SANS EMEA

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

Formations et certifications en cybersécurité
CATALOGUE

100+
Formateurs SANS certifiés

300+
Sessions de formation dans le monde, en plus de nombreuses options en ligne

Découvrez nos
Catalogue complet de produits SANS disponibles en Europe, Moyen-Orient & Afrique

Cursus de formations SANS
Sécurité, Investigation numérique & Réponse aux incidents, Test d'intrusion, Audit informatique, Développement de logiciels sécurisés, Management, Systèmes de contrôles industriels (SCI) et Cyberdéfense

GIAC CERTIFICATIONS

À Propos De SANS

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

Depuis plus de 25 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 fondamentale est restée constante : la protection des personnes et des biens par le partage des connaissances, des compétences et d'une cybersécurité de pointe.

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 actifs auprès de nombreuses organisations influentes. Ce sont des responsables « Red Team », des agents de lutte contre la cybercriminalité, des directeurs techniques, des RSSI, et des collaborateurs chercheurs.

En outre, nos formateurs SANS affichent non seulement un bagage technique respectable, mais aussi 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 les stagiaires à faire face aux menaces dominantes d'aujourd'hui 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 60 cours, qui s'alignent sur les rôles, responsabilités et disciplines majeurs des équipes de sécurité.

Les programmes de formation SANS incluent: l'investigation numérique, l'audit, la gestion, les tests d'intrusion, systèmes de contrôles industriels (SCI), le développement de logiciels sécurisés et plus. Chaque programme offre une progression de cours qui conduit les professionnels des bases fondamentales du sujet jusqu'aux spécialisations de haut niveau.

Nos formations sont conçues pour être pratiques; immergés en laboratoire, les stagiaires appliquent leurs nouvelles connaissances et affinent leurs compétences.

La promesse SANS

La promesse SANS est au coeur de tout ce que nous entreprenons, 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 documents de recherche sur de nombreux aspects de la sécurité de l'information. Ces documents 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.

Il y a à ce jour plus de 30 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 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 auteurs de cours SANS sont des experts et des professionnels de l'industrie. Leur expérience du monde réel enrichit leur enseignement et le contenu des formations SANS.

SANS et GIAC placent toutes deux une importance capitale à l'apprentissage de compétences pratiques.

Comment s'inscrire à une formation SANS

SANS organise des sessions publiques de formation dans le monde entier qui permettent aux stagiaires de suivre un cours SANS intensif durant 5 à 6 jours.

Les formations SANS fournissent un environnement d'apprentissage idéal et permettent de réseauter avec d'autres professionnels de la sécurité, ainsi qu'avec les formateurs et le personnel SANS.

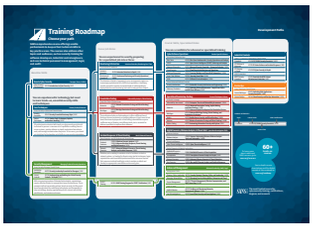
Les stagiaires doivent s'inscrire en ligne sur www.sans.org/emea

Une formation SANS peut également être dispensée en ligne avec « OnDemand », en privé au sein d'une organisation, et dans d'autres langues, notamment en français, allemand, italien et espagnol. Voir pour nos options de formation page 6, ou rendez-vous sur www.sans.org/emea.

Contact SANS
Email: emea@sans.org
Tel: +44 20 3384 3470
Address: SANS EMEA,
PO Box 124, Swansea, SA3 9BB, UK
www.sans.org/emea

Table des matières

4 Training Roadmap



Envisagez-vous une autre formation SANS ou une évolution / changement de carrière ? Consultez nos plans de carrière page 4.

14 Programmes SANS

Êtes-vous inscrit à votre premier stage de formation SANS ? Consultez nos guides de formation page (14), puis la description des cours à partir de la page (21)

Training Roadmap

Choose your path

SANS comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

Baseline Skills

New to Cyber Security — Concepts, Terms, & Skills

Cyber Security Fundamentals	SEC301 **Introduction to Cyber Security** | GISF

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

Core Techniques — Prevent, Defend, Maintain

Every Security Professional Should Know

Security Essentials	SEC401 **Security Essentials Bootcamp Style** | GSEC
Hacker Techniques	SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling** | GCIH

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attacks work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

Security Management — Managing Technical Security Operations

Every Security Manager Should Know

Leadership Essentials	MGT512 **Security Leadership Essentials for Managers** | GSLC
Critical Controls	SEC566 **Implementing and Auditing the Critical Security Controls – In-Depth** | GCCC

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

Focus Job Roles

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

Monitoring & Detection — Intrusion Detection, Monitoring Over Time

Scan Packets & Networks

Intrusion Detection	SEC503 **Intrusion Detection In-Depth** | GCIA
Monitoring & Operations	SEC511 **Continuous Monitoring and Security Operations** | GMON

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Penetration Testing — Vulnerability Analysis, Ethical Hacking

Every Pen Tester Should Know

Networks	SEC560 **Network Penetration Testing and Ethical Hacking** | GPEN
Web Apps	SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking, and different tools, but is essential for defense specialists to improve their defenses.

Incident Response & Threat Hunting — Host & Network Forensics

Every Forensics and IR Professional Should Know

Endpoint Forensics	FOR500 **Windows Forensic Analysis** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA
Network Forensics	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA

Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

CISSP® Training	MGT414 **SANS Training Program for CISSP® Certification** | GISP

Crucial Skills, Specialized Roles

You are a candidate for advanced or specialized training

Cyber Defense Operations — Harden Specific Defenses

Specialized Defensive Area	
Blue Team	SEC450 **Blue Team Fundamentals: Security Operations and Analysis**
OSINT	SEC487 **Open-Source Intelligence (OSINT) Gathering and Analysis**
Advanced Generalist	SEC501 **Advanced Security Essentials – Enterprise Defender** | GCED
Cloud Security	SEC545 **Cloud Security Architecture and Operations**
Windows/Powershell	SEC505 **Securing Windows and PowerShell Automation** | GCWN
Linux/ Unix Defense	SEC506 **Securing Linux/Unix** | GCUX
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA
Other Advanced Defense Courses	
Security Architecture	SEC530 **Defensible Security Architecture and Engineering** | GDSA
Adversary Emulation	SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** | GDAT

Specialized Penetration Testing — Focused Techniques & Areas

In-Depth Coverage	
Vulnerability Assessment	SEC460 **Enterprise Threat and Vulnerability Assessment** | GEVA
Networks	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN SEC760 **Advanced Exploit Development for Penetration Testers**
Web Apps	SEC642 **Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques**
Mobile	SEC575 **Mobile Device Security and Ethical Hacking** | GMOB
Wireless	SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN
Python Coding	SEC573 **Automating Information Security with Python** | GPYC

Digital Forensics, Malware Analysis, & Threat Intel — Specialized Investigative Skills

Malware Analysis	
Malware Analysis	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM
Threat Intelligence	
Cyber Threat Intelligence	FOR578 **Cyber Threat Intelligence** | GCTI
Digital Forensics & Media Exploitation	
Battlefield Forensics & Data Acquisition	FOR498 **Battlefield Forensics & Data Acquisition**
Smartphones	FOR585 **Smartphone Forensic Analysis In-Depth** | GASF
Memory Forensics	FOR526 **Advanced Memory Forensics & Threat Detection**
Mac Forensics	FOR518 **Mac and iOS Forensic Analysis and Incident Response**

Advanced Management — Advanced Leadership, Audit, Legal

Management Skills	
Planning, Policy, Leadership	MGT514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
Managing Vulnerabilities	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
Project Management	MGT525 **IT Project Management, Effective Communication, and PMP® Exam Prep** | GCPM
Audit & Legal	
Audit & Monitor	AUD507 **Auditing and Monitoring Networks, Perimeters & Systems** | GSNA
Law & Investigations	LEG523 **Law of Data Security and Investigations** | GLEG

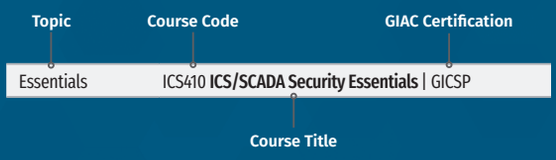
Industrial Controls

Every ICS Security Professionals Should Know	
Essentials	ICS410 **ICS/SCADA Security Essentials** | GICSP
ICS Defense & Response	ICS515 **ICS Active Defense and Incident Response** | GRID
ICS Security In-Depth	ICS612 **ICS Cyber Security In-Depth**
NERC Protection	
NERC Security Essentials	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

DevSecOps

Every Developer Should Know	
Secure Web Apps	DEV522 **Defending Web Applications Security Essentials** | GWEB
Secure DevOps	SEC540 **Cloud Security and DevOps Automation** | GCSA

COURSE LISTING KEY:



60+ hands-on courses

To learn more about additional SANS courses, go to: **sans.org/courses**

See in-depth course descriptions and the digital version of this roadmap at: **sans.org/roadmap**

SANS EMEA **The most trusted source for cybersecurity training, certifications, degrees, and research**

SANS Training Formats

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

SANS Training Events

Les évènements des formations SANS, dispensées dans une salle de classe par des formateurs SANS qualifiés, proposent plusieurs cours et sont organisées dans des hôtels de qualité dans des grandes villes ou des centres d'accueil événementiels de premier ordre.

Les évènements de formation SANS sont particulièrement prisés, car ils permettent d'apprendre, de réseauter et de socialiser avec des pairs, des collègues et le personnel SANS.

Les frais d'inscription incluent des pauses, le déjeuner et des discours en soirée (lorsqu'elles sont prévues), mais n'incluent pas l'hébergement. Les évènements de formation pour la région EMEA se déroulent partout en Europe et dans les régions du Golfe.

Rendez-vous sur SANS www.sans.org/emea pour consulter les dernières mises à jour du calendrier.

SANS Summits

Ces conférences, qui durent un ou deux jours, se présentent sous forme de présentations et de séances plénière animés par des leaders et professionnels reconnus de l'industrie.

Une conférence SANS est une source inestimable d'apprentissage ciblé qui se déroule généralement avant ou après un évènement de formation SANS, et pour laquelle la participation est proposée à un prix réduit pour ceux qui sont inscrits à une des formations proposées durant l'évènement.

SANS Security Awareness Training

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 médicaux et pharmaceutiques.

Des modules en format vidéo dispensent une formation pointue et percutante à un grand nombre de salariés, et produisent des résultats concrets et 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 qui peuvent être mise en pratique dès le retour sur le lieu de travail.

SANS On-Demand

Les cours SANS sont disponibles à tout moment via E-learning. Ils incluent des supports pédagogiques : livres, DVD/Outils logiciels, et quatre mois d'accès à la plateforme SANS OnDemand e-learning. Idéal pour ceux qui souhaitent étudier à leur propre rythme.
www.sans.org/ondemand

SANS Private Training

Une formation en intra dispensée pour les équipes de sécurité d'une organisation, dans une salle de classe, dans des locaux de l'organisation ou dédiés à la formation. La formation sur site est idéale pour les organisations qui ont besoin de former 25 salariés ou plus et/ou qui exigent une confidentialité totale.

La formation en intra permet au formateur SANS de se concentrer sur des sujets particulièrement pertinents pour l'organisation et offre des avantages financiers, notamment liés à l'absence de déplacements et d'hébergement.

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

Bespoke Training Solutions and Cyber Academy

SANS crée des parcours de formation sur mesure pour répondre aux besoins spécifiques des organisations. 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 de 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.

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

Obtenir une **approbation** et un **budget** pour une formation

La forme compte aussi

Formuler une demande officielle

- Une formation constitue un investissement significatif en temps et en argent et si toutes les organisations fonctionnent différemment, la plupart des demandes de formation qui aboutissent ont été formulées par écrit via un document (mémo et/ou présentation Powerpoint) qui explique les besoins et les bénéfices escomptés. Et la majorité des responsables apprécient et valorisent cet effort.
- Fournir toutes les informations nécessaires en une fois. Mettez toutes les chances de votre côté en ajoutant les pages Why SANS?, Plan de formations, la biographie de l'instructeur et les avantages supplémentaires disponibles lors des événements en live ou en ligne.

Les intérêts doivent apparaître clairement

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 gagner en expertise pour un rôle plus spécifique ? Ceux qui prennent la décision doivent comprendre le plan et le contexte au mieux.
- Mettez l'accent sur ce que vous serez en mesure de faire une fois la formation soit terminée. Chaque cours SANS dispose d'une description comprenant – entre autres – une section « Les compétences acquises ». Pensez à l'inclure dans votre demande. Il est important de montrer combien cette formation vous sera utile (voire indispensable) dans votre travail.

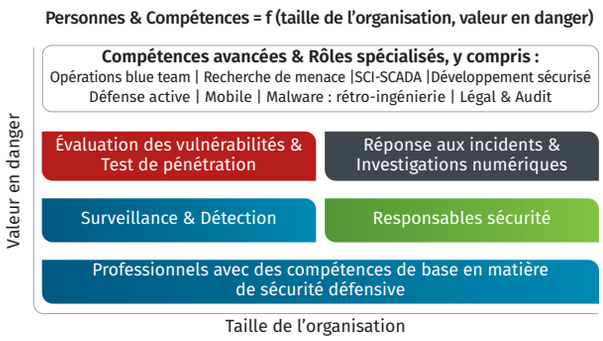
Un contexte bien défini

Construisez des attentes à long terme

- La sécurité de l'information est une spécialisation de carrière en informatique avec des pratiques qui évoluent en fonction des attaques. De ce fait, tout organisme devrait allouer 6 à 10 % des salaires à la veille technologique et à l'amélioration des compétences. 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.
- Passez un examen pour la certification GIAC de façon à valider votre formation. Les employeurs accordent une valeur certaine à cette validation des compétences et des connaissances par la GIAC. Les examens ont été conçus par des experts en psychométrie, de façon à évaluer les capacités d'un individu à réaliser un travail spécifique.
- Envisagez les compromis possibles vis-à-vis de l'investissement. Nombre de professionnels prévoient l'intégration de frais annuels de formation dans leur contrat avant même d'accepter un nouveau poste.

Construire une organisation de sécurité ultra performante

Tout professionnel à qui l'on confie des tâches pratiques, pour assurer la sécurité des systèmes et une défense en profondeur, se doit de posséder un solide tronc commun de compétences. Il doit aussi être en mesure de comprendre le fonctionnement des attaques et savoir gérer les incidents lorsqu'ils se produisent. Il vous faut donc placer haut la barre lorsque vous définissez ce fameux tronc commun de compétences de base.



À mesure que les organisations gagnent en taille, risque et/ou complexité, elles voient apparaître quatre rôles typiques :

- **Professionnels de la surveillance sécurité & détection** - Surveiller et détecter ce qui se passe dans votre environnement nécessite un ensemble de compétences et de capacités de plus en plus sophistiqué. Bien trop souvent, les formations des vendeurs permettent d'apprendre à utiliser un outil et ne vont pas plus loin. Elles n'expliquent pas comment celui-ci fonctionne, ni pourquoi il existe, ni comment le déployer au mieux. Identifier des anomalies de sécurité nécessite une compréhension fine pour déployer les outils de détection et de surveillance, mais aussi pour interpréter les résultats.
- **Analyste test d'intrusion & vulnérabilité** - Un professionnel capable de trouver des faiblesses se distingue souvent de celui qui se concentre exclusivement sur la construction de défense. Véritable principe fondamental du déploiement red team/blue team, la recherche de vulnérabilité requiert une façon de penser et des outils spécifiques. Il s'agit cependant d'une approche essentielle pour améliorer les défenses.
- **Chargé d'investigation numérique & réponse aux incidents** - Qu'il vous faille suivre une série d'indices dans un système de serveurs/réseaux ou que vous cherchiez des menaces qui font appel à des techniques similaires, les grandes organisations ont besoin de professionnels capables d'aller au-delà de la simple gestion primaire des incidents. Dans ce domaine, il convient en effet d'analyser une attaque et de développer aussi bien des mesures appropriées qu'un plan de retour à la normale.
- **Responsables sécurité** - Le nombre de professionnels talentueux augmentant, les organisations ont de plus en plus besoin de chefs d'équipe capables. Ces responsables n'auront pas nécessairement besoin de traiter eux-mêmes certaines tâches, mais ils doivent en savoir suffisamment sur les technologies sous-jacentes et les cadres de travail pour contribuer à l'élaboration des stratégies, développer des règles appropriées, interagir avec des professionnels compétents et prendre la mesure des résultats.

Considérant ces quatre domaines (mais sans s'y limiter), les organisations de haute sécurité auront à former des individus de manière spécifique, l'objectif étant soit que le groupe profite de compétences avancées, soit d'apporter des réponses à des besoins précis. SANS offre plus de 30 cours dans tous les domaines (Défense active à Défense sur le cloud en passant par le Python pour chargés de test de pénétration et Rétro-ingénierie des malwares) afin de former des professionnels pour des rôles spécifiques ou de manière plus poussée sur certains sujets, répondant ainsi à tous les besoins ou presque en matière de sécurité.

Stratégies pratiques pour la formation d'un groupe en cybersécurité, d'après nos recherches et nos observations globales :

Utilisez des principes d'organisation pratique pour élaborer vos plans et gérer vos efforts. La quasi-totalité des cadres de travail les plus complexes peuvent se résumer à des expressions simples. Par exemple : « Construction et maintenance des défenses - Surveillance et détection des intrusions - Auto-évaluation proactive - Répondre aux incidents ».

Définissez vos priorités dans ces domaines en utilisant le **CIS Critical Controls** à mesure que votre organisation grandit.

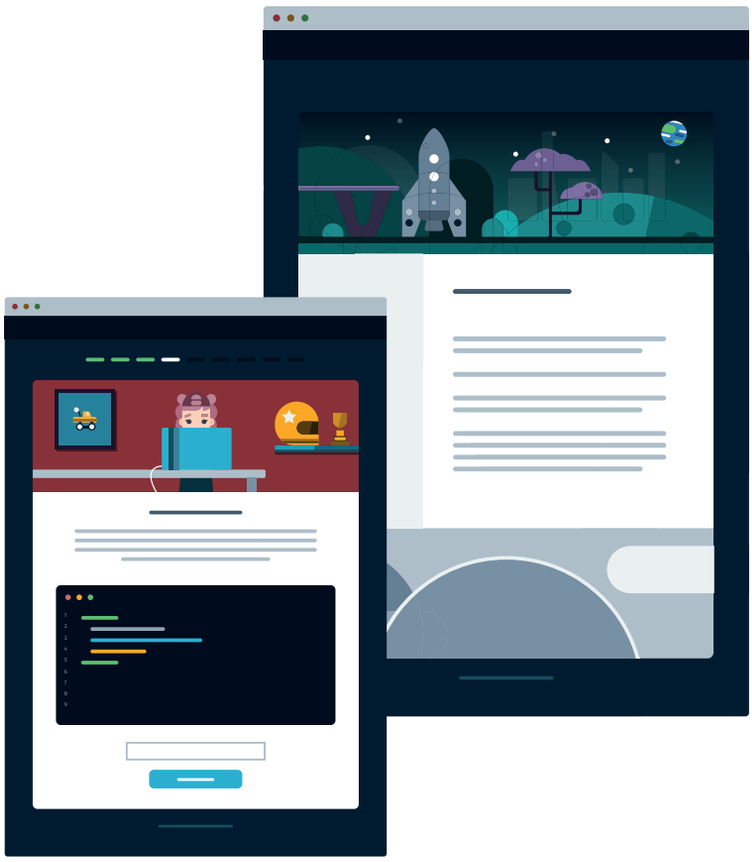
Déterminez le nombre et le type de professionnels dont vous avez besoin pour réaliser les travaux pratiques. **Vous devez initier et maintenir une campagne permanente** visant à développer votre équipe de professionnels afin de réunir les compétences et les capacités nécessaires. La cybersécurité est un champ d'expertise de l'informatique et à ce titre, elle nécessite une formation spécialisée.

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. Cherchant à se protéger contre les cybermenaces, les gouvernements et entreprises doivent pouvoir s'adresser à tout un vivier de professionnels talentueux en cybersécurité. Problème : les personnes compétentes se font rares, partiellement en raison du fait que les jeunes sont peu nombreux à s'engager dans la sécurité informatique.

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 option de carrière attrayante, passionnante et accessible, tout en aidant les organisations gouvernementales à développer leurs capacités nationales en cybersécurité.



L'OFFRE DE CYBERSTART

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

CyberStart Assess : Outil d'évaluation

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

CyberStart Game : Défis en ligne

Avec CyberStart Game, les étudiants endossent le rôle d'un agent de sécurité et doivent rassembler des informations, craquer du code informatique, trouver des failles de sécurité et suivre les pistes numériques de criminels. Les étudiants découvrent de manière ludique des domaines comme Linux, le chiffrement et la programmation.

CyberStart Essentials : Connaissance théorique

CyberStart Essentials, c'est une suite de labos interactifs, de vidéos, d'examens et de quizz, pour acquérir les connaissances théoriques sous-jacentes à des thèmes pointus comme le test d'intrusion et l'interconnexion réseau.

CyberStart Elite : Compétitions

Les événements CyberStart Elite permettent aux étudiants de se rencontrer les uns les autres et de s'affronter dans des compétitions de Capture The Flag. Ce type de rencontre amène les étudiants à travailler en équipe et à utiliser leurs nouvelles compétences en cybersécurité pour relever des défis contre la montre.

QU'EST-CE QUI DISTINGUE CYBERSTART ?

On ne peut pas enseigner à de jeunes gens comme à des adultes. Ce serait prendre le risque 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 en entier.

COMMENT SE LANCER

Le programme CyberStart et ses composants offrent une certaine souplesse et peuvent être adaptés aux besoins individuels des organisations. L'équipe dédiée de SANS travaille en collaboration avec les organisations pour prendre en compte leurs spécificités et garantir qu'elles puissent tirer le plein potentiel du programme CyberStart.

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

LE MANQUE DE COMPÉTENCES EN CYBERSÉCURITÉ

Le manque de compétences en cybersécurité est l'un des principaux enjeux actuels dans le secteur. SANS travaille activement à trouver des solutions, et CyberStart est un produit développé précisément en ce sens.

SANS Cyber Academy est un programme qui identifie, forme, certifie et déploie les nouveaux talents de la cybersécurité. Cyber Academy débute par une évaluation des participants et un test visant à détecter les attributs généralement rencontrés chez les experts de la cybersécurité. SANS fait intervenir des technologies comme sa suite de produits CyberTalent pour identifier les candidats les plus prometteurs.

Les sélectionnés reçoivent ensuite 6 à 8 semaines de formation intensive en cybersécurité, dont le contenu est issu du répertoire de formation SANS. Les étudiants passent également plusieurs Certifications GIAC au cours de la Cyber Academy.

