécurité dans un environnement DevOps
- Migrer vos workflows DevOps vers le cloud
- Utiliser les services cloud pour sécuriser les applications cloud
- Cartographier et mettre en œuvre un projet de déploiement/livraison continus

SEC 555

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

SIEM with Tactical Analytics

De nombreuses organisations disposent de capacités de journalisation sans pour autant avoir le personnel et les processus pour analyser les fichiers générés. Les systèmes de journalisation collectent de surcroît de grandes quantités de données auprès de sources diverses qu'il faut d'abord comprendre pour ensuite en analyser les données. Dans ce cours, les stagiaires sont formés aux méthodes et aux processus qui permettent d'améliorer les solutions de journalisation. Les informations de chaque entrée y sont expliquées (quand, quoi, pourquoi). Il s'agit ici d'un cours à forte dominante labo et qui fait appel à SOF-ELK, une solution gratuite de gestion des événements et des informations de sécurité (Security Incident and Events Management, SIEM) sponsorisée par SANS, afin d'apporter l'expérience pratique et la réflexion nécessaires aux analyses de données de grande ampleur.

Les opérations de sécurité d'aujourd'hui ne souffrent pas d'un problème de « volume », mais plutôt d'un problème « d'analyse des données ». Regardons les choses en face : il existe une multitude de méthodes de stockage et de traitement de grandes quantités de données qui ne s'intéressent pas à la compréhension des informations collectées. À cela, ajoutons qu'il existe un nombre infini de systèmes qui autorisent la collecte de journaux. Rien de plus facile, donc, que de se sentir perdu face à la saturation de données. Ce cours s'éloigne des systèmes d'enregistrement classiques et cherche à élaborer une collecte de données exploitables ainsi qu'à développer un Centre des opérations de sécurité (SOC) tactique.

Cette formation a été élaborée pour démystifier l'architecture SIEM et ses processus en amenant le stagiaire à concevoir et déployer un SIEM au sein d'un SOC. Le matériel pédagogique aborde de nombreuses bases dans le cadre d'une « utilisation appropriée » d'une plateforme SIEM afin d'enrichir les données enregistrées déjà disponibles dans les environnements d'entreprise et pour effectuer une collecte de données exploitables. Une fois la collecte effectuée, les stagiaires apprendront à présenter les informations dans des formats pratiques afin de dégager d'éventuelles corrélations. Ils parcourront les informations et les événements du journal pour en analyser les composants clés et en découvrir toute la richesse. Ils seront à même de mettre les données en corrélation, de mener des investigations sur la base des données agrégées et, pour finir, de valoriser ces nouvelles connaissances. Ils apprendront également à déployer des alertes internes post-exploitation et des leurres pour détecter habilement les intrusions sophistiquées. Les textes et les labos de ce cours leur apprendront non seulement à effectuer ces actions, mais aussi à automatiser nombre de processus qui pourront être ensuite déployés dès leur retour au bureau.

Le fil conducteur de cette formation est d'appliquer activement les techniques de supervision continue et d'analyse en utilisant des cyberattaques modernes. Les exercices en labo sont l'occasion d'analyser des données d'attaque capturées pour obtenir une idée concrète.

Le mot du concepteur du cours

« Les opérations de sécurité d'aujourd'hui ne souffrent pas d'un problème de "volume", mais plutôt d'un problème "d'analyse des données".Regardons les choses en face : il existe une multitude de méthodes de stockage et de traitement de grandes quantités de données qui ne s'intéressent pas à la compréhension des informations collectées. À cela, ajoutons qu'il existe un nombre infini de systèmes qui autorisent la collecte de journaux. Rien de plus facile, donc, que de se sentir perdu face à la saturation de données. Ce cours s'éloigne des systèmes d'enregistrement classiques et cherche à élaborer une collecte de données exploitables ainsi qu'à développer un Centre des opérations de sécurité (SOC) tactique. »

– Justin Henderson

Public visé :

- Analystes sécurité
- Architectes sécurité
- Ingénieurs sécurité séniors
- Responsables sécurité technique
- Analystes SOC
- Ingénieurs SOC
- Responsables SOC
- Analystes défense réseau CND
- Spécialistes en supervision de la sécurité
- Administrateurs système
- Spécialistes en investigation numérique
- Personnes travaillant à la mise en place d'une supervision continue de la sécurité
- Membres d'une équipe de *threat hunting*

Vous apprendrez à...

- Déployer la VM SANS SOF-ELK en environnement de production
- Expliquer pourquoi la plupart des SIEM sont à la traîne des solutions open source (telles queSOF-ELK)
- Mettre à niveau les stagiaires en matière d'utilisation, d'architecture et de pratiques SIEM
- Connaître les sources de données utiles pour la journalisation
- Déployer une solution de journalisation évolutive qui offre plusieurs méthodes de récupération des journaux
- Valoriser de simples journaux en données tactiques
- Développer des méthodes permettant de gérer des milliards de journaux issus de sources de données différentes
- Comprendre les bonnes pratiques liées à la collecte de journaux
- Exploiter des techniques de manipulation de journaux qui rivalisent avec les solutions SIEM
- Générer des graphes et des tableaux qui permettent de détecter les activités malveillantes et les anomalies
- Transformer les données en tableaux de bord actifs stratégiques pour les analystes

CERT. GIAC : GCDA
46 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCDA

SEC 566

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

Implementing and Auditing the Critical Security Controls – In-Depth

Les cyberattaques se multiplient et évoluent à une vitesse telle qu'il est de plus en plus difficile de s'en prémunir et de s'en protéger. Votre organisation dispose-t-elle d'un protocole efficace pour détecter, contrer et surveiller les menaces externes et internes afin de prévenir les brèches de sécurité ? Ce cours vous aide à maîtriser les techniques et outils spécifiques et éprouvés dont vous avez besoin pour mettre en œuvre et évaluer les contrôles de sécurité critiques (CSC) documentés par le Center for Internet Security (CIS).

La sécurité d'une organisation doit évoluer en même temps que les menaces. Pour que votre organisation soit à la page dans ce monde aux menaces changeantes, SANS a élaboré un cours complet qui enseigne aux stagiaires les contrôles de sécurité critiques, une approche de la sécurité axée sur les risques et la détermination des priorités. Conçus par des experts du privé et du public du monde entier, ces contrôles constituent la meilleure défense actuelle contre les attaques connues et permettent de limiter les dégâts en cas d'intrusion effective. Parmi les organismes à les avoir adoptés citons le ministère américain de la Sécurité intérieure, des gouvernements d'États fédérés, des universités et de nombreuses sociétés privées.

Ces contrôles sont en fait des directives spécifiques que les RSSI, les DSI, les IG, les administrateurs système et le personnel de sécurité des systèmes d'information peuvent utiliser pour gérer et mesurer l'efficacité de leurs défenses. Ils ont été conçus pour compléter les normes, cadres et programmes de conformité déjà existants en accordant la priorité aux menaces les plus graves et aux défenses les plus efficaces, tout en définissant une base commune d'actions contre les risques auxquels nous faisons face. Ces contrôles constituent un cadre de sécurité efficace dans la mesure où ils résultent de l'analyse d'attaques récentes, lancées périodiquement contre les réseaux. La priorité est accordée aux contrôles (1) qui atténuent les attaques connues, (2) qui répondent à une vaste gamme d'attaques et (3) qui identifient et arrêtent rapidement les attaquants dans le cycle de compromission. Le Centre de protection des infrastructures nationales (CPNI) du gouvernement britannique décrit ces contrôles comme « le référentiel des contrôles et des mesures de sécurité informatique à haute priorité ; une base qui peut être appliquée à l'échelle de l'organisation pour en améliorer la cyberdéfense ».

> **« Je débute dans ce domaine. Ce cours me permet d'acquérir des connaissances indispensables pour mon poste. »**
> - Wafa Al Raisi
> *CENTRAL BANK OF OMAN*

La formation pratique et approfondie de SANS vous apprendra à maîtriser les techniques et outils spécifiques dont vous avez besoin pour mettre en œuvre et évaluer les contrôles critiques. Ce cours aide les professionnels de la sécurité non seulement à comprendre comment parer à une menace, mais aussi la raison d'être de cette menace et comment s'assurer que les mesures de sécurité déployées aujourd'hui resteront efficaces contre les menaces de demain.

Il leur montre comment mettre en œuvre les contrôles dans un réseau grâce à une automatisation rentable. Pour les auditeurs, les DSI et les chargés de réponse aux risques, ce cours est le meilleur moyen de comprendre comment mesurer l'efficacité de la mise en œuvre de ces contrôles.

Public visé :

- Chargés d'audit de l'assurance de l'information
- Chargés de mise en œuvre ou administrateurs système
- Ingénieurs sécurité réseau
- Administrateurs IT
- Personnels et prestataires du ministère de la Défense
- Personnels et clients d'agences fédérales
- Organisations du secteur privé qui cherchent à améliorer leurs processus d'assurance de l'information et à sécuriser leurs systèmes
- Fournisseurs et consultants en sécurité qui cherchent à rester à jour en matière de cadres de travail pour l'assurance de l'information
- Stagiaires ayant suivi les cours SEC440, SEC401, SEC501, SANS Audit et MGT512

Vous apprendrez à...

- Appliquer un cadre de sécurité qui repose sur des menaces actuelles, qui est mesurable, évolutif et parfaitement capable de faire obstacle aux attaques connues et de protéger les informations et systèmes critiques des organisations
- Comprendre l'importance de chaque contrôle, la forme des compromissions en cas de négligence, et expliquer les objectifs défensifs qui donnent lieu à des victoires rapides et qui accroissent la visibilité des réseaux et systèmes
- Identifier et utiliser des outils qui permettent de mettre en œuvre ces contrôles de manière automatique
- Créer des outils de notation pour mesurer l'efficacité de chaque contrôle
- Utiliser des métriques spécifiques pour établir un référentiel et mesurer l'efficacité des contrôles
- Comprendre comment les contrôles s'alignent sur des normes (NIST 800-53, ISO 27002, norme australienne Top 35, etc.)
- Réaliser un audit de chaque contrôle avec des modèles, des checklists et des scripts, spécifiques et éprouvés, fournis pour faciliter le processus

CERT. GIAC : GCCC
30 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCCC

SEC 599

LIVE ONLINE | TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defences

Vous êtes recruté pour développer une capacité de cybersécurité dans notre nouvelle organisation virtuelle « SYNCTECHLABS ». C'est votre premier jour. Votre responsable vous confie : « Nous avons consulté des rapports sur les tendances cyber actuelles et nous ne nous y retrouvons pas. Menaces persistantes et avancées (APT), rançongiciel, déni de service... nous ne savons même pas par où commencer ! »

Les cybermenaces sont en plein essor : les attaques par rançongiciel touchent tout type d'entreprises sans distinction de taille, pendant que les adversaires étatiques tentent de s'ouvrir un accès à vos actifs les plus précieux. SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defences vous apporte les connaissances et l'expertise nécessaires pour venir à bout des menaces actuelles. Comme les stratégies préventives seules ne suffisent pas, nous présentons des contrôles de sécurité pour détecter et arrêter les adversaires et intervenir.

Les concepteurs du cours, Stephen Sims et Erik Van Buggenhout, certifiés GIAC Security Expert, sont des professionnels aguerris. Ils ont acquis une compréhension approfondie des cyberattaques et de leurs modes opératoires par les tests d'intrusion et la réponse aux incidents. Dans leurs cours sur les tests d'intrusion, une question revient : « Comment prévenir ou détecter ce type d'attaque ? ». Le cours SEC599, qui donne aux stagiaires des exemples réels de prévention d'attaques, est leur réponse : en plus de 20 labos, il consacre une journée entière à un exercice de défense du drapeau où les stagiaires défendent notre entreprise virtuelle contre plusieurs vagues d'attaques différentes ciblant son environnement.

Le parcours en six étapes débute avec l'analyse d'attaques récentes via des études de cas approfondies. Nous examinerons les différents types d'attaques et présenterons les descriptions formelles des comportements des adversaires d'après les modèles Cyber Kill Chain et MITRE ATT&CK. Afin de comprendre le fonctionnement des attaques, vous aurez à compromettre l'organisation virtuelle SyncTechLabs dès la première partie des exercices.

Au cours des parties deux à cinq, nous verrons la mise en œuvre efficace de contrôles de sécurité pour prévenir et détecter les cyberattaques et y répondre.

« Les méthodologies de ce cours sont incontournables dans notre secteur ! »
- Jayce Hill
ORACLE

Public visé :

- Architectes sécurité
- Ingénieurs sécurité
- Responsables sécurité technique
- Directeurs, ingénieurs et analystes des centres des opérations de sécurité
- Administrateurs IT
- Quiconque cherche à mieux comprendre le fonctionnement des attaques persistantes et avancées et les mesures à prendre dans l'environnement IT pour mieux prévenir, détecter et lutter contre les incidents

Vous apprendrez à...

- Comprendre le déroulement d'attaques récentes de haut niveau et les moyens de les arrêter
- Mettre en œuvre des contrôles de sécurité aux différentes phases des modèles Cyber Kill Chain et MITRE ATT&CK pour prévenir, détecter et lutter contre les attaques

CERT. GIAC : GDAT
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GDAT

NETWARS EXPERIENCE

Défis pratiques en sécurité de l'information

Vivez l'expérience **NetWars**

Jouez en solo ou dans une équipe de cinq personnes

> **NetWars est l'occasion de mettre en pratique les notions vues en cours. Fortement recommandé !**
> – **Kyle McDaniel**, Lenovo

Au choix :

- Core NetWars
- DFIR NetWars
- Cyber Defense NetWars
- ICS NetWars
- GRID NetWars

Développez vos compétences en :

- Cyberdéfense
- Tests d'intrusion
- Inforensique et réponse aux incidents
- Systèmes de contrôle industriel

Participation gratuite aux défis NetWars pour les stagiaires en formation de 4 jours ou plus.

Le soir, après le cours, NetWars est l'occasion d'appliquer immédiatement les connaissances acquises dans un environnement ludique, compétitif, pratique et pédagogique !

Inscrivez-vous à NetWars en même temps qu'au cours.

www.sans.org/netwars

SEC 460

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Enterprise Threat and Vulnerability Assessment

L'exploitation de failles informatiques est en plein essor. Face à des adversaires aux techniques avancées toujours plus nombreux, compétents et destructeurs, les organisations doivent apprendre à limiter plus efficacement les risques de sécurité informatique à l'échelle de l'entreprise. SEC460 est le premier cours axé sur l'acquisition de compétences et de techniques d'évaluation technique des points de vulnérabilité. Il propose en outre des approches pratiques éprouvées pour en tirer parti à tous les niveaux de l'entreprise. Ce cours traite de la gestion des menaces, introduit les composants fondamentaux de l'évaluation globale des points de vulnérabilité et fournit les instructions pratiques nécessaires à l'élaboration d'une stratégie défensive efficace dès le premier jour. Il vise à former le personnel de cybersécurité chargé de sécuriser efficacement 10 000 systèmes ou plus dans leurs organisations.

Après une introduction aux fondamentaux de l'évaluation des points de vulnérabilité en matière de sécurité informatique, SEC460 examine en profondeur le référentiel d'évaluation des vulnérabilités. La suite du cours porte sur les composants structurels d'un programme dynamique et itératif de sécurité informatique. À travers une analyse pratique et détaillée des renseignements disponibles sur les menaces, la modélisation et l'automatisation, les stagiaires apprendront les compétences nécessaires non seulement pour utiliser les outils, mais aussi pour mettre en place un programme d'évaluation transformationnel des points de vulnérabilité.

SEC460 vous apprendra à vous servir des outils de sécurité utilisés par les professionnels sur le terrain pour évaluer, gérer et limiter les points de vulnérabilité. Seul cours à présenter une méthodologie globale d'évaluation des points de vulnérabilité, il met aussi l'accent sur les défis des grandes entreprises. Vous apprendrez sur une gamme complète de machines cibles représentatives d'un environnement d'entreprise, avec des outils utilisables en production et selon une méthodologie de test éprouvée.

Plus qu'une simple liste de contrôle, ce cours vous fera découvrir le point de vue des attaquants, une démarche indispensable pour mettre au jour la cible de la prochaine attaque. Un opérateur ne se résume pas à son outil. SEC460 met l'accent sur cette approche centrée sur l'humain : le cours examine les lacunes de nombreux programmes d'évaluation des points de vulnérabilité afin de vous transmettre les tactiques et les techniques nécessaires pour sécuriser les réseaux contre toutes les attaques, même les plus avancées.

Nous terminons les cinq premiers jours de formation par une discussion sur le triage, la remédiation et la restitution, puis, le dernier jour, vos compétences sont mises à l'épreuve dans une simulation cyber de type entreprise aux nombreux systèmes cibles qu'il vous faudra analyser et explorer. La simulation cyber range est constituée d'un vaste environnement de serveurs, d'utilisateurs finaux et d'appareils réseau représentatifs de nombreux systèmes et topologies d'entreprise. Les compétences d'évaluation des vulnérabilités acquises dans le cadre d'une approche de bout en bout seront d'autant plus précieuses dans les organisations de moyenne et grande taille.

> **« La gestion de la vulnérabilité est essentielle dans toute stratégie de cybersécurité, ce cours est simplement indispensable. »**
> - Simphiwe Khulu
> *MTN*

Public visé :

- Auditeurs techniques (vulnérabilité)
- Administrateurs système
- Auditeurs sécurité
- Agents de conformité
- Experts en tests d'intrusion
- Responsables du programme sur les vulnérabilités
- Analystes sécurité
- Architectes sécurité
- Ingénieurs sécurité séniors
- Responsables sécurité technique

Vous apprendrez à...

- Réaliser des évaluations de bout en bout des points de vulnérabilité
- Développer des plans sur mesure de découverte, de gestion et de remédiation des vulnérabilités
- Collecter et analyser le renseignement d'intérêt cyber afin de créer un plan de cybersécurité sur mesure qui intègre différentes structures de modélisation des vulnérabilités et des attaques
- Implémenter une méthodologie de test éprouvée en utilisant les tactiques et techniques les plus modernes
- Adapter les approches cybersécurité pour répondre aux enjeux réels des entreprises
- Configurer et gérer des outils d'évaluation des vulnérabilités pour limiter les risques que le testeur ajoute à l'environnement

36 CRÉDITS CPE/CMU

SEC 542

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Web App Penetration Testing and Ethical Hacking

Les applications web jouent un rôle vital pour toutes les organisations modernes. Cela étant, si votre organisation ne procède pas à des tests appropriés et ne sécurise pas ses applications web, des personnes malveillantes peuvent en profiter pour les compromettre, porter atteinte à vos activités et même voler vos données. Il est malheureux de constater que de nombreuses organisations confient à tort l'intégralité de la détection des failles à des scanneurs de sécurité.

Le cours SEC542 aide les stagiaires à dépasser le stade du scanneur lambda pour acquérir une méthodologie de tests d'intrusion professionnelle, à haute valeur ajoutée.

Les clients attendent des applications web qu'elles fournissent des fonctionnalités significatives et un accès aux données. Au-delà même de l'importance des applications web orientées clients, les applications web en interne constituent la majorité des outils d'entreprise et occupent une place grandissante. Il n'existe malheureusement pas de « jour de patch » pour les applications web personnalisées, et des études montrent que les failles logiques sur ces applications jouent un rôle majeur dans les brèches de sécurité et les intrusions. Les attaquants concentrent de plus en plus leurs efforts sur ces cibles de grande valeur, soit en abusant directement des applications orientées public soit en visant certaines applications web une fois à l'intérieur des systèmes.

La cyberdéfense moderne nécessite une compréhension réaliste et approfondie des problèmes de sécurité liés aux applications web. N'importe qui peut faire un peu de piratage, mais un test d'intrusion appliqué aux applications web demande plus de connaissances.

Le cours SEC542 permet aux stagiaires de déterminer l'état de sécurité d'une application web et de faire la démonstration convaincante de l'impact d'une sécurité inadéquate, véritable fléau à l'heure actuelle.

Les stagiaires analyseront en profondeur la majorité des faiblesses des applications web et leur exploitation. Plus important, ils apprendront des processus éprouvés et répétables pour détecter systématiquement ces faiblesses et remonter les résultats à la hiérarchie.

Même les surdoués de la sécurité ont régulièrement du mal à faire comprendre à leur organisation les risques encourus. Dans les faits, l'art du test d'intrusion relève moins de la capacité à découvrir comment l'adversaire va s'introduire dans un système et davantage de la faculté à faire comprendre l'ampleur des risques et convaincre son employeur de déployer des contre-mesures appropriées. L'objectif du cours SEC542 n'est pas de faire de vous un pirate de salon, mais de vous armer pour mieux sécuriser les organisations au moyen de tests d'intrusion. Ce cours vous apprendra à démontrer l'impact véritable que peuvent avoir les faiblesses d'une application web.

En plus de son contenu de grande qualité, SEC542 met particulièrement l'accent sur des labos pratiques pour que les stagiaires soient en mesure d'appliquer rapidement ce qu'ils ont appris.

Cette formation compte plus de 30 labos pratiques et se termine en beauté par un tournoi de tests d'intrusion sur application web mené dans le cadre de SANS NetWars Cyber Range. Cette compétition finale de capture du drapeau (CTF) amène les stagiaires à travailler en équipe et leur demande d'appliquer les techniques de test d'intrusion sur application web qu'ils viennent d'acquérir. L'événement se déroule dans une atmosphère ludique qui renforce l'apprentissage.

Public visé :

- Professionnels de la sécurité en général
- Experts en tests d'intrusion
- Hackeurs éthiques
- Développeurs d'applications web
- Concepteurs et architectes de sites web

Vous apprendrez à...

- Appliquer une méthodologie détaillée en quatre phases à vos tests d'intrusion pour applications web :reconnaissance, cartographie, recherche et exploitation
- Analyser les résultats des outils d'automatisation des tests web pour éliminer les faux positifs, valider les résultats et déterminer leur impact sur l'activité
- Rechercher les principales failles dans les applications web
- Utiliser Python pour créer des scripts de test et d'exploitation lors d'un test d'intrusion
- Rechercher et exploiter les failles par injection SQL pour déterminer les risques encourus
- Créer des configurations et tester des charges dans d'autres attaques web
- Tester de façon aléatoire les entrées potentielles pour détecter les attaques par injection
- Expliquer l'impact opérationnel des failles logiques sur les applications web
- Analyser le trafic entre le client et le serveur d'applications à l'aide d'outils tels que Zed Attack Proxy et Burp Suite pour identifier des problèmes dans le code côté client
- Rechercher et exploiter des attaques Cross-Site Request Forgery (CSRF)
- Utiliser BeEF (Browser Exploitation Framework) pour harponner le navigateur des victimes, attaquer le logiciel client et le réseau, et évaluer l'impact potentiel des failles XSS dans une application
- Effectuer un test d'intrusion de web complet à l'occasion de l'exercice CTF (capture du drapeau) pour utiliser l'ensemble des techniques et des outils et les tester de façon exhaustive

CERT. GIAC : GCIH
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GWAPT

SEC 560

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Network Penetration Testing and Ethical Hacking

En tant que professionnel de la cybersécurité, votre responsabilité est de trouver et de comprendre les vulnérabilités de votre organisation, et de tout faire pour limiter leur importance avant que des personnes malveillantes ne s'en servent. Êtes-vous prêt ? SANS SEC560 est notre cours de test d'intrusion par excellence : le suivre, c'est se préparer parfaitement à la tâche.

SEC560 est un cours indispensable pour tous les professionnels accomplis de la sécurité.

Cette formation couvre de manière exhaustive les outils, techniques et méthodologies du test d'intrusion réseau pour vous préparer parfaitement à mener pas à pas et de bout en bout des projets de tests délicats. Toutes les organisations ont besoin d'un personnel compétent en cybersécurité, capable de trouver les vulnérabilités et d'en limiter les effets. Ce cours a été entièrement conçu en ce sens, pour vous préparer à remplir ce rôle. Vous commencerez par élaborer une planification appropriée avec exploration et reconnaissance du système, puis vous effectuerez des analyses approfondies et des exploitations de cibles, suivies d'attaques de mot de passe et de manipulations d'applications web, le tout au travers de plus de 30 labos pratiques et détaillés. Ce cours vous transmettra un large volume de conseils pratiques et concrets directement issus de l'expérience des plus grands professionnels des tests d'intrusion afin de vous aider à faire votre travail en toute sécurité, avec efficacité… et d'une main de maître.

Découvrez les meilleures méthodes pour tester vos propres systèmes avant que des personnes malintentionnées ne vous attaquent.