Pour finir, SANS travaille avec des organisations partenaires pour former les diplômés de la Cyber Academy aux fonctions et aux postes vacants en cybersécurité.

D'autre part, SANS est le sponsor fondateur du Cyber Security Challenge UK, une initiative lancée pour encourager et promouvoir le vivier national de talents en cybersécurité. Le programme Challenge propose des compétitions et des sessions conçues pour attirer de nouvelles personnes dans le secteur de la cybersécurité grâce à tout un ensemble d'activités ludiques suscitant l'intérêt pour le domaine. SANS soutient également des programmes similaires en Europe et dans les États arabes du Golfe. Cette démarche s'inscrit dans l'engagement de SANS en matière d'amélioration de la cybersécurité au travers la proposition de formations, le soutien à la communauté et le partage d'informations quant au vivier de professionnels talentueux en cybersécurité, l'objectif ultime étant d'assurer la sécurité des organisations, des employés et des clients.

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

Partenariats et solutions

SANS collabore avec des entreprises et des gouvernements pour élaborer des solutions 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 : le recrutement, l'évaluation du personnel, la sélection des candidats à l'embauche, le développement d'équipe, ou la 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 dispensées sur site. »

Toutes les formations en cybersécurité SANS peuvent être dispensées en privé, au le site d'une entreprise, ou encore dans ses locaux dédiés à la formation. Les formations en milieu privé 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 dirigeants 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, la formation ou la mise à niveau des nouvelles recrues ».

Commencez à discuter avec SANS

Pour un premier entretien avec un Directeur de SANS Institute, contactez SANS via emea@sans.org ou au +44 20 33 84 34 70. Vous pouvez également contacter:

Stephen M Jones

Managing Director UK & Nordics
sjones@sans.org

Ned Baltagi

Managing Director ME & GCC Regions
nbaltagi@sans.org

Jan Pieter Spaans

Managing Director, Mainland Europe
jspaans@sans.org

HMG Cyber Schools Programme

SANS a été selectionné, grâce au fruits de la collaboration d'avec plusieurs partenaires, pour concevoir et diriger le premier programme d'enseignement parascolaire en cybersécurité pour les écoles d'Angleterre. Cyber Discovery est un programme multi phase qui utilise un outil d'évaluation et une plateforme d'apprentissage ludique développée par SANS ainsi que des initiatives en ligne et en face à face pour améliorer les compétences et les connaissances du jeune public en cybersécurité.

Stephen Jones, SANS Managing Director 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 National Cyber Security Strategy du Royaume-Uni et nous espérons grandement voir de plus en plus de jeunes gens envisager la cybersécurité comme future carrière potentielle. Nous évaluons, sélectionnons et formons des étudiants ayant des affinités naturelles pour l'informatique, et ce afin de contribuer à combler le manque de compétences qui existe aujourd'hui partout dans le monde. » Le programme HMG Cyber Schools a été lancé à l'automne 2017 et rejoint l'initiative CyberFirst du gouvernement du Royaume-Uni.

SANS dispose d'une expérience dans la mise en œuvre de programmes de formation similaires auprès d'étudiants dans plusieurs autres pays.

Des formations sur mesure

La formation sur site est idéale pour les organisations qui ont un besoin de former toute une équipe sur un sujet ou un cours spécifique. Cependant, une organisation a souvent besoin de mettre en œuvre un programme de formation sur mesure qui intègre plusieurs des cours SANS.

SANS collabore étroitement avec les organisations, et prend le temps de comprendre leurs besoins spécifiques. Après un processus de consultation initial, une solution de formation unique est élaborée pour répondre à ces besoins - en fonction des cours offerts dans l'ensemble du programme de formation de SANS Cyber Security et les offres complémentaires de SANS.

Nous sommes en particulier à même de vous conseiller, puis de dispenser nous-mêmes les cours.

Évaluation et sélection du candidat

SANS travaille régulièrement avec les entreprises, en les aidant à rationaliser leurs processus et leurs procédures de recrutement.

« Le mode traditionnel de sélection de candidats consiste généralement à filtrer des C.V. » explique Ned Baltagi, Director, SANS ME & GCC Regions. « Les organisations nous confient souvent que cela représente une perte de temps considérable sans pour autant donner des résultats fiables et prévisibles lorsqu'il s'agit de pourvoir à aux postes d'un personnel qui est en première ligne de la cybersécurité. »

SANS CyberTalent est l'un de ces produits de sélection. C'est une suite d'outils d'évaluation qui améliorent l'efficacité d'un processus de recrutement et de sélection pour la cybersécurité.

Les produits SANS CyberTalent utilisent des tests psychométriques et des tests de compétences pour évaluer l'aptitude et les qualités des candidats pour accomplir des missions particulières. Les évaluations en ligne s'appuient sur l'expérience de SANS dans le domaine de la formation en cybersécurité et sur la certification GIAC pour évaluer les compétences et les connaissances techniques.

CyberTalent apporte aux gestionnaires et équipes RH une meilleure compréhension du niveau technique et conceptuel des candidats

Évaluation des forces et des faiblesses de l'équipe

SANS CyberTalent et d'autres solutions sur mesure vont au-delà de la simple sélection de candidats à l'embauche. SANS collabore étroitement avec de nombreuses organisations, pour assurer le développement continu et l'évolution de leurs équipes de sécurité.

« Les équipes de sécurité doivent changer et s'adapter – de nouveaux vecteurs d'attaque émergent, les technologies évoluent et les entreprises elles-mêmes doivent changer » déclare Jan Pieter Spaans. « La formation est une composante intégrale de ce processus de développement...mais les besoins de formation varient d'une équipe à l'autre. En matière de formation, la taille unique, ça n'existe pas. »

Pour aider les responsables à développer et à améliorer leur équipe, SANS fournit des produits d'évaluation tels que SANS NetWars, SANS CyberCity et SANS CyberTalent. Ceux-ci permettent aux responsables de la sécurité et des ressources humaines d'avoir une vision claire des forces et des faiblesses de leurs équipes et des besoins de formation.

SANS élabore ensuite un programme de formation unique qui se concentre sur les besoins d'une équipe ou sur les besoins spécifiques individuels.

Le développement de carrière contribue également à la stabilité du personnel et assure qu'une équipe de sécurité reste efficace. À l'aide de son vaste programme de formations, SANS aide les employeurs à mettre en place des plans de formation sur mesure.

Après un processus initial de consultation, SANS propose des programmes qui répondent aux besoins des entreprises tout en offrant un plan de carrière aux professionnels de la sécurité.

Programmes de formation

SANS a l'expérience des programmes de formation conçus sur mesure pour répondre aux besoins spécifiques d'une organisation — que ce soit pour les gouvernements, les entreprises, ou les institutions militaires — quelles que soient les zones géographiques et les cultures d'entreprise.

Ces programmes varient en taille et en orientation. Sans Cyber Academy est un exemple de l'un de ces programmes de cybersécurité créé par SANS.

« Les programmes de la Cyber Academy identifient, forment et affectent de nouveaux talents de la cybersécurité à des postes clés. Le succès de la Cyber Academy 2015 au Royaume-Uni repose sur la formation experte de personnel de sécurité, qualifié et certifié GIAC, et démontre notre capacité en matière de conception de formation sur mesure » déclare Stephen Jones, SANS Managing Director for UK and Nordics. « Nous allons aussi dispenser un nouveau programme en 2017 : La Cyber Retraining Academy, en partenariat avec HM Government, dans le cadre d'une stratégie initiée par la UK National Cyber Security »

« SANS identifie d'abord des candidats à fort potentiel pour réussir dans le domaine de la cybersécurité. Ces candidats sont ensuite évalués à l'aide de l'outil SANS CyberTalent. »

«Les candidats retenus s'inscrivent ensuite à la Cyber Academy et s'investissent de formation intensif en cybersécurité - dont le contenu est basé sur les cours du répertoire de formations SANS.»

Comme pour la UK Cyber Academy 2015, les diplômés de la Cyber Retraining Academy seront affectés à des postes clés de la cybersécurité.

Cyber Defense Essentials

Tous les professionnels chargés de cybersécurité pratique doivent disposer d'un ensemble commun de compétences permettant de comprendre le fonctionnement des pirates informatiques, de mettre en place des défenses approfondies et d'apporter des réponses en cas d'incident de façon à limiter les risques et sécuriser les systèmes de manière appropriée.

Pour garantir votre sécurité, il vous faut établir une solide base de compétences dans votre organisation. Les cours SANS Cyber Defence Essentials vous permettront d'apprendre à :

- Appliquer des techniques pour résoudre les problèmes de sécurité critiques dans votre organisation
- Établir une base solide de politiques et de pratiques fondamentales afin que vous et vos équipes de sécurité puissiez répondre correctement en cas d'incident
- Déployer tout un panel de stratégies et de techniques de façon à contribuer à la défense globale d'une entreprise
- Identifier les vecteurs d'attaques les plus récents et mettre en place des contrôles pour les prévenir et les détecter
- Utiliser des stratégies et des outils pour détecter les attaques
- Développer des indicateurs de sécurité efficaces formant un ensemble précis que le département informatique peut ensuite mettre en place, que des chargés d'audit peuvent valider et que des responsables peuvent comprendre
- Mettre en place un programme de sécurité complet avec l'accent sur la prévention, la détection et la réponse aux attaques
- Établir une carte de sécurité en interne capable de s'adapter aux besoins futurs

"This training has given me a great overview of everything security related ... showing you such a broad amount of information that you will use to determine security issues you may not have considered before."

— Frank Perrilli, **IESO**

Penetration Testing

Les organisations procèdent à des tests d'intrusion pour découvrir et comprendre les points de vulnérabilité dans leurs systèmes de façon à résoudre les problèmes connus avant que des personnes mal intentionnées n'en profitent.

Les chargés de test d'intrusion doivent suivre l'évolution des cybercriminels et des cyber-attaques, toujours plus sophistiquées. Pour ce faire, ils doivent reproduire des techniques modernes d'attaque dans le monde réel, découvrir les problèmes et dresser des rapports utiles concernant leurs découvertes pour apporter une valeur significative à l'équipe de sécurité.

Les cours SANS Penetration Testing vous permettront d'apprendre à :

- Reproduire aussi bien les attaques communes que les attaques les plus puissantes d'aujourd'hui
- Découvrir les points de vulnérabilité dans les systèmes cibles
- Exploiter les points de vulnérabilité dans des circonstances précises
- Faire preuve d'excellence technique lors de l'identification et de la documentation des risques et de leur impact potentiel sur les activités de l'organisation
- Conduire des tests professionnels et sûrs suivant un cadre et des règles d'engagement soigneusement établis
- Aider une organisation à correctement organiser ses ressources

Les postes de chargé de test d'intrusion

- Chargé de test d'intrusion Système/réseau
- Chargé de test d'intrusion Application
- Chargé d'incident
- Chercheur en vulnérabilité
- Développeur d'exploit

"In one week, my instructor built a bridge from typical vulnerability scanning to the true art of penetration testing. Thank you SANS for making myself and my company much more capable in information security."

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

Incident Response, Threat Hunting and Digital Forensics

Quelle que soit leur taille, toutes les organisations doivent avoir du personnel maîtrisant les techniques de réponse aux incidents de manière à pouvoir identifier correctement les systèmes compromis, à isoler efficacement les brèches de sécurité, et à rapidement remédier aux incidents.

De la même manière, les agences gouvernementales et en charge de faire appliquer la loi nécessitent du personnel compétent pour exploiter le matériel récupéré et collecter des preuves directement dans les systèmes et appareils adverses. Les cours SANS Incident Response, Threat Hunting and Digital Forensics vous permettront d'apprendre à :

- Pister les attaquants avant et pendant un incident dans toute votre entreprise
- Acquérir une connaissance approfondie en investigation numérique des systèmes d'exploitation Microsoft Windows et Apple OSX
- Examiner les téléphones portables, smartphones et autres appareils mobiles en quête de logiciels malveillants et artefacts pertinents
- Incorporer l'investigation réseau à vos connaissances de façon à proposer davantage de découvertes et à accélérer votre travail
- Ne laisser passer aucune piste en incorporant l'investigation mémoire à vos connaissances
- Comprendre les capacités des logiciels malveillants à détourner les renseignements sur les menaces, répondre aux incidents de sécurité informatique, et fortifier les défenses
- Identifier, extraire, prioriser et exploiter les renseignements en cybermenaces à partir d'intrusions de menaces persistantes avancées (APT)
- Reconnaître qu'un chargé de réponse aux incidents bien formé peut constituer la seule et unique défense en cas de brèche

"This training is invaluable to a practitioner! The tools and knowledge that you gain from it is just outstanding!"

— James Tayler, **Context Information Security**

Security Management, Legal, and Audit

Le paysage des menaces évolue et avec lui, la cybersécurité prend toujours plus de valeur pour les organisations. Les chefs d'entreprises sont aujourd'hui bien conscients de la nécessité de sécuriser les actifs informatiques de grandes valeurs et le risque - significatif - qu'ils encourent en cas de brèche ou d'attaque.

De ce fait, les organisations doivent disposer de cadres et de responsables en cybersécurité capables d'associer leurs connaissances techniques à des compétences fondamentales de chef d'équipe, afin de pouvoir diriger des projets, des équipes et des initiatives qui soutiennent les objectifs de l'entreprise.

Ces cours visent à fournir une approche pratique et applicable en matière de gestion du cyber-risque. Son contenu interactif et pratique aide les cadres et responsables (actuels et en devenir) en cybersécurité à grandement améliorer leurs compétences de gestionnaires.

- Développer vos compétences de gestion et de chef d'équipe
- Comprendre et analyser les risques
- Créer une politique de cybersécurité efficace
- Concevoir un programme de gestion des vulnérabilités
- Développer des plans stratégiques de sécurité qui tiennent compte des objectifs de l'activité et de l'organisation
- Susciter l'engagement et communiquer de manière efficace avec les parties prenantes clés
- Mesurer l'impact de votre programme de sécurité
- Sensibiliser votre personnel à l'importance de la cybersécurité et aux moyens d'aider à la protection de l'organisation

"This training applies to all aspects of my job, from network management to project management."

— David Chaulk, **Enbridge**

DevSecOps

L'adoption de DevSecOps a modifié de manière radicale la manière dont les organisations conçoivent, construisent, déploient, sécurisent et exploitent les systèmes modernes.

DevSecOps a permis aux équipes de mettre à jour leurs produits et systèmes bien plus rapidement et plus bien souvent qu'avec les méthodes traditionnelles en associant des processus d'automatisation – historiquement manuels – aux unités de développement et d'exploitation. Pour garantir la sécurité des applications et des produits, les organisations intègrent les tâches de cybersécurité automatisées dans le processus DevOps.

Cette pratique, connue sous le nom de DevSecOps, aide les organisations à construire des applications sûres tout en soutenant une stratégie agile de développement de logiciel. Les cours SANS DevSecOps vous permettront d'apprendre à :

- Intégrer les pratiques et les protocoles de la sécurité dans les opérations de production
- Appliquer des techniques défensives pour empêcher la compromission de votre application
- Utiliser les pratiques DevOps pour améliorer l'état de la cybersécurité
- Comprendre la méthodologie DevSecOps et sa toolchain
- Exploiter les services cloud pour accélérer la mise sur le marché et automatiser les déploiements
- Déployer des mécanismes de défense de manière proactive contre les adversaires et reconnaître les points de vulnérabilités communs en matière de sécurité dans les applications web

"Mind-blowing! If you are a traditional security architect, tip-toeing around DevOps, attend SEC540. It takes you into into the depths of DevSecOps and sets you up for the future!"
— Jatin Sachdeva, **CISCO**

DEV 522 **Defending Web Applications Security Essentials**

PAGE 66

Industrial Control Systems

Le paysage actuel présente un ensemble varié et chaotique de menaces pesant sur les propriétaires et exploitants de systèmes de contrôles industriels.

Les attaques qui entraînent des dégâts physiques ou qui impactent les processus physiques ne sont désormais plus théoriques ou de simples objets de spéculations. Nous assistons aujourd'hui à des incidents au cours desquels des acteurs malveillants parviennent à pénétrer dans des systèmes, à les endommager et à impacter les activités grâce à des logiciels malveillants spécifiquement conçus pour les ICS. Nous devons être prêts à défendre nos systèmes de contrôle contre des adversaires toujours plus astucieux et sophistiqués.

Les cours SANS Industrial Control Systems Security vous apprendront à :

- Reconnaître les éléments, les objectifs et les déploiements d'ICS, ainsi que les drivers importants et les contraintes associées
- Identifier les actifs ICS et leurs topologies réseaux, et comment contrôler les points critiques d'ICS en quête d'anomalies et de menaces
- Comprendre les approches des architectures et techniques de défenses systèmes et réseaux
- Mener une réponse aux incidents ICS axée sur les opérations de sécurité, avec la priorité sur la sécurité et la fiabilité des opérations
- Mettre en place des contrôles d'accès virtuel et physique efficaces

"The training starts with theory and quickly progresses into full hands-on interaction with all components. This experience is not easy to find."

– Bassem Hemida, **Deloitte**

SANS

Cyber Security Summits

Chez SANS, nous nous sommes fixé pour mission de partager la connaissance avec tous ceux qui sont désireux d'apprendre, et ce afin de rendre le monde plus sûr. **Et cela commence avec vous.**

Venez vous former avec les experts des différents secteurs lors des SANS Summits et profitez-en pour établir des relations avec vos pairs et vous inspirer des bonnes pratiques directement sur le terrain.

8 JUN, 2020
ICS Europe
MUNICH

20 JUI, 2020
Pen Test HackFest Europe
BERLIN

4 OCT, 2020
DFIR Europe
PRAGUE

26 OCT, 2020
Purple Team Europe
AMSTERDAM

29 NOV, 2020
Sec Ops Europe
LONDRES

Pour rester au courant des événements SANS, rendez-vous sur **www.sans.org/emea**

SEC 301

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Introduction to Cyber Security

Pour déterminer si le cours SANS SEC301 est adapté à vos besoins, posez-vous cinq questions simples :

- Êtes-vous nouveau dans le domaine de la sécurité informatique, et bien que vous disposiez de connaissances informatiques de base, avez-vous besoin d'une introduction aux fondamentaux ?
- Êtes-vous assaillis par des termes techniques complexes que vous ne comprenez pas ?
- Êtes-vous un cadre dirigeant, autre qu'un responsable de sécurité informatique (avec quelques connaissances techniques) qui se réveille la nuit, angoissé à l'idée que votre entreprise pourrait faire l'objet d'un piratage massif et faire la une du journal de 20 heures ?
- Avez-vous besoin d'être familier avec les concepts de base, les concepts et le jargon de la sécurité, même si vous n'avez pas besoin de rentrer dans les détails?
- Avez-vous décidé de changer de carrière pour tirer parti des possibilités d'emploi dans la sécurité de l'information et pour ce faire, vous faut-il une formation et une certification?

Si vous répondez oui à l'une de ces questions, le cours SEC301 est idéal.. Nos connaissances et notre enseignement dispensé par de véritables experts de la sécurité reconnus mondialement, sur des sujets fondamentaux pour la sécurité de l'information, vous donneront une longueur d'avance. Ce cours complet et entièrement actualisé de cinq jours couvre tout, de la terminologie essentielle aux bases des réseaux informatiques, politiques de sécurité, gestion des incidents, mots de passe, et même une introduction aux principes cryptographiques.

Ce cours est conçu pour les étudiants qui ont une connaissance de base des ordinateurs et de la technologie, mais aucune connaissance préalable de la cybersécurité. Notre approche pédagogique pragmatique, vous permettra, étape par étape, de comprendre toutes les informations présentées, même si certains des sujets sont nouveaux pour vous. Vous apprendrez les principes fondamentaux de la sécurité de l'information qui serviront de base à vos compétences et connaissances en matière de sécurité de l'information pour les années à venir.

"I very much appreciate the passion of the instructors. Their knowledge is incredible and the presentation of their knowledge is down-to-earth and helpful. SANS training is far better than privacy-related certification."

Ron Hoffman,
MUTUAL OF OMAHA

Public visé :

- Tout novice en cybersécurité qui cherche une initiation aux fondamentaux de la sécurité
- Tous ceux qui se sentent démunis face à une avalanche de termes techniques complexes dont la signification leur échappe
- Les responsables sécurité non informatique qui traitent des problèmes techniques, qui les comprennent et qui s'inquiètent de voir leur entreprise victime d'un piratage massif au point que la perspective de faire la une du journal de 20 heures les empêche de dormir
- Les professionnels ayant des connaissances informatiques et techniques de base qui ont besoin de se familiariser avec les concepts, principes et jargons généraux, sans pour autant avoir besoin de rentrer dans le détail
- Les professionnels qui décident de changer de carrière pour tirer parti des possibilités d'emploi dans la cybersécurité et qui ont besoin d'une formation et d'une certification reconnues

Vous apprendrez à..

- Communiquer avec confiance sur divers sujets concernant sécurité de l'information, les termes et les concepts.
- Comprendre et appliquer les principes de moindre privilège
- Comprendre et appliquer la triade Confidentiality, Integrity, Availability (CIA)
- 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
- Avoir une compréhension fondamentale d'un certain nombre d'acronymes techniques clés de réseau tels que TCP / IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, et DNS
- Utiliser des outils intégrés de Windows pour voir vos paramètres réseau
- celle-ci peut renforcer la cybersécurité

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

SEC 401

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Security Essentials Bootcamp Style

Ce cours abordera avec vous les méthodes les plus efficaces pour prévenir une attaque et détecter les intrusions avec des techniques exploitables que vous pouvez utiliser directement une fois de retour au bureau. Vous recevrez des conseils et des astuces de la part d'experts de façon à remporter le combat contre les nombreux cyber ennemis qui cherchent à pénétrer et endommager votre environnement.

ARRÊTEZ-vous et demandez-vous :

- Est-ce que vous comprenez réellement pourquoi certaines organisations se retrouvent compromises et d'autres non ?
- Êtes-vous sûr de pouvoir trouver les systèmes compromis dans votre réseau s'il y en a ?
- Connaissez-vous l'efficacité de chaque appareil de sécurité et êtes-vous sûr qu'ils sont tous configurés correctement ?
- Est-ce que des indicateurs de sécurité adaptés ont été définis et communiqués à vos responsables pour qu'ils puissent prendre les bonnes décisions en matière de sécurité ?

> **"It is making me question my own beliefs. I will be challenging colleagues and strategies when I return to work. The course is full of logical, workable solutions."**
> Anthony Usher
> *HMRC*

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

Le cours SEC401: Security Essentials Bootcamp Style vise à vous enseigner les compétences et techniques fondamentales de cybersécurité dont vous avez besoin pour protéger et sécuriser les ressources informatiques clés et les systèmes de votre organisation. Et bien sûr, notre formation vous montrera comment faire pour éviter de voir votre entreprise comptée au nombre 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. Défendre contre les cyberattaques est un défi permanent, avec de nouvelles menaces qui font sans cesse leur apparition et les développements dont elles font l'objet. Les organisations doivent comprendre quelles sont les méthodes efficaces en matière de cybersécurité. Ce qui a marché par le passé et ce qui marchera toujours, c'est adopter une approche basée sur le risque. Il convient de répondre à trois questions avant de dépenser le moindre euro dans un budget informatique et avant d'allouer du temps et des ressources au nom de 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 vous assurer que vous intervenez 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 obtiendrez les connaissances fondamentales mais efficaces dont vous avez besoin si une organisation vous confie la responsabilité de sécuriser ses systèmes. Ce cours tient les deux promesses que SANS fait à ses étudiants : 1), vous développerez des compétences de pointe que vous pourrez immédiatement mettre en pratique une fois de retour au bureau et 2) vous suivrez l'enseignement des meilleurs formateurs dans le domaine de la sécurité.

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

Public visé :

- Les professionnels de la sécurité qui veulent combler des lacunes dans leur compréhension de la sécurité des systèmes d'information
- Les responsables qui veulent acquérir une compréhension de la sécurité
- Le 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
- Les ingénieurs IT et les superviseurs qui ont besoin de construire un réseau défendable
- Les administrateurs chargés de la construction et de l'entretien des systèmes ciblés par des attaquants
- Les spécialistes de l'inforensique, les testeurs d'intrusion, et les auditeurs qui ont besoin les fondamentaux de la sécurité pour être aussi performants que possible
- Toute personne nouvelle dans le domaine de la sécurité informatique ayant une certaine expérience des systèmes d'information et des réseaux

Vous apprendrez à...

- Concevoir et construire une architecture de réseau à l'aide de VLAN, NAC et 802.1x basée sur un indicateur de compromis APT
- 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 Linux (ps, ls, netstat, etc.) pour automatiser le fonctionnement de programmes et effectuer une surveillance continue de divers outils
- Installer VMWare pour créer un laboratoire virtuel dans lequel vous pourrez 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 contrôles pour valider la sécurité, créer des métriques alliant formation et sensibilisation.
- Identifier les faiblesses visibles d'un système en utilisant différents outils (dont dumpsec and OpenVAS) et une fois les vulnérabilités identifiées, déterminer comment configurer le système pour le faire gagner en sécurité

SEC 450

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Blue Team Fundamentals: Security Operations and Analysis | NOUVEAU

Votre entreprise recherche-t-elle un moyen rapide et efficace d'intégrer de nouveaux analystes, ingénieurs et architectes spécialisés en sécurité ? Les gestionnaires de votre centre des opérations de sécurité (SOC) ont-ils besoin d'acquérir des compétences techniques supplémentaires pour améliorer la qualité des analyses, réduire les changements d'équipe et administrer un SOC efficace ?
Le SEC450 est une formation accélérée sur le terrain conçue pour les nouveaux membres des équipes de cyberdéfense et les responsables de SOC. Ce cours présente aux stagiaires les outils communs aux environnements de travail des défenseurs et regroupe toutes les explications essentielles concernant les outils, processus et flux de données administrés par tous les membres des forces régulières, ou « Blue Team ».
Les stagiaires apprendront les différentes étapes qui composent les opérations de sécurité : mode de collecte des données, lieu de collecte et méthodes d'identification des menaces à l'intérieur de ces données. Le cours présente de façon approfondie les tactiques de tri et d'investigation des événements identifiés comme malveillants, ainsi que les moyens d'éviter les erreurs communes et de produire des analyses continues de haute qualité. Les stagiaires apprendront le fonctionnement interne des protocoles les plus connus, ainsi que la manière d'identifier les fichiers infectés et les attaques visant les hôtes et données sur leur réseau.

Ce cours s'appuie sur des instructions pratiques et concrètes déployées dans une simulation d'environnement de SOC, au moyen d'un kit d'outils réels entièrement intégré tels que :

- Gestion des informations et événements de sécurité (SIEM)
- Système de suivi et de gestion des incidents
- Plateforme de renseignement sur les menaces
- Interception et analyse de paquets
- Outils d'automatisation

Alors que le monde de la cyberdéfense laisse entrevoir des carrières passionnantes et riches en défis, de nombreux SOC pâtissent d'un nombre élevé de remplacements de postes. Afin de résoudre ce problème de manière préventive, la formation cours présente des informations étayées par des recherches relatives à la prévention du burn-out et au maintien de la motivation grâce la croissance continue, l'automatisation et la réduction des faux positifs. Les stagiaires achèveront leur formation par une vision intégrale englobant les modes de collecte et de détection, l'utilisation et la coordination des outils SOC, ainsi que le maintien opérationnel de leur SOC sur le long terme..

" Visualizing logs and understanding how they go to SIEM was super helpful, especially for someone about to become a SIEM admin. Malware Analysis portion was fantastic for analysts at every level."
Tony Dinkel
Aires

Public visé : ?

- Analystes de la sécurité
- Enquêteurs sur les incidents
- Ingénieurs et architectes spécialisés en sécurité
- Responsables techniques de la sécurité
- Gestionnaires de centre des opérations de sécurité (SOC) souhaitant acquérir des compétences techniques supplémentaires pour améliorer la qualité des analyses, réduire les changements d'équipe et administrer un SOC efficace
- Toute personne souhaitant débuter sa carrière au sein d'un Blue Team

36 CRÉDITS CPE/CMU

SEC 487

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 mettons à jours au quotidien accumulent des quantités incroyables de données personnelles et potentiellement incriminantes. Les citoyens, les gouvernements et les entreprises, avec l'aide d'un professionnel, peuvent se servir de ces informations pour solutionner des questions financières, des problèmes financiers, et voire des affaires criminelles.

Le cours SEC487 enseigne aux stagiares des méthodes légitimes et efficaces qui permettent de trouver, rassembler et analyser ces données. Vous apprendrez à appliquer des méthodes et à utiliser des outils manuels et automatiques pour récupérer ces données là où elles sont stockées à coup sûr. Une fois les données rassemblées, nous vous montrerons comment les analyser et garantir l'absence d'anomalie pour ensuite mener sereinement vos investigations.

Il s'agit ici d'un cours fondamental en renseignement d'origine source ouverte (open source intelligence, OSINT en anglais) et à ce titre, vous aborderez rapidement de nombreux domaines. Ce cours vous fera apprendre les compétences et les techniques modernes et concrètes (avec les outils qui vont avec) que les forces de l'ordre, les enquêteurs privés, les pirates informatiques et les cyberdéfenseurs utilisent pour rassembler des quantités phénoménales d'informations sur Internet pour en analyser ensuite les résultats et s'appuyer sur certains jeux de données intéressants pour découvrir de nouveaux domaines d'investigation. Notre objectif est de fournir les connaissances de base en OSINT aux étudiants pour qu'ils réussissent dans leur domaine, et ce que vous soyez professionnel de la défense informatique, analyste renseignements et menaces, enquêteur privé, enquêteur spécialisé en assurance, analyste renseignements, gardien des forces de l'ordre ou simple curieux en la matière.

Les stagiares participent tout au long de la semaine à de nombreux laboratoires pratiques afin d'aborder les outils et les techniques de base de la collecte de données libres sur Internet. Les 20 labos de ce cours vous feront évoluer aussi bien sur Internet que dans les profondeurs du darknet pour que vous gagniez en assurance. Une fois ce cours terminé, non seulement vous saurez comment utiliser des fonctions de recherche sur un site web, mais vous connaîtrez également la totalité des scénarios et leurs critères ainsi que les techniques OSINT nécessaires pour rassembler les données OSINT qui vous intéressent vraiment.

Public visé :

- Chargés de réponse aux cyber incidents
- Analystes inforensique
- Chargés de test d'intrusion
- Ingénieurs sociaux
- Forces de l'ordre
- Personnel des services de renseignement
- Recruteurs/Sources
- Enquêteurs privés
- Chargés d'enquête en assurance
- Personnel des ressources humaines
- Chercheurs

Vous apprendrez à..

- Comprendre le cycle de vie de la collecte de données
- Créer une plateforme sécurisée pour la collecte de données
- Analyser les besoins du client
- Capturer et enregistrer des données
- Créer des comptes leurres
- Créer votre propre processus OSINT
- Collecter des données internet
- Effectuer des recherches pour des individus
- Accéder aux données des réseaux sociaux
- Évaluer un emplacement à distance en utilisant des caméras en ligne et des cartes.
- Examiner des réseaux sociaux géolocalisés
- Recherche des sociétés
- Utiliser les données fournies par le gouvernement
- Collecter des données à partir du Dark Web
- Exploiter des sites internationaux et des outils

36 CRÉDITS CPE/CMU

SANS TRAINING CATALOGUE

SEC 501

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 s'avèrent néfastes à la réputation.

SEC501: Advanced Security Essentials – Enterprise Defender construit de solides fondations en matière de règles et pratiques de base afin de permettre aux équipes de sécurité de défendre correctement leurs entreprises.

Il y a un dicton dans l'univers de la sécurité : « La prévention est idéale, mais la détection est un must. » Mais détecter sans réagir ne sert à rien. La sécurité réseau doit faire l'objet d'une amélioration constante de façon à pouvoir prévenir autant d'attaques que possible, mais aussi pour détecter rapidement les éventuelles 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, appareil mobile...).

Mais tous les efforts du monde ne peuvent garantir une défense et une protection absolues, et 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 a été détectée, il est indispensable de réagir rapidement et de réaliser des investigations numériques en conséquence. Comprendre les agissements d'un attaquant permet de tirer des leçons qui pourront servir à renforcer les mesures de défense, de prévention et de détection, et compléter ainsi le cycle de la sécurité.

"By far the best course I have ever attended. Every day I have learnt things that can be applied at work"

Stuart Long,
BANK OF ENGLAND

"Great course content very interesting and comprehensive."

John O'brien,
AIRBUS DEFENCE & SPACE

Public visé :

- Les testeurs d'intrusion et personnes chargées de répondre aux incidents
- Les analystes et ingénieurs des centres opérationnels
- Les 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
- Éffectuer des tests d'intrusion contre une organisation afin de déterminer les vulnérabilités et les points de compromis.
- Appliquer le processus en six étapes de gestion d'incident
- Utiliser divers outils pour identifier et remédier aux malwares dans toute l'organisation
- 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

GIAC CERT: GCED
36 CPE/CMU CREDITS
WWW.GIAC.ORG/GCED

SEC 503

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

Intrusion Detection In-Depth

Les cas d'organisations importantes ayant fait l'objet de piratage et dont la réputation a grandement souffert font désormais partie du quotidien. Comment faire pour que votre société ne soit pas la prochaine victime d'une cyberattaque majeure ?

Préserver la sécurité de votre organisation est aujourd'hui plus difficile que jamais dans un monde où la cybermenace est omniprésente. Le paysage de la sécurité évolue constamment. L'époque du simple périmètre de protection fait désormais place à la protection des systèmes exposés et des appareils mobiles, des cibles connectées en permanence ou presque et parfois vulnérables. Le personnel de sécurité en mesure de détecter et prévenir les intrusions est en conséquence particulièrement recherché. Notre objectif avec le cours SEC503: Intrusion Detection In-Depth est de vous faire acquérir les connaissances fondamentales, les outils et les techniques dont vous avez besoin pour défendre votre réseau. Cette formation vous prépare à utiliser vos nouvelles compétences et connaissances immédiatement à votre retour dans votre environnement de travail.

Comme le disait Mark Twain, « Il est plus facile de tromper les gens que de les convaincre qu'ils ont été trompés. » Trop nombreuses sont les solutions IDS/IPS qui se contentent de proposer une simple évaluation rouge/vert ou bon/mauvais du trafic et trop nombreux sont les analystes sans formation qui acceptent ces résultats comme vérité absolue. Ce cours vise à faire comprendre qu'un analyste correctement formé se servira d'une alerte IDS comme point de départ à une évaluation du trafic et ne la considérera pas comme évaluation finale. Le module SEC503 a pour philosophie qu'un analyste doit pouvoir accéder et examiner les alertes afin de pouvoir leur donner du sens 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 à ne pas prendre en compte.

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 afin de vous permettre d'appliquer immédiatement vos acquis. Ces exercices de base incluent des astuces fonctionnelles tandis que les options avancées offrent un défi plus important pour les étudiants qui connaissent déjà le contenu du cours ou qui l'ont rapidement maîtrisé.

"In order to defend a network you need to understand how it works, this course is both enjoyable and challenging"

Holly C
MOD UK

Public visé :

- Analystes de détection d'intrusion
- Ingénieurs réseau
- Administrateurs système, sécurité, et réseau
- Responsables de la sécurité en première ligne

Vous apprendrez à...

- Configurer et exécuter open source Snort et écrire des signatures Snort
- Configurer et exécuter 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 de réseau pour enquêter sur le trafic, identifier et enquêter sur une possible intrusion
- Utiliser Wireshark pour détacher des pièces jointes suspectes
- Écrire des filtres tcpdump pour examiner de façon sélective un caractère particulier du trafic
- Synthétiser des fichiers journaux disparates afin d'élargir l'analyse
- 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 de réseau et du matériel pour customiser les senseurs IDS
- Intercepter le traffic du réseau (sniff traffic off the wire)

"I loved the course. I had big expectations, because I have also taken the 401 security essentials course and it was amazing too. All my expectations have been completed. I had great classmates and we had a lot of fun during the day and the evenings."

Diana Moldovan
BETFAIR

GIAC CERTIFIED INTRUSION ANALYST — GCIA

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

SEC 504

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Hacker Tools, Techniques, Exploits, and Incident Handling

Internet est rempli de puissants outils de piratage et de personnes mal intentionnées prêtes à s'en servir sans vergogne. Si votre organisation dispose d'une connexion à Internet et d'un ou deux employés 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 furtivité. Les coups de sonde par cinq, dix ou même cent contre votre infrastructure informatique et la personne malveillante en interne qui fait tranquillement mais sûrement son chemin dans vos installations numériques n'en sont que quelques exemples. En tant que défenseurs, il est indispensable de nous familiariser au mieux avec ces outils et ces techniques de hacking.

Ce cours vous permettra de renverser 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. Au cours de cette formation, 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 se contenter d'enseigner quelques astuces de pirate, ce cours apporte un processus éprouvé et pas à pas permettant de répondre aux incidents informatiques. Il fournit également une description détaillée des méthodes que les hackeurs utilisent pour affaiblir un système, et ce afin que vous puissiez vous préparer en conséquence. Ou le cas échéant, les détecter et 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 les systèmes de scan, d'exploitation et de défense. Ce cours vous permettra de découvrir les failles dans votre système avant vos adversaires !

Il conviendra tout particulièrement aux individus qui dirigent ou qui font partie d'une équipe de gestion des incidents. Les professionnels de la sécurité générale, les administrateurs systèmes et les architectes sécurité profiteront de cet enseignement en approfondissant leurs connaissances au niveau de la conception, de l'élaboration et du fonctionnement de leurs systèmes afin de prévenir, détecter et répondre aux attaques.

> **"Very structured and well prepared course. Interesting and engaging for people new to the field as well as experienced professionals"**
> Ewe konkolska
> *PRUDENTIAL*

Public visé :

- Chargés d'incident
- Chef d'équipe 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 lors de l'attaque d'un système

Vous apprendrez à...

- Analyser la structure des techniques d'attaque courantes pour évaluer la portée de l'attaquant sur un système ou réseau, anticiper et éviter d'autres attaques
- Utiliser des outils et des preuves pour déterminer le type de malware utilisé dans une attaque (notamment les rootkits, portes dérobées et chevaux de Troie) et pour choisir les modes de défense et les tactiques de réponse appropriés, selon le cas.
- Utiliser des outils en ligne de commande intégrés tels que Windows tasklist, wmic et reg, ainsi que Linux netstat, ps et lsof pour détecter la présence d'un assaillant sur une machine.
- Analyser les tables ARP du routeur et du système ainsi que les tables CAM de switch pour suivre les activités d'un assaillant sur un réseau et identifier un suspect.
- Utiliser des mémoires dump et l'outil Volatility pour identifier les activités d'un assaillant sur une machine, le type de malware installé et autres machines utilisées par un assaillant comme pivots sur le réseau.
- Accéder à une machine cible à l'aide de Metasploit, détecter des artefacts et l'impact du piratage par l'analyse des processus, des fichiers, de la mémoire et des registres.
- Analyser un système pour comprendre comment les assaillants déplacent des fichiers, créent des portes dérobées et mettent en place des relais dans un environnement cible à l'aide de Netcat.

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

SEC 505

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Securing Windows and PowerShell Automation | NOUVEAU

Les hackeurs savent comment utiliser PowerShell pour leurs activités malveillantes. Mais vous, savez-vous en servir pour la bonne cause ? Le cours SEC505 vous apprendra à utiliser PowerShell et à renforcer la sécurité de Windows en même temps. SecOps nécessite une automatisation et l'automatisation sur Windows implique PowerShell.

Vous avez lancé un scan de vulnérabilité et appliquer des correctifs. Et maintenant ? Un des principaux thèmes de ce cours est la conception défensive : il faut partir du principe qu'il y aura des brèches et il convient donc d'anticiper la gestion des dégâts dès le début de la conception. Une réponse aux incidents au cas par cas, par à-coup, ne peut constituer la seule stratégie de défense, sans quoi l'adversaire garde systématiquement l'initiative et donc l'avantage. Le temps que votre système de surveillance vous informe qu'un compte Administrateur de domaine a été corrompu, IL EST TROP TARD.

Fort de ce constat, il convient de sélectionner consciencieusement les privilèges administratifs à accorder pour que les dégâts ne soient pas catastrophiques dans l'éventualité d'un compte administrateur compromis. La gestion des privilèges administratifs est un problème épineux et en raison de l'aspect critique qu'il revêt, ce cours lui accorde une journée entière.

> **"I have been to other windows training, but never one with a focus on security. Has been an eye-opening experience. I hope to attend more events like this in the future.."**
>
> Dewayne Wasson, *KELLOGG COMPANY*

L'apprentissage de PowerShell s'avère également utile à un autre type de sécurité : un poste dans la sécurité. Les personnes qui maîtrisent ces compétences sont activement recherchées. Nul besoin d'avoir des connaissances en PowerShell pour suivre ce cours : nous verrons tout cela ensemble. Près de la moitié des labos de la semaine abordent PowerShell et le reste permet de découvrir des outils de sécurité graphiques.

PowerShell est un logiciel open-source gratuit et qui est aussi compatible avec Linux et Mac OS. Il ne s'agit pas avec ce cours de vous convaincre d'acheter une nouvelle application de sécurité ou d'installer un énième agent terminal. L'idée ici est d'utiliser les outils de sécurité intégrés à Windows et dans Active Directory lorsque c'est possible, de faire intervenir des outils gratuits lorsque ce n'est pas le cas (en particulier PowerShell et Group Policy) et de n'acheter des produits commerciaux que lorsqu'il n'est absolument pas possible de faire autrement.

Si vous êtes responsable informatique ou DSI, vous pouvez vous attendre à avoir rentabilisé ce cours au moins 10 fois dans les deux prochaines années : eh oui, SecOps et DevOps ne sont pas les seuls à profiter de l'automatisation, votre budget aussi.

Ce cours s'adresse aux ingénieurs systèmes, architectes de sécurité et au personnel des équipes d'Opérations de sécurité (SecOps). Il aborde principalement l'automatisation des 10 procédés de mitigation de la NSA et les Contrôles critiques de sécurité CIS en lien avec Windows, en particulier ceux qui s'avèrent difficiles à mettre en œuvre dans des environnements de grande taille. C'est un cours ludique qui bénéficie à tous, même aux administrateurs Windows qui ont des années d'expérience derrière eux. Nous n'abordons pas la gestion des correctifs, l'octroi de permission ni les autres bases - l'objectif est d'aller bien au-delà. Venez apprendre à utiliser PowerShell et à développer une sécurité Windows des plus agiles dans un environnement ludique et stimulant.

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

Public visé :

- Toute personne qui veut apprendre PowerShell
- Les ingénieurs sécurité Windows et les administrateurs systèmes
- Toute personne chargée de l'implémentation de contrôles de sécurité critiques
- Ceux qui doivent appliquer des politiques de sécurité sur les hôtes Windows
- Ceux qui déploient ou gèrent les smart cards ou PKI
- Toute personne ayant besoin de réduire le nombre d'infections dues à des malwares APT

Vous apprendrez à...

- Exécuter des commandes PowerShell sur des systèmes à distance et écrire vos propres scripts PowerShell
- Renforcer PowerShell lui-même contre des abus et activer l'enregistrement de la transcription
- Utiliser Group Policy pour exécuter des scripts PowerShell sur un nombre quasiment illimité d'hébergeurs tout en utilisant des permissions Group Policy Object, des unités organisationnelles et la Windows Management Instrumentation (WMI) pour ne cibler que les systèmes qui ont besoin d'un script actif
- Utiliser la Desired State Configuration (DSC) de PowerShell et le script Server Manager pour l'automatisation SecOps/DevOps du renforcement serveur
- Partant du principe qu'une brèche aura lieu, utiliser Group Policy et PowerShell pour accorder des privilèges administratifs de manière à réduire les dommages en cas d'attaque réussie
- Configurer PowerShell remoting pour utiliser les règles Just Enough Admin (JEA) afin de créer une version Windows de Linux sudo et setuid root
- Configurer des limitations contre des attaques comme les pass-the-hash, Kerberos golden tickets, Remote Desktop Protocol (RDP) man-in-the-middle, abus de Security Access Token et autre
- Utiliser PowerShell et Group Policy pour gérer le Microsoft Enhanced Mitigation Experience Toolkit (EMET), les règles de whitelisting AppLocker, les templates de sécurité INF, les règles de pare-feu Windows, les règles IPSec et bien d'autres paramètres de sécurité

SEC 506

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Securing Linux/Unix

SEC506: Securing Linux/Unix aborde en profondeur les problèmes de sécurité de Linux et Unix. Cette formation propose également des guides de configuration spécifiques et des exemples pratiques concrets ainsi que des trucs et astuces. Ce cours aborde la manière de réduire ou d'éliminer les problèmes généraux qui s'appliquent à tous les systèmes d'exploitation Unix et similaires, y compris les vulnérabilités dans le système d'authentification mot de passe, les fichiers systèmes, les systèmes de mémoire virtuelle et les applications communes sur Linux et Unix.