Vous apprendrez à effectuer une reconnaissance détaillée en étudiant l'infrastructure d'une cible via l'analyse du contenu des infrastructures internet et intranet (blogs, moteurs de recherche, sites de réseaux sociaux, etc.). Nos labos pratiques vous enseigneront à analyser des réseaux cibles en utilisant les meilleurs outils disponibles. Outre les configurations et options classiques, nous étudierons des possibilités moins connues, mais particulièrement utiles, que les meilleurs outils de test d'intrusion proposent.

Après l'analyse, vous apprendrez des dizaines de méthodes d'exploitation de systèmes cibles afin d'évaluer les véritables risques associés aux failles que vous avez détectées. Vous approfondirez la post-exploitation, les attaques de mot de passe et les applications web, et vous ferez le tour de l'environnement cible pour modéliser des attaques que l'on retrouve dans le monde réel afin de mettre en lumière l'importance d'une défense en profondeur.

Vous repartirez avec des connaissances complètes en test d'intrusion et un savoir-faire important en piratage éthique.

Le cours SEC560 a été conçu pour vous préparer à mener des tests d'intrusion à haute valeur ajoutée et à grande échelle. Et c'est précisément ce que vous expérimenterez le dernier jour de la formation. Vous passerez les cinq premiers jours à développer vos compétences grâce à des labos complets et stimulants avant d'attaquer le point culminant de la formation : un scénario concret de test d'intrusion d'une journée complète. Vous mènerez un test d'intrusion de bout en bout en appliquant les connaissances, les outils et les principes abordés tout au long des cours, et ce afin de découvrir et d'exploiter les vulnérabilités d'une organisation factice, mais réaliste. L'idéal pour faire la démonstration de votre maîtrise nouvelle.

CERT. GIAC : GPEN
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GPEN

Public visé :

- Personnel de sécurité qui ont la tâche d'évaluer les réseaux et les systèmes pour trouver et corriger les vulnérabilités
- Experts en tests d'intrusion
- Hackeurs éthiques
- Défenseurs soucieux de mieux comprendre les méthodologies, outils et techniques offensifs
- Auditeurs ayant besoin d'approfondir leurs compétences techniques
- Membres d'une *Red Team* ou d'une *Blue Team*
- Spécialistes inforensiques soucieux de mieux comprendre les tactiques offensives

Vous apprendrez à…

- Développer un champ d'application et des règles d'engagement sur mesure pour des projets de tests d'intrusion afin d'assurer que le travail est correctement ciblé, défini et mené de façon sécurisée
- Effectuer une reconnaissance détaillée en utilisant les métadonnées du document, les moteurs de recherche, et d'autres sources d'information accessibles au public pour acquérir une compréhension technique et organisationnelle de l'environnement cible
- Utiliser Nmap pour effectuer des scans complets de réseau, analyser des ports, relever l'empreinte du système d'exploitation et détecter les versions afin de développer une carte des environnements cible
- Choisir et exécuter les scripts du moteur de script de Nmap pour extraire des informations détaillées des systèmes cibles
- Configurer et lancer le scanneur de vulnérabilités Nessus de façon sécurisée pour découvrir les vulnérabilités, à la fois avec des scans authentifiés et non authentifiés, et personnaliser les résultats pour établir une représentation du risque économique que court l'organisation

SEC 562

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

CyberCity Hands-on Kinetic Cyber Range Exercise

Les ordinateurs, les réseaux et les automates programmables industriels font fonctionner la majeure partie de l'infrastructure physique du monde moderne, depuis les réseaux électriques, les réseaux de distribution d'eau et les systèmes de transport jusqu'aux systèmes de ventilation-climatisation et aux automates industriels. Les professionnels de la sécurité ont chaque jour davantage besoin des compétences pour évaluer et défendre ces infrastructures importantes. Dans ce cours innovant et à la pointe de la technologie issue de la séquence SANS CyberCity Kinetic Range, vous apprendrez à analyser et évaluer la sécurité des systèmes de contrôle et des infrastructures afférentes, et à trouver les vulnérabilités susceptibles d'entraîner des effets cinétiques considérables.

Dans le cours SEC562, vous apprendrez à :

- Analyser les cyberinfrastructures qui contrôlent et impactent les infrastructures cinétiques
- Manipuler différents grands protocoles industriels notamment Modbus, CIP, DNP3, Profinet et d'autres protocoles SCADA
- Réaliser rapidement des prototypes d'outils d'attaque informatique contre un type de vulnérabilité
- Mettre au jour des failles de sécurité dans différents systèmes SCADA et de contrôle industriel (ICS), et contrecarrer les attaques qui les visent
- Mener des tests d'intrusion et des audits de sécurité associés aux infrastructures cinétiques

Un mot des concepteurs

« Le monde fait face à une pénurie critique de profils compétents pour défendre les systèmes informatiques et les infrastructures réseau qui contrôlent notre monde physique. Pour combler ce déficit, notre cours enseigne aux cyberguerriers à analyser, contrôler et défendre un nombre incalculable de systèmes de contrôle, de protocoles et d'autres infrastructures cinétiques auxquels ils seront de plus en plus confrontés à l'avenir. Il regorge de compétences pratiques que les professionnels de la sécurité pourront utiliser dans leur mission. En outre, l'écran dans la salle montre en temps réel aux stagiaires les conséquences de leurs travaux pratiques sur la ville. Par exemple, quand vous restaurez le réseau électrique, les lumières de la ville s'allument (et un journal publie immédiatement un article sur la fin de la panne). Presque chaque mission du cours donne à voir les conséquences, une source d'intérêt et de curiosité pour les stagiaires comme pour les formateurs. »

— Ed Skoudis, Josh Wright et Tim Medin

> **« Dans ce cours, l'avantage est qu'on met la main dans les systèmes de commande des équipements du secteur industriel comme les automates programmables industriels et SCADA. À ma connaissance, aucune autre formation ne s'intéresse à ce sujet émergent. »** — Phillip A. Smith

36 CRÉDITS CPE/CMU

Public visé :

- Membres de *Red Team* et de *Blue Team*
- Cyberguerriers
- Chargés de réponse aux incidents
- Experts en tests d'intrusion
- Hackeurs éthiques
- Tout autre personnel de sécurité intervenant en premier lieu en cas d'attaque d'un système

Vous apprendrez à…

- Rechercher et découvrir les informations associées aux actifs d'ICS, de réseaux et d'ordinateurs
- Analyser et manipuler les protocoles courants, très puissants, mais mal compris comme Profinet, DNP3, Modbus et d'autres
- Analyser en équipe les actions de l'attaquant et prévenir les conséquences cinétiques sur les systèmes de contrôle industriel
- Chercher les vulnérabilités dans les systèmes associés à la distribution d'électricité et d'eau, les systèmes de transport et d'autres infrastructures
- Utiliser différents outils pratiques à des fins d'analyse et d'interaction avec les systèmes cibles, notamment Wireshark, tcpdump, Nmap, Metasploit et bien d'autres
- Contrôler différents terminaux d'interface opérateur et interfaces homme-machine d'usage courant avec SCADA et d'autres systèmes de contrôle industriel (ICS)
- Empêcher les attaques de semer le chaos en prenant la main sur des ordinateurs de commande d'infrastructures physiques

SEC 573

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Automating Information Security with Python

Tous les professionnels de la sécurité (experts en tests d'intrusion, analystes en investigation numérique, défenseurs réseau, administrateurs sécurité, chargés de réponse aux incidents...) doivent faire face à un même problème : le CHANGEMENT. Les outils, les technologies et les menaces évoluent constamment. Avec Python, langage simple et convivial, vous pouvez rester en phase en concevant des outils personnalisés et des tâches automatisées. Vous êtes à même de gérer des menaces spécifiques et d'y répondre efficacement.

Que vous soyez novice ou codeur depuis des années, le cours SEC573:Automating Information Security with Python vous apprendra à créer des programmes pour simplifier vos tâches et gagner en efficacité. Ce cours s'adapte à votre rythme et reprend les bases en partant du principe que vous n'avez aucune connaissance ni expérience dans le domaine de la programmation. Nous abordons la totalité des fondamentaux de ce langage. Si vous les connaissez déjà, vous découvrirez que l'environnement labo pyWars permet aux développeurs avancés d'accélérer et de passer à du contenu plus approfondi.

La technologie, les menaces et les outils sont en perpétuelle évolution. Si nous n'évoluons pas avec eux, nous risquons de devenir inefficaces et inutiles, incapables de fournir la défense vitale dont nos organisations ont de plus en plus besoin. Le système d'exploitation que vous avez choisi dispose peut-être d'une nouvelle fonctionnalité qui crée des données forensiques prometteuses, mais encore vous faut-il les outils pour les exploiter. Et il arrive souvent que ces outils n'aient pas encore été développés. Vous pouvez essayer d'avancer sans chercher à en savoir plus... ou bien vous pouvez développer vous-même cet outil.

Prenons un autre exemple : un attaquant a pénétré votre réseau il y a plusieurs mois. Si des outils avaient été en mesure de détecter cette attaque, le problème ne se poserait pas. En attendant, des données sensibles vous échappent et le long processus de détection et d'éradication des attaques vampirise votre organisation, sans parler de ses ressources financières. Pourtant, si vous en êtes capable, la réponse est simple : il suffit de créer des outils qui automatisent vos défenses.

Si vous êtes expert en tests d'intrusion, vous devez évoluer à la même vitesse que les menaces que vous êtes censés émuler. Que faites-vous lorsque vos outils « génériques » et vos exploits ne suffisent pas ? Si vous êtes doué, vous développez un outil ou vous en personnalisez un pour adapter ses fonctionnalités à vos besoins.

Le cours SEC573 vise à vous apporter les compétences dont vous avez besoin pour ajuster, personnaliser et développer vos propres outils. Nous vous apprendrons à créer vos outils et vous donnerons les moyens d'automatiser la routine quotidienne d'un professionnel moderne de la cybersécurité, pour une valeur accrue et un gain de temps certain. Une fois de plus, n'oubliez pas que les organisations préoccupées par leur sécurité recherchent activement des collaborateurs compétents et capables de développer leurs outils. La demande concerne des professionnels capables de comprendre un problème et de développer rapidement un prototype de code en conséquence (défense ou attaque, peu importe). Inscrivez-vous à notre formation Python approfondie et devenez imbattable.

Public visé :

- Professionnels de la sécurité qui veulent apprendre à développer des applications Python
- Experts en tests d'intrusion qui veulent dépasser la simple utilisation d'outils de sécurité pour concevoir ou modifier ces outils
- Techniciens qui ont besoin d'outils personnalisés pour tester leur infrastructure et veulent les concevoir eux-mêmes

Vous apprendrez à...

- Développer un outil d'inforensique pour extraire des artefacts à partir de preuves lorsqu'il n'existe pas d'outil, ou utiliser des modules tiers pour des artefacts connus et des preuves cachées qui s'avèrent pertinents pour vos enquêtes
- Créer des outils défensifs pour automatiser l'analyse de fichiers journaux et de paquets réseau en utilisant des techniques de recherche de menaces ou *threat hunting* pour pister les attaquants sur votre réseau
- Mettre en place de manière personnalisée de listes blanches, de listes noires, de détection de signature, des analyses à traîne longue/courte et d'autres techniques d'analyse de données pour découvrir des attaques non détectées par les méthodes conventionnelles
- Créer des outils de tests d'intrusion, y compris plusieurs ***backdoors*** avec des fonctionnalités comme l'exécution de processus, les charges en téléchargements ascendant et descendant, l'analyse de port, etc.
- Développer des outils fondamentaux qui échappent aux antivirus et vous permettent de mettre un pied dans l'environnement cible

CERT. GIAC :GPYC
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GPYC

SEC 575

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Mobile Device Security and Ethical Hacking

Imaginez une surface d'attaque présente à l'échelle de votre organisation et entre les mains de tous les utilisateurs. Elle passe régulièrement d'un endroit à un autre, elle stocke des données extrêmement sensibles et stratégiques, et elle est dotée de nombreuses technologies sans fil, toutes mûres pour une attaque. Ce type de surface existe déjà : les appareils mobiles. Ils constituent la plus grande surface d'attaque pour la majorité des organisations. Et pourtant, ces dernières n'ont souvent pas les compétences nécessaires pour évaluer les risques concomitants.

LE COURS SEC575 COUVRE DÉSORMAIS ANDROID PIE et iOS 12

Le cours SEC575:Mobile Device Security and Ethical Hacking a été conçu pour vous permettre de développer les compétences dont vous avez besoin pour comprendre les forces et les faiblesses des appareils fonctionnant sous Apple iOS et Android. Les appareils mobiles ne sont plus seulement une technologie grand public ;il s'agit désormais d'un outil fondamental, que tout le monde ou presque a avec soi, et qui remplace souvent l'ordinateur traditionnel pour les besoins professionnels quotidiens en données. On constate cette tendance dans les entreprises, les hôpitaux, les banques, les écoles et les commerces partout dans le monde. Les utilisateurs se servent plus que jamais des appareils mobiles ; nous en sommes conscients et les personnes malintentionnées aussi. Le cours SEC575 fait le tour de ces appareils.

APPRENEZ À EFFECTUER UN TEST D'INTRUSION SUR LA PLUS GRANDE SURFACE D'ATTAQUE DE VOTRE ORGANISATION

Une fois doté des compétences acquises dans le cours SEC575, vous pourrez évaluer les faiblesses de sécurité des applications tierces et intégrées. Vous apprendrez à contourner le chiffrement d'une plateforme et à manipuler les applications pour outrepasser les techniques sécurité côté client. Vous exploiterez des outils permettant d'analyser les applications mobiles de manière automatique et manuelle pour identifier les anomalies dans le trafic réseau de l'application, dans son stockage système et dans les canaux de communication interapplications. Vous travaillerez en toute sécurité avec des échantillons de malwares mobiles pour comprendre l'exposition des données et les menaces d'accès qui pèsent sur les appareils Android et iOS, et vous contournerez l'écran de verrouillage pour exploiter des appareils perdus ou volés.

EXPLOREZ L'ÉVALUATION DES APPLICATIONS MOBILES, DES SYSTÈMES D'EXPLOITATION ET DES INFRASTRUCTURES ASSOCIÉES

Comprendre et identifier les vulnérabilités et les menaces qui entourent les appareils mobiles est une compétence très appréciable, mais qui perd sa valeur si vous n'arrivez pas à convaincre votre hiérarchie de prendre au sérieux les risques que vous avez détectés. Heureusement, il s'agit ici d'une compétence que vous apprendrez à maîtriser tout au long de la formation.Vous exploiterez des outils comme Mobile App Report Cards pour caractériser les menaces pour vos supérieurs et les décideurs tout en identifiant des codes et des bibliothèques d'échantillons que les développeurs pourront utiliser pour réduire les risques au niveau des applications en interne.

VOS APPAREILS MOBILES VONT SE FAIRE ATTAQUER... AIDEZ VOTRE ORGANISATION À SE PRÉPARER POUR L'ASSAUT !

Public visé :

- Experts en tests d'intrusion
- Hackeurs éthiques
- Auditeurs ayant besoin d'approfondir leurs compétences techniques
- Personnel de sécurité chargé d'évaluer, de déployer ou de sécuriser des téléphones et tablettes mobiles
- Administrateurs système et réseau qui gèrent les téléphones et tablettes mobiles

Vous apprendrez à...

- Utiliser des outils ***jailbreak*** pour Apple iOS et pour les systèmes Android
- Faire une analyse des données de fichiers de système iOS et Android pour exploiter les dispositifs compromis et en extraire des données sensibles relatives à l'utilisation du dispositif mobile
- Analyser les applications Apple iOS et Android avec des outils de rétro-ingénierie
- Modifier les fonctionnalités des applications iOS et Android afin de contourner la sécurité ***anti-jailbreak*** ou d'achat intégré
- Effectuer une évaluation automatisée de la sécurité des applications mobiles
- Utiliser des outils d'analyse de réseau sans fil pour identifier et exploiter les réseaux sans fil utilisés par les dispositifs mobiles
- Intercepter et manipuler les activités de réseau d'un dispositif mobile
- Tirer parti des infrastructures d'exploit spécifiques aux dispositifs mobiles pour obtenir un accès non autorisé aux dispositifs ciblés
- Manipuler le comportement des applications mobiles pour contourner les restrictions de sécurité

CERT. GIAC : GMOB
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GMOB

SEC 588

LIVE ONLINE | TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Cloud Penetration Testing

Depuis des années, on assiste à la migration vers le cloud des charges de travail liées au calcul. Selon les analystes, la plupart voire toutes les entreprises auront prochainement des charges de travail dans des environnements cloud publics ou autres. Certes, les nouvelles organisations qui privilégient l'environnement cloud peuvent évoluer vers une solution hybride alliant le cloud à un datacenter en local, mais le recours au cloud ne va pas drastiquement diminuer. Ainsi, pour déterminer les risques qui pèsent sur les organisations, nous devons nous préparer à évaluer la sécurité des services fournis en cloud. Dans ce cours, vous apprendrez les techniques d'intrusion les plus récentes ciblant le cloud dans la perspective d'évaluer ces environnements cloud.

Les questions les plus courantes sur la sécurité du cloud concernent la pertinence d'une formation aux tests d'intrusion spécifiquement appliqués au cloud et l'éventuelle portabilité des compétences en tests d'intrusion génériques dans le cloud. Dans les deux cas, la réponse est affirmative mais, pour en comprendre les raisons, nous devons expliciter l'importance des tests d'intrusion pensés pour le cloud. Dans les environnements des prestataires cloud, les experts en tests d'intrusion n'ont pas à faire à un design classique de datacenter. Pour clarifier, les postulats valables dans les environnements traditionnels, par exemple sur le propriétaire du système d'exploitation, celui de l'infrastructure et le mode d'exécution des applications, seront probablement très différents. Les applications, les services et les données seront stockés dans un environnement d'hébergement partagé vraisemblablement propre à chaque prestataire cloud.

En quoi l'environnement cloud natif est-il différent ? Selon la Cloud Native Computing Foundation (CNCF), mise en place pour accompagner le développement des applications cloud, aussi bien *cloud-first* que *cloud-native,* l'application et l'environnement seront formés de conteneurs, de maillages de services, de microservices, d'infrastructure immuable et d'API déclaratives.

Si certains éléments sont disponibles dans les autres environnements, dans le cloud, ils se décomposent encore en services mis à disposition par le prestataire cloud. Dans cet environnement, la complexité est bien illustrée dans l'architecture par microservices où l'on peut trouver une machine virtuelle, un conteneur et même une zone d'hébergement « sans serveur ». Ainsi, nous devons prendre en compte ce surcroît de complexité dans l'évaluation de l'environnement, rester dans le cadre légal, et apprendre des moyens nouveaux de mener des attaques pourtant classiques.

Le cours SEC588 s'intéresse à ces sujets ainsi qu'à d'autres, nouveaux et issus du cloud comme les microservices, les datastores en mémoire, les fichiers dans le cloud, les fonctionnalités sans serveur, les maillages Kubernetes et les conteneurs. Il couvre aussi spécifiquement les tests d'intrusion sur Azure et AWS, d'autant plus important que ces services cloud représentent à eux seuls plus de la moitié du marché. Il ne s'agit pas de faire la démonstration de ces technologies, mais de vous apprendre à évaluer et à communiquer le risque réel auquel l'entreprise devrait faire face en l'absence de sécurisation des services.

« Le cours SANS SEC588 m'a appris bien plus que ce que je pensais. SEC588 définit le cadre des tests d'intrusion cloud que l'essor des nouvelles technologies des prestataires cloud rendait nécessaire. »

- Jonus Gerrits

Public visé :

- Professionnels de la sécurité en attaque comme en défense pour acquérir une compréhension approfondie des vulnérabilités, des configurations peu sécurisées et du risque associé que leur organisation court
- Experts en tests d'intrusion
- Analystes vulnérabilité
- Auditeurs risque
- Ingénieurs DevOps
- Ingénieurs de fiabilité de site (SRE)

Vous apprendrez à...

- Mener des tests d'intrusion cloud
- Évaluer les environnements cloud et dégager de la valeur en localisant les vulnérabilités
- Appréhender de visu la construction des environnements cloud et l'insertion de facteurs d'échelle dans la collecte de preuves
- Évaluer les risques de sécurité dans les environnements AWS et Microsoft Azure, les deux principales plateformes actuelles

SEC 617

LIVE ONLINE | TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Wireless Penetration Testing and Ethical Hacking

Ce cours a été conçu pour les professionnels qui cherchent à acquérir une expertise technique complète pour comprendre, analyser et défendre les différentes technologies sans fil, omniprésentes dans nos environnements et véritables points d'entrée pour les attaquants.

Les concepteurs du cours SEC617, experts en tests d'intrusion, savent que de nombreuses organisations ne considèrent pas la sécurité des appareils sans fil comme une surface d'attaque et ne déploient pas les défenses et la supervision requises. Et cela en dépit du fait que les technologies sans fil sont largement déployées dans les suites exécutives des hôtels, les services financiers, les administrations publiques, les chaînes de fabrication, les réseaux de vente au détail, les dispositifs médicaux et les systèmes de contrôle du trafic aérien. Dans le contexte établi des technologies sans fil, peu sécurisées et faisant l'objet d'attaques, le cours SEC617 a été conçu pour aider les stagiaires à développer les compétences indispensables pour identifier, évaluer et estimer les menaces et pour y résister. Ces compétences sont incontournables pour les organisations de sécurité exigeantes.

NOUVEAUX THÈMES : WI-FI, ZIGBEE, Z-WAVE, DECT, RFID ET RADIO RÉALISÉE PAR LOGICIEL

Pour de nombreux analystes, « sans fil » était synonyme de « Wi-Fi », la technologie de réseau omniprésente, et un grand nombre d'organisations déployaient des systèmes de sécurité complexes pour protéger ces réseaux. Aujourd'hui, « sans fil » a un sens bien plus large et englobe non seulement la sécurité des systèmes Wi-Fi, mais aussi celle des systèmes Bluetooth, Zigbee, Z-Wave, DECT, RFID, NFC, des cartes sans contact et même des systèmes sans fil propriétaires. Pour être à même d'évaluer efficacement la sécurité des systèmes sans fil, vous devez maîtriser un large panel de technologies.

ÉTUDIEZ LES ATTAQUES SUR LE WI-FI SOUS WINDOWS, macOS, iOS ET ANDROID

Le cours SEC617 vous permettra de développer les compétences dont vous avez besoin pour comprendre les forces et les faiblesses de sécurité des systèmes sans fil. Vous apprendrez à mesurer la cacophonie qui règne encore entre les réseaux Wi-Fi et à identifier les points d'accès Wi-Fi (access points, AP) et les appareils client qui menacent votre organisation. Vous découvrirez comment évaluer, attaquer et exploiter les défauts des déploiements Wi-Fi actuels au moyen de la technologie WPA2, notamment des réseaux évolués WPA2-Enterprise. Vous comprendrez très concrètement les nombreuses faiblesses des protocoles Wi-Fi et serez à même de faire le lien avec les systèmes sans fil actuels. Avec l'identification et l'attaque des points d'accès Wi-Fi, vous apprendrez à identifier et à exploiter les différences de comportement des appareils clients en matière de recherche, d'identification et de sélection des AP. Une attention particulière sera portée au comportement des piles Wi-Fi Windows 10, macOS, Apple iOS et Android.

« Le cours SEC617 est parfait pour ceux qui cherchent un topo détaillé sur les attaques sans fil. »

- Garret Picchioni, *SALESFORCE*

CERT. GIAC : GAWN
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GAWN

Public visé :

- Hackers éthiques et experts en tests d'intrusion
- Personnel de sécurité réseau
- Administrateurs système et réseau
- Équipes de réponse aux incidents
- Décideurs des politiques de sécurité des systèmes d'information
- Auditeurs de sécurité
- Consultants en SSI
- Ingénieurs systèmes sans fil
- Développeurs de systèmes sans fil embarqués

Vous apprendrez à...

- Identifier et localiser les points d'accès des hackers malveillants en utilisant des outils gratuits ou peu coûteux
- Mener un test d'intrusion sur les technologies sans fil à faible consommation pour identifier des systèmes de contrôle et les vulnérabilités qui leur sont associées
- Identifier des vulnérabilités et contourner les mécanismes d'authentification des réseaux Bluetooth
- Utiliser des outils de capture sans fil pour extraire des conversations audio et du trafic de réseau à partir des téléphones sans fil DECT
- Implémenter un test d'intrusion WPA2-Enterprise afin d'exploiter les systèmes client sans fil vulnérables pour en récolter les authentifiants
- Utiliser Scapy pour forcer les paquets personnalisés à manipuler autrement les réseaux sans fil, en développant rapidement des outils d'attaque personnalisés qui répondent aux exigences des tests d'intrusion
- Identifier les attaques Wi-Fi en utilisant le suivi de paquets réseau capturés et les outils d'analyse gratuits
- Identifier et exploiter les défauts de sécurité des systèmes de badges d'accès sans contact
- Décoder les signaux radio propriétaires issus de radios logicielles

SEC 642

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

Vos applications web peuvent-elles résister aux assauts portés par les techniques avancées actuelles ?