Ces cours vous apprendront à utiliser des outils disponibles gratuitement pour gérer les problèmes de sécurité (SSH, AIDE, sudo, lsof, et bien d'autres). L'approche pratique de SANS fait intervenir des exercices quotidiens pour s'assurer que vous êtes capables d'utiliser ces outils dès votre retour au travail. Nous mettrons également ces outils à profit dans un module spécial qui couvre des techniques simples d'investigation pour effectuer des recherches dans des systèmes compromis.

Thèmes
- Attaques mémoire, Buffer Overflows
- Attaques fichiers systèmes, Conditions race
- Programmes et rootkits pour chevaux de Troie
- Outils de surveillance et d'alerte
- Audit Connexion et noyau Unix
- Construire une infrastructure de rapports centralisées
- Outils de sécurité réseau
- SSH pour une administration sécurisée
- Blocage serveur pour Linux et Unix
- Contrôler l'accès racine avec sudo
- SELinux et chroot() pour la sécurité applicative
- DDNSSEC Déploiment et automatisation
- Pare-feux mod_security et Web Application
- Configuration sécurisée de BIND, Sendmail, Apache
- Investigation numérique des systèmes Linux

> **"I have been a unix systems administrator for a couple of decades, but in SEC506 I learned something new every day"**
> Sheryl Coppenger, *NCI INC.*

Le mot de l'auteur du cours

Un sage a dit un jour : « Comment allez-vous apprendre quoi que ce soit si vous savez déjà tout ? » Il semble pourtant y avoir une forme d'arrogance silencieuse dans la communauté Unix qui prétend avoir identifié et réglé la totalité des problèmes de sécurité de leur système d'exploitation à coup de « je suis allé là, j'ai fait ça. » En ce qui me concerne, je poursuis l'aventure Unix – et plus particulièrement dans le domaine de la sécurité – précisément parce qu'il y a toujours quelque chose de nouveau à apprendre, à découvrir ou à inventer. Si j'ai bien appris une chose en 20 ans d'expérience, c'est combien il me reste encore à apprendre. Et je crois que c'est également valable pour les stagiaires qui suivent mes cours. J'entends régulièrement des commentaires des stagiaires qui disent « ça fait ving ans que j'utilise Unix, mais ça ne m'a pas empêché de beaucoup apprendre au cours de cette formation. » C'est très gratifiant.

- Hal Pomeranz

Public visé :
- Professionnels de la sécurité qui souhaitent apprendre les bases pour sécuriser les systèmes d'exploitation Unix
- Administrateurs expérimentés qui cherchent à connaître en détail les mécanismes d'attaque sur systèmes Unix et comment prévenir ces attaques
- Administrateurs qui souhaitent apprendre à sécuriser des applications internet classiques sur plateforme Unix
- Chargés d'audit, de réponse aux incidents et autres analystes en sécurité de l'information qui cherchent à mieux comprendre les outils de sécurité, les procédures et les bonnes pratiques sur Linux et Unix.

Vous apprendrez à...
- Réduire de manière significative le nombre de points faibles dans les systèmes Linux/Unix classiques en désactivant les services non nécessaires
- Protéger vos systèmes contre les Buffer Overflows, dénis de service et attaques physiques en exploitant les paramètres de configuration de l'OS
- Configurer des pare-feux hébergés pour bloquer les attaques en provenance de l'extérieur
- Déployer SSH pour protéger les sessions administratives et exploiter les fonctionnalités de SSH pour automatiser de manière sécurisée des tâches administratives de routine
- Utiliser sudo pour contrôler et surveiller les accès administratifs
- Créer une infrastructure de rapports centralisées avec Syslog-NG et déployer des outils de surveillance connexion pour rechercher les événements significatifs
- Utiliser SELinux pour isoler de manière efficace les applications compromises et les empêcher d'endommager les autres services systèmes
- Configurer de manière sécurisée les applications classiques connectées à Internet comme Apache et BIND
- Mener des investigations sur des systèmes Linux/Unix compromis avec Sleuthkit, Isof et d'autres outils open-source
- Comprendre les rootkits des attaquants et comment les détecter avec AIDE et rkhunter/chkrootkit

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

SEC 511

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, mais cela n'empêche pas certaines de connaître des brèches et des intrusions en dépit de tous leurs efforts. L'approche traditionnelle de l'architecture sécurité, qui se concentre sur le périmètre de sécurité et qui privilégie la prévention, ne suffit en effet pas toujours à prévenir ces attaques. Aucun réseau n'est impénétrable et il s'agit d'une réalité que les responsables et professionnels de la sécurité doivent 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 au travers des mailles du filet.

Quant aux organisations victimes d'une attaque, elles sont confrontées à un défi sous-jacent : la détection des incidents en temps opportun. Les données disponibles suggèrent que la majorité 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 sécurité défendable, la Surveillance sécurité réseau (NSM), les Diagnostics et mitigations continus (CDM) et la Surveillance sécurité continue (CSM), des notions qui permettront à votre organisation ou à votre Centre des opérations de sécurité (SOC) d'analyser les menaces et de détecter les anomalies pouvant indiquer 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. Le National Institute of Standards and Technology (NIST) a développé des directives dans son NIST SP 800-137 pour une Surveillance continue (CM). Notre cours vous permettra d'approfondir grandement votre compréhension et vos compétences dans la mise en œuvre d'un CM en utilisant le cadre de travail NIST.

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

Le voyage SEC511 se terminera enfin au 6e jour par l'organisation d'une compétition de type « Capture du drapeau » 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 auteurs de ce cours, Eric Conrad et Seth Misenar, ont conçu cette compétition de façon à ce qu'elle soit amusante, attrayante, complète et stimulante. Vous ne serez pas déçu !

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

Public visé :

- Architectes de sécurité
- Ingénieurs de sécurité
- Responsables de la sécurité technique
- Analystes SOC
- Ingénieurs SOC
- Responsables SOC
- Analystes CND
- Toute personne impliquée dans la mise en œuvre des CDM (Continuous Diagnostics and Mitigation, CSM (Continuous Security Monitoring, ou NSM Network Security Monitoring

Vous apprendrez à...

- Analyser une architecture de sécurité pour mettre à 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 d'opérations sécuritaires (SOC)
- Identifier les composants clés de Network Security, Monitoring (NSM)/Continuous Diagnostics et de Mitigation (CDM)/ Continuous Monitoring (CM)
- Déterminer les besoins adaptés de surveillance de la sécurité pour des organisations de toutes tailles
- Implementer un NSM/CSM robustes (Network Security Monitoring / Continuous Security Monitoring)
- Déterminer les capacités de surveillance requises pour un environnement SOC
- Déterminer les capacités nécessaires pour étayer la surveillance continue des contrôles clés de sécurité critique
- Utiliser des outils pour étayer la mise en œuvre de la surveillance continue (CM) conformément aux lignes directrices du NIST SP 800-137

> **"Very comprehensive, hands-on and can be applied to working environment."**
> Ewa Konkolska
> *PRUDENTIAL, PGDS*

SEC 530

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Defensible Security Architecture and Engineering

SEC530: Defensible Security Architecture a été conçue pour aider les stagiaires à construire et maintenir une architecture sécurité défendable. « Le périmètre est mort » est une phrase classique de l'ère du téléphone mobile, du cloud et de l'Internet des objets. Nous vivons en effet dans un nouveau monde de « déparamétrisation » où les vieilles limites entre « l'intérieur » et « l'extérieur » ou encore entre « fiable » et « non fiable » n'ont désormais plus de sens.

Ce paysage en pleine mutation impose un changement d'état d'esprit ainsi qu'une modification des objectifs pour de nombreux appareils. Que deviennent dès lors des logiciels classiques comme le pare-feu ? Quelles sont les ramifications de l'état d'esprit du « tout chiffrer » pour des appareils comme les systèmes de détection des intrusions ?

Dans ce cours, les stagiaires apprendront les fondamentaux de la toute dernière architecture sécurité défendable. L'accent sera en particulier mis sur l'exploitation de l'infrastructure actuelle (et des investissements), ce qui inclut les interrupteurs, routeurs et pare-feux. Les stagiaires apprendront à reconfigurer ces appareils pour mieux affronter le paysage de menaces de notre époque. Ce cours introduira également de nouvelles technologies qui contribueront à la construction d'une infrastructure sécurité robuste.

S'il ne s'agit pas ici d'un cours de surveillance, son contenu s'accordera cependant très bien avec la surveillance sécurité continue, avec pour effet de garantir que l'architecture sécurité gère non seulement la prévention mais apporte également les logs critiques pouvant être transmis au système Information de sécurité et Gestion des événements (SIEM en anglais) dans un Centre des opérations de sécurité.

Des laboratoires pratiques permettront enfin de renforcer les points clés du cours et de développer des compétences opérationnelles afin que les stagiaires soient en mesure de les exploiter dès leur retour dans leurs organisations.

Public visé :

- Architectes sécurité
- Ingénieurs réseaux
- Architectes réseaux
- Analystes sécurité
- Ingénieurs sécurité chevronnés
- Administrateurs systèmes
- Responsables sécurité techniques
- Analystes CND
- Spécialistes surveillance sécurité
- Enquêteurs cybermenace

Vous apprendrez à...

- Analyser une architecture sécurité à la recherche de défaillance
- Appliquer les principes appris en cours pour concevoir une architecture sécurité défendable
- Déterminer les besoins précis en surveillance sécurité pour des organisations de toutes tailles
- Tirer au maximum profit des investissements existant en architecture sécurité en reconfigurant les ressources existantes
- Déterminer les capacités requises pour supporter la surveillance continue des Contrôles critiques de sécurité clés
- Configurer un journal et un monitorage appropriés afin d'assister un Centre d'opérations de sécurité et un programme de surveillance continue

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

SEC 540

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

Cloud Security and DevOps Automation

SEC540 propose aux développeurs, aux opérateurs et aux professionnels de la sécurité une méthodologie leur permettant de concevoir et de livrer des logiciels et infrastructures sécurisés en utilisant des services DevOps et cloud.

Les étudiants abordent les principes, les pratiques et les outils de DevOps et découvrent comment améliorer la fiabilité, l'intégrité et la sécurité des applications sur site et celles hébergées sur le cloud. 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 leur preuve. Vous vous construirez une expérience pratique en utilisant des outils open-source populaires comme Puppet, Jenkins, GitLab, Vault, Grafana, et Docker pour automatiser la Gestion de la configuration (« infrastructure comme code »), l'Intégration continue (IC), la Livraison continue (LC), la compartimentation, la micro-segmentation et la conformité automatisée (« conformité comme code ») et la Surveillance continue. L'environnement laboratoire débute avec un projet IC/LC qui, de manière automatique, conçoit, test et déploie des infrastructures et des applications. Les étudiants exploitent ensuite des chaînes de compilation au cours de plusieurs labos visant à sécuriser le projet IC/LC grâce à toute une variété d'outils, de protocoles et de techniques de sécurité.

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 des chaînes de compilation d'Amazon Web Services (AWS) et aborde rapidement les services similaires offerts par Microsoft Azure. Grâce aux chaînes de compilation IC/LC, les étudiants développent une infrastructure cloud capable d'héberger des applications compartimentées et des micro services. Des exercices pratiques permettent ensuite d'analyser et de corriger les vulnérabilités des applications et de l'infrastructure cloud grâce à des services et à des outils de sécurité comme API Gateway, Identity and Access Management (IAM), CloudFront, Signing, Security Token Service (STS), Key Management Service (KMS), des services WAF géré, des fonctions sans serveur, CloudFormation, AWS Security Benchmark, et bien d'autres.

> **"SEC540 opened my eyes to a new way of thinking about operations and security unlike anything since SEC401: Security Essentials."**
> Todd Anderson
> *OBE*

Public visé :

- Quiconque travaille ou se prépare à travailler dans un environnement cloud public
- Quiconque travaille ou se prépare à travailler dans un environnement DevOps
- Quiconque souhaite découvrir où ajouter des contrôles et des 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 Amazon Web Services (AWS)
- Quiconque souhaite être capable d'exploiter les services de sécurité applicative cloud proposés par AWS
- Développeurs
- Architectes logiciels
- Ingénieurs opérationnels
- Administrateurs système
- Analystes sécurité
- Ingénieurs sécurité
- Chargés d'audit
- Chargés de gestion des risques
- Consultant sécurité

Vous apprendrez à...

- Comprendre les principes et protocoles fondamentaux sous-jacents aux 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 charges de travail DevOps vers le cloud
- Utiliser les services cloud pour sécuriser les applications cloud
- Localiser et mettre en œuvre une Livraison continue/un projet de déploiement

SEC 545

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

Cloud Security Architecture and Operations

Au fur et à mesure que le nombre d'organisations qui transfèrent des données et des infrastructures vers le cloud s'accroit, la sécurité devient une priorité majeure. Les équipes opérationnelles et de développement trouvent de nouveaux usages pour les services cloud et les dirigeants sont désireux de faire des économies, d'acquérir de nouvelles capacités et une efficacité opérationnelle en utilisant ces services. Mais, la sécurité de l'information sera-t-elle un talon d'Achille ? De nombreux fournisseurs du cloud ne fournissent pas d'informations détaillées sur le contrôle de leurs environnements internes, et un certain nombre de contrôles de sécurité courants utilisés en interne peuvent ne pas se répercuter 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, nous passerons aux principes de la sécurité technique et des contrôles pour tous les principaux types de cloud (SaaS, PaaS et IaaS). Nous explorerons la structure de 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, la détection d'intrusion, etc.), ainsi que toutes les autres couches de la pile de sécurité du cloud.

Nous examinerons chaque couche et ses composants, y compris 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 pénétration, ainsi que les toutes dernières et plus importantes recherches sur la sécurité du cloud. Concernant la défense, nous nous intéresserons à la gestion des incidents, l'expertise numérique, la gestion des incidents et la sécurité des applications.

Nous terminons 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 nous explorerons 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.

Public visé :

- Analystes sécurité
- Architectes sécurité
- Ingénieurs sécurité expérimenté
- Responsable sécurité techniques
- Analystes surveillance expérimenté
- Architectes sécurité cloud
- Ingénieurs DevOps et DevSecOps
- Administrateurs systèmes
- Administrateurs cloud

Vous apprendrez à...

- Réviser et élaborer des règles internes pour garantir l'efficacité de la sécurité cloud
- Comprendre les facettes majeures des risques du cloud, dont les menaces, les points de vulnérabilité et l'impact
- Articuler les thèmes de sécurité clé et les risques associés aux modèles de déploiement cloud SaaS, PaaS, and IaaS
- Évaluer les Cloud Access Security Brokers (CASBs) afin de mieux protéger et mieux surveiller les déploiements SaaS
- Construire la sécurité pour toutes les couches d'un environnement cloud hybride en commençant par les hyperviseurs et en travaillant sur les contrôles des applications de chaque couche
- Évaluer les contrôles de sécurité de base de l'hyperviseur de virtualisation
- Concevoir et implémenter les contrôles d'accès sécurité du réseau et surveiller les capacités dans un environnement cloud public
- Concevoir une architecture réseau cloud hybride qui inclut des tunnels IPSec
- Intégrer une identité cloud et une gestion d'accès (IAM) dans l'architecture sécurité
- Évaluer et implémenter divers types et formats de chiffrage cloud Développer des architectures cloud multi-tiers dans un Cloud virtuel privé (VPC) en utilisant des sous réseaux, des zones de disponibilité, des portails et une sécurité intégrée NAT dans les équipes DevOps, créant ainsi une structure efficace d'équipe DevSecOps
- Élaborer des flux de développement automatisés en utilisant AWS et des outils natifs
- Incorporer la gestion vulnérabilité, le scan et le test de pénétration dans les environnements cloud

30 CRÉDITS CPE/CMU

SEC 555

TRAINING EVENTS | PRIVATE TRAINING

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

SIEM with Tactical Analytics

De nombreuses organisations disposent de capacités de logging sans pour autant avoir le personnel et les processus pour analyser les fichiers générés. Les systèmes de logging collectent de surcroît de grandes quantités de données auprès de sources de données diverses, des sources qui doivent d'abord être comprises pour pouvoir procéder à une analyse appropriée. Cette classe a été conçue pour former chaque étudiant de manière individuelle en proposant des méthodes et des processus adaptés afin d'améliorer les solutions d'enregistrement qui existent. Cette classe vous aidera également à comprendre les informations de chaque entrée (quand, quoi, pourquoi). Il s'agit ici d'un cours à forte dominante labo et qui fait appel à SOF-ELK, une solution gratuite d'Incident sécurité et Gestion des événements (SIEM en anglais) sponsorisée par SANS afin d'apporter une expérience pratique et l'état d'esprit nécessaire 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 plusieurs manières de stocker et traiter de grandes quantités de données sans pour autant chercher à obtenir un aperçu des informations collectées. À cet aspect, on peut ajouter l'idée effrayante d'un nombre infini de systèmes à partir desquels il est possible de collecter des logs. Rien de plus facile, donc, que de se laisser emporter par les périls de la saturation de données. Cette classe s'éloigne des systèmes d'enregistrement typiques et cherche à élaborer une collecte de données manœuvrable ainsi qu'à développer un Centre des opérations de sécurité (SOC) tactique.

Ce cours a été élaboré pour démystifier l'architecture SIEM et ses processus en amenant l'étudiant 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 manœuvrable. Une fois la collecte effectuée, l'étudiant apprendra à présenter les informations réunies dans des formats utilisables afin de dégager d'éventuelles corrélations. Les étudiants parcourront les informations et les événements du log pour en analyser les composants clés qui leur permettront de découvrir la richesse de ces informations, mais aussi de mettre les données en corrélation, de mener des investigations sur la base des données agrégées, et pour finir, de découvrir comment utiliser 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 permettront non seulement d'apprendre à effectuer ces actions, mais aussi à automatiser nombre de processus de sorte que les étudiants puissent déployer ces connaissances dès leur retour dans leurs entreprises.

Un thème sous-jacent aborde l'application active des techniques de Surveillance continue et d'analyse en utilisant des attaques modernes de cybermenace. Les labos vous feront analyser des données d'attaque capturées afin de vous donner une idée concrète.

Le mot de l'auteur 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 plusieurs manières de stocker et traiter de grandes quantités de données sans pour autant chercher à obtenir un aperçu des informations collectées. À cet aspect, on peut ajouter l'idée effrayante d'un nombre infini de systèmes à partir desquels il est possible de collecter des enregistrements. Rien de plus facile, donc, que de se laisser emporter par les périls de la saturation de données. Cette classe s'éloigne des systèmes d'enregistrement typiques et cherche à élaborer une collecte de données manœuvrable ainsi qu'à développer un Centre des opérations de sécurité (SOC) tactique. » -Justin Henderson

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

Public visé :

- Analystes sécurité
- Architectes sécurité
- Ingénieurs sécurité chevronnés
- Responsable sécurité technique
- Analystes SOC
- Ingénieurs SOC
  Responsables SOC
- Analystes CND
- Spécialistes en surveillance sécurité
- Administrateur système
- Enquêteur cybermenace
- Individus travaillant à la mise en place d'une Surveillance sécurité continue
- Individus travaillant dans une équipe de recherche

Vous apprendrez à...

- Concevoir et réviser des règles internes pour garantir une sécurité cloud adéquate
- Comprendre les principaux aspects du risque que représente le cloud, y compris les menaces, les vulnérabilités et l'impact qu'elles peuvent représenter
- Articuler les thèmes clés de la sécurité et les risques associés aux modèles de déploiement cloud SaaS, PaaS, et IaaS
- Évaluer les Cloud Access Security Brokers (CASB) pour mieux protéger et surveiller 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 surveiller les capacités d'un environnement cloud public
- Concevoir une architecture réseau cloud hybride qui inclut des tunnels IPSec
- Intégrer la gestion d'identité et d'accès cloud (IAM) dans l'architecture de sécurité
- Évaluer et mettre en œuvre divers types et formats de chiffrement cloud
- Développer des architectures cloud multi-niveaux dans un Virtual Private Cloud (VPC) en utilisant des sous-réseaux, des zones de disponibilité, des passerelles et des NAT

SEC 566

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 par la pratique dont vous avez besoin pour mettre en œuvre et évaluer les Critical Security Controls documentés par le Center for Internet Security (CIS).

La sécurité d'une organisation doit évoluer en même temps que les menaces. Pour permettre à votre organisation de toujours rester à la page dans ce monde aux menaces changeantes, SANS a élaboré un cours complet qui enseigne aux stagiaires les Critical Security Controls, une approche de la sécurité qui repose sur la priorisation des tâches et sur les risques eux-mêmes. Conçus par des experts du privé et du public issus 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 se trouve le ministère américain de la sécurité intérieure, des gouvernements étatiques, des universités et de nombreuses sociétés privées.

> **"I am a new employee in This field. This course Gives me really good knowledge for my work."**
> Wafa Al Raisi
> *CENTRAL BANK OF OMAN*

Ces Contrôles sont en fait des directives spécifiques que les CISO, les CIO, les IG, les administrateurs système et le personnel de sécurité informatique peuvent utiliser pour gérer et mesurer l'efficacité de leurs défenses. Ils ont été conçus pour compléter les normes, cadres de travail et programmes de conformité déjà existant 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 travail de sécurité efficace dans la mesure où ils résultent de l'analyse d'attaques récentes, lancées régulièrement 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 pour la protection de l'infrastructure nationale du gouvernement britannique décrit ces contrôles comme « la base des contrôles et des mesures de sécurité informatique à haute priorité, une base qui peut être appliquée dans toute une organisation pour en améliorer la cyberdéfense ». 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.

Ce cours montre aux professionnels de la sécurité comment mettre en œuvre les contrôles dans un réseau existant grâce à une automatisation rentable. Pour les chargés d'audit, les CIO et les chargés de réponse aux risques, c'est le meilleur moyen pour comprendre comment mesurer l'efficacité de la mise en œuvre de ces Contrôles.

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

Public visé :

- Chargés d'audit de la protection de l'information
- Chargés de mise en œuvre ou administrateurs système
- Ingénieurs sécurité réseau
- Administrateurs informatiques
- Personnels et prestataires du Ministère de la Défense
- Personnels et clients d'agences fédérales
- Organisations du secteur privé qui cherchent à améliorer leurs processus de protection de l'information et à sécuriser leurs systèmes
- Vendeurs et consultants en sécurité qui cherchent à rester à jour en termes de cadres de travail pour la protection de l'information
- Stagiaires ayant suivi SEC440, SEC401, SEC501, des classes 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 de 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
- Apprendre à créer des outils de notation pour mesurer l'efficacité de chaque Contrôle
- Utiliser des métriques spécifiques pour établir une base et mesurer l'efficacité des Contrôles
- Comprendre comment les Contrôles permettent d'accéder aux normes comme NIST 800-53, ISO 27002, l'Australian Top 35 et bien d'autres
- Réaliser un audit de chaque Contrôle avec des modèles spécifiques éprouvés, des checklists et des scripts fournis pour faciliter le processus d'audit

SEC 599

TRAINING EVENTS | PRIVATE TRAINING

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Defeating Advanced Adversaries - Implementing Kill Chain Defenses

Ce cours vous apportera la connaissance et l'expertise dont vous avez besoin pour détecter et répondre aux menaces d'aujourd'hui. Sachant que la stratégie de la prévention ne suffit pas, nous vous présenteront des contrôles de sécurité conçus pour faire obstacle aux adversaires avancés.

SEC599 fournit aux étudiants des exemples concrets des méthodes qui permettent de prévenir les attaques, avec plus de 20 labos et une journée entière dédiée à un exercice « Défendre le drapeau » au cours duquel les étudiants devront défendre notre organisation virtuelle contre différentes attaques.

Ce voyage de six jours débute avec une analyse d'attaques récentes via des études de cas approfondies. Nous examinerons les types d'attaques en cours et introduirons le Cycle d'attaque des Menaces persistantes et avancées (APT en anglais) sous forme d'approche structurée permettant de décrire les attaques. Afin de comprendre le fonctionnement des attaques, vous aurez à compromettre notre organisation virtuelle « SyncTechLabs » durant les exercices de la première journée.

À partir du deuxième jour et les jours suivants, nous engagerons une discussion sur les contrôles de sécurité efficaces qui peuvent être mis en œuvre pour prévenir, détecter et répondre aux cyberattaques. Certains des sujets qui seront abordés incluent :

- La construction de votre propre solution mail sandbox pour détecter le spear phishing.
- Le développement de politiques de groupe efficaces pour stopper l'exécution de code malveillant.
- L'arrêt des 0-day exploits en utilisant des techniques de mitigation d'exploits et le placement d'applications en liste blanche.
- La détection et l'évitement de malwares persistants.
- La détection et la prévention d'un mouvement latéral avec sysmon, la surveillance d'évènement Windows et des politiques de groupe.
- La détection et le blocage d'un commandement et contrôle par l'analyse du trafic sur le réseau
- L'optimisation de la threat intelligence pour améliorer votre posture de sécurité

Au cours du défi « Défendre le drapeau » du dernier jour de formation, vous devrez faire face à des adversaires avancés et aurez à maintenir la sécurité de votre réseau. Saurez-vous protéger votre environnement contre les différentes vagues d'attaques ? La menace ne prend jamais de vacances. Alors qu'attendez-vous ?

Public visé :

- Architectes de sécurité
- Ingénieurs de sécurité
- Directeurs techniques de sécurité
- Directeurs et analystes des centres d'opérations de sécurité
- Administrateurs IT
- Toute personne voulant mieux comprendre comment des cyber adversaires sophistiqués opèrent et comment l'environnement IT peut être amélioré pour mieux prévenir, détecter et répondre aux incidents

Vous apprendrez à...

- Comprendre comment les attaques récentes de haut niveau ont été menées et comment elles auraient pu être arrêtées
- Mettre en œuvre des contrôles de sécurité tout au long des différentes phases de la Cyber Kill Chain et du cadre de travail MITRE ATT&CK pour prévenir, détecter et répondre aux attaques

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

NETWARS EXPERIENCE

Défis pratiques sur la sécurité des réseaux et des systèmes

Experience **NetWars**

Jouez en solo ou en équipe (jusqu'à cinq joueurs)

« **NetWars reprend les concepts abordés en classe et vous permet de les mettre en pratique. Je recommande vivement !** »

- **Kyle McDaniel**, Lenovo

Choix entre :

Core NetWars | DFIR NetWars | Cyber Defense NetWars | ICS NetWars

Développer des compétences en :

- **Cyberdéfense**
- **Test d'intrusion**
- **Investigation numérique & Réponse aux incidents**
- **Supervision**

Les stagiaires inscrits à une formation longue (4, 5 ou 6 jours) proposée dans le cadre d'un évènement de formation SANS, peuvent participer au tournoi sans frais additionnels, lorsqu'un tournoi est compris pendant l'évènement.

NetWars se déroule après les cours de la journée et vous permet de mettre immédiatement en application ce que vous avez appris. Et tout se déroule dans un environnement ludique avec une ambiance de compétition saine !

Les places sont limitées, alors n'hésitez pas à vous inscrire à NetWars lorsque vous vous inscrivez à un cours.

www.sans.org/netwars

SEC 460

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Enterprise Threat and Vulnerability Assessment

L'exploitation informatique est en plein essor. Les adversaires avancés se font de plus en plus nombreux, compétents et destructeurs, et face à cette menace, les organisations doivent apprendre à limiter plus efficacement les risques de sécurité informatique de niveau entreprise. SEC460 est le premier cours qui tourne autour de la construction de compétences et de techniques d'évaluation technique des points de vulnérabilité tout en soulignant des approches pratiques éprouvées afin d'en garantir la valeur 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. Ce cours vise à former le personnel de cybersécurité dont la tâche consiste, au sein de leurs organisations, à sécuriser efficacement 10 000 systèmes ou plus.

SEC460 débute avec une introduction aux fondamentaux de l'évaluation des points de vulnérabilité en matière de sécurité informatique, et poursuit en traitant de manière approfondie le cadre de travail entourant l'évaluation des points de vulnérabilité. La suite du cours porte sur les composants structurels d'un programme dynamique et itératif en matière de sécurité informatique. À travers une analyse pratique et détaillée des renseignements disponibles sur les menaces, la modélisation et l'automatisation, les étudiants apprendront les compétences nécessaires non seulement pour utiliser les outils, mais aussi pour mettre en place un programme d'évaluation transformationel des points de vulnérabilité. SEC460 vous apprendra à vous servir des outils de sécurité utilisés dans le milieu industriel pour l'évaluation des points de vulnérabilité, la gestion et la mitigation. Il s'agit du seul cours à enseigner une méthodologie holistique de l'évaluation des points de vulnérabilité tout en mettant l'accent sur les défis auxquels les grandes entreprises sont confrontées. Vous apprendrez sur une gamme complète de machines cibles représentatives d'un environnement d'entreprise, en utilisant des outils prêts à la production et une méthodologie de test éprouvée.

Ce cours vous emmènera au-delà des simples listes de contrôle et vous fera découvrir le point de vue des attaquants, un aspect qui prendra tout son sens lorsque votre organisation sera victime d'une prochaine attaque. Un opérateur représente davantage que l'outil qu'il emploie. SEC460 met l'accent sur cette approche centrée sur le personnel en examinant 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 l'établissement de rapports avant de mettre vos compétences à l'épreuve le dernier jour en regard d'une gamme cyber d'entreprises avec de nombreux systèmes cibles que vous aurez à analyser et explorer. Cette gamme cyber est constituée d'un vaste environnement de serveurs, d'utilisateurs finaux et d'appareils réseau qui représentent la majorité des systèmes et topologies que les entreprises utilisent. Le fait d'adopter une approche de bout en bout pour évaluer les points de vulnérabilité aura pour effet de valoriser encore davantage vos compétences, en particulier vis-à-vis des organisations de moyenne et grande taille qui en sont très friandes.

Vous apprendrez à...

- Réaliser de bout en bout des évaluations des points de vulnérabilité
- Développer une recherche, une gestion et une remédiation personnalisées des points de vulnérabilité
- Conduire une collecte et une analyse des informations sur la menace afin de créer un plan de cybersécurité sur mesure qui intègre différentes attaques et différents cadres de modélisation des vulnérabilités
- Implémenter une méthodologie de test éprouvée en utilisant des tactiques et des techniques à la pointe de l'industrie
- 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
- Utiliser des outils d'énumération comme Nmap, Masscan, Recon-ng, et WMI pour identifier les nœuds réseau, les services, les configurations et les vulnérabilités qu'un attaquant pourrait utiliser
- Conduire une énumération des vulnérabilités infrastructure au niveau de différents segments réseau, et ce malgré des infrastructures réseau divergentes et des configurations non standards
- Conduire une énumération des vulnérabilités d'application web dans des environnements d'entreprises tout en résolvant des défis complexes imposés par la taille des entreprises
- Effectuer une recherche et une validation manuelle des vulnérabilités pouvant être étendue à des applications et des systèmes personnalisés et uniques
- Gérer de vastes jeux de données de vulnérabilités, effectuer une évaluation des risques et une notation en regard des risques spécifiques
- Implémenter un tri des vulnérabilité et dresser une liste de priorités en matière de mitigation
- Utiliser des logiciels commerciaux haut de gamme (dont Acunetix WVS et Rapid7 Nexpose (InsightVM))
- Élaborer des scripts PowerShell personnels pour améliorer vos activités, gagner en visibilité, mettre à l'échelle vos tactiques de mitigation et confier des tâches à des membres de l'équipe ayant moins de compétences

36 CPE/CMU CREDITS

SEC 542

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 la détection de failles à des scans de sécurité.

SEC542 aide les étudiants à dépasser le stade du scan lambda pour acquérir une méthodologie professionnelle, et des compétences en test de pénétration web application de grande valeur.
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 pour les organisations 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 dans les applications web jouent un rôle majeur dans les brèches de sécurité et les intrusions. Les adversaires concentrent de plus en plus leurs efforts sur ces cibles de grande valeur, soit en abusant directement des applications orientées public, soit en se concentrant sur des applications web précises 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 le test de pénétration appliqué aux applications web demande plus de connaissances.

SEC542 permet aux étudiants de déterminer l'état de sécurité d'une application web et de faire la démonstration convaincante qu'une sécurité inadéquate (véritable fléau à l'heure actuelle) peut avoir en terme d'impact.
Dans ce cours, les étudiants aborderont de manière approfondie la majorité des faiblesses des applications web et comment ces faiblesses sont exploitées. Plus important, ils apprendront des processus éprouvés et répétables de façon à détecter systématiquement ces faiblesses pour remonter ensuite les résultats à la hiérarchie. Mêmes les surdoués de la sécurité ont régulièrement du mal à faire comprendre à leurs organisations les risques encourus. Dans les faits, l'art du test de pénétration 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 l'employeur de déployer des contremesures appropriées. L'objectif de SEC542 est de mieux sécuriser les organisations grâce à des tests de pénétration et non à simplement faire état de ses compétences en piratage. Ce cours vous apprendra à démontrer l'impact véritable que peuvent avoir des faiblesses dans une application.

En plus de son contenu de grande qualité, SEC542 met particulièrement l'accent sur des labos pratiques afin de s'assurer que les étudiants sont en mesure d'appliquer rapidement ce qu'ils ont appris.
Cette formation compte plus de 30 labos pratiques et se termine en beauté avec un tournoi de test de pénétration sur application web et mené par la SANS NetWars Cyber Range. La compétition Capture de drapeau ayant lieu le dernier jour amène les étudiants à travailler en équipe et leur demande d'appliquer les techniques de test de pénétration sur application web qu'ils viennent d'acquérir. L'événement se déroule dans une atmosphère ludique qui permet de renforcer l'apprentissage.

Public visé :

- Professionnels de la sécurité en général
- Testeurs d'intrusion
- Hackers éthiques
- Développeurs d'applications web
- Concepteurs de sites web et architectes

Vous apprendrez à...

- Appliquer une méthodologie détaillée en quatre étapes à vos tests d'intrusion pour applications web, notamment : Recon, Mapping, Discovery, et Exploitation
- Analyser les résultats d'outils de test web automatisés pour éliminer les faux positifs, et valider les résultats
- Utiliser Python pour créer des scripts de test et d'exploitation lors d'un test d'intrusion
- Créer des configurations et tester des charges utiles au sein de Burp Intruder pour effectuer l'injection SQL, XSS, et d'autres attaques pour le web
- Utiliser FuzzDB pour générer du trafic d'attaque permettant de découvrir des failles telles que les problèmes liés à Command Injection et File Include
- Évaluer la logique et la faille d'opération dans une application cible pour trouver des failles logiques et des vulnérabilités
- Utiliser Durzosploit pour masquer les charges utiles XSS, contourner WAF et le filtrage d'application
- Analyser le trafic entre le client et le serveur d'applications à l'aide d'outils tels que Ratproxy et Zed Attack Proxy permettant d'identifier des problèmes dans le code côté client
- Utiliser BeEF 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 "Capture the Flag" pour utiliser l'ensemble des techniques et des outils et les tester de façon exhaustive.

GIAC CERT: GWAPT
36 CPE/CMU CREDITS
WWW.GIAC.ORG/GWAPT

"CTF is a great way to practice the course content, really enjoyed it."
Chris Campbell, *RBS*

SEC 560

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, vous avez la responsabilité unique de trouver et comprendre les vulnérabilités de votre organisation, ainsi que de travailler au mieux à limiter leur importance avant que des personnes malveillantes ne s'en servent. Êtes-vous prêt ? SANS SEC560 est notre cours de test de pénétration par excellence : le suivre, c'est se préparer parfaitement à la tâche.

SEC560 est un cours parfaitement indispensable pour tous les professionnels accomplis de la sécurité.
Couvrant de manière exhaustive les outils, techniques et méthodologies du test de pénétration réseau, cette formation vous prépare véritablement à mener pas à pas et de bout en bout des projets de tests pour obtenir des résultats de grande valeur. 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 scans approfondis, des exploitations de cibles, suivis d'attaques de mot de passe et de manipulations d'application 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 de pénétration 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 mal intentionnées ne vous attaquent.
SEC560 a été conçu pour vous préparer à mener des tests de pénétration de haute valeur et à grande échelle. Et c'est précisément ce que vous ferez lors du dernier jour de cours. 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 de pénétration d'une journée complète. Vous mènerez un test de pénétration 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.

Vous rapporterez des connaissances complètes en matière de test de pénétration et un savoir-faire important en piratage éthique.
Vous apprendrez à effectuer une reconnaissance détaillée en étudiant l'infrastructure d'une cible via le blog mining, les moteurs de recherche, les réseaux sociaux et les autres infrastructures internet et intranet. Nos labos pratiques vous enseigneront à scanner des réseaux cibles en utilisant les meilleurs outils disponibles. Nous ne nous contentons pas simplement d'aborder les configurations et les options classiques, nous verrons également certaines possibilités moins connues mais particulièrement utiles que les meilleurs outils de test de pénétration proposent. Une fois le scan terminé, vous apprendrez des dizaines de méthodes permettant d'exploiter les systèmes cibles afin d'évaluer les véritables risques associés aux failles que vous avez détectées. Vous plongerez dans 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 concrètes que l'on retrouve dans le monde réel afin de mettre en lumière l'importance d'une défense en profondeur.

> **"It introduces the whole process of pen testing from start of engagement to end."**
> Barry Tsang,
> *DELOITTE*

GIAC CERT: GPEN
37 CPE/CMU CREDITS
WWW.GIAC.ORG/GPEN

Public visé :

- Le personnel de sécurité dont le travail consiste à évaluer les réseaux et les systèmes pour trouver et corriger les vulnérabilités
- Testeurs d'intrusion
- Hackers éthiques
- Les auditeurs qui ont besoin d'acquérir des compétences techniques plus approfondies
- Membre de red team et blue team
- Spécialistes en investigation numérique qui cherchent à 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, des analyses de ports, relever les empreintes digitales du système d'exploitation, et numériser la version afin de développer une carte des environnements cible.
- Configurer et lancer le scan de vulnérabilité 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 commercial que court l'organisation.
- Analyser les résultats produits par les outils d'analyse pour effectuer une vérification manuelle et réduire les faux positifs à l'aide des outils Netcat et Scapy packet.
- Pousser les tests d'intrusion plus loin en utilisant les lignes de commande Windows et Linux pour exploiter les systèmes cible afin d'en extraire des informations capitales, établir des pivots permettant de démultiplier les atteintes, et aider l'entreprise à déterminer les risques.

SEC 573

TRAINING EVENTS | PRIVATE TRAINING

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Automating Information Security with Python

Tous les professionnels de la sécurité, y compris les chargés de test de pénétration, les analystes en investigation numérique, les défenseurs réseaux, les administrateurs sécurité et les chargés de réponse aux incidents doivent faire face à un même problème : le CHANGEMENT. Le changement est la seule constante. 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 offre des perspectives intéressantes au niveau de l'investigation numérique, mais encore vous faut-il avoir les outils pour exploiter ces perspectives. Et il arrive souvent que ces outils n'aient pas encore été développés. Vous pouvez essayer d'avancer dans votre affaire sans ces preuves, ou espérer que quelqu'un développera un outil avant que la piste refroidisse... Ou bien vous pouvez développer vous-même cet outil.

Autre possibilité, un attaquant a pénétré votre réseau il y a plusieurs mois. Si les outils existant étaient en mesure de détecter cette attaque, le problème évoqué ne se poserait pas. Des données sensibles vous échappent et le processus de détection et d'éradication des attaques prend un temps considérable, sans parler des ressources financières. Si vous en êtes capable, la réponse est toute simple : il suffit de créer un outil qui automatise vos défenses.

Ou si vous êtes chargé des tests de pénétration, il vous faut évoluer à la même vitesse que les menaces que vous êtes censés imiter. Que faites-vous lorsque vos outils « en accès libre » et vos exploits ne suffisent pas ? Si vous êtes bon, vous développez votre propre outil.

Plus facile à dire qu'à faire, pas vrai ? Et pourtant... Le Python est un langage simple et ergonomique conçu pour permettre aux professionnels de la sécurité d'automatiser plus facilement et plus rapidement certaines de leurs tâches. Que vous soyez novice ou codeur depuis des années, SEC573: Automating Information Security with Python est une formation qui vous apprendra à créer des programmes pour vous simplifier le travail et vous faire gagner en efficacité. Cette classe s'adapte à votre rythme et reprend tout depuis le début en partant du principe que vous n'avez aucune connaissance ni aucune 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. En se calant sur votre vitesse de progression et sur votre niveau, les cours de ce module vous permettent de tirer profit au maximum de la formation. Au-delà des fondamentaux, nous verrons l'analyse de fichiers et de paquets, l'extraction d'artefact dans le cadre d'investigation numérique, la mise en réseau, l'accès aux bases de données, l'exécution de processus, la gestion des exceptions, le code orienté objet, etc.

Ce cours a été conçu pour vous apporter les compétences dont vous avez besoin pour mettre au point, personnaliser ou même pour développer purement et simplement vos propres outils. Nous vous apprendrons à créer vos propres 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 individus compétents et capables de développer leurs propres outils. Ils sont en effet particulièrement demandés, les gens capables de comprendre un problème et de développer rapidement un prototype de code en conséquence (défense ou attaque, peu importe). Rejoignez-nous et découvrez la face cachée et armée du Python.

Public visé :

- Les professionnels de la sécurité qui veulent apprendre à développer des applications Python
- Les testeurs d'intrusion qui veulent aller au-delà de la simple utilisation d'outils de sécurité et passer à la conception ou modification d'outils
- Les techniciens qui ont besoin d'outils personnalisés pour tester leur infrastructure et les concevoir eux-mêmes

Vous apprendrez à...

- Développer des outils d'investigation numérique pour extraire des artefacts à partir de preuves pour lesquelles 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 investigations
- Créer des outils défensifs pour automatiser l'analyse de fichiers log et de paquets réseau en utilisant des techniques de chasse en équipe pour pister les attaquants sur votre réseau. Mettre en place de manière personnalisée des listes blanches, des listes noires, une 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
- Écrire des outils de test de pénétration, y compris plusieurs backdoors avec des fonctionnalités comme l'exécution de processus, les charges en téléchargements ascendant et descendant, le scan de port, etc. Développer des outils fondamentaux qui échappent aux antivirus et vous permettent de mettre un pied dans l'environnement cible
- Comprendre les fondamentaux du code Python et qui sont nécessaires à l'automatisation de tâches communes en cybersécurité Maîtriser les fondamentaux de langage comme les variables, les boucles, les opérations if then else, logic, file, les arguments de ligne de commande et le débogage (aucune connaissance prérequise)
- Puiser dans la richesse des modules Python existants afin de compléter les tâches en utilisant des expressions régulières, des interactions entre bases de données avec SQL, la mise en réseau IP, la gestion des exceptions, l'interaction avec les autres sites web en utilisant des techniques de requête, d'analyses paquets et de réassemblage de paquet. Et bien d'autre encore

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

SEC 575

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Mobile Device Security and Ethical Hacking

Imaginez une surface d'attaque existant dans toute votre organisation et retrouvable entre les mains de tous les utilisateurs. Elle se déplace d'un endroit à l'autre avec régularité, elle stocke des données critiques et hautement sensibles, et elle est dotée de nombreuses technologies sans fil, toutes mûres pour une attaque. Nul besoin de poursuivre cette expérience de pensée, elle existe déjà : les appareils mobiles. Ces appareils 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. Les appareils mobiles ne constituent plus simplement une technologie pratique : il s'agit désormais d'un outil fondamental – que tout le monde ou presque a avec soi – qui remplace souvent l'ordinateur traditionnel pour les besoins quotidiens en données. On constate cette tendance dans les entreprises, les hôpitaux, les banques, les écoles et les magasins de vente partout dans le monde. Les utilisateurs se reposent plus que jamais sur leur appareil mobile – nous en sommes conscients et les personnes mal intentionnées aussi.

Ce cours a été conçu pour vous permettre de développer les compétences dont vous avez besoin pour comprendre les forces et les faiblesses de sécurité des appareils fonctionnant sous iOS et sous Android, y compris les Apple Watch et les produits Android Wear. Une fois doté de ces compétences, vous évaluerez les faiblesses de sécurité des applications tierces et intégrées. Vous apprendrez à contourner le cryptage d'une plateforme et à manipuler les applications Android pour outrepasser les techniques sécurité. Vous exploiterez des outils permettant d'analyser les applications mobiles de manière automatique et manuelle pour identifier les défauts dans le trafic réseau de l'application, dans son stockage système et dans les canaux de communication inter-app. 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, puis vous exploiterez des appareils perdus ou volés pour collecter des données sensibles d'application mobile. 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 et les rendre compréhensibles pour vos supérieurs 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.