À mesure que l'industrie développe de nouvelles technologies plus géniales les unes que les autres, les applications web modernes gagnent chaque jour un peu plus en complexité et en sophistication et doivent gérer de plus en plus d'opérations critiques. L'ère des requêtes et réponses HTML basiques est révolue depuis longtemps. Même à l'heure du Web 2.0 et d'AJAX, le HTTP et les applications web modernes voient leur complexité croître à grande vitesse. Dans les faits, l'environnement actuel impose une forte demande en clusters web à haute disponibilité et en déploiements cloud, avec pour les applications la nécessité d'être encore plus fonctionnelles tout en étant moins lourdes, sur fond de diminution des exigences imposées aux infrastructures terminales. Bienvenue dans un monde où cryptographie truquée, WebSockets et HTTP/2 ne sont que quelques-uns des concepts avec lesquels il faut composer… Question évaluation des applications web et tests d'intrusion, vous sentez-vous au point ? Êtes-vous prêt à affronter ces nouvelles technologies, paré à les sécuriser ?

Êtes-vous prêt à soumettre vos applications web à votre examen rigoureux d'expert à la pointe de la technologie ?

Cette formation aux tests d'intrusion a été conçue pour vous enseigner les compétences et techniques avancées dont vous avez besoin pour tester les applications web modernes et les technologies de nouvelle génération. Au travers d'une combinaison de cours, d'expériences concrètes et d'exercices pratiques, vous apprendrez à maîtriser les techniques qui permettent de tester la sécurité des technologies web éprouvées et utilisées en interne dans les entreprises, mais aussi celle des applications de pointe orientées vers internet. Vous terminerez enfin votre apprentissage par une compétition CTF (capture du drapeau) au cours de laquelle vous devrez déployer les connaissances acquises en formation, le tout dans un environnement ludique reprenant les technologies du monde réel.

Enseignement pratique de compétences avancées en matière d'exploitation d'applications web

Nous commencerons par explorer des techniques et des attaques avancées face auxquelles toutes les applications complexes d'aujourd'hui sont potentiellement vulnérables. Nous aborderons ensuite les nouvelles infrastructures web et les back-ends web, puis nous plongerons dans le chiffrement et son rapport avec les applications web en analysant la cryptographie déployée sur le web et en utilisant des techniques permettant d'identifier le chiffrement utilisé dans l'application ciblée. Il y aura bien sûr un passage obligé par les méthodes visant à exploiter ou détourner ces chiffrements. Nous examinerons les front-ends alternatifs de plusieurs applications web et services web comme les applications mobiles et nous nous pencherons sur les nouveaux protocoles comme HTTP/2 et WebSockets. La phase finale de la formation vous fera découvrir comment identifier et contourner les pare-feu d'application web, le filtrage et d'autres techniques de protection.

« On apprend des techniques et méthodes de haut vol, utiles à tout nouveau testeur d'application. »
- Vivek Veerappan, *GEMALTO*

Public visé :

- Experts en tests d'intrusion web
- Membres de *Red Team*
- Personnel chargé de l'évaluation des vulnérabilités
- Experts en tests d'intrusion réseau
- Consultants en sécurité
- Développeurs
- Testeurs QA
- Administrateurs système
- Responsables IT
- Architectes système

Vous apprendrez à…

- Mener à un niveau avancé des détections et exploitations Local File Include (LFI)/Remote File Include (RFI), Blind SQL injection (SQLi) et Cross-Site Scripting (XSS) associées à Cross-Site Request Forger (XSRF)
- Exploiter des vulnérabilités avancées communes à la plupart des langages back-end comme Mass Assignments, Type Juggling et Object Serialisation
- Effectuer une injection de code JavaScript sur ExpressJS, Node.js et NoSQL
- Comprendre les méthodes de test réservées aux systèmes de gestion de contenu comme SharePoint et WordPress
- Identifier et exploiter les implémentations de chiffrement dans les applications web et les infrastructures
- Découvrir les vulnérabilités XML Entity et XPath dans les services web SOAP ou REST et dans les banques de données
- Utiliser des outils et des techniques pour travailler avec HTTP/2 et WebSockets et les exploiter
- Identifier et contourner les pare-feu d'applications web et les techniques de filtrage pour exploiter le système

36 CRÉDITS CPE/CMU

SEC 660

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ce cours est conçu comme la suite logique du cours SEC560: Network Penetration Testing and Ethical Hacking, mais il s'adresse également aux personnes ayant déjà une expérience en tests d'intrusion. Les stagiaires ayant démontré les connaissances nécessaires à ce cours analyseront des dizaines d'attaques réelles utilisées par les experts en tests d'intrusion les plus accomplis. La méthodologie de chaque attaque sera abordée, puis suivie d'exercices dans un environnement labo représentatif de l'environnement réel afin que les stagiaires s'approprient ces concepts avancés et soient rapidement à pied d'œuvre de retour sur leur lieu de travail. Chaque soir, deux heures de formation intensive *bootcamp* permettent d'approfondir encore la maîtrise acquise via des exercices pratiques supplémentaires. Parmi les thèmes abordés, on retrouve l'arsenalisation de Python pour les experts en tests d'intrusion, les attaques contre les contrôles d'accès réseau (NAC) et la manipulation VLAN, l'exploitation d'appareils réseau, la pénétration dans des environnements Linux et Windows à accès restreint, IPv6, l'élévation des privilèges Linux et l'écriture d'exploit, le test des chiffrements en place, le *fuzzing*, le contournement des contrôles OS modernes comme ASLR et DEP, la programmation orientée retour (ROP), l'écriture d'exploit Windows et bien d'autres encore !

Les attaquants se font de plus en plus astucieux et leurs attaques de plus en plus complexes. Connaître les méthodes d'attaque les plus récentes nécessite un réel investissement personnel, du soutien et, bien sûr, l'occasion de pratiquer pour se forger une expérience. Le cours SEC660 permet aux stagiaires de développer une connaissance approfondie des vecteurs d'attaques majeurs, dans un environnement adapté où ils peuvent tester ces attaques à l'occasion d'essais pratiques. Cette formation va plus loin que la simple analyse avec ses résultats limités. Elle enseigne aux experts en tests d'intrusion comment reproduire le comportement d'un attaquant avancé afin de détecter les faiblesses significatives dans un environnement ciblé et de démontrer les risques encourus pour le système et l'organisation.

Le cours SEC660 commence par présenter le concept d'intrusion avancée avant d'exposer la suite du programme. Le premier jour est consacré aux attaques réseau, un domaine souvent négligé par les testeurs. Sont ainsi développés l'accès au réseau, la manipulation et l'exploitation du réseau et la grande variété de cibles : NAC, VLAN, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, etc. Le deuxième jour commence par un module technique sur la mise en œuvre de tests d'intrusion sur différentes implémentations cryptographiques. La journée se poursuit par la perpétration d'attaques via le démarrage par le réseau, l'évasion d'environnements restreints Linux, tels que chroot, et d'environnements de bureau restreints Windows. Le troisième jour est consacré à une introduction à Python pour les tests d'intrusion, à Scapy pour la création de paquets, aux tests de sécurité de produits, aux tests *fuzz* pour les applications et le réseau, et aux techniques de couverture de code. Aux quatrième et cinquième jours, le cours explore l'exploitation de programmes sur les systèmes Linux et Windows. Vous apprendrez à identifier les programmes à privilèges, à rediriger l'exécution de code, à effectuer la rétro-ingénierie des programmes pour localiser le code vulnérable, à obtenir l'exécution de code pour les accès au Shell d'administration et à faire échouer les contrôles des systèmes d'exploitation récents (comme ASLR, les leurres et DEP) en utilisant différentes techniques, dont la programmation ROP. Les exploits locaux et distants, et les techniques d'exploitation côté client sont traités. Le dernier jour est consacré à de nombreux défis de tests d'intrusion qui soumettent les stagiaires à des problèmes complexes et à des exercices de type « capture du drapeau ».

CERT. GIAC : GXPN
46 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GXPN

Public visé :

- Experts en tests d'intrusion réseau et système
- Chargés de réponse aux incidents
- Développeurs d'application
- Ingénieurs sécurité IDS

Vous apprendrez à…

- Réaliser des tests *fuzz* pour améliorer le processus SDL de votre société
- Exploiter les dispositifs réseau et évaluer les protocoles d'applications réseau
- Échapper aux environnements restrictifs sur Linux et Windows
- Tester les implémentations cryptographiques
  Modéliser les techniques utilisées par les assaillants pour réaliser des découvertes de vulnérabilité de type *zero day* et le développement d'exploits
- Développer des appréciations quantitatives et qualitatives des risques plus précises par la validation
- Démontrer la nécessité et les effets de l'optimisation des techniques récentes d'atténuation des exploits
- Effectuer la rétro-ingénierie du code vulnérable pour écrire des exploits personnalisés

SEC 699

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Purple Team Tactics – Adversary Emulation for Breach Prevention & Detection

Avec le cours SEC699, SANS s'adresse aux *Purple Team* avancées. Il met l'accent sur l'émulation d'attaques afin de détecter et prévenir les atteintes aux données. Pendant toute la formation, les stagiaires découvrent les moyens d'émuler des acteurs réels dans un environnement réaliste d'entreprise. Dans l'esprit *Purple Team*, l'objectif du cours est d'apprendre aux stagiaires les méthodes et moyens d'émuler et détecter les techniques d'attaque.

Suite naturelle du SEC599, ce cours avancé de SANS consacre 60 % du temps à la pratique. Les activités comprennent notamment :

- Un développement approfondi sur l'élaboration de playbooks Ansible pour déployer un environnement d'entreprise multidomaine complet à des fins d'émulation d'attaque simplement en appuyant sur un bouton.
- Le développement de modules personnalisés Caldera MITRE pour automatiser l'émulation d'attaque. La clé de la construction d'un pipeline d'émulation, c'est l'automatisation !
- L'élaboration de plans d'émulation d'attaques qui imitent de véritables auteurs comme APT-28, APT-34 et Turla.
- L'élaboration d'un véritable processus, de l'outillage et de la planification pour le fonctionnement en *Purple Team*.
- Les attaques « transforestières » où les stagiaires tentent d'étendre les privilèges de leur propre forêt isolée à celle du cours commun.
- Les méthodes d'évitement de certaines techniques défensives courantes, par exemple la mise sur liste blanche d'applications ou la réduction de la surface d'attaque.
- L'élaboration de règles SIGMA de détection de techniques d'attaque avancée.
- La conclusion en point d'orgue qui oppose les équipes, *Red Team* contre *Blue Team*. En attaque, les Rouges tentent d'infiltrer l'organisation, alors que les Bleus construisent leurs capacités de détection pour repérer les techniques d'attaque.
- Les concepteurs de la formation, Erik Van Buggenhout, principal concepteur de la partie SEC599, et James Shewmaker, co-concepteur de SEC660, sont tous deux experts certifiés GIAC Security Experts (GSE). De leur expérience pratique, ils tirent une compréhension profonde du fonctionnement des cyberattaques acquise des points de vue de la *Red Team*, en intrusion, et de la *Blue Team*, dans des activités de réponse à incident, de supervision de la sécurité et de recherche de compromissions. Dans ce cours, ils combinent leurs compétences pour apprendre aux stagiaires des méthodes d'émulation d'attaque à des fins de détection et de prévention des atteintes aux données.

Public visé :

- Experts en tests d'intrusion
- Hackeurs éthiques
- Défenseurs soucieux de mieux comprendre les méthodologies, outils et techniques offensifs
- Membres de *Red Team*
- Membres de *Blue Team*
- Membres de *Purple Team*
- Spécialistes inforensiques soucieux de mieux comprendre les tactiques offensives

Vous apprendrez à...

- Monter une équipe *Purple Team* dans votre organisation
- Élaborer des plans d'émulation d'attaque réalistes pour mieux protéger l'organisation
- Développer des outils propres et des compléments aux outils existants pour affiner vos activités de *Red Team* et de *Purple Team*
- Lancer des attaques avancées notamment par contournement de liste blanche applicative, par attaque transforestière (abus de délégation) et stratégies de persistance furtive
- Élaborer des règles SIGMA de détection de techniques d'attaque avancée

36 CRÉDITS CPE/CMU

SEC 760

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Exploit Development for Penetration Testers

Les vulnérabilités des systèmes d'exploitation prédominants, tels que Microsoft Windows 7/8 et Server 2012, et les distributions Linux les plus récentes, sont souvent très complexes et subtiles. Et pourtant, elles peuvent exposer les organisations à des attaques majeures et affaiblir leurs défenses lorsqu'elles sont exploitées par des assaillants habiles. Peu de professionnels de la sécurité ont les compétences requises pour découvrir, et encore moins pour comprendre foncièrement, pourquoi une vulnérabilité existe et comment écrire un exploit pour la compromettre. Paradoxalement, les assaillants doivent entretenir ces compétences, quel que soit le degré de complexité. Le cours SEC760:Advanced Exploit Development for Penetration Testers enseigne les compétences requises pour effectuer la rétro-ingénierie des applications 32 et 64 bits, déboguer à distance des noyaux et des applications d'utilisateurs, chercher des exploits *1-day* dans les correctifs et écrire des exploits complexes (tels que les attaques *use-after-free*) contre des logiciels et des systèmes d'exploitation récents.

Voici un aperçu des compétences que vous développerez dans le cours SEC760 :

- Écriture d'exploits modernes sur les systèmes d'exploitation Windows 7/8/10
- Exécution d'attaques complexes telles que *use-after-free*, techniques d'exploitation du Kernel, exploitation *1-day* au moyen de l'analyse de correctifs, etc.
- Apport essentiel des approches SDL (Security Development Lifecycle) et Secure SDLC, et de la modélisation des menaces
- Utilisation efficace de divers débogueurs et plug-ins pour améliorer et accélérer la recherche de vulnérabilités
- Gestion des techniques récentes d'atténuation des exploits visant à les entraver et à les faire échouer

> **« SEC760 est une formation unique en son genre. »**
> Jenny Kitaichit,
> *INTEL*

Public visé :

- Experts séniors en tests d'intrusion réseau et système
- Développeurs d'applications sécurisées (C et C++)
- Professionnels de la rétro-ingénierie de systèmes
- Gestionnaires séniors d'incidents
- Analystes des menaces séniors
- Spécialistes dans la recherche de vulnérabilités
- Chercheurs en sécurité

Vous apprendrez à...

- Découvrir les vulnérabilités *zero-day* des programmes qui fonctionnent sur les systèmes d'exploitation récents et patchés
- Créer des exploits pour tirer parti de vulnérabilités à l'aide d'un processus détaillé de test d'intrusion
- Utiliser les fonctionnalités avancées d'IDA Pro et rédiger des scripts Python IDC et IDA
- Déboguer à distance les applications Linux et Windows
- Comprendre et exploiter les débordements de tas Linux
- Écrire du Return Oriented Shellcode
- Comparer les correctifs (*patch diffing*) des programmes, des bibliothèques et des pilotes pour identifier les vulnérabilités corrigées
- Effectuer des débordements de tas dans Windows et utiliser des attaques *use-after-free*
- Utiliser avec précision la technique *heap spray* pour améliorer l'exploitabilité
- Déboguer le noyau Windows jusqu'à Windows 8 64 bits
- Vous lancer dans l'exploitation du noyau Windows

46 CRÉDITS CPE/CMU

«Ma certification GIAC ne me rend pas dépositaire de toute la connaissance en sécurité, mais elle garantit que les enjeux de sécurité seront portés à l'attention diligente de la direction. »
- Jenet Hensley, GCED, GWAPT, GSEC, GISP

GIAC développe et administre des certifications premium en cybersécurité pour les professionnels. Chaque certification sanctionne une formation SANS et la maîtrise de domaines critiques et spécialisés de l'InfoSec. Pour nos clients du secteur privé, de l'administration ou des armées partout dans le monde, elle valide les connaissances et les compétences en cybersécurité avec la rigueur la plus stricte.

GIAC **Pour en savoir plus, rendez-vous sur GIAC.ORG**

La certification la plus exigeante en cybersécurité

II GIAC PRÉSENTE

CYBERLIVE

Les certifications GIAC toujours plus ambitieuses

Avec CyberLive, les professionnels de la cybersécurité sont confrontés à des machines virtuelles en conditions réelles pour démontrer leurs compétences, leurs aptitudes et leur compréhension. Le tout en temps réel.
Pour en savoir plus, rendez-vous sur **giac.org/cyberlive**

« L'aspect pratique prend toujours plus d'importance pour valider les compétences des professionnels de la cyber. »
– Ben Boyle
GXPN, GDAT, GWAPT

GIAC
CERTIFICATIONS
GIAC.ORG

SANS

SANS Virtual Summits Will Be FREE for the Community in 2021

The very best part about SANS Summits going virtual in 2020 has been bringing even more of the community together from across the world — over 40,000 of you! We look forward to continuing to offer world-class content and actionable information that will leave you walking away with a fresh perspective and new tools that you can immediately leverage in your work to protect your organization from ever-evolving threats.

View the full line up of events
www.sans.org/cyber-security-summit/

**Virtual Summits listed here are free for the community to attend. Please note: other specialty Summit events, including CyberThreat, may charge a fee.*

FOR 308

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Digital Forensics Essentials NOUVEAU

Plus de la moitié des emplois du monde moderne exigent un ordinateur. La grande majorité des personnes âgées de 18 à 30 ans ont une certaine aisance informatique, habituées qu'elles sont aux smartphones, téléviseurs intelligents, tablettes et assistants virtuels, en plus des ordinateurs, dans leur quotidien. Et pourtant, parmi elles, combien comprennent vraiment ce qui se passe sous le capot ? Savez-vous ce que votre ordinateur ou votre téléphone peut révéler de vous ? Savez-vous qu'il n'est pas si difficile d'accéder à ces données et de les exploiter ? Vous en avez assez de ne pas comprendre les personnes qui s'y connaissent en ordinateurs, fichiers, données et métadonnées ? Savez-vous ce qui se passe vraiment quand vous supprimez un fichier ? Voulez-vous en savoir plus sur l'inforensique et la réponse aux incidents ? Si vous avez répondu « oui » à l'une de ces questions, cette formation s'adresse à vous. Cette introduction vise à donner aux personnes peu techniques une bonne compréhension du stockage des fichiers sur ordinateur ou téléphone, sans jargon. La formation explique ce que sont l'inforensique et la réponse aux incidents et ce dont les professionnels de cet art sont capables quand ils ont un appareil entre les mains.

Point de départ dans l'offre de formation de SANS, ce cours établit un socle de connaissances d'où partiront d'autres cours plus spécialisés.

L'informatique légale ou inforensique qui, jusque dans les années 1990, suivait les méthodes et techniques des enquêteurs pour collecter les éléments de preuve informatique sur les ordinateurs s'est muée en une discipline complexe et à part entière. Avec la multiplication des appareils et l'explosion des volumes de données exploitables à des fins d'enquête, l'inforensique n'était plus cantonnée aux investigations policières. Elle formait désormais une branche propre de la criminalistique. La justice y recourait dans les procès civils. Les services de renseignement et les armées l'utilisaient pour collecter renseignement et données exploitables. Elle servait à identifier les usages licites et frauduleux des appareils. Elle permettait de repérer les moyens utilisés pour compromettre les systèmes d'information et les réseaux et d'apprendre à mieux protéger ces infrastructures. Pour ne nommer que quelques exemples d'usages actuels de l'inforensique.

Toutefois, l'inforensique et la réponse aux incidents restent souvent mal comprises hors de leur petit secteur de niche, malgré leurs nombreux usages dans les milieux plus connus de l'entreprise, de la sécurité des informations, de la justice, des armées, du renseignement et des forces de l'ordre.

Souvent, les formations à l'inforensique et à la réponse aux incidents sont axées sur les techniques et méthodes à suivre et font l'impasse sur les fondamentaux, à savoir ce que sont l'inforensique et la réponse aux incidents et l'utilisation des investigations numériques et des éléments de preuve informatique. C'est le sujet de ce cours. Il s'agit de former les personnes qui ont ou pourraient avoir recours aux services des équipes d'inforensique et de réponse aux incidents pour les amener à mieux comprendre le travail de ces équipes et à mieux valoriser leurs prestations. Ces utilisateurs regroupent notamment des dirigeants, des cadres, des législateurs, des praticiens du droit, des opérateurs et enquêteurs des armées et du renseignement. Socle des futurs praticiens, ce cours sert de remise à niveau des fondamentaux pour les professionnels de l'inforensique et de la réponse aux incidents en exercice qui cherchent à passer un cap.

Public visé :

- Agents fédéraux et des forces de l'ordre qui veulent apprendre les bases de l'inforensique, qui débutent en inforensique, qui sont responsables d'une unité d'investigation numérique, ou qui veulent savoir utiliser les preuves informatiques dans les enquêtes et dans d'autres opérations de police.
- Analystes inforensiques qui souhaitent consolider et accroître leur maîtrise des fondamentaux de l'inforensique en tant que discipline.
- Professionnels de la cybersécurité qui veulent comprendre les fondamentaux de l'inforensique et son exploitation dans leurs environnements opérationnels.
- Juristes qui doivent comprendre l'inforensique, son rôle éventuel de preuve devant la justice, les différents usages des éléments de preuve informatique, et le lien entre l'inforensique et la preuve informatique.
- Militaires et agents de renseignement soucieux de comprendre le rôle de l'investigation numérique et de la collecte de renseignement, ainsi que les apports de l'inforensique dans leurs missions.

Vous apprendrez à...

- Utiliser efficacement les méthodologies d'investigation numérique
- Poser les bonnes questions sur les preuves informatiques
- Conduire des missions d'inforensique en conformité avec les normes et pratiques connues
- Développer et maintenir une capacité d'inforensique
- Comprendre les modes opératoires et les procédures de réponse aux incidents et savoir le moment où faire appel à l'équipe
- Décrire les éventuelles options de récupération des données en cas de suppression

36 CRÉDITS CPE/CMU

FOR 498

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Battlefield Forensics & Data Acquisition NOUVEAU

L'HEURE TOURNE. VOUS DEVEZ CLASSER PAR PRIORITÉ LES PREUVES LES PLUS PRÉCIEUSES POUR TRAITEMENT. NOUS VOUS MONTRONS COMMENT FAIRE !

FOR498: Battlefield Forensics & Acquisition vous apprend à :

1. Acquérir avec efficacité les données des sources suivantes :
   - ordinateurs PC, Microsoft Surface et Tablet PC
   - appareils Apple, Mac et Macbook
   - mémoire et RAM
   - smartphones et appareils mobiles portables
   - stockage et services cloud
   - stockages réseau
2. Produire des renseignements exploitables en 90 minutes ou moins

Dans toute enquête, la première étape consiste à recueillir des preuves. Il en est de même pour les investigations inforensiques. Les éléments de preuve sont alors des données que l'on trouve en divers formats et emplacements. Il faut tout d'abord identifier les données potentiellement utiles, déterminer où elles résident, puis formuler un plan et des procédures de collecte. Pour obtenir des preuves numériques, vous n'avez généralement qu'une seule chance de collecter correctement les données. Si vous menez mal cette phase, vous risquez, en plus de nuire à l'enquête, de détruire les données qui auraient autrement servi de preuve.

La grande variété actuelle des supports de stockage implique que toute méthodologie universelle est tout simplement irrecevable. Beaucoup d'erreurs sont commises pendant la collecte des preuves numériques, avec le risque que le coupable s'en sorte mais, plus grave encore, que l'innocent soit incarcéré. Les bits et octets que vous êtes chargé de collecter et d'interpréter avec soin peuvent décider du sort de millions de dollars.

Un enquêteur ne peut plus se contenter d'une image disque à froid (*dead box*) d'un seul disque dur. Dans la sphère cyber actuelle, nous sommes nombreux à utiliser un poste de travail, un portable, une tablette et un téléphone au cours d'une même journée. À ces usages vient s'ajouter l'essor du recours au stockage et aux fournisseurs cloud : la collecte des données sur toutes ces sources dans de bonnes conditions peut s'avérer herculéenne.

Dans cette formation approfondie au traitement des données et à l'obtention d'éléments de preuve numérique, les premiers intervenants et les investigateurs acquièrent les compétences avancées pour répondre à un incident et identifier, collecter et conserver les données d'une large gamme de dispositifs de stockage en garantissant l'intégrité incontestable des éléments de preuves. Régulièrement actualisée, la formation FOR498 comble le besoin qu'ont les investigateurs de connaître et comprendre toute l'étendue des défis et techniques qu'ils utiliseront dans leurs enquêtes.