Vous mettrez ensuite vos nouvelles compétences en pratique pour mettre en place, pas à pas, un test de pénétration orienté appareil mobile. Vous commencerez ainsi par obtenir l'accès à des réseaux sans fil pour déployer des attaques de type « man-in-the-middle » puis vous procéderez à l'exploitation des appareils mobiles touchés et procéderez enfin à la collecte de données. Ce faisant, vous apprendrez étape par étape à mener ce type de test au travers d'exercices pratiques, d'instructions détaillées et de conseils et astuces provenant de centaines de tests de pénétration. Une fois ces compétences développées, vous pourrez retourner dans votre environnement de travail en étant prêt à déployer vos propres tests, sachant mieux ce que vous devez chercher et comment analyser un test de pénétration externalisé. Le déploiement d'appareils mobiles fait peser de nouvelles menaces sur les organisations avec, entre autres, les malwares avancés, la fuite de données, la divulgation de secrets d'entreprise, les risques sur la propriété intellectuelle et l'accès à des informations personnelles de valeur. Et pour couronner le tout, il n'y a tout simplement pas assez de personnes possédant les compétences nécessaires en cybersécurité pour identifier et gérer la sécurité des déploiements d'appareils mobiles. Une fois cette formation achevée, vous vous distinguerez des autres professionnels par votre capacité à évaluer la sécurité des appareils mobiles, par vos compétences dans l'évaluation et identification efficace des faiblesses des applications mobiles, et par votre aptitude à mener des tests de pénétration sur appareils mobiles. Autrement dit, vous aurez tout le bagage indispensable pour protéger et défendre les déploiements d'appareils mobiles.

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

Public visé :

- Testeurs d'intrusion
- Hackers éthiques
- Les auditeurs ayant besoin d'approfondir leurs compétences techniques
- Le personnel de sécurité dont la mission est d'évaluer, de déployer, ou de sécuriser des téléphones et tablettes mobiles
- Les administrateurs système et réseau qui gèrent les téléphones et les 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 pour contrer ou contourner les exigences d'achat intégrées.
- 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 en contournant les restrictions de sécurité

"I am learning a lot regarding mobile platforms and key differences between all of them. I recommend this course for anyone that wants to learn about mobile OS."
Hilal Lootah, *TRA*

SEC 617

TRAINING EVENTS | PRIVATE TRAINING

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Wireless Ethical Hacking, Penetration Testing, and Defenses

Malgré les préoccupations sécuritaires que nous sommes nombreux à partager au sujet de la technologie sans fil, celle-ci ne va pas disparaître; bien au contraire, elle est en pleine croissance. Vous êtes témoin du déploiement et de l'utilisation de la technologie LAN sans fil et Wifi dans d'autres applications, notamment les téléphones sans fil, les maisons connectées, les dispositifs intégrés, et bien plus encore. Des technologies telles que ZigBee et Z-Wave offrent de nouvelles méthodes de connectivité pour les dispositifs, alors que d'autres technologies sans fil, notamment Wifi, Bluetooth, Bluetooth Low Energy, et DECT continuent à progresser à un rythme exponentiel - chacune avec son lot de défis sécuritaires et d'opportunités d'attaque pour les malfaiteurs.

Pour être des experts de la sécurité sans fil, les professionnels ont besoin d'une compréhension exhaustive de ces technologies, des menaces, des exploits et des techniques défensives. Une expérience en matière d'évaluation et d'attaque des technologies sans fil est indispensable. Les professionnels ne doivent pas se limiter à leurs compétences en matière de Wifi. Les technologies sans fil basiques et brevetées doivent aussi être évaluées.

Le cours SEC617 aborde de façon approfondie les défis sécuritaires posés par de nombreuses technologies sans fil, en mettant les stagiaires dans la peau d'un assaillant afin de les sensibiliser aux menaces sécuritaires du sans-fil. À l'aide d'outils disponibles librement et d'outils personnalisés, les stagiaires explorent les techniques utilisées par les assaillants pour exploiter les réseaux Wifi.

Celles-ci incluent les attaques contre : WEP, WPA/WPA2, PEAP, TTLS, et d'autres systèmes, y compris le développement de techniques d'attaque tirant parti de Windows 7 et de Mac OS X.

Le cours traite aussi les menaces fréquemment négligées, associées à Bluetooth, ZigBee, DECT, et à d'autres systèmes sans fil brevetés. Dans le cadre de ce cours, les stagiaires reçoivent le kit d'outil SWAT, utilisé dans les travaux pratiques pour compléter le contenu du cours et renforcer les techniques éthiques de hacking dans un environnement sans fil.

En utilisant des techniques d'analyse et d'évaluation, ce cours montre comment identifier les menaces qui rendent la technologie sans fil vulnérable, et comment construire à partir de ses connaissances des techniques défensives pouvant être utilisées pour protéger les systèmes sans fil.

"SEC617 is great for someone looking for a top-to-bottom rundown in wireless attacks."

Garret Picchioni,
SALESFORCE

Public visé :

- Hackers éthiques et testeurs d'intrusion
- Administrateurs système et réseau
- Équipes de gestion d'incident
- Auditeurs techniques
- Ingénieurs système sans fil
- Développeurs de systèmes sans fil intégrés
- Personnel de la sécurité réseau
- Décideurs en matière de politique de sécurité informatique
- Consultants dans le domaine de la sécurité de l'information

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 contre les technologies sans fil à faible consommation, notamment ZigBee, 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, à l'aide d'Ubertooth, CarWhisperer, et btaptap, pour collecter des informations sensibles provenant de casques d'écoute, de claviers sans fil, et de dispositifs LAN 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 afin d'identifier les menaces de divulgation d'informations posant un risque pour l'organisation.
- Implémenter un test de pénétration WPA2 pour l'entreprise afin d'exploiter les systèmes client sans fil vulnérables pour en récolter les authentifiants
- Utiliser les outils sans fil de test fuzz, notamment Metasploit, file2air, et Scapy pour identifier de nouvelles vulnérabilités sur les dispositifs sans fil.

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

SEC 642

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 innombrables et diversifiés des techniques avancées du cyber environnement moderne ?
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 depuis longtemps révolue. Même à l'heure du Web 2.0 et d'AJAX, le HTTP et les applications web modernes voient leur complexité croître en accélérant. Dans les faits, l'environnement actuel impose une forte demande en cluster web à forte 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 et test de pénétration, est-ce que vous vous sentez au point ? Est-ce que vous êtes 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 au test de pénétration 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 la prochaine génération. Au travers d'un mélange de cours, d'expériences concrètes et d'exercices pratiques, vous apprendrez des techniques qui vous permettront 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 « Capture du drapeau » au cours de laquelle vous devrez déployer les connaissances que vous avez acquises, le tout dans un environnement ludique basé sur des technologies du monde réel.

Enseignement pratique de compétences avancées en matière d'exploitation d'application 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 nouveaux cadres de travail sur le web et les back-ends web, puis nous plongerons dans le chiffrement et son rapport avec les applications web en analysant la cryptographie utilisée 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 abuser 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-feux d'application web, le filtrage et d'autres techniques de protection.

"Very good techniques and methods covered which will be useful to any new app tester."
Vivek Veerappan,
GEMALTO

"Hands-on and to the point!"
Frans Kollé,
MADISON GUIRKHA B.V.

Public visé :

- Chargés de test de pénétration
- Membres de red team
- Personnel en charge de l'évaluation des vulnérabilités
- Testeurs d'intrusion
- Consultants de la 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-ends comme Mass Assignments, Type Juggling, et Object Serialisation
- Effectuer une injection à base JavaScript contre ExpressJS, Node.js, et NoSQL
- Identifier et contourner les pare-feux d'application web et les techniques de filtrage d'application afin d'exploiter le système
- Utiliser les techniques d'exploitation apprises en cours pour effectuer des attaques de haut niveau telles que XSS, l'injection SQL et CSRF contre des applications web
- Découvrir les vulnérabilités XML Entity et XPath dans les services web SOAP, REST et les autres banques de données
- Utiliser des outils et des techniques pour travailler avec HTTP/2 et WebSockets et les exploiter
- Identifier et contourner les pare-feux d'applications web et les techniques de filtrages pour exploiter le système

36 CRÉDITS CPE/CMU

SEC 660

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ce cours a été élaboré de façon à être la suite logique pour ceux qui ont suivi SEC560: Network Penetration Testing and Ethical Hacking, mais il s'adresse également au personnel ayant déjà une expérience en test de pénétration. Les étudiants ayant démontré les connaissances pré-requises à ce cours analyseront des dizaines d'attaques réelles utilisées par les chargés de test de pénétration les plus accomplis au monde. La méthodologie de chaque attaque sera abordée puis suivie d'exercices dans un environnement labo concret afin que les étudiants puissent s'approprier ces concepts avancés grâce à une application immédiate des techniques vues en cours. Chaque jour comporte une soirée « camp d'entraînement » de deux heures qui permet d'approfondir un peu plus la maîtrise obtenue via des exercices pratiques supplémentaires. Parmi les thèmes abordés, on retrouve l'utilisation de Python sous forme d'arme, les attaques contre les contrôles d'accès réseau (NAC en anglais) et la manipulation VLAN, l'exploitation d'appareil 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, les contrôles OS modernes comme ASLR et DEP et comment en venir à bout, 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. Maintenir une veille technologique pour connaître les méthodes d'attaque les plus récentes nécessite un fort désir d'apprendre, d'aider les autres, et bien sûr d'avoir l'occasion de pratiquer pour se forger une expérience. SEC660 permet aux étudiants de développer une connaissance approfondie des vecteurs d'attaques majeurs dans un environnement adapté, de manière à mettre en pratique ces attaques dans de nombreux scénarios pratiques. Cette formation va plus loin que le simple scan avec ses résultats limités. Elle enseigne aux chargés de tests de pénétration 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 une introduction de concepts d'intrusion avancés, et donne une vue d'ensemble aux stagiaires pour les préparer à ce qui les attend. L'objectif du premier jour porte sur les attaques de réseau, un domaine souvent négligé par les testeurs. Les sujets incluent l'accès, la manipulation et l'exploitation du réseau. les attaques sont effectuées contre des NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, et autres. Le second jour commence par un module technique sur la mise en œuvre de tests d'intrusion contre diverses implémentations cryptographiques. La journée se poursuit par la perpétration d'attaques au démarrage de 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 de Python pour les tests d'intrusion, de Scapy pour la confection de paquets, des tests de sécurité de produits, des tests fuzz pour les applications, et des techniques de couverture de code. Au quatrième et cinquième jour, le cours explore l'exploitation de programmes sur les systèmes Linux et Windows. Le dernier jour, le cours est consacré à de nombreux défis de tests d'intrusion exigeant que les stagiaires résolvent des problèmes complexes et participent à des exercices « Capture the Flag ».

Public visé :

- Testeurs d'intrusion réseau et système
- Gestionnaires d'incident
- Développeurs d'application
- Ingénieurs IDS

Vous apprendrez à...

- Réaliser des tests fuzz pour améliorer le processus SDL de votre société
- Exploiter les dispositifs de réseau et évaluer les protocoles d'application de 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 "zero day" et le développement d'exploits
- Développer des évaluations quantitatives et qualitatives plus précises par la validation
- Démontrer les besoins et les effets de l'optimisation des mesures modernes pour atténuer les exploits

"From high-level concepts to hands-on training, this course provides enough detail and depth to allow me to show the skillsets learned immediately after the learning, allowing my employer to see their return on investment."

Brian Anderson,
NORTHROP GRUNMAN CORP

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

SEC 760

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 sont souvent très complexes et subtiles. Et pourtant, elles peuvent exposer les organisations à des attaques majeures, affaiblir leurs défenses lorsqu'elles sont exploitées par des assaillants hautement compétents. Peu de professionnels de la sécurité ont les compétences requises pour découvrir, voire comprendre à un niveau basique, 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-bit et 64-bit, déboguer à distance des noyaux et des applications d'utilisateurs, et écrire des exploits complexes (tels que les attaques « use-after-free ») contre des logiciels et des systèmes d'exploitation modernes. Certaines des compétences que vous apprendrez dans le cours SEC760 incluent :

- L'écriture d'exploits modernes contre des systèmes d'exploitation prédominants
- La réalisation d'attaques complexes telles que « use-after-free », des techniques Kernal exploit
- L'utilisation essentielle du SDL (Security Development Lifecycle) ou d'un Secure SDLC, ainsi que la modélisation de menace
- L'utilisation avec efficacité de divers débogueurs et plug-ins pour améliorer et accélérer la recherche de vulnérabilités
- La gestion des commandes modernes d'atténuation des exploits visant à les entraver et à les faire échouer

> **"SEC760 is a kind of training we could not get anywhere else"**
>
> Jenny Kitaichit,
> *INTEL*

Public visé :

- Testeurs d'intrusion réseau et système
- Développeurs d'applications sécurisées (C & C++)
- Professionnels de la rétro-ingénierie
- Gestionnaires d'incident
- Analystes de menace
- Chercheurs spécialisés dans la vulnérabilité
- Chercheurs spécialisés dans la sécurité

Vous apprendrez à...

- Découvrir les vulnérabilités « zero-day » des programmes qui fonctionnent sur les systèmes d'exploitation modernes patchée
- 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 and IDA
- Déboguer à distance les applications
  Linux et Windows
- Comprendre et exploiter les débordements de tas Linux
- Écrire du Return Oriented Shellcode
- Effectuer le patch diffing pour des programmes, des bibliothèques, et des commandes afin d'identifier les vulnérabilités corrigées
- Effectuer des débordements de tas dans Windows et utiliser des attaques
  "use-after-free"
- Utiliser « precision heap sprays » pour améliorer l'exploitabilité
- Déboguer Windows Kernel jusqu'à
  Windows 8 64-bit
- Plonger dans l'exploitation de Windows Kernel

46 CPE/CMU CREDITS

Développer la prochaine génération de chefs d'équipe en 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

FOR 498

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Battlefield Forensics & Data Acquisition | Nouveau

LE COMPTE À REBOURS EST LANCÉ. VOUS DEVEZ FOURNIR LES PREUVES LES PLUS IRRÉFUTABLES EN VUE DE LEUR TRAITEMENT. NOS FORMATIONS SONT LÀ POUR VOUS Y AIDER.
Le cours FOR498 : Battlefield Forensics & Data Acquisition vous aidera à::

Acquérir efficacement des données à partir de:
- PC, périphériques Microsoft Surface et tablettes
- Périphériques Apple, Mac et MacBook
- Ressources en RAM et mémoires
- Smartphones et appareils mobiles
- Ressources de stockage et services dans le cloud
- Référentiels de stockage réseau
- Générer des renseignements traduisibles en action en moins de 90 minutes

Dans n'importe quelle enquête, la première étape consiste à rassembler des preuves. Les investigations numérique n'échappent pas à cette règle. Les preuves employées dans ce type d'enquête sont des données, lesquelles peuvent revêtir de nombreuses formes et résider dans des lieux variés. Votre mission consiste à identifier en premier lieu les données dont vous pourriez avoir besoin, à en déterminer l'emplacement, puis à élaborer un plan et des procédures de collecte des données. Dans le cas d'acquisitions inforensique portant sur des données , vous ne disposez généralement que d'une seule opportunité de collecter celles-ci correctement. En cas d'acquisition défectueuse, vous risquez non seulement d'entraver l'investigation, mais aussi et surtout de détruire les seules données qui auraient été exploitables comme preuves..
Compte tenu de la diversité des supports de stockage actuellement disponibles sur le marché, toute méthodologie présentée comme une panacée est au bas mot indéfendable. De nombreuses erreurs sont en effet commises lors de la collecte de preuves numériques, ce qui peut entraîner la libération de coupables ou, chose plus grave, la condamnation d'innocents. Le déploiement de budgets représentant plusieurs millions de dollars peut reposer sur les simples bits et octets que vous avez la charge de collecter et d'interpréter correctement.
Dès lors, un enquêteur ne peut plus se fier à l'imagerie d'un disque dur unique sous forme de boîte inactive : dans la cybersphère d'aujourd'hui, bon nombre d'utilisateurs jonglent entre un ordinateur de bureau, un portable, une tablette et un téléphone mobile au cours d'une même journée classique. Le recours croissant au stockage de données et à des fournisseurs dans le cloud, de même que la collecte adéquate de données depuis l'ensemble de ces domaines, peuvent se révéler des tâches proprement accablantes.
Cette formation approfondie consacrée à l'acquisition et à la gestion de données numériques procure aux enquêteurs et premiers intervenants les compétences de premier plan nécessaires pour répondre, identifier, collecter et conserver ces données, le but étant de maintenir leur intégrité au-dessus de tout soupçon. Le cours 498, réactualisé en permanence, répond aux besoins actuels en matière de connaissance et de compréhension des défis et techniques nécessaires aux enquêteurs pour traiter les cas réels.
De nombreux travaux pratiques viendront, tout au long du cours, faire bénéficier les premiers intervenants, enquêteurs et équipes inforensique d'une expérience pratique lors de l'acquisition de données à partir de disques durs, clés USB, téléphones cellulaires, espaces de stockage réseau et toutes leurs formes apparentées. Lorsqu'une organisation mène une intervention et une enquête au moyen d'une méthode numérique, elle doit s'entourer des intervenants les plus qualifiés, sauf lorsque l'investigation s'achève avant même d'avoir commencé.
Le cours FOR498 vous formera, vous et votre équipe, à identifier, collecter, préserver et répondre aux données, quel que soit le lieu où celles-ci sont cachées ou hébergées.

Public visé :

- Fonctionnaires et forces de police
- Premiers intervenants l
- Analystes de l'investigation numérique
- Membres d'équipes de réponse aux incidents
- Analystes de l'exploitation des supports
- Professionnels des ministères de la Défense et services de renseignement
- Toute personne souhaitant mieux comprendre les méthodes adéquates de préservation des systèmes d'information

Vous apprendrez à :

- Apprentissage et maîtrise des outils, techniques et procédures nécessaires pour localiser, identifier et recueillir efficacement des données, quel que soit leur lieu de stockage
- Gestion et manipulation appropriées d'une scène d'intervention afin de maintenir l'intégrité des preuves
- Identification des nombreux lieux où les données nécessaires à une enquête peuvent résider
- Exécution d'analyses sur le terrain en passant de la saisie de preuves à des renseignements exploitables en moins de 90 minutes
- Aide à l'élaboration de la documentation nécessaire pour communiquer avec des entités en ligne telles que Google, Facebook, Microsoft, etc
- Compréhension des concepts et exploitation des technologies de stockage massif tels que les systèmes JBOD, stockages RAID, périphériques NAS et autres systèmes accessibles en réseau à grande échelle
- Identification et collecte de données utilisateur dans les environnements d'entreprise étendus où elles sont accessibles par des PME
- Collecte des données volatiles telles que la mémoire RAM d'un système informatique
- Restauration et préservation appropriées des données numériques stockées sur les téléphones mobiles et autres périphériques portatifs

36 CRÉDITS CPE/CMU

SANS TRAINING CATALOGUE

FOR 500

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 investigations dans le cas de fraudes, de menaces internes, d'espionnage industriel, d'abus par un employé et d'intrusions information n'ont jamais été autant recherchés. Les agences gouvernementales nécessitent de plus en plus des spécialistes entraînés, formés à exploiter les médias pour collecter des renseignements clés à partir de systèmes Windows. Consciente de ces besoins, SANS forme actuellement la nouvelle génération de professionnels en investigation numérique, 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.

FOR500 : Windows Forensic Analysis vise à inculquer une connaissance inforensique approfondie des systèmes d'exploitation de Microsoft Windows. Vous ne pouvez protéger ce que vous ne connaissez pas. De ce fait, la compréhension des capacités inforensiques et des artefacts est une composante essentielle de la sécurité de l'information. Les stagiaires apprennent à récupérer, analyser et authentifier des données numériques 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 la gestion d''un incident, une investigation interne, et pour un contentieux civil ou criminel. Les stagiaires acquièrent aussi de nouvelles compétences pour valider les outils de sécurité, améliorer les évaluations de vulnérabilité, identifier les menaces internes, suivre les hackers, et améliorer leurs politiques de sécurité. Windows enregistre silencieusement une énorme quantité de données concernant 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 à l'aide de l'aide de nouveaux exercices pratiques réalisés en laboratoire intégrant les éléments de preuves identifiés dans les dernières technologies de Microsoft Windows (Windows 7, Windows 8/8.1, Windows 10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). À l'issue du cours, les stagiaires sont armés avec les tout derniers outils et techniques de pointe, pour mener leurs investigations même sur les systèmes les plus complexes. Les participants apprennent à faire une analyse exhaustive sur les systèmes Windows XP hérités afin de découvrir les artefacts de Windows 10.

Ce cours est basé sur une affaire de vol de propriété intellectuelle et d'espionnage en entreprise qui a nécessité six mois de développement. Vous travaillez dans le monde réel : votre formation se doit d'inclure des données pratiques et concrètes. Notre équipe de développement s'est servi d'incidents issus de leurs propres expériences pour créer un scénario incroyablement riche et détaillé afin de plonger les étudiants dans une atmosphère d'investigation aussi réelle que possible. Cette affaire présente les artefacts et technologies les plus récentes 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 suivre pour résoudre une affaire.

"Course is very up to date and challenges existing ideas to help become a better investigator. Course is well prepared."
Frank Visser,
PWC

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

Public visé :

- Professionnels de la sécurité de l'information
- Membres des équipes de gestion d'incident
- Enquêteurs : représentants des forces de l'ordre, agents du renseignement de la justice et d'autres administrations de l'État
- Analystes spécialisés dans l'exploitation des médias
- Toute personne souhaitant approfondir sa compréhension de l'inforensique pour Windows

Vous apprendrez à...

- Mener des investigations numériques sous Windows en bonne et due forme en appliquant des techniques clés
- Utiliser toute la gamme des outils et des méthodes d'analyse disponibles pour détailler toutes les actions ou presque d'un suspect dans un système Windows, y compris l'auteur d'un artefact (identité, procédure), l'exécution de programmes, l'ouverture de fichier/dossier, la géolocalisation, l'historique navigateur, le profilage d'utilisation d'appareil USB, etc.
- Découvrir l'heure exacte à laquelle un utilisateur a utilisé un programme pour la dernière fois grâce à une analyse artefact du Registre et de Windows, et comprendre comment utiliser cette information pour prouver les intentions dans le cas de vol de propriété intellectuelle, de systèmes compromis par un hackeur et d'autres crimes traditionnels
- Déterminer le nombre d'ouvertures d'un fichier par un suspect grâce à une analyse navigateur, une analyse des raccourcis (LNK), une analyse des e-mails et l'analyse du Registre Windows
- Identifier les mots-clés recherchés par un utilisateur spécifique dans un système Windows pour cibler les fichiers et les informations qui intéressaient le suspect, puis mener une évaluation détaillée des dommages occasionnés
- Utiliser des outils d'analyse shellbags Windows pour articuler chaque dossier et répertoire qu'un utilisateur a ouvert tout en parcourant des lecteurs locaux, amovibles et réseaux

FOR 508

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Digital Forensics, Incident Response, and Threat Hunting

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 et remédier aux incidents
- Développer des sources clés en matière de renseignements sur les menaces
- Chercher et détecter des brèches additionnelles en utilisant les connaissances 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 que vous avez de fortes chances d'être prochainement attaqué. Ils ne vous expliqueront pas comment ils sont au courant, mais ils pensent que certains de vos systèmes sont déjà compromis. Une menace persistante et avancée (APT en anglais) est très probablement en jeu. Il s'agit là 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 qu'elles ont mises en place sont parfaites et impénétrables, et ce quel que soit le niveau de sécurité. Les systèmes de prévention seuls ne peuvent suffire à contrer un adversaire humain concentré qui sait comment contourner la plupart des outils de sécurité et de surveillance.