Dans les nombreux exercices en labo, les premiers intervenants, les enquêteurs et les équipes inforensiques acquièrent l'expérience pratique nécessaire à la collecte d'éléments de preuve numérique sur des disques durs, clés USB, téléphones cellulaires, espaces de stockage réseau et toutes autres sources semblables. Dans une organisation, les investigations et la réponse inforensiques font appel aux chargés de réponse les plus compétents possibles, pour éviter que l'enquête ne se termine avant même d'avoir commencé.

Le cours FOR498: Battlefield Forensics & Acquisition vous forme, vous et votre équipe, à l'identification, la collecte et la conservation des données et à la réponse à apporter où que ces données se cachent ou résident.

Public visé :

- Agents fédéraux et des forces de l'ordre
- Premiers intervenants
- Analystes inforensiques
- Professionnels de la cybersécurité
- Équipes de réponse aux incidents
- Analystes spécialistes de l'exploitation des médias
- Personnels du ministère de la Défense et professionnels du renseignement
- Quiconque cherche à comprendre la conservation des données des systèmes dans les règles de l'art

Vous apprendrez à...

- Maîtriser les outils, techniques et procédures de localisation, d'identification et de collecte efficaces des données où qu'elles se trouvent
- Gérer et traiter une scène de crime pour préserver l'intégrité de la preuve
- Réaliser les acquisitions de données sur des stockages au repos, notamment des disques mécaniques et à semiconducteurs (SSD)
- Identifier les nombreux emplacements susceptibles d'accueillir les données d'une enquête
- Mener une analyse inforensique de terrain en partant de la saisie des éléments de preuve jusqu'à l'exploitation des renseignements en 90 minutes ou moins
- Participer à la préparation de la documentation nécessaire à la communication avec des entités en ligne telles que Google, Facebook, Microsoft, etc.
- Comprendre les concepts et l'usage des technologies de stockage de grand volume, notamment les stockages JBOD ou RAID, les dispositifs NAS et d'autres stockages réseau adressables
- Identifier et collecter des données utilisateur dans des environnements de grande entreprise où les accès se font par le protocole SMB

CERT. GIAC : GBFA
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GBFA

FOR 500

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Windows Forensic Analysis

Toutes les organisations doivent se préparer à l'éventualité de cyberattaques contre leurs systèmes et leurs réseaux. Les analystes capables de mener des enquêtes sur les cas de fraudes, de menaces internes, d'espionnage industriel, d'abus par un employé et d'intrusion dans les systèmes informatiques n'ont jamais été autant recherchés. Les agences gouvernementales font de plus en plus appel à des spécialistes formés à l'exploitation des médias pour récupérer des renseignements clés sur des systèmes Windows. Conscient de ces besoins, SANS forme actuellement la nouvelle génération de professionnels en inforensique, de chargés de réponse aux incidents et d'experts en exploitation des médias ; des individus capables de comprendre ce qui s'est passé seconde par seconde dans un système informatique.

Le cours FOR500: Windows Forensic Analysis vise à inculquer une connaissance inforensique approfondie des systèmes d'exploitation de Microsoft Windows. On ne protège bien que ce que l'on connaît bien. De ce fait, la compréhension des capacités et des artefacts inforensiques est une composante essentielle de la sécurité de l'information. Les stagiaires apprennent à récupérer, analyser et authentifier des données d'inforensique sur les systèmes Windows. Les équipes apprennent à suivre en détail les activités d'un utilisateur sur un réseau et à organiser leurs résultats pour une utilisation future telle que gestion des réponses aux incidents, enquêtes internes et contentieux civil ou criminel. Les stagiaires acquièrent des compétences pour valider les outils de sécurité, améliorer les évaluations des vulnérabilités, identifier les menaces internes, suivre les hackers et améliorer leurs politiques de sécurité. Windows enregistre silencieusement une énorme quantité de données sur les utilisateurs. FOR500 vous apprend à exploiter cette source de données.

Une bonne analyse exige des données réelles. Constamment actualisé, le cours FOR500 forme les analystes inforensiques au moyen d'exercices pratiques et innovants réalisés en laboratoire et intégrant les éléments de preuves identifiés dans les dernières technologies de Microsoft (Windows 7/8/10, Office et Office365, stockage dans le cloud, Sharepoint, Exchange, Outlook). À l'issue du cours, les stagiaires maîtrisent les tout derniers outils et techniques de pointe et sont en mesure de mener leurs enquêtes, même sur les systèmes les plus complexes. Ils apprennent à faire une analyse sur tous les systèmes sans exception, des plus anciens comme Windows XP aux nouveaux artefacts de Windows 10. Le cours FOR500 est actualisé en permanence.

Ce cours est basé sur une nouvelle affaire de vol de propriété intellectuelle et d'espionnage industriel qui a nécessité plus de six mois de développement. Vous évoluez dans le monde réel ; votre formation se doit donc d'inclure des données pratiques et concrètes. Notre équipe de développement a puisé dans ses propres expériences et enquêtes pour créer un scénario riche et détaillé qui plonge les stagiaires dans une enquête aussi réelle que possible. Cette affaire présente les artefacts et technologies les plus récents qu'un enquêteur puisse rencontrer dans le cadre d'une analyse de systèmes Windows. Incroyablement détaillé, le manuel revient longuement sur les outils et les techniques que tout enquêteur qui se respecte doit maîtriser pour résoudre une affaire.

« Ce cours à la pointe de l'actualité bouscule les idées reçues et nous aide à être de meilleurs enquêteurs. Il est vraiment bien préparé. »
- Frank Visser,
PWC

Public visé :

- Professionnels de la cybersécurité
- Équipes de réponse aux incidents
- Représentants des forces de l'ordre, agents fédéraux et enquêteurs
- Analystes spécialistes de l'exploitation des médias
- Toute personne souhaitant approfondir sa compréhension de l'inforensique pour Windows

Vous apprendrez à...

- Mener des analyses inforensiques Windows en bonne et due forme en appliquant des techniques clés pour Windows 7/8/10
- Utiliser la gamme des outils et des méthodes d'analyse inforensiques disponibles pour détailler toutes les actions ou presque d'un suspect dans un système Windows : auteur d'un artefact (identité, procédure), exécution de programmes, ouverture de fichiers/dossiers, géolocalisation, historique navigateur, profilage d'utilisation d'appareil USB, etc.
- Découvrir l'heure exacte à laquelle une personne a utilisé un programme pour la dernière fois, grâce à une analyse de la base de registre et des artefacts Windows, et comprendre comment utiliser cette information pour prouver les intentions dans le cas de vol de propriété intellectuelle, de compromission de systèmes par un hackeur et d'autres infractions courantes
- Déterminer le nombre d'ouvertures d'un fichier par un suspect grâce à l'analyse inforensique du navigateur, l'analyse des raccourcis (LNK), des e-mails et du Registre Windows
- Identifier les mots-clés recherchés par un utilisateur dans un système Windows pour cibler les fichiers et les informations qui intéressaient le suspect, puis mener une évaluation détaillée des dommages occasionnés

CERT. GIAC : GCFE
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCFE

FOR 508

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Digital Forensics, Incident Response, and Threat Hunting

Le cours FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting vous aidera à :

- Détecter l'apparition d'une brèche (date et nature)
- Identifier les systèmes affectés et compromis
  Identifier ce que les attaquants ont volé ou modifié
- Contenir les incidents et y remédier
- Développer des sources de référence en matière d'informations sur les menaces
- Chercher et détecter des brèches additionnelles en utilisant votre connaissance de l'adversaire

JOUR 0 : une agence gouvernementale vous informe de l'existence d'un groupe de menaces avancées qui cible des organisations comme la vôtre et vous signale que vous êtes sur la liste des prochaines cibles potentielles. Elle ne vous donne pas ses sources, mais pense que certains de vos systèmes sont déjà compromis. Une menace persistante avancée (advanced persistent threat, APT) est très probablement en jeu. Il s'agit de la menace la plus sophistiquée à laquelle vous pourriez être confronté dans vos efforts pour défendre vos systèmes et vos données. Et il est également possible que vos adversaires fouillent dans votre réseau depuis plusieurs mois, voire plusieurs années, sans jamais avoir été détectés.

C'est bien sûr une situation hypothétique, mais il y a tout de même de fortes chances que des menaces cachées soient déjà actives dans les réseaux de votre organisation. Les organisations ne peuvent se permettre de croire que les mesures de sécurité en place sont parfaites et impénétrables, et ce quel que soit le niveau de sécurité. Les systèmes de prévention seuls ne suffisent pas à contrer un adversaire humain obstiné qui sait comment contourner la plupart des outils de sécurité et de supervision.

Ce cours approfondi de réponse aux incidents et de recherche de menaces permet aux équipes concernées de monter en compétences pour traquer, identifier et contrer un large spectre de menaces à l'intérieur des réseaux d'entreprise (incluant aussi bien des APT d'États-nations hostiles, de syndicats du crime organisé et d'hacktivistes) et d'y répondre. Constamment remis à jour, le cours FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting répond aux incidents d'aujourd'hui en fournissant des tactiques et des techniques que l'élite des professionnels utilise quotidiennement pour détecter les brèches de sécurité qui se produisent dans le monde réel, les contrer et y répondre.

« Nous sommes en train de développer une nouvelle compétence inforensique, et ce cours m'a apporté exactement ce qu'il fallait pour cela. »
- Simon Fowler,
VIRGIN MEDIA

Public visé :

- Équipes de réponse aux incidents
- Équipe de recherche de menaces (*threat hunters*)
- Analystes inforensiques séniors
- Professionnels de la cybersécurité
- Administration fédérale et forces de l'ordre
- Membres d'une *Red Team*, experts en tests d'intrusion, développeurs d'exploits
- Stagiaires ayant suivi les cours SANS FOR408 et SEC504

Vous apprendrez à...

- Maîtriser les outils, techniques et procédures nécessaires pour traquer, détecter et contenir toute une variété d'adversaires et pour répondre à des incidents
- Détecter et traquer des malwares inconnus actifs, dormants et personnalisés dans la mémoire et sur différents systèmes Windows dans un environnement d'entreprise
- Traquer les incidents et y répondre à travers plusieurs centaines de systèmes uniques simultanément en utilisant F-Response Enterprise et la station de travail SIFT
- Identifier et suivre le balisage sortant des malwares vers leur canal de commande et de contrôle (C2) grâce à l'inforensique mémoire, l'analyse des registres et les résidus de connexion réseau
- Déterminer le déroulement d'une brèche en identifiant la pointe de l'attaque et les mécanismes de hameçonnage ciblé (*spear-phishing*)
- Repérer les techniques avancées des adversaires visant à déjouer l'inforensique, comme les malwares furtifs et à horodatage falsifié ou *time-stomped*, et les logiciels utilitaires servant à se déplacer dans le réseau et maintenir une présence d'attaquant

CERT. GIAC : GCFA
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCFA

FOR 518

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Mac and iOS Forensic Analysis and Incident Response

Les experts en investigation numérique ont l'habitude de travailler sur des machines Windows, mais que se passe-t-il lorsqu'ils sont confrontés à un nouveau Mac ou appareil Apple ? La popularité croissante des appareils Apple est manifeste, des cafés jusqu'aux conseils d'administration, pourtant la plupart des enquêteurs maîtrisent exclusivement les appareils sous Windows.

Les temps et les tendances changent ; les enquêteurs et les analystes ont besoin d'évoluer avec eux. Le nouveau cours FOR518:Mac Forensic Analysis apporte les outils et techniques nécessaires pour affronter et traiter résolument un incident impliquant un Mac.

Les compétences pratiques et approfondies en expertise numérique enseignées dans ce cours permettent aux enquêteurs Windows d'élargir leurs capacités d'analyse, et d'avoir la confiance et les connaissances nécessaires pour analyser les systèmes Mac ou iOS.

Dans le cours FOR518: Mac Forensic Analysis, vous apprendrez...

- Les fondamentaux Mac : comment analyser et décomposer manuellement le système de fichiers propriétaire HFS+ (Hierarchical File System Plus) et reconnaître les domaines spécifiques du système de fichiers logique et les types de fichiers Mac.
- L'activité utilisateur : comment comprendre et profiler un utilisateur grâce à ses fichiers de données et à la configuration de ses préférences.
- L'analyse et la corrélation avancées : comment déterminer l'utilisation qui a été faite d'un système ou son niveau de compromission à l'aide des fichiers système et des fichiers de données utilisateur en corrélation avec les fichiers journaux système.
- Les technologies Mac : comment comprendre et analyser diverses technologies Mac, dont Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop et FaceTime.

Le cours FOR518: Mac Forensic Analysis a pour objectif de compléter la formation d'un spécialiste en inforensique sous Windows et de lui faire découvrir l'équivalent sous Mac. Ce cours développe des thèmes tels que le système de fichiers HFS+, les fichiers de données Mac, le pistage de l'activité utilisateur, la configuration système, l'analyse et la corrélation de journaux Mac, d'applications Mac et de technologies Mac. Un spécialiste en inforensique qui suit la totalité de ce cours sera parfaitement armé pour mener des enquêtes sous Mac.

« Le meilleur cours d'inforensique Mac sur la place ! »
- David Klopp,
J.P.MORGAN

« Le temps consacré aux exercices était bluffant.On devine le travail de préparation qu'il y a derrière. »
- Gary Titus,
STROZ FRIEDBERG LLC

Public visé :

- Analystes inforensiques séniors qui souhaitent renforcer et élargir leur compréhension de l'inforensique des fichiers système et de l'analyse Mac avancée
- Agents des forces de l'ordre, de l'administration fédérale ou enquêteurs qui veulent maîtriser l'inforensique avancée et développer leurs compétences en investigation
- Analystes spécialistes de l'exploitation des médias qui ont besoin de savoir comment trouver les données critiques dont ils ont besoin sur un système Mac
- Membres d'une équipe de réponse aux incidents qui font face à des incidents de sécurité et/ou à des intrusions complexes émanant d'adversaires de haut niveau, et qui ont besoin de savoir quoi faire lorsqu'ils examinent un système compromis
- Professionnels de la cybersécurité qui veulent développer une connaissance des systèmes d'exploitation Mac OS X et iOS
- Stagiaires qui ont déjà suivi les cours SANS FOR500 (auparavant 408), FOR508, FOR526, FOR585 et FOR610 qui veulent parfaire leur expertise numérique

Vous apprendrez à...

- Analyser manuellement les systèmes de fichiers HFS+ en utilisant uniquement un aide-mémoire et un éditeur hexadécimal
- Déterminer l'importance de chaque domaine de système de fichiers
- Mener une analyse temporelle sur un système en corrélant les fichiers de données et les analyses de log
- Profiler l'utilisation des systèmes par des individus : fréquence d'utilisation, applications utilisées, préférences système personnelles, etc.
- Déterminer les sauvegardes de données locales ou à distance, les images disque et les autres appareils rattachés

36 CRÉDITS CPE/CMU

FOR 526

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Memory Forensics & Threat Detection

Les experts de l'inforensique et chargés de réponse aux incidents (Digital Forensics and Incident Response, DFIR) ont besoin d'une formation avancée en inforensique mémoire sous Windows pour s'assurer d'être au meilleur niveau. Les enquêteurs qui n'analysent pas la mémoire volatile laissent des preuves sur la scène de crime. La RAM contient des preuves concernant les actions d'un utilisateur, les processus malveillants et les comportements furtifs implémentés par un code nuisible. Ce sont ces preuves qui se révèlent souvent être la clé de ce qui s'est passé sur un système.

Le cours FOR526: Memory Forensics In-Depth apporte des compétences essentielles aux experts spécialisés dans la réponse aux incidents et l'investigation numérique qui leur permettent de faire un triage de la mémoire sur un système actif et d'analyser des images de mémoire capturées. Le cours utilise les logiciels gratuits et en open source les plus efficaces de l'industrie ; il permet de comprendre dans le détail comment ces outils fonctionnent. Le cours FOR526 est essentiel pour tout enquêteur DFIR sérieux qui veut maîtriser l'inforensique de haut niveau et la réponse aux incidents et souhaite intervenir sur des incidents impliquant des délits d'initiés. De nos jours, pour l'inforensique, il est tout aussi essentiel de comprendre les structures de la mémoire que celles du disque et du registre. L'analyste qui a une connaissance détaillée des éléments internes de la mémoire Windows peut accéder à des données ciblées spécifiques aux besoins de l'enquête en cours. Pour les enquêteurs qui analysent des plateformes autres que Windows, ce cours aborde également l'analyse et l'acquisition de l'inforensique mémoire sur OSX et Linux par des exercices pratiques.

Les enquêteurs et les assaillants se livrent une véritable course aux armements. Les malwares et les modules de post-exploitation récents utilisent de plus en plus des techniques d'autodéfense incluant des rootkits plus sophistiqués et des mécanismes contre l'analyse de mémoire qui détruisent ou détournent des données volatiles. Les analystes doivent donc avoir une connaissance très fine des éléments internes de la mémoire pour discerner les intentions des assaillants ou des initiés malveillants. Le cours FOR526 s'appuie sur les meilleures pratiques et recommandations d'experts dans le domaine qui guident les professionnels DFIR dans l'acquisition, la validation et l'analyse de mémoire en utilisant des images de mémoire réelles chargées de malwares.

Dans le cours FOR526: Memory Forensics In-Depth, vous apprendrez...

- L'acquisition mémoire : capturez la mémoire ciblée en garantissant l'intégrité des données et surmontez les obstacles aux comportements d'acquisition/anti-acquisition.
- L'identification d'un vice en mémoire : détectez des processus malveillants, cachés et injectés, des rootkits au niveau du noyau, le détournement de bibliothèques de liens dynamiques (DLL), le *process hollowing* et les mécanismes sophistiqués de persistance.
- Des techniques efficaces et pas à pas d'analyse mémoire : utilisez une chronologie du processus et des analyses de niveau haut/bas, et parcourez l'arborescence des descripteurs d'adresses virtuelles (Virtual Address Descriptors, VAD) pour détecter des comportements anormaux.
- Des techniques d'excellence : sachez quand implémenter un triage, une analyse sur un système actif, découvrez des techniques alternatives d'acquisition et apprenez à concevoir des scripts d'analyse personnalisés pour une analyse mémoire ciblée.

Public visé :

- Équipes de réponse aux incidents qui, régulièrement confrontées à des incidents/intrusions complexes, voudraient ajouter l'inforensique mémoire à leurs compétences
- Analystes inforensiques séniors qui souhaitent consolider et accroître leur maîtrise de l'inforensique mémoire
- Membres d'une *Red Team*, experts en tests d'intrusion et développeurs d'exploits qui souhaitent savoir comment ne pas se faire identifier par leurs adversaires
- Agents des forces de l'ordre, de l'administration fédérale ou enquêteurs qui souhaitent acquérir une expertise en inforensique mémoire
- Stagiaires ayant suivi les cours SANS FOR508 et SEC504 et qui veulent passer au niveau suivant de leur formation en inforensique mémoire
- Enquêteurs en inforensique dans des organisations où la mémoire est régulièrement récupérée par les premiers intervenants et qui veulent rehausser le niveau en analysant les images

46 CRÉDITS CPE/CMU

FOR 572

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

Mettez en pratique vos connaissances en inforensique. Intégrez des données de réseau dans vos enquêtes, produisez de meilleures conclusions et effectuez le travail plus rapidement. Il est extrêmement rare de mener une enquête inforensique sans élément de réseau. L'investigation numérique sur les points de terminaison reste et restera une compétence cruciale et fondamentale dans cette carrière, mais ignorer leurs communications réseau équivaut à ignorer les images des caméras de sécurité captant une infraction. Que vous preniez en charge un incident d'intrusion, un vol de données, une utilisation à mauvais escient par les employés ou que vous participiez à une découverte proactive d'adversaires, le réseau offre souvent une vue sans pareil de l'incident. Il peut produire la preuve nécessaire pour démontrer l'intention, démasquer des attaquants actifs depuis des mois ou plus, ou même s'avérer utile pour prouver sans équivoque une infraction.

Le cours FOR572: Advanced Network Forensics and Analysis a été conçu de A à Z pour aborder les compétences essentielles à l'organisation d'enquêtes inforensiques efficaces et optimales. Il s'articule autour des connaissances nécessaires pour élargir l'approche inforensique, en commençant par les données résiduelles sur les supports de stockage d'un système ou d'un dispositif jusqu'aux communications transitoires passées ou encore présentes. Même si l'attaquant distant le plus qualifié a compromis un système avec un exploit indétectable, le système doit toujours communiquer sur le réseau. Sans canaux de commande et de contrôle et d'extraction de données, la valeur d'un système informatique compromis est presque nulle. Autrement dit, les adversaires parlent, et nous vous apprendrons à écouter.

Ce cours porte sur les outils, la technologie et les processus requis pour intégrer les sources de preuves réseau dans vos enquêtes, et met l'accent sur l'efficacité et l'optimisation. Vous partirez à la fin de la semaine avec une boîte à outils bien remplie et les connaissances nécessaires pour vous en servir dès votre première journée de travail. Nous étudierons toute la gamme des preuves réseau : analyse NetFlow de haut niveau, exploration de PCAP de bas niveau, examen du journal de réseau auxiliaire, et plus encore. Nous expliquons comment tirer parti des dispositifs d'infrastructure existants qui peuvent contenir des mois ou des années de preuves valables, ainsi que la façon de placer de nouvelles plateformes de collecte pendant qu'un incident est déjà en cours.

Que vous soyez un consultant intervenant sur le site d'un client, chargé de l'assistance aux victimes de cybercrime et des poursuites contre les responsables, praticien de l'inforensique en entreprise ou membre des rangs toujours plus nombreux des *threat hunters*, ce cours vous offre une expérience pratique dont les scénarios issus du monde réel vous aideront à progresser dans votre travail. Les anciens stagiaires du programme SANS SEC et les défenseurs de réseau en général bénéficieront de la perspective du cours FOR572 sur les opérations de sécurité, alors qu'ils prennent en charge plus de réponses aux incidents et d'enquêtes. Les stagiaires ayant déjà suivi les cours FOR500 (anciennement FOR408) et FOR508 peuvent utiliser leurs connaissances et les appliquer directement aux attaques de réseau quotidiennes. Le cours FOR572 s'attaque aux problèmes de même envergure issus du monde réel, mais sans le recours aux images de disque ou de mémoire.

CERT. GIAC : GNFA
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GNFA

Public visé :

- Membres de l'équipe de réponse aux incidents et cyberenquêteurs
- Membres d'une *Hunt Team*
- Forces de l'ordre, administration fédérale et inspecteurs de police Responsables de la sécurité des systèmes d'information
- Défenseurs de réseau
- Professionnels de l'informatique
- Ingénieurs réseau
- Toute personne intéressée par les intrusions réseau et les enquêtes dans ce domaine
- Professionnels de la cybersécurité et personnel de Centre des opérations de sécurité

Vous apprendrez à...

- Extraire des fichiers à partir de paquets réseau capturés et de fichiers de cache proxy pour procéder à l'analyse subséquente des malwares ou établir la perte de données définitive
- Utiliser les données historiques de NetFlow pour identifier les occurrences de réseau antérieures pertinentes et mesurer précisément la portée de l'incident
- Effectuer la rétro-ingénierie des protocoles réseau personnalisés pour identifier les capacités et les actions de commande et de contrôle d'un attaquant
- Déchiffrer le trafic SSL capturé pour identifier les actions des attaquants et les données qu'ils ont dérobées à la victime
- Utiliser les données des protocoles de réseau typiques pour augmenter la fidélité des résultats de l'enquête
- Identifier les opportunités de collecte de preuves supplémentaires en fonction des systèmes et plateformes d'une architecture de réseau
- Examiner le trafic en utilisant des protocoles de réseau courants pour identifier des formes d'activité ou des actions spécifiques justifiant une enquête plus approfondie

FOR 578

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Cyber Threat Intelligence

Ne vous y trompez pas : actuellement, la défense réseau, la recherche de menaces ou ***threat hunting*** et la réponse aux incidents sont des pratiques qui exploitent largement le renseignement et le contre-renseignement, des aspects que les cyberanalystes doivent comprendre et exploiter s'ils veulent défendre efficacement les réseaux, les données propriétaires et les organisations dont ils ont la responsabilité.

Le cours FOR578: Cyber Threat Intelligence aidera les défenseurs réseau, les équipes de *threat hunting* et les chargés de réponse aux incidents à :

- Maîtriser et développer des compétences en renseignement sur les menaces aux niveaux tactiques, opérationnels et stratégiques
- Obtenir des renseignements sur les menaces pour détecter des menaces persistantes et avancées (APT), y répondre et les contrecarrer
- Valider les informations reçues de la part d'autres organisations pour réduire les dépenses induites par de mauvais renseignements
- Exploiter le renseignement de sources ouvertes (OSINT) pour compléter le travail d'une équipe de sécurité, quelle que soit sa taille
- Créer des indicateurs de compromission (IOC) dans des formats comme YARA, OpenIOC et STIX

La collecte, la classification et l'exploitation des connaissances sur l'adversaire

– des processus que l'on regroupe sous le nom de renseignement sur les cybermenaces ou CTI (*Cyber Threat Intelligence*) – donnent aux défenseurs réseau un avantage certain sur les attaquants et limitent ainsi le risque de voir une attaque réussir lors d'une tentative d'intrusion. Les chargés de réponse doivent disposer d'informations précises, récentes et détaillées afin de surveiller les nouvelles attaques et les évolutions d'attaques existantes. Il leur faut aussi des méthodes pour exploiter ces informations de façon à mettre en place une posture défensive améliorée.

Le renseignement sur les cybermenaces constitue donc un atout majeur pour les organisations qui cherchent à actualiser leurs programmes de réponse et de détection dans un monde où les menaces persistantes et avancées sont toujours plus sophistiquées. Les malwares ne sont que des outils : c'est l'individu qui les manie qui représente la véritable menace. Le renseignement sur les cybermenaces cherche en priorité à contrer cette menace humaine à la fois persistante et flexible en lui opposant des défenseurs humains outillés et entraînés.

En cas d'attaque ciblée, une organisation doit disposer d'une équipe de *threat hunting* ou de réponse aux incidents dont les membres font état de compétences de premier ordre. Ces équipes doivent en outre disposer des renseignements dont elles ont besoin pour comprendre le fonctionnement des attaquants et leur faire obstacle. Le cours FOR578: Cyber Threat Intelligence vous permettra, à vous et à votre équipe, de développer des compétences en matière de renseignement sur les cybermenaces et d'assurer une cybersécurité solide, une chasse aux menaces plus précise et une réponse aux incidents plus efficace. Vous serez en outre capable de mieux sensibiliser les organisations en la matière.

> **« Je débute en CTI et j'ai trouvé que ce cours était très bien adapté pour des personnes avec différents niveaux d'expertise. »**
> - Ben Hargreaves, *PWC*

CERT. GIAC : GCTI
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCTI

Public visé :

- Professionnels de la sécurité
- Équipes de réponse aux incidents
- Équipe de recherche de menaces (*threat hunters*)
- Personnel du centre des opérations de sécurité (SOC)
- Analystes inforensiques et en malwares
- Agents fédéraux et agents des forces de l'ordre
- Gestionnaires de la technologie
- Stagiaires ayant déjà suivi les cours SANS FOR500, FOR572, FOR508 ou FOR610

Vous apprendrez à...

- Développer des compétences d'analyse pour mieux appréhender, synthétiser et exploiter des scénarios complexes
- Identifier et créer des critères de renseignement grâce à des pratiques comme la modélisation de menace
- Maîtriser et développer des compétences en renseignement sur les menaces aux niveaux tactiques, opérationnels et stratégiques
- Générer des renseignements pour détecter des menaces précises, y répondre et les contrecarrer
- Identifier les différentes sources pour collecter les données de l'adversaire et les exploiter à votre avantage
- Valider des informations de provenance extérieure pour réduire les dépenses liées aux mauvais renseignements
- Créer des indicateurs de compromission (IOC) dans des formats comme YARA, OpenIOC et STIX
- Migrer vers une sécurité plus mature (en délaissant les anciens IOC) pour mieux comprendre et contrecarrer les techniques comportementales des menaces
- Établir des techniques analytiques structurées pour remplir aux mieux les missions des postes en sécurité

FOR 585

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Smartphone Forensics

Les appareils mobiles jouent souvent un rôle essentiel dans les affaires criminelles, les intrusions, les vols d'adresse IP, les menaces à la sécurité, etc. Savoir exploiter correctement leurs données est déterminant pour résoudre une affaire et pour la suite de votre carrière de spécialiste. Le cours FOR585: Advanced Smartphone Forensics enseigne toutes ces compétences.

À chaque fois que le téléphone « réfléchit » ou fait une suggestion, les données sont enregistrées. On peut donc rapidement être perdu devant la masse de données récupérée par les outils d'inforensique. L'inforensique des smartphones ne consiste pas à simplement presser le bouton « Chercher la preuve » pour obtenir des réponses. Bien au contraire, il est essentiel de comprendre comment utiliser correctement ces outils pour diriger l'enquête plutôt que de laisser l'outil rapporter ce qu'il déduit à partir de l'utilisation de l'appareil. Il est impossible pour les outils commerciaux de tout analyser sur les smartphones et de comprendre comment les données sont arrivées sur le dispositif. L'analyse et l'interprétation des données sont de votre ressort. Ce cours donne aux stagiaires la capacité et la confiance nécessaires pour extraire de bonnes preuves à partir des smartphones.

Ce cours détaillé sur l'inforensique des smartphones apporte aux enquêteurs et analystes les compétences pour détecter, décoder, déchiffrer et interpréter correctement les preuves récupérées sur des dispositifs mobiles. Il comprend 17 ateliers pratiques. Ceux-ci vont permettre aux stagiaires d'analyser divers ensembles de données provenant de smartphones afin de comprendre comment les données d'un tel appareil se dissimulent et comment elles peuvent être mieux exploitées avec d'excellents outils inforensiques et des scripts personnalisés. Chaque atelier aborde un sujet particulier applicable à d'autres smartphones. Les stagiaires acquièrent une expérience avec les différents formats de données sur des plateformes multiples et apprennent comment les données sont enregistrées et chiffrées sur chaque type de dispositif mobile. Ils apprendront pourquoi il ne faut pas compter exclusivement sur les outils d'inforensique.

Le cours FOR585 est continuellement actualisé avec les derniers malwares, systèmes d'exploitation de smartphones, applications de tiers et systèmes de chiffrement. Ce cours intensif de six jours arme les stagiaires avec les connaissances inforensiques les plus récentes sur les dispositifs mobiles qu'ils pourront immédiatement appliquer dans leurs missions.

Les technologies des smartphones évoluent en permanence et la plupart des professionnels de l'inforensique connaissent mal les formats de données des différentes technologies. Passez à la vitesse supérieure : il est temps pour les gentils de se montrer rusé et pour les méchants de savoir que leurs scripts et leurs applications peuvent être utilisés contre eux !

« Ce que j'ai particulièrement apprécié dans le cours Advanced Smartphone Forensics, c'est l'apprentissage concret des technologies d'enquête inforensique, loin des approches classiques de type pointer-cliquer. »

- Brad Wardman,
PAYPAL

Public visé :

- Analystes inforensiques séniors
- Analystes spécialistes de l'exploitation des médias
- Professionnels de la cybersécurité
- Équipes de réponse aux incidents
- Représentants des forces de l'ordre, agents fédéraux et enquêteurs
- Chargés d'audit informatique
- Stagiaires ayant suivi les cours SANS SEC575, FOR500 (anciennement FOR408), FOR508, FOR518 et FOR572 qui souhaitent passer à la vitesse supérieure

Vous apprendrez à...

- Sélectionner les outils, techniques et procédures d'inforensique les plus efficaces, et mener une analyse critique des données d'un smartphone
- Reconstruire des événements relatifs à une infraction en utilisant les informations des smartphones, notamment le développement chronologique et l'analyse des liens (par exemple, qui communique avec qui, où et comment)
- Comprendre comment les systèmes de fichiers d'un smartphone enregistrent les données, comment elles se distinguent et comment les preuves sont conservées sur chaque dispositif
- Interpréter les systèmes de fichiers sur des smartphones et localiser les informations qui ne sont généralement pas accessibles aux utilisateurs
- Repérer comment les preuves sont arrivées sur l'appareil mobile. Lorsque vous saurez dire si les données ont été créées par l'utilisateur, vous ne commettrez plus l'erreur de signaler des faux positifs obtenus par le biais des outils
- Incorporer des techniques de décodage manuelles pour récupérer des données enregistrées sur des smartphones et dispositifs mobiles et supprimées

CERT. GIAC : GASF
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GASF

FOR 610

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Apprenez à examiner les malwares sous toutes les coutures ! Particulièrement apprécié, ce cours aborde en profondeur les outils et techniques d'analyse de malwares. FOR610 permet aux enquêteurs spécialisés en inforensique, aux chargés de réponse aux incidents, aux ingénieurs sécurité et aux administrateurs informatiques de développer des compétences pratiques nécessaires pour analyser les programmes malveillants qui ciblent et infectent les systèmes Windows.

Connaître le potentiel des malwares est un enjeu majeur pour les organisations : sans les renseignements qui en découlent, elles sont dans l'impossibilité de réagir aux incidents de cybersécurité et ne peuvent pas non plus renforcer leurs défenses. Ce cours vous permet d'acquérir des bases solides en rétro-ingénierie appliquée aux logiciels malveillants en vous familiarisant avec divers utilitaires de supervision système et réseau, un désassembleur, un débogueur et de nombreux autres outils disponibles gratuitement.

Vous apprendrez d'abord à analyser les malwares d'une façon autrement plus efficace qu'en vous fiant aux découvertes des outils d'analyse automatisée. Vous verrez ensuite comment mettre en place un laboratoire flexible pour examiner le fonctionnement interne d'un logiciel malveillant, puis comment vous servir de ce labo pour analyser des échantillons de malwares réels et en découvrir les caractéristiques. Ce cours abordera également les manières de rediriger et d'intercepter le trafic réseau dans le labo pour explorer les capacités du spécimen en interagissant avec le programme malveillant.

Les malwares sont souvent intégrés à des fichiers ou des programmes en apparence inoffensifs de façon à échapper aux analyses, mais cette formation vous enseignera à décompresser les fichiers exécutables. Vous apprendrez à supprimer ces programmes de la mémoire grâce à un débogueur et à d'autres outils spécialisés, et vous verrez comment reconstruire la structure des fichiers pour contourner la protection qui entoure le malware. Vous apprendrez également à disséquer les malwares qui affichent des fonctionnalités de rootkit pour masquer leur présence dans un système : ce cours aborde précisément à cet effet l'analyse de code et des approches d'inforensique de mémoire.

FOR610 enseigne également à faire face aux logiciels malveillants qui cherchent à se protéger des analyses. Vous verrez comment reconnaître et contourner les mesures courantes d'autodéfense, telles que l'injection de code, l'évasion de sandbox, le détournement de flux, etc.

Les exercices pratiques en labo prennent une importance particulière dans cette formation. Ils vous permettront ainsi d'appliquer les techniques d'analyse de malware en examinant des logiciels malveillants de manière contrôlée et systématique. En réalisant ces exercices, vous étudierez les schémas comportementaux des spécimens et vous examinerez des portions clés de leurs codes. Dans le cadre de ces activités, il vous sera remis des machines virtuelles Windows et Linux prémontées et dotées des outils nécessaires pour examiner les malwares étudiés et interagir avec eux.

« Ce cours nous permet d'appréhender de façon très réaliste les problèmes complexes liés à l'analyse des logiciels malveillants. »

- Markus Jeckeln,
LUFTHANSA

Public visé :

- Personnes ayant traité des incidents impliquant des malwares et qui souhaitent comprendre les principaux aspects des programmes malveillants
- Techniciens ayant expérimenté de manière informelle des aspects de l'analyse des malwares avant le cours et cherchant à formaliser et étendre leur expertise dans ce domaine
- Analystes en inforensique et responsables IT cherchant à élargir leurs compétences pour assurer un rôle central dans le processus de réponse aux incidents

Vous apprendrez à...

- Construire un environnement de laboratoire isolé et contrôlé pour analyser le code et le comportement des programmes malveillants
- Utiliser des outils de supervision du réseau et du système pour examiner la manière dont les malwares interagissent avec le système de fichiers, le registre, le réseau et d'autres processus dans un environnement Windows
- Découvrir et analyser les composants malveillants JavaScript et VBScript des pages web, souvent utilisés par les kits d'exploitation pour les attaques *drive-by*
- Contrôler les aspects pertinents du comportement du programme malveillant grâce à l'interception du trafic réseau et au *code patching* pour effectuer une analyse efficace des malwares
- Utiliser un désassembleur et un débogueur pour examiner le fonctionnement interne des exécutables Windows malveillants
- Contourner différents outils de compression d'exécutables ou *packers* et d'autres mécanismes défensifs conçus par des auteurs de malwares pour égarer, embarrasser et ralentir l'analyste

CERT. GIAC :GREM
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GREM

La protection de votre organisation passe obligatoirement par une sensibilité à la sécurité.

Quelles sont vos actions de sensibilisation ?

SANS EMEA
SECURITY AWARENESS

Expertise

La sensibilisation à la sécurité SANS Security Awareness a été élaborée par des professionnels reconnus du monde de la cybersécurité. Des experts en sciences cognitives, en conception créative et en sensibilisation à la sécurité créent des modules de formation visant à protéger les organisations et à faire évoluer les comportements humains.

Pertinence

Notre contenu est constamment actualisé pour répondre aux menaces actuelles. Disponibles en plusieurs formats et accompagnées de nombreux supports complémentaires, les formations touchent des publics divers et variés, quelle que soit la langue.

Souplesse

Les modules sont conçus pour couvrir les menaces importantes. Ils se déclinent en un socle fondamental et en formations avancées dans un souci d'exhaustivité.

Formations de premier ordre dispensées par les meilleurs experts, disponibles dans des formats variés et adaptées à un public international. Suivez les modules de formation SANS Security Awareness pour apprendre à gérer le risque humain.

Pour en savoir plus :
sans.org/security-awareness

MGT 414

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

SANS Training Program for CISSP® Certification

Le cours de préparation accélérée SANS MGT414: SANS Training Program for CISSP® Certification accompagne les candidats dans la préparation de la certification en sécurité des systèmes d'information CISSP®.

La formation porte exclusivement sur la révision des 8 principaux domaines de connaissance identifiés par (ISC)² et sur lesquels porte l'examen CISSP®. Chaque domaine de connaissance est décomposé pour étudier la relation des composants entre eux et avec d'autres domaines de la sécurité des systèmes d'information.

À l'issue de la formation, les stagiaires auront acquis :

- Une connaissance fine des 8 domaines de connaissance
- Les capacités d'analyse indispensables pour réussir l'examen CISSP®
- Les capacités techniques nécessaires pour comprendre les questions
- Les informations fondamentales pour obtenir la certification CISSP® (Certified Information Systems Security Professional)

Obtenir votre certification CISSP®, c'est :

- Remplir les critères minimaux en termes d'expérience professionnelle
- Remplir l'Accord candidat
- L'examen de votre CV
- Répondre aux 250 questions à choix multiple du CISSP® et obtenir la note de 700 points ou plus
- Soumettre un Formulaire de validation dûment complété
- Passer l'audit périodique des crédits de formation (CPE) pour conserver la certification

> **« C'est la meilleure formation sur la sécurité que j'aie jamais suivie, avec un dosage parfait des informations pour chaque domaine. »**
> - Tony Barnes,
> *UNITED STATES SUGAR CORP*

CERT. GIAC : GISP
46 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GISP

Public visé :

- Professionnels de la sécurité qui cherchent à connaître les concepts couverts par l'examen CISSP® comme définis par (ISC)²
- Responsables qui cherchent à connaître les domaines critiques de la sécurité de l'information
- Administrateurs système, sécurité et réseau désireux d'appliquer les huit domaines de connaissance à leurs activités
- Professionnels et responsables sécurité qui cherchent des moyens pratiques pour appliquer les huit domaines de connaissances

Vous apprendrez à...

- Comprendre les huit domaines de connaissance compris dans l'examen CISSP®
- Analyser les questions posées au cours de l'examen et sélectionner les bonnes réponses
- Appliquer les connaissances et les compétences de test acquises pour réussir l'examen CISSP®
- Comprendre et expliquer tous les concepts couverts par les huit domaines de connaissance
- Appliquer les compétences acquises dans les huit domaines pour résoudre des problèmes de sécurité dès votre retour sur le terrain

MGT 512

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

CINQ JOURS • ORDINATEUR PORTABLE CONSEILLÉ

Security Leadership Essentials For Managers

Les responsables de la sécurité doivent allier connaissances techniques et compétences en gestion pour gagner le respect et comprendre les tâches de l'équipe technique, et aussi pour planifier et gérer correctement les projets et les initiatives de sécurité. Leur mission est cruciale et exige des connaissances considérables en sécurité.

Ce cours vous donne les clés de l'efficacité et vous permet de vous mettre rapidement à niveau sur les questions et la terminologie liées à la sécurité des systèmes d'information. Au-delà des connaissances théoriques, vous apprendrez à gérer la sécurité.

Pour vous aider à atteindre cet objectif, le cours MGT512 couvre un large panel de sujets liés à la pile de sécurité. Contrôle des données, des réseaux, des hôtes, des applications et des utilisateurs sont traités en même temps que les points de gestion qui touchent au cycle de vie de la sécurité globale. Les contrôles de la gouvernance et techniques axés sur la protection, la détection et la réponse aux questions de sécurité sont également abordés.

Ce cours vous prépare à :

- Comprendre les différents référentiels de cybersécurité
- Comprendre et analyser le risque
- Comprendre les avantages et les inconvénients des différents rapports hiérarchiques
- Gérer le personnel technique
- Élaborer un programme de gestion des vulnérabilités
- Sécuriser les workflows DevOps évolués
- Exploiter de manière stratégique un SIEM
- Faire évoluer les comportements et développer une culture de la sécurité
- Gérer de manière efficace les projets de sécurité
- Favoriser les architectures de sécurité récentes et le cloud

Le cours MGT512 s'appuie sur des études de cas, des discussions de groupe, des exercices en équipe et des jeux en classe pour aider les stagiaires à assimiler des sujets à la fois techniques et de gestion.

> **« Ce cours a été d'une aide précieuse pour acquérir les compétences de base générales et techniques solides indispensables pour piloter une équipe efficace. »**
> - Richard Ward
> *REA GROUP*

Public visé :

- Nouveaux officiers de sécurité des systèmes d'information
- Nouveaux responsables sécurité qui souhaitent acquérir un socle de sécurité pour diriger et constituer des équipes
- Administrateurs experts techniques avec de nouvelles responsabilités d'encadrement
- Dirigeants qui ont besoin de comprendre le jargon technique
- Dirigeants qui ont besoin d'appréhender la sécurité du point de vue de la gestion

Vous apprendrez à...

- Comprendre les différents référentiels de cybersécurité
- Comprendre et analyser le risque
- Comprendre les avantages et les inconvénients des différents rapports hiérarchiques
- Gérer le personnel technique
- Élaborer un programme de gestion des vulnérabilités
- Sécuriser les workflows DevOps évolués
- Exploiter de manière stratégique un SIEM
- Faire évoluer les comportements et développer une culture de la sécurité
- Gérer de manière efficace les projets de sécurité
- Favoriser les architectures de sécurité récentes et le cloud

CERT. GIAC : GSLC
30 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GSLC

MGT 514

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

Security Strategic Planning, Policy, and Leadership

Les professionnels de la sécurité ont vu l'environnement évoluer. La cybersécurité est maintenant plus vitale et plus pertinente que jamais pour la croissance de votre organisation. En conséquence, les équipes de sécurité des systèmes d'information ont plus de visibilité, plus de budgets et plus d'opportunités. Mais cette responsabilité élargie est assortie de contrôles minutieux.

Ce cours enseigne aux professionnels de la sécurité à maîtriser trois éléments :

Développer des plans stratégiques

La planification stratégique est difficile pour les professionnels de l'informatique et de la sécurité informatique, car vous consacrez beaucoup de votre temps à répondre et à réagir. Il est rare que vous ayez l'opportunité de pratiquer avant d'être promus à un poste supérieur et lorsque cela arrive, vous ne disposez pas des compétences indispensables pour intégrer le peloton. Apprenez à développer des plans stratégiques qui trouveront un écho particulier auprès des responsables IT et des autres acteurs.

Créer une politique de sécurité de l'information efficace

Une politique est l'occasion d'exprimer les attentes à l'égard des effectifs, de fixer les limites d'un comportement acceptable et d'habiliter les personnes à faire ce qu'elles devraient faire. Tout le monde peut faire une erreur. Avez-vous déjà été confronté à une politique à laquelle votre réponse était : « Jamais je ne ferai cela » ? La politique d'une organisation doit être alignée sur sa culture. Nous décomposerons les étapes du développement de la politique afin que vous puissiez développer et évaluer une politique qui vous permettra de guider votre organisation.

Développer des compétences en gestion et en leadership

Être un leader s'apprend. La capacité à diriger doit être exercée et développée pour mieux assurer la réussite de l'organisation. Un leadership fort se manifeste principalement par un dévouement désintéressé envers l'organisation et le personnel, des efforts inlassables pour donner l'exemple et la vision pour voir et utiliser efficacement les ressources disponibles afin d'atteindre l'objectif final. Une direction efficace consiste à persuader les membres de l'équipe d'atteindre leurs objectifs tout en éliminant les obstacles et en maintenant le bien-être de l'équipe à l'appui de la mission de l'organisation. Apprenez à utiliser les outils et les structures de gestion pour mieux diriger, inspirer et motiver vos équipes.

Comment se déroule le cours

Études de cas provenant de la Harvard Business School, exercices en équipe, discussions axées sur des exemples réels : les stagiaires participent à des activités qu'ils pourront ensuite mettre en œuvre avec leur propre équipe de retour sur le terrain. La nouvelle génération de responsables de la sécurité doit combler le fossé entre le personnel de sécurité et les hauts dirigeants en planifiant stratégiquement la façon de construire et de gérer des programmes de sécurité efficaces. Après avoir suivi ce cours, vous aurez les compétences fondamentales pour créer des plans stratégiques qui protégeront votre entreprise, permettront des innovations clés et vous rapprocheront efficacement de vos partenaires commerciaux.

Public visé :

- RSSI
- Officiers de sécurité des systèmes d'information
- Directeurs sécurité
- Responsables sécurité
- Futurs chefs sécurité
- Personnel de sécurité ayant des responsabilités d'équipe ou de gestion

Vous apprendrez à...

- Élaborer des plans stratégiques de sécurité en fonction des objectifs opérationnels et organisationnels
- Développer et évaluer la politique de sécurité de l'information
- Utiliser des techniques de gestion et de leadership pour motiver et inspirer vos équipes

CERT. GIAC : GSTRT
30 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GSTRT

MGT 516

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

CINQ JOURS • ORDINATEUR PORTABLE CONSEILLÉ

Managing Security Vulnerabilities: Enterprise and Cloud NOUVEAU

Partout se cachent des vulnérabilités. Chaque jour révèle de nouvelles faiblesses dans nos systèmes et logiciels, avec en corollaire une augmentation en nombre et en gravité des attaques réussies.

Les vulnérabilités d'une organisation, quelle que soit sa taille, représentent un défi à gérer. Et dans les environnements d'entreprise, l'échelle et la variété viennent ajouter au fardeau des équipes de sécurité informatique et des opérations. Si on rajoute le cloud et la vitesse toujours plus grande à laquelle les organisations doivent fournir systèmes, applications et fonctionnalités à leurs clients internes comme externes, la sécurité semble un objectif inaccessible.

Cette formation explique les raisons pour lesquelles les organisations se débattent encore aujourd'hui avec la gestion des vulnérabilités et montre aux stagiaires les moyens de résoudre ces questions. Comment bien gérer les actifs ? Comment analyser et hiérarchiser les vulnérabilités ? Quels sont les rapports les plus efficaces ? Comment gérer les vulnérabilités de nos applications ? Comment les traiter ? Nous étudierons les réponses à ces questions et leur évolution selon que nous nous intéressons au cloud ou mettons en œuvre un cloud privé ou DevOps dans nos organisations. Comment donner un peu d'éclat à la gestion des vulnérabilités et mobiliser tout le monde ? Ce sont quelques-uns des thèmes importants que nous traitons dans ce cours.

L'objectif principal est de vous aider à réussir là où beaucoup échouent et de vous présenter des solutions aux problèmes que beaucoup doivent ou devront affronter. Que votre programme de gestion des vulnérabilités soit bien établi ou en gestation, cette formation vous aide à le faire mûrir et à repenser la gestion des vulnérabilités.

La bonne compréhension des problématiques courantes et de leurs solutions vous prépare d'autant mieux à répondre à vos défis actuels ou futurs et à décider de ce qui convient le mieux à votre organisation. Par des discussions en groupe et d'autres exercices, vous apprenez des techniques spécifiques d'analyse et de restitution qui viennent alimenter la discussion avec vos pairs sur les problèmes que vous rencontrez les uns les autres et les solutions à apporter.