Ce cours approfondi de réponse aux incidents et de chasse aux menaces permet aux équipes en charge de développer des compétences avancées afin de traquer, identifier et contrer une vaste gamme de menaces à l'intérieur des réseaux entreprises, y compris les adversaires de niveau national, les syndicats du crime organisé et l'hactivisme. La formation accorde aussi une place importante à la récupération des systèmes une fois la menace écartée. Constamment remis à jour, 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, contrer et répondre aux brèches de sécurité qui se produisent dans le monde réel.

"We're setting up a new forensic capability and this course has given me everything I need to do just that."
Simon Fowler,
VIRGIN MEDIA

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

Public visé :

- Les membres d'une équipe de réponse aux incidents
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement
- Les membres d'une « Red Team »,les testeurs d'intrusion, et les développeurs d'exploits
- Étudiants 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 à travers différents systèmes Windows dans un environnement d'entreprise
- Traquer et répondre aux incidents à travers plusieurs centaines de systèmes uniques simultanément en utilisant F-Response Enterprise et la station de travail SIFT
- Identifier et traquer le balisage sortant des malwares vers leur canal de commande et de contrôle (C2) grâce à une investigation numérique de la mémoire, une analyse de registre et les résidus de connexion réseaux
- Déterminer le déroulement d'une brèche en identifiant la pointe de l'attaque et les mécanismes de harponnage
- Maîtriser les techniques des adversaires avancés en matière de contre-investigation numérique, comme les malwares cachés et de type time-stomped, en parallèle de logiciels utilitaires utilisés pour se déplacer dans le réseau et maintenir une présence d'attaquant
- Utiliser l'analyse mémoire, la réponse aux incidents et les outils de chasse aux menaces dans la station de travail SIFT pour détecter des processus cachés, des malwares, des lignes de commandes malveillantes, des rootkits, des connexions réseaux, etc.
- Traquer l'activité utilisateur et attaquant seconde par seconde dans le système que vous analysez grâce à une analyse approfondie de la chronologie et de la super chronologie Récupérer les données effacées en utilisant des techniques de contre-investigation numérique via Volume Shadow Copy et l'analyse du point de restauration

FOR 518

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Mac and iOS Forensic Analysis and Incident Response

Les investigateurs numériques ont traditionnellement travaillé sur des machines Windows, mais que se passe-t-il lorsqu'ils sont confrontés à un nouveau dispositif ou à un nouveau Mac d'Apple ? La popularité croissante des dispositifs Apple est constatée partout, depuis les coffee shops jusque dans les salles de conseil d'administration, et pourtant les investigateurs ne sont familiers qu'avec des machines Windows.

Les temps et les tendances évoluent et les investigateurs et les analystes ont besoin d'évoluer avec eux. Le nouveau cours FOR518 : Mac Forensic Analysis apporte les outils et techniques nécessaires pour réagir et traiter sans hésitation un incident impliquant un Mac. Les compétences pratiques et intensives d'analyse numérique enseignées dans ce cours permettent aux investigateurs Windows d'élargir leurs capacités d'analyse, et d'avoir la confiance et les connaissances pour analyser aisément tout système Mac ou iOS.

Le contenu du cours FOR518: Mac Forensic Analysis :

- Fondamentaux Mac : Comment analyser à la main le Hierarchical File System (HFS+) et reconnaître les domaines spécifiques du système fichier logique et les types de fichier Mac.
- Activité utilisateur : comment comprendre et profiler un utilisateur grâce à ses fichiers de données et la configuration de ses préférences.
- Analyse avancée et corrélation : comment déterminer l'utilisation qui a été faite d'un système ou son niveau de compromission en utilisant les fichiers système et les fichiers de données utilisateur en corrélation avec les fichiers logs systèmes.
- Technologies Mac : comment comprendre et analyser diverses technologies Mac, dont Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, et FaceTime.

FOR518: Mac Forensic Analysis a pour objectif de compléter la formation d'un spécialiste en investigation numérique sous Windows et de lui faire découvrir l'équivalent sous Mac. Ce cours met l'accent sur des thèmes comme 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 logs Mac, d'applications Mac et de technologies Mac. Un spécialiste de l'investigation numérique qui suit la totalité de ce cour sera parfaitement armé pour mener des enquêtes sous Mac.

> **"Best Mac forensics course available."**
>
> David Klopp,
> *J.P.MORGAN*

> **"The depth of time exercise was outstanding. One can tell the amount of work that went into it."**
>
> Gary Titus,
> *STROZ FRIEDBERG LLC*

Public visé :

- Les analystes expérimentés de l'investigation numérique qui souhaitent renforcer et élargir leur compréhension de l'inforensique des fichiers système et de l'analyse Mac avancée
- Les forces de l'ordre, les agents du renseignement, ou les enquêteurs qui veulent maîtriser l'inforensique avancée et élargir l'ensemble de leurs compétences en investigation
- Les analystes de l'exploitation des médias qui ont besoin de savoir comment trouver les données critiques dont ils ont besoin sur un système Mac
- Les membres d'une équipe de gestion d'incident qui font face à des incidents de sécurité et/ou à des intrusions complexes venant d'adversaires sophistiqués et qui ont besoin de savoir quoi faire lorsqu'ils examinent un système compromis
- Les professionnels de la sécurité de l'information qui veulent développer une connaissance des systèmes d'exploitation Mac OS X et iOS
- Les stagiaires qui ont déjà suivi les cours SANS FOR408, FOR508, FOR526, FOR610, FOR585 qui veulent parfaire leurs compétences inforensiques

Vous apprendrez à...

- Analyser manuellement les systèmes de fichiers HFS+ en n'utilisant qu'une cheat sheet 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 de systèmes par des individus, y compris la fréquence d'utilisation, les applications utilisées et les préférences système personnelles
- Déterminer les sauvegardes de données locales ou à distance, les images disque et les autres appareils rattachés
- Trouver des conteneurs cryptés et des volumes FileVault, comprendre les données Keychain et craquer les mots de passe Mac

36 CRÉDITS CPE/CMU

FOR 526

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Memory Forensics In-Depth

Les professionnels DFIR ont besoin d'une formation avancée en inforensique de mémoire Windows pour répondre à leurs besoins. Les investigateurs qui ne se penchent pas sur la mémoire volatile laissent des preuves sur la scène de crime. La RAM détient 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 investigateurs numériques et aux gestionnaires d'incidents qui leur permettent de faire un triage de la mémoire et analyser des images de mémoire capturées avec succès. Le cours utilise les logiciels et les outils les plus efficaces de l'industrie en open-source; il permet de comprendre dans le détail comment ces outils fonctionnent. Le cours FOR526 est un cours essentiel pour tout investigateur DFIR sérieux qui veut maîtriser l'expertise inforensique de haut niveau, et intervenir sur des incidents impliquant des abus d'initiés.

De nos jours, il est tout aussi essentiel de comprendre les structures de la mémoire que les structures de disque et de registre pour l'investigation numérique. 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'investigation en cours. Pour les plateformes d'investigation autres que Windows, ce cours apporte aussi une introduction pratique à l'analyse et l'acquisition numérique de mémoire OSX et Linux par des exercices.

Il y a une véritable course à l'armement entre les investigateurs et les assaillants. Les malwares modernes et les modules post-exploitation 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 investigateurs doivent avoir une connaissance plus approfondie des éléments internes de la mémoire afin de pouvoir 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 leur acquisition, validation, et analyse de mémoire en utilisant des images de mémoire réelles, chargées de malwares.

Le contenu du cours FOR526: Memory Forensics In-Depth :

- Acquisition mémoire : capturer la mémoire ciblée en garantissant l'intégrité des données et surmonter les obstacles aux comportements d'acquisition/anti-acquisition
- Le diable est dans les détails : détecter des processus malveillants, cachés et injectés, des rootkits au niveau du noyau, le détournement de Dynamic Link Libraries (DLL), le process hollowing et les mécanismes sophistiqués de persistance
- Techniques efficaces et pas à pas d'analyse mémoire : utiliser un calendrier processus, des analyses de niveau haut/bas et parcourir l'arbre des descripteurs d'adresses virtuelles (VAD en anglais) pour détecter des comportements anormaux
- Les bonnes pratiques/techniques : apprendre quand implémenter un triage, une analyse système live et les techniques alternatives d'acquisition, et comment concevoir des scripts d'analyse personnalisés pour une analyse mémoire ciblée

Public visé :

- Équipes de réponse aux incidents qui doivent régulièrement faire face à des incidents/intrusions complexes et qui voudraient ajouter l'investigation de la mémoire vive à leurs compétences
- Professionnels expérimentés en investigation numérique qui souhaitent consolider et accroître leur maîtrise de l'analyse de la mémoire vive
- Red team, chargés de test de pénétration et développeurs d'exploits qui souhaitent savoir comment ne pas se faire identifier par leurs adversaires
- Représentants des forces de l'ordre, agents fédéraux et enquêteurs qui souhaitent ajouter une compétence approfondie en analyse de mémoire vive
- Anciens étudiants ayant suivi les cours SANS FOR508 et SEC504 et qui veulent passer au niveau suivant de leur formation
- Chargés d'investigation numérique travaillant dans des organisations où la mémoire est régulièrement récupérée par les premiers intervenants et qui veulent relever le niveau en analysant les images

> **"This training opened my eyes to the need to collect memory images, as well as physical images for single computer analysis, such as theft of IP or other employee investigations."**
>
> Greg Caouette, *KROLL*

36 CPE/CMU CREDITS

FOR 572

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Network Forensics and Analysis

Transférez votre connaissance de l'expertise numérique des systèmes sur le fil. Intégrez des données de réseau dans vos enquêtes, produisez de meilleurs résultats et effectuez le travail plus rapidement. Il est extrêmement rare de mener une enquête numérique sans élément de réseau. L'analyse numérique des points de terminaison « End Points »

sera toujours cruciale et constitue une compétence fondamentale pour cette carrière, mais ignorer leurs communications réseau équivaut à ignorer les images de caméra de sécurité d'une scène de crime. 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, découvrir des attaquants qui ont été actifs pendant des mois ou plus, ou même s'avérer utile pour prouver sans équivoque qu'un crime s'est réellement produit.

FOR572 : Advanced Network Forensics and Analysis a été construite pierre par pierre pour couvrir les compétences les plus cruciales nécessaires pour monter des réponses post-incident efficaces et optimales. Nous nous concentrerons sur les connaissances nécessaires pour élargir la mentalité inforensique en commençant par les données résiduelles sur les supports de stockage d'un système ou d'un dispositif, puis les communications transitoires qui se sont produites dans le passé ou continuent à se produire. 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 commandement et de contrôle et sans 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 de réseau dans vos enquêtes, en mettant 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 une utilisation dès votre première journée de travail. Nous couvrirons toute la gamme des preuves réseau, y compris l'analyse NetFlow de haut niveau, l'exploration de PCAP de bas niveau, l'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, un professionnel des forces de l'ordre assistant les victimes de la cybercriminalité qui veut engager des poursuites judiciaires contre les responsables, un praticien de l'expertise numérique sur place ou un membre des rangs grandissant des «threat hunters », ce cours offre une expérience pratique avec des scénarios issus du monde réel qui vous aideront à progresser dans votre travail. Les anciens stagiaires du programme SANS SEC et d'autres défenseurs de réseau 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 existantes et les appliquer directement aux attaques de réseau quotidiennes. Avec FOR572, nous résolvons le même calibre de problèmes issus du monde réel sans l'utilisation d'images de disque ou de mémoire.

Public visé :

- Membres de l'équipe de réponse aux incidents et investigateurs numérique
- Membres d'une « hunt team »
- Agents d'application de la loi, agents fédéraux, détectives, et gestionnaires de la sécurité des systèmes d'information
- Défenseurs de réseau
- Professionnels de l'informatique
- Ingénieurs de réseau
- Toute personne intéressée par l'analyse et investigations numérique
- Personnel du centre des opérations de sécurité (SOC) et spécialistes de la sécurité de l'information

Vous apprendrez à...

- Extraire des fichiers à partir de captures de paquets réseau et de fichiers de cache proxy, permettant ainsi l'analyse subséquente des programmes malveillants ou la détermination définitive des pertes de données
- Utiliser les données historiques de NetFlow pour identifier les occurrences de réseau antérieures pertinentes, permettant une définition précise de l'incident
- Inverser des protocoles réseau personnalisés pour identifier les capacités et les actions de commandement 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 basées sur les systèmes et plateformes existants dans une architecture de réseau
- Examiner le trafic en utilisant des protocoles de réseau communs pour identifier les modes d'activité ou les actions spécifiques justifiant une enquête plus approfondie

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

FOR 578

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

Cyber Threat Intelligence

Ne vous y trompez pas : actuellement, la défense réseau, la chasse aux menaces et la réponse aux incidents sont des pratiques qui contiennent de fortes proportions de renseignement et de contre-renseignement, des aspects que les cyberanalystes doivent comprendre et exploiter s'ils veulent pouvoir défendre efficacement les réseaux, les données propriétaires et les organisations dont ils ont la responsabilité.

FOR578: Cyber Threat Intelligence aidera les défenseurs réseaux, les équipes de chasse aux menaces et les chargés de réponse aux incidents à :

- Comprendre et développer des compétences en matière de renseignement aux niveaux tactiques, opérationnels et stratégiques
- Obtenir des renseignements sur les menaces pour détecter, répondre et vaincre des menaces persistantes et avancées (APT)
- Valider les informations reçues de la part d'autres organisations pour minimiser les dépenses en mauvais renseignements
- Exploiter les renseignements en open-source pour compléter le travail d'une équipe de sécurité de n'importe quelle taille
- Créer des indicateurs de compromission (IOC en anglais) 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 – permettent aux défenseurs réseaux d'avoir 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 posséder des méthodes permettant d'exploiter ces informations de façon à mettre en place une posture défensive améliorée.

Les renseignements sur les cybermenaces constituent donc un atout majeur pour les organisations qui cherchent à mettre à jour leurs programmes de réponse et de détection dans un monde où les menaces persistantes et avancées se font toujours plus sophistiquées. Les malwares ne sont que des outils : c'est l'individu qui les manie qui représente la véritable menace. Les renseignements sur les cybermenaces cherchent en priorité à contrer cette menace humaine à la fois persistante et flexible en leur opposant des défenseurs humains armés et entraînés.

En cas d'attaque ciblée, une organisation doit disposer d'une équipe de chasse aux menaces 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. FOR578: Cyber Threat Intelligence vous permettra à vous et à votre équipe de développer des compétences en matière de renseignements sur les cybermenaces afin que vous puissiez 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.

> **"I am new to CTI and this course was really well put together to cater for people with different levels of expertise"**
>
> Ben Hargreaves,
> *PWC*

Public visé :

- Équipes chargées de la réponse aux incidents
- Chasseurs de menaces
- Analystes accomplis en investigation numérique
- Professionnels de la cybersécurité et personnel de Centre des opérations de sécurité
- Agents fédéraux et agents des forces de l'ordre
- Étudiants ayant suivi les cours SANS FOR500 (anciennement FOR408), FOR572, FOR508, ou FOR610 qui souhaitent faire passer leurs compétences au niveau suivant

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
- Comprendre et développer des compétences en renseignements tactiques, opérationnels et stratégiques sur les menaces
- 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 en anglais) 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 n'importe quel poste de sécurité

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

FOR 585

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Advanced Smartphone Forensics

Les dispositifs mobiles sont souvent un facteur clé dans les enquêtes criminelles, les intrusions, les vols de propriété intellectuelle, les menaces sécuritaires, et bien plus. Comprendre comment exploiter les données à partir du dispositif de façon correcte peut aussi bien résoudre que lancer une affaire FOR585: Advanced Smartphone Forensics enseigne toutes ces compétences.

L'investigation numérique des smartphones ne consiste pas à simplement presser le bouton « Trouver la preuve » et obtenir des réponses. Bien au contraire, il est essentiel de comprendre comment utiliser correctement ces outils pour diriger l'investigation plutôt que de laisser l'outil rapporter ce qu'il déduit à partir de l'utilisation du dispositif.

Il est impossible pour les outils commerciaux de tout analyser sur les smartphones et de comprendre comment les données sont arrivées sur le dispositif. Le cours donne aux stagiaires la capacité et la confiance nécessaires pour extraire de bonnes preuves à partir des smartphones.

Ce cours détaillé sur l'investigation numérique des smartphones apporte aux investigateurs et analystes les compétences pour détecter, décoder, déchiffrer, et interpréter correctement les preuves récupérées sur des dispositifs mobiles. Le cours 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 smartphone se dissimulent et comment elles peuvent être facilement mal interprétées par les outils inforensiques.

Chaque atelier aborde un sujet particulier qui peut être appliqué 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.

Le cours FOR585 est continuellement actualisé pour être à jour avec les derniers malwares, les derniers systèmes d'exploitation de smartphones, les applications de tiers, et l'encryption. Ce cours intensif de six jours arme les stagiaires avec une connaissance inforensique des dispositifs mobiles qui peut être mise en pratique immédiatement dans leurs missions.

Les technologies des smartphones évoluent en permanence et la plupart des professionnels de l'investigation numérique ne sont pas familiarisés avec les formats de données des différentes technologies. Faites passer vos compétences au niveau supérieur : 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 !

"The best part about Advanced Smartphone Forensics is it provides real world technologies for forensically investigating devices without the typical point and click approaches."

Brad Wardman,
PAYPAL

Public visé :

- Analystes expérimentés en investigation numérique
- Analystes exploitation média
- Professionnels de la cybersécurité
- Équipes de réponse aux incidents
- Représentants des forces de l'ordre, agents fédéraux et enquêteurs
- Chargés d'audit informatique
- Étudiants ayant suivi les cours SEC575, FOR500 (anciennement FOR408), FOR508, FOR518, et FOR572 qui souhaitent faire passer leurs compétences au niveau suivant

Vous apprendrez à...

- Sélectionner les outils, les techniques, et les procédures d'investigation numérique 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 ex., qui communique avec qui, où et comment)
- Comprendre comment les systèmes de fichiers d'un smartphone enregistrent les données, comment elles diffèrent, et comment les preuves sont conservées sur chaque dispositif
- Interpréter les systèmes de fichiers sur des smartphones et localiser l'information qui n'est généralement pas accessible aux utilisateurs
- Identifier comment la preuve est arrivée sur le dispositif mobile
- Incorporer des techniques de décodage manuelles pour récupérer des données supprimées, enregistrées sur des smartphones et dispositifs mobiles
- Associer un utilisateur à un smartphone à une heure/date spécifique et des géolocalisations diverses
- Decrypt or decode application data that are not parsed by your forensic tools Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyse mobile malware using open-source tools

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

FOR 610

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 les techniques d'analyse de malwares. FOR610 permet aux chargés d'investigation numérique, 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 fortifier leurs défenses. Ce cours pose des bases solides en rétro-ingénierie appliquée aux logiciels malveillants en utilisant divers utilitaires de surveillance système et réseau ainsi qu'un désassembleur, un débogueur et de nombreux autres outils disponibles gratuitement.

Vous commencerez par une introduction poussée de l'analyse de malware et vous poursuivrez sur cette voie en suivant les découvertes que vous ferez grâce aux outils d'analyse automatisée. Vous apprendrez comment mettre en place un laboratoire flexible pour examiner le fonctionnement interne d'un logiciel malveillant, puis vous verrez 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 inoffensif de façon à échapper aux analyses, mais cette formation vous enseignera à repérer 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 leurs présences dans un système : ce cours aborde précisément à cet effet l'analyse de code et des approches d'investigation numérique 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 communes d'auto-défense, y compris 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 dans un environnement sécurité et 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 pré-montées et dotées des outils nécessaires pour examiner et interagir avec les malwares étudiés.

"It really gives a nice realistic guidance on how to approach complex problems in Malware Analysis."
Markus Jeckeln,
LUFTHANSA

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

Public visé :

- Personnes ayant traité des incidents impliquant des logiciels malveillants et qui souhaitent apprendre à comprendre les principaux aspects des programmes malveillants
- Technologues ayant expérimenté de manière informelle des aspects de l'analyse des logiciels malveillants avant le cours et cherchent à formaliser et étendre leur expertise dans ce domaine
- Analyste inforensique et Responsable IT cherchant à élargir leurs compétences et apprendre à jouer 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
- Utilisez des outils de surveillance du réseau et du système pour examiner la manière dont les programmes malveillants interagissent avec le système de fichiers, le registre, le réseau et d'autres processus dans un environnement Windows.
- Découvrez et analysez les composants malveillants JavaScript et VBScript des pages web, qui sont 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 aux code patching pour effectuer une analyse efficace des malwares.
- Utilisez un désassembleur et un débogueur pour examiner le fonctionnement interne des exécutables Windows malveillants
- Contourner une variété de packers et d'autres mécanismes défensifs conçus par des auteurs de logiciels malveillants pour détourner, confondre et ralentir l'analyste

La sensibilisation à la sécurité est cruciale dans la protection de votre organisation

Quel est le contenu de votre formation ?

SANS EMEA
SECURITY AWARENESS

Expert Led

Le contenu des modules de SANS Security Awareness a ont été élaborés par des experts leaders en matière de cybersécurité. Des experts en sciences cognitives, des animateurs en théorie de la conception et des experts leader en sensibilisation à la sécurité dispensent des modules de formation visant à protéger les organisations et à changer les comportements humains.

Pertinent

Notre contenu fait l'objet de mises à jour constantes pour répondre aux menaces actuelles. La formation est disponible en plusieurs format avec toute une variété de matériels supplémentaires, de façon à pouvoir toucher des publics divers et variés, quelle que soit la langue.

Facile

Les modules sont conçus pour couvrir les menaces importantes, avec des modules de formation aux bases et des modules de formation avancées pour couvrir tous les aspects.

Une formation de classe mondiale dispensée par des experts à la pointe, disponible dans de nombreux formats, et préparée pour une audience globale. 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

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

SANS Training Program for CISSP® Certification

Le cours SANS MGMT414 est une préparation à la certification CISSP®. Conçu spécifiquement pour préparer les stagiaires à passer l'examen CISSP® avec succès. La formation MGT414 se présente sous forme de révision accélérée, portant sur les 8 domaines de connaissances clés identifiés par (ISC)2 et sur lesquels porte l'examen CISSP®. Chaque domaine de connaissance est disséqué et une discussion s'ensuit concernant la relation qui unit chaque composant critique les uns aux autres dans divers domaines de la sécurité informatique.