La formation s'appuie sur le modèle PIACT (Préparer, Identifier, Analyser, Communiquer et Traiter) :

- Préparer : définir, élaborer et améliorer en permanence le programme.
- Identifier : repérer les vulnérabilités présentes dans nos environnements d'exploitation.
- Analyser : analyser et hiérarchiser les vulnérabilités et les autres indicateurs du programme pour apporter une assistance et des conseils pertinents aux parties prenantes et aux participants au programme.
- Communiquer : présenter les conclusions issues de l'analyse de manière pertinente et efficace pour chaque type de partie prenante.
- Traiter : mettre en œuvre, tester et surveiller les solutions apportées aux vulnérabilités, aux groupes de vulnérabilités et aux problèmes plus larges que le programme a identifiés.

Puisque nos environnements adoptent les services cloud et s'intègrent toujours plus à eux, nous examinerons aussi bien les environnements cloud que non cloud tout au long du cours. Nous relèverons notamment les outils, processus et procédures valables dans les deux environnements et présenterons les tendances nouvelles et émergentes.

Dans un exercice qui clôture la dernière partie du cours MGT516, un scénario pratique inclut les deux types d'environnements, entreprise et cloud. Les stagiaires analysent et abordent les meilleures façons de mettre en œuvre et maintenir un programme de gestion des vulnérabilités en exploitant des connaissances acquises pendant la formation.

30 CRÉDITS CPE/CMU

Public visé :

- RSSI
- Directeurs, responsables et officiers de sécurité des systèmes d'information
- Architectes, analystes et consultants en sécurité de l'information
- Futurs responsables en sécurité de l'information
- Professionnels en gestion des risques
- Équipes de planification et opérationnelles de la continuité d'activité et de la reprise d'activité
- Responsables IT et auditeurs
- Chefs de projets IT
- Administrateurs réseau/système/IT
- Responsables des opérations
- Administrateurs et gestionnaires de services cloud
- Gestionnaires des risques et de la sécurité cloud
- Intégrateurs, développeurs et intermédiaires (***broker***) cloud
- Professionnels de la sécurité IT chargés de la gestion des vulnérabilités de l'environnement entreprise ou cloud
- Professionnels de l'informatique du service public chargés de la gestion des vulnérabilités de l'environnement entreprise ou cloud
- Professionnels de la sécurité et des systèmes informatiques en responsabilité (équipe ou gestion)
- Professionnels de la sécurité et des systèmes informatiques qui utilisent des services cloud ou l'envisagent

Vous apprendrez à...

- Créer, mettre en œuvre ou améliorer votre programme de gestion des vulnérabilités
- Mettre en place un environnement d'entreprise et cloud défendable et sûr
- Inventorier avec précision et pertinence les actifs informatiques de l'entreprise et du cloud
- Identifier les vulnérabilités présentes et comprendre le degré de gravité de chacune
- Hiérarchiser les vulnérabilités pour les traiter

MGT 525

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE NON REQUIS

IT Project Management, Effective Communication, and PMP® Exam Prep

Ce cours est proposé par SANS Institute en qualité d'établissement de formation Registered Education Provider (R.E.P.) certifié par le PMI®. Les organismes R.E.P. apportent la formation nécessaire pour obtenir et maintenir la certification PMP® (Project Management Professional) entre autres qualifications professionnelles. PMP® est une marque déposée du Project Management Institute, Inc.

Ce cours a été récemment actualisé pour vous préparer pleinement à l'examen PMP® modifié en 2016. Au cours de cette formation, vous apprendrez à améliorer votre méthodologie de planification de projet et l'ordonnancement des tâches de projet pour tirer le meilleur parti de vos ressources informatiques essentielles. Nous étudierons des cas de projets où les services de technologie de l'information sont des livrables. Le cours MGT525 suit la structure élémentaire de gestion de projet du Guide PMBOK® - Cinquième édition et fournit des techniques spécifiques pour les initiatives d'assurance de l'information. Tout au long de la semaine, nous aborderons tous les aspects de la gestion de projets informatiques, depuis le démarrage et la planification, en passant par la gestion des coûts, des délais et de la qualité en cours de projet, jusqu'à l'intégration, la clôture et les communications en fin de projet. Un exemplaire en anglais du Guide PMBOK® - Cinquième édition est fourni à tous les participants. Vous pouvez vous appuyer sur le Guide PMBOK®, le matériel de cours et les connaissances acquises en classe pour vous préparer à l'examen 2016 Project Management Professional (PMP)® et à l'examen GIAC Certified Project Manager.

Le processus de gestion de projet est divisé en groupes de processus principaux qui peuvent être appliqués à plusieurs domaines, quels que soient le projet et le secteur. Bien que notre objectif principal soit l'application au domaine de l'InfoSec, notre approche est transférable à tous les projets qui créent et entretiennent des services ainsi qu'au développement de produits en général. Nous couvrirons en détail comment le coût, les délais, la qualité et les risques affectent les services que nous fournissons. Nous aborderons également la gestion pratique des ressources humaines ainsi que la communication efficace et la résolution des conflits. Vous apprendrez à manier des outils spécifiques pour combler le fossé des communications entre les gestionnaires et le personnel technique.

> **« C'est vraiment l'un des meilleurs cours que j'aie jamais suivis. J'ai le sentiment d'avoir des milliers de choses à mettre en pratique maintenant. »**
> - Ryan Spencer,
> *REED ELSEVIER INC.*

GIAC CERT: GCPM
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GCPM

Public visé :

- Professionnels de la sécurité intéressés par la compréhension des concepts de gestion de projet informatique
- Gestionnaires qui veulent comprendre les points essentiels à la réussite des projets
- Personnes travaillant avec des contraintes de délais, de coûts et de qualité et sur des projets et applications sensibles au risque
- Toute personne souhaitant utiliser des techniques de communication efficaces et des méthodes éprouvées pour mieux communiquer avec les autres
- Toute personne occupant un poste clé ou principal d'ingénieur ou de concepteur travaillant régulièrement avec le personnel de gestion de projet
- Personnes souhaitant préparer l'examen Project Management Professional (PMP)®

Vous apprendrez à...

- Reconnaître les principaux mécanismes de défaillance liés aux projets informatiques et InfoSec, afin que vos projets puissent éviter les pièges courants
- Créer une charte de projet définissant la participation du sponsor du projet et des parties prenantes
- Documenter les exigences du projet et créer une matrice de traçabilité de ces exigences pour suivre les évolutions tout au long du cycle de vie du projet
- Définir clairement la portée d'un projet en matière de coûts, de calendrier et de livrables techniques
- Établir un plan de travail décomposé pour définir les ensembles de tâches, les livrables du projet et les critères d'acceptation
- Développer un calendrier détaillé du projet, incluant les tâches cruciales pour son avancement et les jalons
- Élaborer un budget détaillé du projet, incluant les bases de coûts et les mécanismes de suivi

AUD 507

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

Auditing & Monitoring Networks, Perimeters, and Systems

Réaliser des audits de sécurité informatique à l'échelle de l'entreprise peut être une tâche redoutable. Par quels systèmes commencer ? Comment évaluer les risques encourus par l'organisation en matière de systèmes d'information et de processus métier ? Quels paramètres d'un système doivent être vérifiés ? Existe-t-il un ensemble de procédés qui permettrait à un auditeur de se concentrer sur les processus métier plutôt que sur les paramètres de sécurité ? Comment en faire un processus de supervision continu ? Toutes ces questions et bien d'autres trouveront des réponses dans ce cours.

Le cours AUD507 apprend aux stagiaires à appliquer la prise de décisions axée sur les risques à l'audit de sécurité de l'entreprise.

Ce cours apporte une méthode basée sur les risques pour s'atteler à la tâche immense que représente la conception d'un programme de validation de la sécurité d'une entreprise. Initialement, les stagiaires explorent divers problèmes de haut niveau relatifs aux audits, ainsi que les bons procédés en matière d'audit en général. Ils entrent ensuite dans le vif du sujet en détaillant les contrôles clés nécessaires à la sécurité d'une entreprise. À partir d'exemples concrets, ils apprennent à vérifier ces contrôles de façon répétée et découvrent un panel de techniques de supervision continue et de validation automatique de la conformité. Ces mêmes cas leur permettent de maîtriser les meilleures techniques de communication des risques aux équipes de gestion et opérationnelle.

Les labos pratiques du cours AUD507 permettent d'exercer de nouvelles compétences de façon réaliste.

Chaque jour, les stagiaires peuvent tester les outils et techniques abordés pendant les cours. Les labos mettent en scène les défis de l'audit en entreprise et permettent aux stagiaires de s'approprier les différents moyens de les résoudre. Formés aux tests techniques, ils sont en mesure de développer les preuves nécessaires pour étayer leurs conclusions et leurs recommandations. L'apprentissage théorique des outils et des techniques est systématiquement accompagnépar une pratique efficace : les stagiaires sont parés pour mesurer et signaler les risques dans leur organisation.

« J'ai apprécié ce cours de A à Z et je suis paré pour réaliser un audit complet.Je suis également parfaitement formé aux opérations pour améliorer la posture de sécurité réseau. »
- Srinath Kannan,
ACCENTURE

Public visé :
- Auditeurs qui cherchent à identifier les contrôles clés des systèmes informatiques
- Auditeurs professionnels qui veulent approfondir des détails techniques pour effectuer un audit
- Dirigeants responsables du travail effectué par une équipe de sécurité ou d'audit
- Professionnels de la sécurité qui se voient attribuer de nouvelles responsabilités d'audit
- Administrateurs système et réseau qui cherchent à mieux comprendre ce que recherche un auditeur, sa logique, et qui veulent se préparer pour un audit
- Administrateurs système et réseau qui cherchent à mettre en place des systèmes élaborés de détection et de gestion des modifications pour l'entreprise

Vous apprendrez à...
- Comprendre les différents types de contrôles (par exemple, techniques et non techniques) essentiels pour un audit réussi
- Bien apprécier les risques relatifs aux réseaux pour identifier les vulnérabilités et déterminer les priorités d'audit
- Établir des normes sécuritaires de référence pour les ordinateurs et les réseaux, qui serviront de cadre de référence de l'audit
- Effectuer un audit de périmètre et de réseau à l'aide d'un processus en sept étapes
- Contrôler les pare-feu pour valider le bon fonctionnement des paramètres et des règles tels qu'ils ont été conçus, par exemple en bloquant le trafic au besoin
- Utiliser des outils d'évaluation des vulnérabilités de façon efficace pour que les dirigeants aient en permanence les données leur permettant de prendre les mesures correctives et les décisions adaptées concernant le risque et les ressources

CERT. GIAC : GSNA
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GSNA

LEG 523

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

CINQ JOURS • ORDINATEUR PORTABLE NON REQUIS

Law of Data Security and Investigations

- Arrestation et inculpation de deux experts en tests d'intrusion de Coalfire en Iowa
- Confidentialité des données et sécurité des données dans le cadre du RGPD
- Invocation du secret professionnel de l'avocat pour assurer la confidentialité des tests de sécurité tels que les tests d'intrusion
- Une décision de justice montre comment améliorer une enquête officielle en recourant à l'intelligence artificielle
- Une formation unique en son genre et indispensable pour les délégués à la protection des données
- Élaboration d'un contrat pour inviter des responsables de réponse aux incidents externes – forces de l'ordre, agents contractuels, armée, agences de défense à l'échelle mondiale – afin d'apporter une assistance en cas de crise de cybersécurité

Intégrer les nouvelles lois sur la confidentialité, la découverte électronique et la sécurité des données crée un besoin urgent de professionnels capables de faire le lien entre les services juridique et informatique. SANS LEG523 est une formation professionnelle exclusive en matière d'analyse et d'utilisation des contrats, des politiques et des procédures de gestion des dossiers.

Le cours couvre le droit des affaires et des contrats, la législation en matière de fraude, de criminalité, de cybersécurité, de responsabilité et de politiques ; le tout articulé autour des enregistrements stockés et transmis électroniquement. Il enseigne aux enquêteurs comment préparer des rapports crédibles et défendables, qu'il s'agisse de cybercriminalité, d'inforensique, de réponse aux incidents, de problèmes relevant des ressources humaines ou d'autres enquêtes.

Cette formation progressive de cinq jours vise à renforcer votre capacité à aider votre entreprise (secteur public ou privé) à faire face aux hackers, botnets, malwares, phishing, fournisseurs négligents, fuites de données, espions industriels, employés malveillants ou peu coopératifs, ou à une mauvaise publicité liée à la sécurité informatique.

Les dernières mises à jour du cours abordent des sujets d'actualité tels que les conseils juridiques sur la confiscation et l'interrogation des appareils mobiles, la conservation des documents commerciaux liés au cloud computing et aux réseaux sociaux tels que Facebook et Twitter, ainsi que l'analyse des risques et des opportunités qui entourent la collecte de renseignement provenant de sources en libre accès et les réponses correspondantes.

Au fil des ans, ce cours sans équivalent a adopté une perspective de plus en plus globale et des professionnels venus du monde entier y participent. Par exemple, une avocate travaillant pour l'administration fiscale d'un pays africain a suivi ce cours, car la dématérialisation des déclarations, des preuves et des enquêtes a pris une place prépondérante dans l'exercice de ses fonctions. Des stagiaires étrangers assistent le formateur américain, et avocat, Benjamin Wright dans son travail de révision constante afin d'inclure toujours plus de contenus transnationaux.

« Excellent contenu, très pertinent, qui ouvre l'esprit. »
- S. Genna,
FACEBOOK

Public visé :
- Enquêteurs
- Professionnels de la sécurité et des systèmes d'information
- Avocats
- Juristes
- Auditeurs
- Comptables
- Gestionnaires de la technologie
- Fournisseurs
- Agents de conformité
- Forces de l'ordre
- Délégués à la protection des données
- Experts en tests d'intrusion
- Équipe de réponse aux incidents et cyberincidents

Vous apprendrez à...
- Mieux travailler avec vos collaborateurs chargés des décisions concernant le droit en matière de sécurité des données et des enquêtes
- Prendre des décisions avec discernement sur la façon de se conformer aux règlements en matière de technologie tant aux États-Unis que dans d'autres pays
- Évaluer le rôle et la signification des contrats pour la technologie, dont les services, les logiciels et l'externalisation
- Aider votre organisation à mieux expliquer sa conduite au public et aux autorités judiciaires
- Anticiper les risques juridiques en matière de technologie avant qu'ils ne soient hors de contrôle
- Mettre en œuvre des mesures pratiques pour faire face au risque juridique relatif à la technologie
- Expliquer de façon plus efficace aux dirigeants ce que votre entreprise doit faire pour se conformer à la loi sur la sécurité de l'information et la confidentialité
- Mieux évaluer les technologies, telles que les signatures numériques, pour être conforme avec la loi et les utiliser comme preuves
- Mieux utiliser les techniques de contrats électroniques pour obtenir de meilleures modalités

CERT. GIAC : GLEG
30 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GLEG

SANS Stay Sharp Training, pour affûter vos compétences rapidement

Formations de 1, 2 ou 3 jours à la cybersécurité | Live Online

Les événements SANS Stay Sharp – Live Online sont des stages courts conçus pour vous doter de compétences en cybersécurité applicables immédiatement. Novice à la recherche d'un point d'entrée dans le secteur ou professionnel aguerri désireux d'affûter des compétences particulières, la formation SANS Stay Sharp vous aide à atteindre vos objectifs.

« J'ai trouvé ce cours extrêmement utile. J'ai suivi d'autres cours ailleurs, mais dans cette formation, avec des labos et un formateur de haut vol, j'en ai appris plus en neuf heures qu'au cours des derniers mois. »
— Sid Palaparthi, Nokia

Formation ciblée à fort impact pour un coût maîtrisé : développez les compétences pratiques spécialisées en cybersécurité les plus demandées actuellement. Participez à une formation virtuelle en immersion et apprenez à défendre votre organisation contre les violations de sécurité et à prévenir des attaques futures.

« Avec SANS, je sais que je suis la meilleure formation à la sécurité de l'information du secteur, et c'est encore le cas avec SANS Live Online ! »
— Harold (Chip) Stockton, Global Payments, Inc.

Découvrez les prochains événements SANS Stay Sharp :
sans.org/cyber-security-training-events

SEC 488

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Cloud Security Essentials

Plus que jamais, les entreprises stockent des données sensibles dans le cloud et y déplacent des charges de travail stratégiques. Et elles font appel non pas à un, mais à plusieurs fournisseurs cloud : les études montrent que la plupart ont pris la décision stratégique de déployer plusieurs plateformes (Amazon Web Services, Azure, Google Cloud, etc.).

« La formation comme les exemples sont géniaux ! Les exercices pratiques en décuplent la valeur. »
- Michael Warthon, *WRPS*

Les organisations sont responsables de la sécurité de leurs données et de leurs applications critiques dans le cloud. En matière de coûts et de performances, les atouts d'une plateforme multicloud dans le développement d'applications métier, leur livraison rapide et l'analyse des données client peuvent rapidement se muer en désastre si les équipes sont mal formées à la sécurisation de l'environnement cloud et à l'analyse et aux investigations des inévitables atteintes à la sécurité.

Le cours SANS SEC488:Cloud Security Essentials vous prépare à conseiller et à communiquer à l'oral sur un grand nombre de sujets. Vous pourrez ensuite accompagner votre organisation dans l'analyse des enjeux de sécurité, mais aussi des opportunités présents dans les services cloud. Les différents environnements cloud se ressemblent par certains côtés et divergent par d'autres, comme les langues entre elles. Le cours SEC488 traite des principaux fournisseurs de services cloud (CSP).

Nous commencerons par montrer l'évolution de vos opérations quotidiennes en fonction de celle à venir du cloud. On s'attend en effet à l'évolution des modèles de responsabilité vers les différents modèles des fournisseurs cloud : services d'infrastructure cloud (IaaS), de plateforme à la demande (PaaS) et de logiciel à la demande (SaaS). Nous poursuivrons avec la sécurisation du cloud, la gestion du risque et les réponses aux problèmes susceptibles de survenir pour atteindre un niveau donné de garantie de sécurité.

À nouvelles technologies, nouveaux risques. À l'issue de ce cours, vous serez armé pour appliquer les contrôles de sécurité appropriés dans le cloud, en vous appuyant sur l'automatisation pour « surveiller ce que vous attendez ». Les fournisseurs de solutions cloud matures ont développé des services de sécurité pour accompagner un usage plus sécurisé des produits chez leurs clients, mais il n'y a pas de panacée. Ce cours tire des leçons du monde réel en s'appuyant sur les services de sécurité des CSP et des outils open source. Chaque jour, les stagiaires consolident leurs acquis par des exercices pratiques. Couche par couche, nous ajoutons des contrôles de sécurité pour arriver à une architecture de sécurité fonctionnelle en cloud à la fin de la semaine.

SEC488 renforce l'apprentissage via des labos quotidiens, tous conçus pour transmettre des compétences pratiques applicables dès le retour dans l'entreprise. Ces labos ne fournissent pas seulement une liste d'instructions, mais permettent aux stagiaires de comprendre pourquoi ces compétences sont importantes et d'appréhender le fonctionnement des différentes technologies.

30 CRÉDITS CPE/CMU

Vous apprendrez à...

- Identifier les risques et la propriété du contrôle des risques d'après les modèles de déploiement et de fourniture de service des produits proposés par les fournisseurs de services cloud
- Évaluer le sérieux des fournisseurs cloud d'après leur documentation de sécurité, les caractéristiques de leurs services, les attestations de tiers et leur position dans l'écosystème cloud global
- Créer des comptes et utiliser les services des principaux fournisseurs cloud ; être à l'aise avec le principe du libre service du cloud public (recherche de documentation, didacticiels, tarifs, fonctions de sécurité)
- Exposer les implications d'une stratégie multicloud en termes d'activité et de sécurité
- Sécuriser l'accès aux consoles utilisées pour accéder aux environnements des fournisseurs cloud
- Utiliser les interfaces de ligne de commande pour interroger les ressources et les identités dans l'environnement cloud
- Utiliser le durcissement des tests de performance, de l'application des correctifs et de la gestion de la configuration pour atteindre et conserver un état de sécurité maximale pour l'environnement cloud
- Évaluer les services de journalisation des différents fournisseurs de cloud et utiliser les journaux pour déterminer la responsabilité des événements qui se produisent dans l'environnement cloud
- Implémenter, configurer et sécuriser l'authentification SSH par certificat sur les machines virtuelles qui s'exécutent dans le cloud
- Configurer l'interface de ligne de commande et protéger les clés d'accès pour minimiser le risque de compromission des informations d'identification
- Utiliser des scripts Bash et Python simples pour automatiser des tâches dans le cloud

SEC 522

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Defending Web Applications Security Essentials

Le cours à suivre pour défendre vos applications Web !

Les volumes et la sensibilité toujours plus grands des données confiées aux applications web imposent aux défenseurs de se former à leur sécurisation. Les défenses classiques des réseaux, telles que les pare-feu, sont impuissantes à protéger les applications web. Partant des 10 grands risques de la liste de l'OWASP, le cours SEC522 vous aide à mieux comprendre les vulnérabilités des applications web afin de protéger correctement les actifs web de votre organisation.

Les discussions portent sur les stratégies de réduction des risques selon trois axes, infrastructure, architecture et programmation, mais aussi sur des applications web éprouvées. Le test de vulnérabilité est également abordé pour que les stagiaires puissent tester leurs propres applications par rapport aux failles analysées en classe.

Pour le plus grand bénéfice du plus grand nombre, les notions étudiées s'appliquent quel que soit le langage de programmation. Le cours est axé sur les stratégies de sécurité, plutôt que sur l'implémentation dans le code.

Le cours SEC522: Defending Web Applications Security Essentials est conçu pour quiconque assure l'implémentation, la gestion et la protection d'applications web. Il convient particulièrement aux analystes sécurité des applications, aux développeurs, aux architectes d'applications, aux experts en test d'intrusion, aux auditeurs qui aspirent à émettre des recommandations de prévention des problèmes de sécurité web, et aux professionnels de la sécurité des infrastructures qui cherchent à mieux défendre leurs applications web.

Le cours aborde aussi d'autres thématiques que ses concepteurs ont jugées importantes dans leur pratique quotidienne du développement d'applications web, notamment :

- La sécurité des infrastructures
- La configuration des serveurs
- Les mécanismes d'authentification
- La configuration de la langue de l'application
- Le code applicatif vulnérable notamment aux injections SQL et au XSS
- La vulnérabilité CSRF
- Le contournement d'authentification
- Les services web et les failles associées
- Le Web 2.0 et son utilisation des services web
- Les langages et injections XPATH et XQUERY
- Les failles de logique métier
- Les en-têtes HTTP qui jouent un rôle protecteur

> **« La formation comme les exemples sont géniaux ! Les exercices pratiques en décuplent la valeur. »**
> - Michael Warthon, *WRPS*

Ce cours s'appuie largement sur des exercices pratiques et se termine par un grand exercice défensif qui renforce les connaissances acquises tout au long de la semaine.

Public visé :

- Développeurs d'application
- Analystes ou responsables de la sécurité des applications
- Architectes d'applications
- Experts en tests d'intrusion curieux des stratégies défensives
- Professionnels de la sécurité curieux d'en savoir plus sur la sécurité des applications web
- Auditeurs qui doivent comprendre les mécanismes défensifs des applications web
- Personnel d'organisations certifiées PCI qui doit se former au respect des normes PCI

Vous apprendrez à...

- Comprendre les risques majeurs et les vulnérabilités courantes des applications web par des exemples concrets
- Atténuer les vulnérabilités courantes des applications web par des techniques de codage, des composants logiciels, la configuration et l'architecture défensive
- Comprendre les bonnes pratiques dans différents aspects de la sécurité des applications web (authentification, contrôle d'accès, validation de la saisie)
- Remplir l'obligation de formation prescrite par les normes de sécurité de l'industrie des cartes de paiement (PCI DSS 6.5)
- Déployer et consommer des services web (SOAP et REST) de façon sûre
- Déployer en amont des mécanismes défensifs de pointe, tels que les en-têtes de réponse défensifs HTTP et la stratégie de sécurité du contenu (*Content Security Policy*) pour sécuriser les applications web
- Déployer un programme de sécurité des applications web de façon stratégique dans un vaste environnement
- Incorporer des technologies web avancées, telles que HTML5 et les requêtes *cross-domain* AJAX d'une façon sûre et sécurisée

CERT. GIAC : GWEB
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GWEB

SEC 540

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

Cloud Security and DevOps Automation

SEC540 propose aux développeurs, aux opérationnels et aux professionnels de la sécurité une méthodologie pour concevoir et livrer des logiciels et infrastructures sécurisés à l'aide de DevOps et des services cloud. Les stagiaires explorent les principes, les pratiques et les outils DevOps et découvrent comment améliorer la fiabilité, l'intégrité et la sécurité des applications sur site et cloud.

SEC540 s'intéresse à la méthodologie Secure DevOps et à sa mise en œuvre en s'appuyant sur les enseignements tirés de programmes de sécurité DevOps. À l'aide d'outils open source courants comme Jenkins, GitLab, Puppet, Vault et Grafana, vous acquerrez une expérience pratique d'automatisation de la gestion de la configuration (infrastructure programmable ou *Infrastructure as Code*), de l'intégration continue (CI), la livraison continue (CD), de l'infrastructure cloud, de la conteneurisation, de la microsegmentation, de l'informatique sans serveur (FaaS, *Function-as-a-Service*), de la conformité automatisée (conformité inscrite dans le code ou *Compliance as Code*) et de la supervision continue.

Les exercices en laboratoire commencent par un projet CI/CD sur site qui, de manière automatique, conçoit, teste et déploie des infrastructures et des applications conteneurisées. Les stagiaires s'appuient sur la chaîne d'outils Secure DevOps pour réaliser une série de labos de sécurisation de projets CI/CD avec des outils, protocoles et techniques de sécurité variés. Après avoir posé les bases DevSecOps, les stagiaires mettent leurs compétences à contribution pour le déploiement et la gestion de l'infrastructure cloud en conditions réelles. Des exercices pratiques les entraînent à déployer des charges de travail conteneurisées dans le cloud, à intégrer la gestion de la configuration sur site avec Puppet, et à gérer les secrets avec HashiCorp Vault et Cloud Key Management Service (KMS). Les stagiaires analysent et corrigent les vulnérabilités de l'infrastructure cloud, mènent des analyses de vulnérabilité des applications hébergées en cloud, et défendent les microservices à l'aide d'outils comme les passerelles d'API et le FaaS. La supervision de l'infrastructure s'appuie sur des outils de sécurisation du cloud notamment les services de pare-feu d'applications Web (WAF) pilotés par le code, l'audit continu avec CloudMapper, et la supervision continue avec Cloud Custodian.

Un mot des concepteurs

« DevOps et le cloud révolutionnent la conception, l'élaboration, le déploiement et l'opération des systèmes en ligne dans les organisations. Les grands acteurs comme Amazon, Etsy et Netflix arrivent à déployer des centaines voire des milliers de modifications chaque jour : ils apprennent, s'améliorent et se développent en permanence, laissant la concurrence loin derrière eux. Nés chez les licornes du web et les prestataires cloud, DevOps et le cloud tracent leur chemin vers les entreprises.

Les approches traditionnelles de la sécurité ne peuvent pas ne serait-ce que se rapprocher de ce rythme de changement accéléré. Les équipes de la conception et de l'opérationnel qui ont fait tomber les « murs de la confusion » dans leurs organisations exploitent de plus en plus les nouveaux moyens d'automatiser, notamment l'infrastructure programmable (IaC), la livraison et le déploiement continus, les microservices, les conteneurs, et les plateformes de services cloud. La question qui se pose est : peut-on valoriser davantage les outils et l'automatisation pour mieux sécuriser les systèmes ?

Dans un monde DevOps et cloud, il faut réinventer la sécurité. »

— Ben Allen, Jim Bird, Eric Johnson et Frank Kim

Vous apprendrez à...

- Élaborer un workflow Secure DevOps dans votre organisation
- Créer des tâches de sécurité automatisées dans des systèmes d'intégration et de livraison continues (CI/CD)
- Configurer et exécuter des analyses depuis la chaîne d'outils Secure DevOps
- Mener des audits de sécurité sur l'infrastructure cloud à la recherche des erreurs de configuration sources de failles
- Gérer les secrets en sécurité grâce aux outils de gestion des secrets hébergés sur le cloud et sur site
- Auditer les architectures de microservices à la recherche de vulnérabilités dans les appliances de passerelle API et sans serveur et dans les conteneurs
- Exploiter l'automatisation cloud pour appliquer les correctifs et déployer les logiciels automatiquement sans interruption de service
- Construire des fonctions sans serveur pour superviser, détecter et défendre activement les services et configurations cloud

CERT. GIAC : GCSA
38 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GWEB

SEC 545

LIVE ONLINE | TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

Cloud Security Architecture and Operations

À l'heure où toujours plus d'organisations transfèrent données et infrastructure vers le cloud, la sécurité s'impose comme une priorité majeure. Les équipes opérationnelles et de développement trouvent de nouveaux usages pour les services cloud ; et les dirigeants cherchent à en tirer des économies, à acquérir de nouvelles capacités et à gagner en efficacité opérationnelle. Mais la sécurité de l'information sera-t-elle un talon d'Achille ? De nombreux fournisseurs cloud ne livrent pas d'informations détaillées sur le contrôle de leur environnement interne, et un certain nombre de contrôles de sécurité courants utilisés en interne ne se répercutent pas directement sur le cloud public.

Le cours SEC545: Cloud Security Architecture and Operations, abordera ces problèmes un par un. Nous commencerons par une brève introduction aux fondamentaux de la sécurité dans le cloud, puis nous couvrirons les concepts critiques de la politique et de la gouvernance du cloud pour les professionnels de la sécurité. Le reste de la première journée et le jour suivant seront consacrés aux principes de la sécurité technique et des contrôles pour les principaux types de clouds (SaaS, PaaS et IaaS). Nous explorerons les référentiels de la Cloud Security Alliance pour les zones de contrôle du cloud, avant de nous immerger dans l'évaluation des risques pour les services cloud, en examinant spécifiquement les domaines techniques essentiels.

Nous poursuivrons avec l'architecture du cloud et la conception de la sécurité, à la fois pour construire de nouvelles architectures et pour adapter des outils et des processus de sécurité éprouvés au cloud. Une discussion exhaustive couvrira la sécurité des réseaux (pare-feu et contrôles d'accès au réseau, détection d'intrusion, etc.), ainsi que toutes les autres couches de la pile de sécurité du cloud. Nous examinerons chaque couche et ses composants, avec la création d'instances sécurisées, la sécurité des données, la sécurité des identités et des comptes, et bien plus encore. Nous consacrerons une journée entière à l'adaptation de nos zones prioritaires d'attaque et de défense au cloud, ce qui impliquera la gestion des vulnérabilités et les tests d'intrusion, ainsi que les développements les plus importants et récents de la recherche sur la sécurité du cloud. Concernant la défense, nous nous intéresserons à la gestion des incidents, à l'inforensique, à la gestion des événements et à la sécurité des applications.

Nous terminerons le cours par une immersion dans SecDevOps et l'automatisation, en explorant les méthodes d'intégration de la sécurité dans l'orchestration et toutes les facettes du cycle de vie du cloud. Nous explorerons les outils et les tactiques éprouvés, et même plusieurs cas d'utilisation de pointe où la sécurité peut être entièrement automatisée dans des scénarios de déploiement, de détection et de réponse aux incidents en utilisant des API et des scripts.

« SEC545 est idéal pour aborder et comprendre la sécurité du cloud. Je ne peux que recommander cette formation à quiconque envisage de mettre en place un programme de sécurité du cloud. »

- Justin Pyle,
Chan Zuckerberg Initiative

30 CRÉDITS CPE/CMU

Vous apprendrez à...

- Concevoir et réviser des règles internes pour garantir une sécurité cloud adéquate
- Comprendre les principaux aspects des risques liés au cloud : menaces, vulnérabilités, impact...
- Exposer clairement les questions liées à la sécurité et aux risques associés aux modèles de déploiement cloud SaaS, PaaS et IaaS
- Évaluer les Cloud Access Security Brokers (CASB) pour mieux protéger et superviser les déploiements SaaS
- Concevoir la sécurité à tous les niveaux d'un environnement cloud hybride, des hyperviseurs aux contrôles de couche applicative
- Évaluer les contrôles de sécurité de base de l'hyperviseur de virtualisation
- Concevoir et mettre en œuvre les contrôles d'accès de sécurité réseau et les capacités de supervision dans un environnement cloud public
- Concevoir une architecture réseau cloud hybride qui inclut des tunnels IPSec
- Intégrer la gestion des identités et des accès cloud (IAM) dans l'architecture de sécurité
- Évaluer et implémenter divers types et formats de chiffrements cloud
- Développer des architectures cloud multiniveaux dans un cloud virtuel privé (VPC) en utilisant des sous-réseaux, des zones de disponibilité, des portails et la traduction d'adresses réseau (NAT)
- Intégrer la sécurité dans les équipes DevOps, créant ainsi une structure efficace d'équipe DevSecOps
- Élaborer des workflows de développement automatisés en utilisant AWS et des outils natifs
- Incorporer la gestion des vulnérabilités, l'analyse et les tests d'intrusion dans les environnements cloud

Former la prochaine génération de responsables cybersécurité

Diplômes Master

Programme conçu pour la formation en alternance
Décrochez votre diplôme en 3 à 5 ans tout en continuant à travailler .

Cours en ligne et en Live
Faites votre choix parmi les cours en ligne ou les options de formation intensive d'une semaine en Live accessibles dans le monde entier.

Obtention de certifications GIAC
Validez vos compétences avec des titres reconnus au niveau sectoriel et obtenus tout au long du programme.

Admission par équivalence
Incorporez vos formations précédentes SANS et certifications GIAC à votre diplôme.

Certificats d'études supérieures

Affinez vos compétences
Maintenez vos connaissances et vos compétences à niveau grâce à des programmes courts axés sur les aspects techniques.

Formation diplômante en 18 à 24 mois
Choisissez le rythme qui correspond à vos exigences personnelles et professionnelles en étudiant en ligne ou en personne lors de formations immersives d'une semaine.

Domaines de spécialisation multiples
Ingénierie en cybersécurité (fondamentaux), opérations de cyberdéfense, réponse aux incidents, sécurité des systèmes de contrôle industriel, tests d'intrusion et hacking éthique.

Certificats de premier cycle

Préparation rapide aux carrières professionnelles
Obtenez votre certificat en 18 à 24 mois tout en travaillant à temps plein ou en poursuivant des études diplômantes, ou choisissez une option accélérée pour terminer en moins d'un an. Sélectionnez des cours dispensés intégralement en ligne ou débutant par des événements immersifs d'une semaine organisés dans le monde entier.

POUR EN SAVOIR PLUS CONSULTEZ: SANS.EDU

SANS Technology Institute

ICS 410

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

ICS/SCADA Security Essentials

SANS collabore avec les principaux acteurs du secteur pour doter les professionnels de la sécurité et les ingénieurs des systèmes de contrôle des compétences essentielles en cybersécurité dont ils auront besoin pour défendre des infrastructures nationales critiques. Le cours ICS410: ICS/SCADA Security Essentials apporte un ensemble de compétences et de connaissances fondamentales pour les professionnels de la cybersécurité industrielle. Ce cours est conçu pour que le personnel impliqué dans la gestion et la défense des systèmes de contrôle industriel soit formé au maintien d'un environnement opérationnel sûr, sécurisé et résistant face aux menaces actuelles et émergentes du cyberespace.

Parmi les thèmes traités :

- Comprendre les composants, les finalités, les déploiements, les moteurs et les contraintes des systèmes de contrôle industriel
- Pratiques en laboratoire des outils, méthodes et surfaces d'attaque des systèmes de contrôle
- Approches qui régissent les architectures et techniques de défense des réseaux et systèmes pour les systèmes de contrôle
- Compétences en réponse aux incidents dans un environnement de système de contrôle
- Ressources et modèles de gouvernance pour les professionnels de la cybersécurité industrielle

Pour analyser les risques et les besoins majeurs dans les secteurs d'infrastructures critiques, les concepteurs du cours ont soigneusement examiné les principes essentiels de la sécurité associés aux tâches quotidiennes de la gestion des systèmes de contrôle. Il existe bien des cours destinés aux experts de haut niveau sur la sécurité qui souhaitent développer des compétences spécifiques (tests d'intrusion des systèmes de contrôle industriel, analyse des vulnérabilités, analyse des malwares, inforensique, codage sécurisé, formation de type *Red Team*), mais la plupart ne sont pas centrés sur les personnes qui exploitent, gèrent, conçoivent, implémentent, surveillent et intègrent les systèmes de contrôle de la production d'infrastructures critiques.

En raison de la nature dynamique des systèmes de contrôle industriel, nombre d'ingénieurs ne maîtrisent pas totalement les caractéristiques et les risques liés à de nombreux dispositifs. En outre, le personnel de service IT qui fournit les voies de communication et les défenses du réseau ne comprend pas toujours les moteurs et les contraintes opérationnels des systèmes. Ce cours est conçu pour aider le personnel IT traditionnel à bien comprendre les principes de conception sur lesquels reposent les systèmes de contrôle et à maintenir ces systèmes pour en assurer l'intégrité et la disponibilité. Parallèlement, il répond au besoin d'aider les ingénieurs et les opérateurs des systèmes de contrôle à mieux comprendre le rôle important qu'ils jouent dans la cybersécurité. Tout commence avec la conception d'un système de contrôle doté d'une cybersécurité intégrée et l'assurance que cette sécurité sera toujours à niveau aussi longtemps que le système sera fiable pendant son cycle de vie.

À l'issue du cours, les stagiaires connaissent, comprennent et partagent un langage commun qui leur permettra de travailler ensemble à la sécurisation des environnements des systèmes de contrôle industriel. Le cours encourage le développement de pratiques d'ingénierie qui intègrent la cybersécurité, ainsi que le soutien en temps réel des systèmes de contrôle IT/OT par des professionnels qui comprennent les conséquences matérielles des actions dans le monde cybernétique.

Public visé :

Cours conçu pour tous les professionnels qui travaillent dans des environnements ICS, qui interagissent avec eux ou peuvent même les affecter (propriétaires d'actifs, fournisseurs, intégrateurs et toute autre tierce partie). Ils sont surtout issus de quatre domaines :

- IT (y compris les services qui soutiennent la technologie opérationnelle)
- Sécurité IT (y compris la sécurité de la technologie opérationnelle)
- Ingénierie
- Normes professionnelles pour l'industrie et l'entreprise

Vous apprendrez à...

- Exécuter des outils de ligne de commande Windows pour analyser le système à la recherche d'éléments à risque élevé
- Exécuter des outils de ligne de commande (ps, ls, netscat, etc.) et du script basique Linux pour automatiser le fonctionnement de programmes afin de superviser en continu divers outils
- Installer VMWare et créer des machines virtuelles pour fabriquer un laboratoire virtuel où les outils et la sécurité des systèmes seront testés et validés
- Mieux comprendre divers systèmes de contrôle industriel, leurs finalités, leur usage, leur fonction et leur corrélation avec les IP de réseau ainsi qu'avec les communications industrielles
- Travailler avec des systèmes d'exploitation (concepts d'administration de systèmes Unix/Linux et/ou Windows)
- Travailler avec la conception des infrastructures de réseau (concepts d'architecture de réseau tels que la topologie, les protocoles et les composants)

CERT. GIAC : GICSP
36 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GICSP

ICS 456

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Essentials for NERC Critical Infrastructure Protection

ICS456: Essentials for NERC Critical Infrastructure Protection est une formation de 5 jours qui s'intéresse en détail aux standards des versions 5, 6 et 7. Ce cours traite du rôle des organisations de fiabilité nord-américaines, la FERC (Federal Energy Regulatory Commission), la NERC (North American Electric Reliability Corporation) et des organisations régionales. Il aborde plusieurs approches d'identification et de catégorisation des systèmes électroniques BES et il aide les propriétaires d'actifs électroniques à déterminer les critères applicables en fonction d'implémentations spécifiques. Ce cours permet en outre de voir les stratégies d'implémentation pour les critères des versions 5, 6 et 7 avec une approche professionnelle qui prend aussi bien en compte l'aspect cybersécurité que le respect de la réglementation.

À la différence d'autres cours sur le référentiel de protection de l'infrastructure essentielle NERC CIP qui se limitent au seul contenu des normes, cette formation fournit les informations nécessaires au développement et au maintien d'un programme de conformité et permet de mieux comprendre les aspects techniques desdites normes. Pour les 25 labos pratiques, nous fournissons aux stagiaires trois machines virtuelles pour qu'ils acquièrent des compétences allant de la sécurisation des postes de travail à l'analyse inforensique et au *lock picking*. Nos stagiaires en témoignent régulièrement : ces labos participent à renforcer les acquis et les préparent à mieux réaliser leur travail.

Vous traiterez les thèmes suivants :

- L'identification et les stratégies des systèmes électroniques BES pour abaisser leur degré d'impact
- Les nuances des termes tels que définis par la NERC et l'applicabilité des normes CIP, notamment les éventuelles conséquences importantes sur votre programme de changements subtils dans les définitions
- L'importance de déterminer correctement les stratégies et les degrés d'impact des systèmes électroniques pour réduire au minimum le risque de non-conformité
- Les approches stratégiques de mise en œuvre des technologies sous-jacentes
- La gestion des tâches et stratégies récurrentes pour la maintenance de programmes de protection de l'infrastructure essentielle
- La mise en œuvre efficace des contrôles d'accès physiques et numériques
- La déconstruction de la complexité des normes NERC CIP pour mieux communiquer avec la hiérarchie
- Prochain audit CIP : les attentes, la préparation des pièces justificatives et les pièges courants à éviter
- Appréhension des efforts les plus récents de l'équipe de conception des normes (SDT pour ***Standards Development Team***) et ses éventuelles conséquences sur votre programme CIP actuel

Public visé :

- Cybersécurité informatique (IT) et opérationnelle (OT des ICS)
- Personnel technique opérationnel
- Opérations de sécurité
- Réponse aux incidents
- Équipe conformité
- Responsables d'équipe
- Gouvernance
- Fournisseurs/intégrateurs
- Auditeurs

Vous apprendrez à...

- Comprendre les objectifs de cybersécurité des normes NERC CIP
- Comprendre le cadre réglementaire NERC, la source de son autorité et la procédure d'élaboration des normes CIP, ainsi que leur lien avec les autres normes de fiabilité BES
- Maîtriser le jargon NERC CIP, appréhender les termes apparemment semblables aux sens très différents avec les conséquences sur votre programme de conformité
- Décomplexifier pour mieux identifier et catégoriser les systèmes et les actifs électroniques BES
- Élaborer de meilleurs contrôles de gestion de la sécurité sur la base des éléments constitutifs de procédures et politiques efficaces en cybersécurité
- Comprendre les contrôles physiques et logiques et les règles de supervision
- Appréhender les critères de gestion des systèmes CIP-007 et leur lien aux critères de gestion de la configuration CIP-010 ; comprendre la différence des chronologies d'évaluation et de remédiation des vulnérabilités
- Déterminer les ingrédients d'un programme adapté d'évaluation des risques et de formation du personnel
- Élaborer des stratégies de protection et de récupération des informations des systèmes électroniques BES

CERT. GIAC : GCIP
31 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GICSP

ICS 515

LIVE ONLINE · TRAINING EVENTS · PRIVATE TRAINING · ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

ICS Active Defence and Incident Response

Le cours ICS515: ICS Active Defence and Incident Response apprend aux stagiaires à disséquer les cyberattaques ICS, à identifier et contrer les menaces ciblant l'ICS grâce à la défense active et à maintenir la sûreté et la fiabilité des opérations.

Ils apprennent également à comprendre l'environnement de leurs systèmes de contrôle industriel en réseau, à surveiller les menaces qui visent ces derniers, à gérer des incidents en fonction des menaces identifiées et à améliorer la sécurité des réseaux en tirant des leçons d'interactions avec des adversaires. Ce processus de surveillance, de réponse et d'apprentissage à partir des menaces internes du réseau est connu sous le nom de « défense active ».

Une défense active est nécessaire pour contrer des adversaires de haut niveau qui ciblent les systèmes de contrôle industriel, comme dans le cas des menaces Stuxnet, Havex et BlackEnergy2. Les stagiaires quittent ce cours avec la capacité de déconstruire des attaques ICS ciblées et de combattre les adversaires. Ce cours utilise une approche pratique et des malwares réels pour décomposer les cyberattaques contre les infrastructures ICS du début à la fin. Les stagiaires acquièrent une compréhension technique et pratique pour optimiser les concepts de défense active. Il s'agit d'utiliser la *threat intelligence,* la mise en place d'une supervision de la sécurité des réseaux, ainsi que l'analyse de malwares et la réponse aux incidents pour assurer la sécurité et la fiabilité des opérations. Les compétences stratégiques et techniques proposées par ce cours servent de base aux installations industrielles qui veulent prouver qu'elles peuvent se défendre.

Ce cours vous prépare à :

- Analyser les réseaux ICS et identifier les actifs et leurs flux de données pour comprendre les informations de référence du réseau, nécessaires pour identifier les menaces avancées
- Utiliser les concepts de défense active (consommation de *threat intelligence*, supervision de la sécurité des réseaux, analyses de malwares et réponse aux incidents, par exemple) pour assurer la sécurité du système ICS
- Concevoir un automate de programme industriel (ou Programmable Logic Controller, PLC) personnalisé avec un kit CYBATIworks, et le conserver après la formation
- Acquérir une expérience pratique en laboratoire sur des échantillons Havex, BlackEnergy2 et Stuxnet, et déconstruire ce type de menaces
- Utiliser des outils techniques (Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, analyseurs PDF, sandboxing de malwares, etc.)
- Créer des indicateurs de compromission (Indicators of Compromise, IOC) dans des formats comme OpenIOC et YARA, et comprendre les normes de partage STIX et TAXII
- Exploiter des modèles (Sliding Scale of Cyber Security, Active Cyber Defence Cycle, ICS Cyber Kill Chain, etc.) pour extraire des informations des menaces et les utiliser pour conforter la sécurité des réseaux ICS à long terme

Public visé :

- Responsables et membres d'équipes de réponse aux incidents ICS
- Personnel des services de sécurité OT et ICS
- Professionnels de la sécurité IT
- Responsables d'équipes et analystes d'un centre des opérations de sécurité (SOC)
- Experts en tests d'intrusion et *Red Team* ICS
- Chargés de défense active

Vous apprendrez à...

- Appliquer une réponse aux incidents ICS axée sur les opérations de sécurité et donnant la priorité aux opérations de sécurité et de fiabilité.
- Comprendre la génération du renseignement sur les menaces ICS et exploiter les informations de la communauté pour assurer la protection des environnements ICS. Vos nouvelles compétences en analyse vous permettront d'avoir un regard critique sur les rapports de renseignement sur les menaces visant les ICS et de les exploiter correctement et de façon régulière.
- Identifier les ressources ICS et leurs topologies réseaux et surveiller les zones sensibles des ICS pour détecter les anomalies et les menaces. Vous familiariser avec des méthodologies telles que la supervision de la sécurité des réseaux ICS et avec des approches visant à limiter les menaces touchant à ces systèmes
- Analyser des malwares ICS et extraire les informations critiques dont vous avez besoin pour mesurer rapidement l'étendue de l'environnement et comprendre la nature de la menace.

CERT. GIAC : GRID
30 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GRID

ICS 612

TRAINING EVENTS · PRIVATE TRAINING

CINQ JOURS • ORDINATEUR PORTABLE REQUIS

ICS Cyber security In-Depth NOUVEAU

LES MALWARES CIBLANT LES SYSTÈMES DE CONTRÔLE INDUSTRIEL (ICS) ET LES ATTAQUES SUR L'INFRASTRUCTURE ESSENTIELLE AUGMENTENT TANT EN FRÉQUENCE QU'EN SOPHISTICATION. IL FAUT IDENTIFIER LES MENACES, MAIS AUSSI LES VULNÉRABILITÉS ET LES MÉTHODES POUR SÉCURISER VOTRE ENVIRONNEMENT ICS. NOUS VOUS MONTRONS COMMENT FAIRE !

Dans le cours ICS612: ICS Cyber security In-Depth, vous allez :

- Apprendre des méthodes passives et actives de collecte sécurisée des informations dans un environnement ICS
- Identifier les vulnérabilités dans les environnements ICS
- Déterminer les modes opératoires frauduleux qui visent à interrompre et contrôler des processus et les défenses pour les contrer
- Mettre en œuvre en amont des mesures pour prévenir, détecter, ralentir ou arrêter les attaques
- Comprendre les opérations ICS et leur aspect « normal »
- Construire des points de passage obligés dans une architecture, déterminer les moyens de les utiliser dans la détection des incidents de sécurité et la réponse à leur apporter
- Gérer les environnements ICS complexes ; développer la capacité de détection des événements de sécurité
- ICS et de réponse à y apporter

Les notions et les objectifs pédagogiques du cours sont principalement abordés par le biais d'exercices pratiques. La configuration de labo en cours est prévue pour simuler un environnement réel où un contrôleur supervise et contrôle les appareils déployés sur le terrain. Une interface homme-machine (IHM) tactile installée à l'atelier est accessible au personnel en local pour lui permettre d'effectuer les changements de procédure nécessaires. Via les postes de travail des opérateurs d'un centre de contrôle distant, les opérateurs système supervisent et contrôlent les équipements industriels avec un système SCADA. Représentatif d'un véritable environnement ICS, la configuration comprend une connexion à l'entreprise pour le transfert de données (à savoir un logiciel d'historisation ou *historian*), l'accès à distance et d'autres fonctions classiques d'entreprise.

Lors des labos, les stagiaires passent par différents exercices qui leur montrent les divers moyens pour l'attaquant d'infiltrer

un ICS à l'architecture médiocre, situation malheureusement courante, et pour les défenseurs de sécuriser et gérer l'environnement.

« Comprendre pleinement les appareils qu'il nous incombe de défendre est indispensable pour mettre en œuvre efficacement des mesures de sécurité. »
- Crystal B.,
ARMÉE DES ÉTATS-UNIS

Public visé :

- Anciens stagiaires du cours ICS410: ICS/SCADA Security Essentials, qui auront acquis les connaissances préalables pour ce cours
- Ingénieurs en contrôle industriel
- Ingénieurs des systèmes ou de la sûreté des systèmes
- Chargés de défense active en ICS
- Quiconque doté d'une expérience significative des systèmes de contrôle souhaitant comprendre les méthodes et procédures de mise en sûreté d'un environnement ICS

Vous apprendrez à...

- Pratiquer sur les actifs typiques d'un environnement industriel, notamment un automate programmable industriel (API ou, en anglais, PLC), des interfaces opérateurs pour la commande en local, des serveurs d'interface homme-machine (IHM), un serveur d'historique (***historian***), des commutateurs, des routeurs et des pare-feu
- Comprendre l'exécution d'un automate programmable industriel par des exercices pratiques
- Identifier des méthodes de sécurité applicables aux systèmes d'entrée/sortie et de contrôle en temps réel
- Appréhender les avantages et les inconvénients de diverses architectures API et IHM, avec des recommandations d'amélioration des approches de sécurité de ces systèmes de contrôle en temps réel
- Identifier les emplacements des actifs essentiels d'un environnement industriel
- Comprendre le rôle et la conception d'une zone démilitarisée industrielle (IDMZ)
- Pratiquer sur des pare-feu placés dans la zone industrielle pour réussir une isolation cellule par cellule et des restrictions de périmètre
- Disséquer plusieurs protocoles industriels pour comprendre les notions de trafic normal et anormal utilisées dans le contrôle opérationnel des actifs

30 CRÉDITS CPE/CMU

Formations courtes en cyberdéfense

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC440: Critical Security Controls: Planning, Implementing, and Auditing

LIVE ONLINE
TRAINING EVENTS
ON-DEMAND

Ce cours vous aide à maîtriser les techniques et outils spécifiques et éprouvés dont vous avez besoin pour mettre en œuvre et évaluer les Critical Security Controls documentés par le Center for Internet Security (CIS). Ces contrôles de sécurité font de plus en plus l'objet d'un consensus et constituent la première des listes des priorités à contrôler pour toute organisation dont les activités revêtent un caractère sensible. Ces contrôles ont été sélectionnés et définis par l'armée américaine et par d'autres organismes publics et privés (NSA, ministère de la Sécurité intérieure et bien d'autres), c'est-à-dire les experts les plus respectés au monde, qui connaissent le déroulement et le fonctionnement des attaques et les procédures pour y parer. Ils ont déterminé collégialement que ces contrôles constituaient le meilleur moyen de bloquer les attaques connues et de localiser et réduire les dommages causés par les attaques réussies. Pour les professionnels de la sécurité, ce cours permet de voir comment automatiser efficacement et à grande échelle ces contrôles dans un réseau, à un budget raisonnable. Pour les auditeurs, les DSI et les chargés de réponse aux risques, ce cours est le meilleur moyen de comprendre comment mesurer l'efficacité de la mise en œuvre de ces contrôles.

> **« Excellent formateur : très compétent, passionné, divertissant et informatif. »**
> - Mike Mayers
> *RIM*

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC455: SIEM Design & Implementation

ON-DEMAND

Un système de gestion des informations et des événements de sécurité ou SIEM (Security Information and Event Management) peut s'avérer un atout extraordinaire pour la sécurité d'une organisation, mais sa compréhension et sa maintenance ne sont pas aisées. De nombreuses solutions nécessitent une infrastructure complexe et des logiciels dédiés, avec en sus un besoin en services professionnels au moment de l'installation. L'intervention de services professionnels peut laisser aux équipes de sécurité l'impression de ne pas parfaitement comprendre le fonctionnement de leur SIEM et de ne pas en avoir le contrôle. Cette situation de solutions complexes associée à une pénurie de compétences, à un manque de documentation simple et aux coûts des logiciels et de la main d'œuvre ne facilite en rien le déploiement des SIEM. Résultat fréquent : un écart important entre les attentes et la réalité. Un SIEM peut constituer le plus puissant des outils d'une équipe de cyberdéfense, encore faut-il qu'il soit exploité à son plein potentiel. Ce cours a ainsi été élaboré pour répondre à ce problème en démystifiant les SIEM et en simplifiant le processus de mise en œuvre, pour une solution utilisable, évolutive et facile à maintenir.

> **« Ce cours est génial. On y construit un SIEM de A à Z ce qui permet d'en savoir beaucoup plus sur ce que fait le SIEM en arrière-plan. »**
> - Billy Davis
> *AWS*

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC402: Cyber security Writing: Hack the Reader

ON-DEMAND

Vous voulez améliorer vos écrits ? Apprenez à voler l'attention du lecteur ! Découvrez comment trouver un angle, faire tomber les défenses de vos lecteurs et capturer leur attention pour délivrer votre message, même s'ils sont trop occupés ou peu intéressés par les communications des autres. Ce cours unique en son genre, conçu sur mesure pour les professionnels de la cybersécurité, va renforcer vos compétences rédactionnelles et booster votre carrière.

FORMATION PRATIQUE • TROIS JOURS • ORDINATEUR PORTABLE REQUIS

SEC403: Secrets to Successful Cybersecurity Presentation | NOUVEAU

ON-DEMAND

Kit de ressources ultime : adhésion des responsables, validation des dossiers et développement professionnel
Peut-être vous êtes-vous engagé sur la voie de la cybersécurité pour mener l'enquête et attraper les méchants, mais les évolutions technologiques, les besoins des utilisateurs et les incidents vous obligeront tôt ou tard à adapter votre communication à d'autres profils, techniques, utilisateurs finaux ou dirigeants. Pour améliorer la forme et progresser dans votre carrière, vous aurez besoin de savoir faire une présentation efficace.
Le cours SEC403 vous donne les clés pour élaborer un briefing de sécurité efficace, susciter l'intérêt et l'adhésion de votre public, et exposer vos présentations avec assurance à différents groupes. Vous apprendrez des techniques utiles pour faire valider vos nouveaux projets et outils de sécurité par vos supérieurs, ainsi que pour répondre aux questions les plus ardues et moduler dans le feu de l'action. Conçu spécifiquement pour les professionnels en cybersécurité, ce cours expose les bonnes pratiques courantes de restitution notamment pour les rapports des tests d'intrusion et d'audit de sécurité, le suivi d'incident, les rapports d'analyse rétrospective des incidents, les briefings de sensibilisation et de vigilance à la sécurité.

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC546: IPv6 Essentials

TRAINING EVENTS
PRIVATE TRAINING

Dans le cadre de la mise en œuvre de l'IPv6, l'impact du nouveau protocole sur la sécurité doit faire l'objet d'une attention particulière. Le simple fait que les systèmes d'exploitation actuels prennent en charge IPv6 peut facilement mener à son implémentation involontaire dans votre réseau, exposant celui-ci au risque cyber. Cette formation commence par une introduction au protocole IPv6 où nous disséquerons de nombreuses fonctionnalités notamment l'en-tête IPv6, les en-têtes d'extension et la configuration automatique. Seule la compréhension approfondie des protocoles et de leur conception permet d'apprécier les différentes attaques et techniques d'atténuation des risques. La formation vous propose de profiter de l'IPv6 pour repenser l'affectation des adresses du réseau et de remédier à ce que certains décrivent comme le plus grand problème de sécurité du protocole : la fin de la traduction d'adresses réseau ! IPv6 a des répercussions au-delà de la couche réseau. De nombreux protocoles de la couche applicative évoluent pour le prendre en charge : nous nous y intéresserons de près, notamment à DNS, à DHCPv6 et à d'autres.

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC582: Mastering TShark Packet Analysis | BÊTA

LIVE ONLINE

Chaque jour, de nouvelles compromissions de système et atteintes aux données sont relevées et davantage d'activités déplacées vers le cloud : les défenseurs de réseau doivent impérativement veiller à posséder les outils et compétences utiles pour détecter le plus tôt possible les compromissions. Si les agresseurs, auteurs d'attaques avancées ou non, font tout leur possible pour cacher leurs activités frauduleuses sur l'hôte compromis, le réseau en garde forcément des traces. Selon la Cyber Kill Chain de Lockheed Martin, c'est un fait, quelle que soit l'activité, reconnaissance comprise, l'action menée ou l'objectif à atteindre. Fondamentalement, il y a des paquets ou il ne s'est rien passé.

FORMATION PRATIQUE • UNE JOURNÉE • ORDINATEUR PORTABLE REQUIS

SEC583: Crafting Packets

LIVE ONLINE

Avez-vous déjà configuré une nouvelle politique de pare-feu, une nouvelle règle de détection et de prévention d'intrusion IDS/IPS ou une fonctionnalité nouvelle génération sans aucun trafic pour la tester ? Et si vous créiez votre propre trafic ? La création de paquets est une formidable compétence pour tout analyste sécurité, ingénieur réseau ou administrateur système. Elle sert à tester les politiques de pare-feu, les règles des systèmes de détection et de prévention d'intrusion, les paramètres serveur/hôte, les configurations des applications, etc. Créer des paquets va aussi améliorer votre compréhension des protocoles TCP/IP et d'application.

Formations courtes aux tests d'intrusion

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC564: Red Team Exercises & Adversary Emulation

LIVE ONLINE
TRAINING EVENTS
ON-DEMAND

Une *Red Team* est un groupe chargé d'utiliser des tactiques, des techniques et des procédures (TTP) qui simulent les menaces du monde réel pour entraîner et mesurer l'efficacité du personnel, des protocoles et des technologies utilisés pour protéger les environnements. La *Red Team* suit une approche globale issue des fondamentaux des tests d'intrusion pour connaître la sécurité générale d'une organisation. L'objectif est de tester la capacité à détecter une attaque, à y répondre et à s'en relever. Bien menées, les activités d'un tel groupe vont améliorer significativement les contrôles de sécurité, affûter les capacités défensives et mesurer l'efficacité des opérations de sécurité d'une organisation. Le concept de *Red Team* nécessite une approche différente des tests de sécurité classiques et repose principalement sur des TTP bien définies, sans lesquelles il est impossible d'obtenir une simulation réaliste de menaces ou d'adversaires. Le bilan que dresse une *Red Team* ne se limite pas à la liste habituelle des vulnérabilités que le test d'intrusion aura révélées. Il inclut une analyse plus approfondie de la réaction potentielle de l'organisation contre une véritable menace et identifie les forces et les faiblesses de sécurité.

Quel que soit votre rôle, défensif ou offensif, comprendre l'intérêt d'une *Red Team* et les améliorations qu'elle peut apporter à la sécurité vous sera précieux. Les organisations consacrent beaucoup de temps et d'argent à la sécurité de leurs systèmes. En retour, il leur est indispensable de disposer de professionnels capables de faire fonctionner efficacement ces systèmes. SEC564 vous permettra de développer les compétences dont vous avez besoin pour gérer et diriger une *Red Team*, mener ses missions, et comprendre son rôle et son importance dans la mise à l'épreuve de la sécurité. Ce cours de deux jours explore en profondeur les concepts de la *Red Team*, traite des fondamentaux de la simulation de menace et vous aide à renforcer la sécurité de votre organisation.

« La formation SEC564 est excellente. Je vais pouvoir l'appliquer immédiatement dans mon entreprise. »
Kirk Hayes
Rapid 7

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC552: Bug Bounties and Responsible Disclosure | BÊTA

LIVE ONLINE
TRAINING EVENTS

Dans un programme de *bug bounty*, littéralement de prime aux bogues, un éditeur recourt aux bonnes volontés du milieu de la cybersécurité pour déceler les failles de sécurité insoupçonnables et exploitables dans leurs applications. Le périmètre du programme inclut les bogues de sécurité des applications web et mobiles, des interfaces de programmation et bien plus. Les grandes entreprises de la Tech comme Google, Facebook, Twitter et PayPal ont déjà recours à de tels programmes. Les chercheurs en sécurité qui suivent les directives de divulgation responsable sont récompensés et reconnus, l'objectif de ces programmes étant d'améliorer et de sécuriser les applications.

SEC552 s'inspire d'études de cas de différents programmes de prime aux bogues, notamment d'exemples récents d'attaques d'applications web et mobiles. En partageant leurs expériences, les différents chercheurs stimulent l'inventivité des développeurs et des experts en test d'intrusion pour imaginer les attitudes et techniques derrière les attaques non conventionnelles.

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC580: Metasploit Kung Fu for Enterprise Pen Testing

ON-DEMAND

Nombre d'entreprises doivent aujourd'hui respecter des normes légales et sectorielles qui les obligent à mener régulièrement des tests d'intrusion et des évaluations des vulnérabilités. Les outils et services commerciaux qui le permettent s'avèrent souvent onéreux. S'il existe des outils gratuits et robustes, comme Metasploit, peu de testeurs en maîtrisent l'ensemble des fonctionnalités et savent les appliquer dans une méthodologie de test professionnelle. Metasploit a été conçu pour aider les testeurs à confirmer des vulnérabilités grâce à une plateforme open source simple d'utilisation. Dans cette formation, vous apprendrez à en tirer tout le potentiel.

Vous découvrirez comment appliquer les incroyables capacités de Metasploit Framework dans un protocole complet de tests d'intrusion et d'évaluation des vulnérabilités grâce à une méthodologie de tests exhaustive et efficace. À l'issue de la formation, vous aurez acquis une compréhension solide de Metasploit et de l'intérêt de l'intégrer au quotidien à vos activités d'évaluation et à vos tests d'intrusion. Vous y gagnerez une compréhension approfondie de Metasploit Framework, qui dépasse largement la simple présentation de l'exploitation d'un système à distance. Vous découvrirez l'exploitation, la reconnaissance postexploitation, la manipulation de jetons, les attaques par hameçonnage ciblé (*spear-phishing*) et le vaste jeu de fonctionnalités de Meterpreter, un environnement shell personnalisé spécialement créé pour exploiter et analyser les failles de sécurité. Le cours couvrira également les nombreux pièges qu'un testeur peut rencontrer lorsqu'il utilise Metasploit Framework, ainsi que la manière de les éviter ou de les contourner, pour des tests plus sûrs et plus efficaces.

« SEC580 est une excellente formation : pour le nombre de participants, le rythme, les exercices pratiques et la pédagogie. »
- Robert Lockwood
Fusion Cell Consulting

Formation en équipe

TBT570: Team-Based Training – Blue Team & Red Team Dynamic Workshop | NOUVEAU

TRAINING EVENTS
PRIVATE TRAINING
ON-DEMAND

Cet exercice interactif vise les personnes qui apprennent mieux par la pratique. Sans cours théorique ni travaux pratiques guidés, cette formation prend la forme d'une immersion dynamique et interactive où les stagiaires défendent en temps réel un environnement attaqué et acquièrent les compétences par ce travail d'équipe. Elle est conçue pour développer l'esprit d'équipe, les capacités de leadership, les techniques de communication et l'expertise technique, le tout sous le feu de l'ennemi dans une série de scénarios à la complexité progressive.

La bataille interactive en direct se déroule sur cinq jours. Le sixième et dernier jour, les équipes *Blue Team* et *Red Team* présentent un débriefing des leçons tirées. Ces rapports seront distribués aux stagiaires, à charge pour eux de les exploiter pour améliorer le niveau de sécurité de leur organisation.

Formations courtes en sécurité du cloud

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC534: Secure DevOps: A Practical Introduction

ON-DEMAND

Ce cours aborde les fondamentaux de DevOps et la manière de concevoir et livrer des logiciels sécurisés. Vous apprendrez les principes, les pratiques et les outils associés à DevOps et leur utilisation pour améliorer la fiabilité, l'intégrité et la sécurité des systèmes. À l'aide d'outils open source courants comme Puppet, Jenkins, GitLab, Vault, Grafana et Docker, vous acquerrez une expérience pratique d'automatisation de la gestion de la configuration (infrastructure programmable ou *Infrastructure as Code*), de l'intégration continue (CI), de la livraison continue (CD), de la conteneurisation, de la microsegmentation, de la conformité automatisée (conformité inscrite dans le code ou *Compliance as Code*) et de la supervision continue. Les stagiaires s'appuient sur la chaîne d'outils Secure DevOps pour réaliser une série de labos de sécurisation de projets CI/CD avec des outils, protocoles et techniques de sécurité variés.

FORMATION PRATIQUE • TROIS JOURS • ORDINATEUR PORTABLE REQUIS

SEC510: Multicloud Security Assessment and Defense | NOUVEAU

LIVE ONLINE
TRAINING EVENTS

Le cours SEC510: Multicloud Security Assessment and Defense apporte aux professionnels de la sécurité cloud, aux analystes et aux chercheurs une compréhension approfondie des rouages des grands fournisseurs de cloud public, Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP). Les stagiaires y apprendront les normes et méthodologies reconnues du secteur, à savoir les référentiels MITRE ATT&CK Cloud Matrix et CIS Cloud Benchmarks, qu'ils appliqueront ensuite lors d'exercices pratiques où ils évalueront une application web moderne exploitant l'offre cloud native de chaque fournisseur. Les stagiaires s'imprégneront ainsi des philosophies de chaque prestataire et de leur traduction dans les services offerts.

FORMATION PRATIQUE • TROIS JOURS • ORDINATEUR PORTABLE REQUIS

SEC584: Cloud Native Security: Defending Containers and Kubernetes | BÊTA

LIVE ONLINE

Grâce aux fournisseurs de services et d'infrastructures cloud natifs, les organisations arrivent à construire et livrer des systèmes modernes en des temps record, ce qui peut s'avérer difficile à superviser et à défendre. Les stagiaires acquièrent une expérience pratique de la construction, de l'exploration et de la sécurisation des systèmes modernes actuels.

Formations courtes en management

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

MGT415: A Practical Introduction to Cyber Security Risk Management

LIVE ONLINE

Pendant ce cours, les stagiaires acquièrent les compétences pratiques nécessaires pour évaluer régulièrement les risques au sein de leur organisation. La capacité à gérer les risques est cruciale pour les organisations qui cherchent à défendre leurs systèmes. Créer une infrastructure impénétrable relève de l'utopie, car il y a tout simplement trop de menaces et de vulnérabilités potentielles pour des ressources insuffisantes. Les organisations doivent donc hiérarchiser, formellement ou non, les décisions à prendre pour défendre au mieux leurs données et leurs actifs d'information. La gestion des risques est le socle des stratégies de défense réfléchies et ciblées.

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Programme

LIVE ONLINE
TRAINING EVENTS
ON-DEMAND

Les organisations investissent des budgets et des ressources astronomiques dans la sécurisation des technologies, mais très peu – sinon rien – dans la sécurisation de leurs employés et de leurs personnels.

Résultat : le maillon faible de la cybersécurité est aujourd'hui l'être humain. Le plus efficace pour sécuriser le facteur humain consiste à mettre en place un programme de sensibilisation à la sécurité à fort impact, avec l'objectif de changer les comportements plutôt que de simplement cocher le critère de la conformité.

MGT433 est un cours intensif de deux jours qui aborde les concepts et compétences clés nécessaires pour construire et maintenir un programme de sensibilisation à la sécurité et en mesurer les résultats. Le cours repose entièrement sur l'expérience acquise lors de centaines de programmes de sensibilisation à la sécurité dans le monde entier. Il valorise deux modes d'apprentissage : la transmission par le formateur SANS et les interactions avec le groupe.

FORMATION PRATIQUE • DEUX JOURS

MGT521: Driving Cyber security Change – Establishing a Culture of Protect, Detect and Respond | NOUVEAU

TRAINING EVENTS

SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Programme. Il ne s'agit pas seulement de faire bouger les mentalités sur la sécurité, mais de définir les priorités et de passer aux actes depuis la direction jusqu'au premier échelon. Dans le cadre d'un changement organisationnel, discipline qui appartient à l'étude du management, une organisation cherche à analyser, planifier et améliorer son fonctionnement et ses structures en s'appuyant sur l'humain et la culture. Dans le cours SANS MGT521, les managers apprennent à mobiliser les principes du changement organisationnel dans le développement, le maintien et l'évaluation d'une culture de la sécurité. Dans cette formation concrète issue de l'expérience, complète avec une série d'exercices et labos interactifs pratiques pour appliquer les concepts du changement organisationnel à des initiatives de sécurité différentes et variées, vous apprendrez rapidement à intégrer la cybersécurité à la culture d'entreprise.

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

MGT551: Building and Leading Security Operations Centers | BÊTA

LIVE ONLINE
TRAINING EVENTS
ON-DEMAND

Ce cours est certes axé sur la gestion et le management, mais il n'est pas que théorique. Pendant les deux jours de formation, les stagiaires réaliseront six exercices pratiques, de l'implémentation du guide opérationnel à la création d'un référentiel de cas d'usage, en passant par la visualisation et la hiérarchisation des priorités de détection et d'attaque, et la planification, l'exécution et la restitution par la *Purple Team*. À l'issue de la formation, les participants auront acquis un cadre pour comprendre les grands axes des efforts du SOC, les moyens de suivi et d'organisation des capacités défensives, et le pilotage, la vérification et la communication des améliorations du SOC.

LA CYBERSÉCURITÉ VOUS TENTE, MAIS VOUS NE SAVEZ PAS PAR OÙ COMMENCER ?

VOUS VOUS DEMANDEZ QUEL COURS SUIVRE ?

SCANNEZ LE CODE POUR DÉCOUVRIR SI VOUS AVEZ LES COMPÉTENCES QU'IL FAUT

www.sans.org/level-up @sansemea | @sansapac

SANS | GIAC CERTIFICATIONS

Créez dès aujourd'hui votre **compte SANS** et profitez de nos ressources gratuites **www.sans.org/account**

Newsletters

NewsBites
Synthèse bihebdomadaire des informations les plus importantes pour les professionnels de la cybersécurité.

OUCH!
Référence mondiale, mensuelle et gratuite des lettres d'information de sensibilisation à la sécurité, cette newsletter s'adresse aux utilisateurs non spécialistes.

@RISK: The Consensus Security Alert
Récapitulatif hebdomadaire fiable sur (1) les vecteurs d'attaque mis au jour, (2) les vulnérabilités exposées à de nouveaux exploits actifs, (3) le fonctionnement des attaques récentes et (4) d'autres informations utiles.

Webcasts

Ask the Experts : la voix des experts
Nos experts SANS vous informent de l'actualité et des nouveautés en cybersécurité.

Analyst : la perspective de l'analyste
Dans la lignée du programme des analystes SANS, ces webcasts Analyst dégagent les informations clés de nos livres blancs et enquêtes.

WhatWorks : témoignages clients
Nos webcasts WhatWorks mettent en avant des expériences client fortes qui montrent comment des utilisateurs finaux ont résolu certains problèmes de sécurité.

Tool Talks : les outils
Les événements Tool Talks visent à vous donner une compréhension solide d'un problème et de l'utilisation d'un outil commercial pour le résoudre ou en réduire le risque.

Autres ressources gratuites
(en accès libre sans compte)

- InfoSec Reading Room, notre salle de lecture
- Top 25 Software Errors, les grandes erreurs de développement
- 20 Critical Controls, les contrôles critiques
- Security Policies, politiques de sécurité
- Intrusion Detection FAQs
- Tip of the Day, le conseil du jour
- Security Posters, nos affiches sur la sécurité
- Thought Leaders, entretiens avec les acteurs qui comptent
- 20 Coolest Careers, les carrières les plus cools de l'InfoSec
- Security Glossary (glossaire en anglais)
- SCORE (Security Consensus Operational Readiness Evaluation)

Suivez-nous sur les réseaux sociaux pour connaître les derniers développements et annonces dans le monde de la cybersécurité autour des événements SANS.

SANS | GIAC CERTIFICATIONS

www.sans.org