Obtenir votre certification CISSP®, c'est :

- Remplir les critères minimaux en termes d'expérience professionnelle pratique Remplir l'Accord candidat
- L'examen de votre CV
- Répondre aux 200 questions à choix multiple du CISSP® et obtenir un score gradué de 700 points ou plus Soumettre un Formulaire de validation dument complété
- Mener régulièrement des audits des CPE pour maintenir la validité des qualifications

> **"Best security training I have ever received and just the right amount of detail for each domain."**
>
> Tony Barnes,
> *UNITED STATES SUGAR CORP*

Public visé :

- Professionnels 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
- Professionnels de la sécurité, responsables, administrateurs systèmes 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 des 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 au bureau

GIAC INFORMATION SECURITY PROFESSIONAL — GISP

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

MGT 512

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

CINQ JOURS • ORDINATEUR PORTABLE REQUIS

SANS Security Leadership Essentials For Managers (with Knowledge Compression™)

Le cours MGT512 permet aux dirigeants en promotion de se mettre rapidement à niveau sur les questions de sécurité de l'information et d'acquérir la terminologie essentielle. Au-delà des connaissances, les stagiaires apprennent à gérer la sécurité.

Les dirigeants acquièrent des connaissances et les compétences cruciales et actualisées requises pour superviser la composante de sécurité dans tout projet relevant de la technologie de l'information. De surcroît, le cours a été conçu pour incorporer les lignes directrices de la série NIST Special Publication 800. Cela signifie que le cours MGT512 est particulièrement utile pour les dirigeants des administrations d'État américaines et leurs fournisseurs.

Les sujets fondamentaux de la sécurité qui sont abordés dans ce cours de gestion incluent: Les fondamentaux de réseau et les applications, l'énergie, et la sécurité, les approches architecturales détaillées concernant la défense, les cyberattaques, la gestion et l'évaluation de la vulnérabilité, les politiques de sécurité, les plans d'urgence et de continuité des opérations, la gestion de la sensibilisation, l'analyse de la gestion du risque, la gestion d'incident, la sécurité des applications web, la guerre offensive et défensive relative à l'information.

Le cours utilise des supports graphiques conçus avec Knowledge Compression™ et d'autres techniques SANS brevetées pour transmettre les points clés de diapositives critiques tout en maintenant le flux d'information au rythme attendu par les dirigeants tout au long du cours.

Ce cours a été évalué et approuvé par by CompTIA's CAQC programme for Security + 2008 pour garantir l'acquisition des concepts et de la terminologie de base dans le domaine de la sécurité. Les dirigeants seront en mesure de mettre en pratique ce qu'ils ont appris dès leur retour au bureau

Knowledge Compression™
Maximisez votre potentiel d'apprentissage !
Knowledge Compression™ est une fonctionnalité optionnelle que vous pouvez ajouter à une classe SANS pour maximiser l'acquisition et la rétention à long terme de grandes quantités d'informations au cours d'une période de temps relativement brève. Le matériel pédagogique spécialisé, les examens en classe et les consignes de test sont autant de paramètres qui permettent à Knowledge Compression™ de garantir aux étudiants de comprendre et retenir un maximum d'informations. En suivant des formations dotées de ce produit avancé, vous participerez à des programmes de formation parmi les plus intenses et les plus efficaces que SANS a à vous offrir !

Public visé :

- Tous les nouveaux cadres dirigeants dans le domaine de la sécurité informatique
- Les administrateurs experts techniques qui se sont vu confier de nouvelles responsabilités d'encadrement
- Les dirigeants chevronnés qui ont besoin de comprendre les processus techniques, et les politiques

Vous apprendrez à...

- Établir des normes de base pour les capacités, compétences et connaissances en matière de sécurité IT. En quelques mots, ce cours reprend tous les sujets non-opérationnels qui sont traités dans le cours Sans Security Essentials, mais sans rentrer dans autant de détails. L'objectif est de permettre aux dirigeants et aux auditeurs de comprendre et de parler le langage des administrateurs système, réseau et sécurité.
- Établir des normes de base pour la gestion des connaissances, des compétences et des capacités IT. Il y a encore des dirigeants qui ignorent ce que signifie TCP/IP. Cela peut paraître anodin, mais implique qu'ils sont incapables de calculer le coût global de possession (TCO) total cost of ownership, et on se demande ce qu'ils savent vraiment.
- Aider la génération émergente de hauts dirigeants qui gravissent des échelons rapidement dans un monde sans pitié, en partageant avec eux tout le savoir que vous auriez aimé avoir vous-même Comme le veut l'adage : On a le droit de faire des erreurs, mais seulement les nouvelles.

"This course is highly useful for giving me a sound baseline of Technical and general skills to help me manage an effective team"
Richard Ward
REA GROUP

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

MGT 514

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

IT Security Strategic Planning, Policy, and Leadership

IT 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 maitriser 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 vous n'êtes pas équipés des compétences dont vous aurez besoin pour rejoindre la meute. Apprenez à développer des plans stratégiques qui trouveront un écho particulier auprès d'autres leaders de l'informatique et du business.

Créer une stratégie de sécurité de l'information efficace
La politique est l'occasion pour le gestionnaire d'exprimer ses attentes à l'égard de la masse salariale, de fixer les limites d'un comportement acceptable et d'habiliter les personnes à faire ce qu'ils devraient faire. Il est facile de faire des erreurs. Avez-vous déjà été confronté à une politique à laquelle votre réponse était : « Jamais de la vie je ne ferai ça ». La politique doit être alignée sur la culture d'une organisation. Nous décomposerons les étapes du développement de la politique afin que vous puissiez développer et évaluer une politique pour guider votre organisation avec succès.

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 le succès organisationnel. 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
En étudiant des cas provenant de Harvard Business School, des exercices en équipe et des discussions qui mettent les stagiaires en situation réelle, les stagiaires participeront à des activités qu'ils pourront ensuite mettre en œuvre avec leurs propres membres d'équipe de retour au travail. La prochaine 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 protègeront votre entreprise, permettront des innovations clés et vous rapprocheront efficacement de vos partenaires commerciaux.

Public visé :

- RSSI
- Agents de sécurité de l'information
- Directeurs de la sécurité
- Responsables de la sécurité
- Leaders aspirants de la sécurité
- Personnel de sécurité ayant des responsabilités d'équipe ou de gestion

Vous apprendrez à...

- Élaborer des plans stratégiques de sécurité incorporant des facteurs 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

"This course is the Rosetta Stone between an MBA and a career in cyber."

Livingston,
DELOITTE

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

MGT 516

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

CINQ JOURS • ORDINATEUR PORTABLE RECOMMANDÉ

Managing Security Vulnerabilities: Enterprise and Cloud | NOUVEAU

Les vulnérabilités existent à tous niveaux. À la moindre occasion, de nouveaux rapports dressent le constat des faiblesses dont souffrent nos systèmes et nos logiciels. Leur cause directe : une recrudescence des attaques qui ciblent ces défaillances, à la fois en termes de quantité et de gravité.

Quelle que soit la taille d'une organisation, la gestion des vulnérabilités est une tâche ardue. Les environnements d'entreprise connaissent des mutations d'échelle et de diversité qui mettent à mal les résistances de nombreuses structures de sécurité et opérations informatiques. L'avènement du cloud, auquel s'ajoute la nécessité pour toutes les entreprises de fournir des systèmes, applications et fonctionnalités à leurs clients internes et externes avec une rapidité croissante, sont autant de facteurs qui peuvent transformer la sécurité en un problème insoluble. Ce cours expose les raisons pour lesquelles de nombreuses entreprises s'empêtrent plus que jamais dans la gestion de leurs vulnérabilités, en enseignant aux stagiaires les moyens de résoudre ces difficultés. Comment gérer les ressources en analysant et en hiérarchisant les vulnérabilités avec succès ? Quels sont les rapports les plus efficaces ? Sous quel angle aborder les vulnérabilités de nos applications, et comment les résoudre ? Nous examinerons l'évolution de la réponse à ces questions selon que nous optons pour une migration dans le cloud, un cloud privé ou une structure DevOps au sein de nos organisations. Comment faire de la gestion des vulnérabilités une activité ludique et inciter tous les collaborateurs à s'impliquer dans ce processus ? Il ne s'agit là que de quelques-uns des thèmes fondamentaux abordés durant ce cours.

L'objectif principal de cette formation est de vous aider à réussir là où bon nombre de gens échouent, en présentant des solutions aux problèmes connus ou susceptibles d'être expérimentés tôt ou tard. Que votre programme de gestion des vulnérabilités soit bien établi ou n'en soit qu'à ses prémices, ce cours vous aidera à mettre au point votre stratégie et à envisager la gestion des vulnérabilités sous une perspective différente.

En appréhendant les problèmes communs et les solutions proposées, vous serez mieux armé pour relever les défis auxquels vous serez confronté un jour ou l'autre, et déterminer les options les plus viables pour votre organisation. Grâce à des discussions en salle de classe complétées par des exercices complémentaires, vous apprendrez des techniques d'analyse et de génération de rapports spécifiques qui vous permettront de discuter des problèmes auxquels vous et vos pairs êtes confrontés, ainsi que de la manière de les résoudre.

Ce cours s'articule autour du modèle de type Préparation, Identification, Analyse, Communication et Traitement (PIACT) ::

- Préparation : définir, déployer et améliorer constamment le programme
- Identification : identifier les vulnérabilités présentes dans nos environnements d'exploitation
- Analyse : analyser et hiérarchiser les vulnérabilités identifiées et les autres indicateurs du programme afin d'offrir une aide et des conseils utiles aux parties prenantes et aux participants impliqués dans le programme
- Communication : présenter les conclusions des analyses de manière appropriée et efficace pour chaque groupe de parties prenantes
- Traitement : mettre en œuvre, tester et surveiller les solutions apportées aux vulnérabilités, groupes de vulnérabilités et problèmes plus génériques identifiés par le programme

Public visé :

- CISO
- Gestionnaires, responsables et administrateurs de la sécurité des informations
- Architectes, analystes et consultants en sécurité des systèmes d'information
- Futurs leaders de la sécurité des systèmes d'information
- Professionnels de la gestion des risques
- Planificateurs et collaborateurs en charge de la continuité des activités et de la reprise après sinistre
- Responsables et audits informatiques
- Chefs de projets informatiques
- Professionnels de l'administration informatique, des systèmes et des réseaux
- Responsables des opérations
- Gestionnaires et administrateurs de services cloud
- Gestionnaires de la sécurité et des risques liés aux services cloud
- Intégrateurs, développeurs et courtiers de services cloud
- Professionnels de la sécurité informatique gérant les vulnérabilités dans l'entreprise ou dans le cloud
- Agents gouvernementaux gérant les vulnérabilités informatiques dans l'entreprise ou dans le cloud (FedRAMP)

Vous apprendrez à..

- Création, mise en œuvre ou amélioration de votre programme de gestion des vulnérabilités
- Établissement d'un environnement d'entreprise et de cloud computing sécurisé et défendable
- Création d'un inventaire précis et utile des ressources informatiques dans l'entreprise et dans le cloud
- ·Identification des vulnérabilités existantes et compréhension de leurs niveaux de gravité respectifs
- Définition des priorités de traitement des vulnérabilités
- Consignation et communication efficaces des données de vulnérabilité au sein de votre entreprise
- Implication des équipes de traitement et approche ludique de la gestion des vulnérabilités

30 CRÉDITS CPE/CMU

SANS TRAINING CATALOGUE

MGT 525

TRAINING EVENTS | PRIVATE TRAINING

SIX JOURS • ORDINATEUR PORTABLE NON REQUIS

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

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

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

Ce cours a été récemment actualisé pour vous préparer pleinement aux modifications de l'examen PMP® en 2016. Au cours de cette formation, vous apprendrez à améliorer votre méthodologie de planification de projet et la planification des tâches de projet pour tirer le meilleur parti de vos ressources informatiques essentielles. Nous étudierons des cas de projets qui soulignent que les services de technologie de l'information sont des prestations. MGT525 suit la structure de gestion de projet de base du Guide PMBOK® - Cinquième édition et fournit également des techniques spécifiques pour assurer le succès des initiatives prises pour assurer l'information. Tout au long de la semaine, nous couvrirons tous les aspects de la gestion de projets informatiques, depuis l'initiation et la planification des projets, en passant par la gestion des coûts, du temps et de la qualité, jusqu'à la finalisation de votre projet. Une copie du Guide PMBOK® - Cinquième édition est fournie à tous les participants. Vous pouvez consulter le Guide PMBOK® et utiliser votre matériel de cours ainsi que 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, quel que soit le projet, quelle que soit l'industrie. Bien que notre objectif principal soit l'application à l'industrie InfoSec, notre approche est transférable à tous les projets qui créent et entretiennent des services ainsi que le développement général du produit. Nous couvrirons de façon détaillée comment le coût, le temps, la qualité et les risques affectent les services que nous fournissons aux autres. 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.

> **"Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job."**
>
> Ryan Spencer,
> *REED ELSEVIER INC.*

Public visé :

- Personnes intéressées à se préparer à l'examen Project Management Professional (PMP)®
- Professionnels de la sécurité intéressés par la compréhension des concepts de gestion de projet informatique
- Gestionnaires qui veulent comprendre les domaines critiques pour réussir les projets
- Personnes travaillant avec des contraintes de temps, 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

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 termes de coûts, de calendrier et de prestations techniques
- Établir un plan de travail décomposé pour définir des ensembles de travaux, les prestations à livrer 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

36 CRÉDITS CPE/CMU

AUD 507

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

SIX JOURS • ORDINATEUR PORTABLE REQUIS

Auditing & Monitoring Networks, Perimeters, and Systems

Un des obstacles les plus importants auxquels sont confrontés les auditeurs est d'être capable de modéliser la sécurité de l'entreprise. Quels sont les systèmes importants ? Comment configurer le pare-feu et les routeurs ? Quels sont les paramètres d'un système qui doivent être vérifiés ? Existe-t-il un ensemble de procédés qui peut permettre à un auditeur de se concentrer sur les processus de l'entreprise, plutôt que sur les paramètres de sécurité ? Comment en faire un processus de surveillance continue ? Toutes ces questions, et bien d'autres, seront abordés et trouveront réponse lors du cours AUD507.

Ce cours apporte une méthode basée sur le risque pour s'atteler à la tâche énorme 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 à l'audit, ainsi que les bons procédés en matière d'audit en général. Les stagiaires entrent ensuite dans le vif du sujet en détaillant les contrôles clés nécessaires à la sécurité d'une entreprise.

Le défi constant que les auditeurs doivent relever est d'aider la direction à comprendre la relation entre les contrôles techniques et les risques encourus par l'entreprise. Dans ce cours, les menaces et les vulnérabilités sont expliquées sur la base d'informations tirées de situations réelles.

Le formateur SANS prend le temps d'expliquer comment utiliser ces informations pour sensibiliser les dirigeants. Les stagiaires apprennent à communiquer sur l'importance de l'audit et des contrôles.

Les stagiaires apprennent aussi à élaborer un système de surveillance continue d'adhésion à la conformité; ils apprennent aussi à valider automatiquement les défenses par l'instrumentation et l'automatisation d'une liste de contrôle.

Pendant les cinq premiers jours, les stagiaires reçoivent des scripts de surveillance continue et des listes de contrôle général. Ceux-ci peuvent être adaptés à des situations d'audit particulières.

Les stagiaires font aussi des expériences pratiques en utilisant les nombreux outils présentés en cours. Ainsi, lorsque les stagiaires quittent le cours AUD507, ils auront acquis le savoir-faire pour auditer les contrôles décrits en classe. Cette approche garantit aussi que les stagiaires sauront à quoi s'attendre en matière de preuve d'audit.

"The entire course has been awesome and prepared me to perform a comprehensive audit. It also provided me excellent information to operations to improve network security posture."
Srinath Kannan,
ACCENTURE

Public visé :

- Les auditeurs qui cherchent à identifier les contrôles clés des systèmes informatiques
- Les auditeurs professionnels qui veulent approfondir des détails techniques pour effectuer un audit
- Les dirigeants responsables du travail effectué par une équipe de sécurité ou d'audit
- Les professionnels de la sécurité qui se voient attribuer de nouvelles responsabilités de contrôle
- Les administrateurs système et réseau qui cherchent à mieux comprendre ce que recherche un auditeur, sa façon de penser, et qui veulent se préparer pour un audit
- Les administrateurs système et réseau qui cherchent à mettre en place un contrôle solide de la gestion des modifications et des systèmes de détection pour l'entreprise

Vous apprendrez à...

- Comprendre les différents types de contrôles (par ex., techniques et non techniques) essentiels pour un audit réussi
- Effectuer une bonne évaluation du risque relatif aux réseaux pour identifier les vulnérabilités et déterminer les priorités en matière d'audit
- Établir des normes sécuritaires de référence pour les ordinateurs et les réseaux - le 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-feux pour valider le bon fonctionnement des paramètres / règles tels qu'ils ont été conçus, et pour bloquer le trafic,si besoin
- Utiliser des outils d'évaluation de vulnérabilité de façon efficace pour que les dirigeants aient en permanence des données indispensables aux mesures correctives et qu'ils puissent prendre des décisions informées concernant le risque et les ressources
- Contrôler la configuration, l'authentification, et la gestion des sessions d'applications web, afin d'identifier les vulnérabilités pouvant être exploitées par des assaillants

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

LEG 523

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

CINQ JOURS • ORDINATEUR PORTABLE NON REQUIS

Law of Data Security and Investigations

- Élaboration d'un contrat pour inviter des responsables d'incidents extérieurs – y compris les forces de l'ordre, des contractants, l'armée et n'importe quelle agence de défense partout dans le monde – afin d'apporter une assistance en cas de cyber crise
- Le nouveau Règlement général européen sur la protection des données et son impact dans le monde
- L'impact du gouvernement Trump et du Brexit sur la loi sur la sécurité des données et sur l'application de réglementations
- L'adoption par l'Europe du « Privacy Shield » qui remplace le « Privacy Safe Harbor » dans le domaine du transfert de données vers les États-Unis
- Les poursuites engagées par les assureurs contre les hôpitaux : refus de couverture après compromission de données et accord juridique de 4,1 millions de dollars avec les patients

Intégrer les nouvelles lois sur la confidentialité, la découverte électronique et la sécurité des données créent un besoin urgent de professionnels capables de combler le fossé entre le service juridique et le service informatique. SANS LEG523 fournit cette formation professionnelle unique, y compris les compétences dans l'analyse et l'utilisation des contrats, des politiques et des procédures de gestion des dossiers.

Ce cours couvre les lois des affaires, des contrats, de la fraude, de la criminalité, de la sécurité informatique, de la responsabilité et de la politique — le tout en mettant l'accent sur les enregistrements stockés et transmis électroniquement. Il enseigne également aux enquêteurs comment préparer des rapports crédibles et défendables, qu'il s'agisse de cybercriminalité, d'expertise numérique, de réponse aux incidents, de problèmes relevant des ressources humaines ou d'autres enquêtes.

Chaque journée de ce cours de cinq jours s'appuie sur les leçons des premiers jours afin de renforcer votre capacité à aider votre entreprise (secteur public ou privé) à faire face aux hackers, botnets, logiciels malveillants, phishing, vendeurs indisciplinés, fuites de données, espions industriels, employés malveillants ou peu coopératifs, ou 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 et la réponse aux risques et opportunités qui entourent la collecte d'intelligence provenant de sources en libre accès.

Au fil des ans, ce cours a adopté une perspective de plus en plus globale. Des professionnels non américains participent au cours LEG523 car il n'y a pas de formation similaire dans le monde. Une femme de loi travaillant dans l'administration fiscale nationale d'un pays africain a suivi ce cours car les déclarations électroniques, les preuves et les investigations numériques ont pris une place prépondérante dans l'exercice de ses fonctions. Des étudiants internationaux assistent l'instructeur Benjamin Wright, avocat américain, dans son travail de révision constante afin d'inclure toujours plus de contenus transnationaux.

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

Public visé :

- Enquêteurs
- Professionnels de la sécurité des systèmes d'information
- Avocats
- Juristes
- Auditeurs
- Comptables
- Gestionnaires de technologie
- Vendeurs
- Agents de conformité
- Forces de l'ordre
- Force de police
- Testeurs d'intrusion
- Responsables d'intervention et de réponse aux incidents de cybersécurité

Vous apprendrez à...

- Mieux travailler avec les autres professionnels dans votre organisation qui prennent les décisions concernant la loi en matière de sécurité des données et des enquêtes
- Exercer un meilleur jugement 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, y compris 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
- Faire un meilleur usage des techniques de contrats électroniques pour obtenir de meilleurs termes et conditions
- Exercer une pensée critique pour comprendre les implications pratiques des lois en matière de technologie et les normes de l'industrie (telles que les normes de sécurité des données de l'industrie des cartes de paiement)

SANS OnDemand

Les cours **SANS OnDemand** conviennent parfaitement aux stagiaires qui cherchent le contenu complet d'une formation SANS et la souplesse d'une formation sans nécessité de se déplacer ou de s'absenter du travail. Un contrôle complet sur le rythme d'apprentissage pour répondre à tous les styles d'apprentissage. Dispensés par les meilleurs formateurs SANS, nos formations OnDemand sont accessibles sur ordinateur fixe, portable, iPad et tablette, pour que vous puissiez apprendre chez vous ou n'importe où ailleurs.

Avec un choix de plus de 40 formations SANS, vous disposez de :

Quatre mois de contenu, disponible 24/7

Vous pourrez accéder au contenu de votre cours pendant toute la durée de votre formation, ce qui vous permet d'avancer à votre rythme et de contrôler aussi bien votre environnement que 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 de l'accès 24/7 au contenu du cours, vous pouvez également accéder à tous les cours magistraux, tous les exercices et tous les labos virtuels associés à chaque module. Grâce à la possibilité de revoir les sujets complexes et difficiles, vous disposerez de tous le temps dont vous avez besoin pour maîtriser le contenu et consolider ce que vous avez appris grâce à des exercices concrets et pratiques.

Spécialistes en la matière

Les SANS Subject-Matter Experts (SME), des spécialistes, sont disponibles à tout moment de votre formation pour répondre à vos questions et pour vous aider à maîtriser les thèmes les plus complexes. Disponibles via la fenêtre de discussion en ligne, nos SME sont là pour garantir votre réussite et vous aider à vous approprier le contenu.

Un ensemble complet de livres, de supports de cours et de rapports de progression

Vos cours contiennent tout ce dont vous avez besoin pour réussir votre formation. Des livrets de cours vous sont envoyés après inscription : les supports de cours, y compris des cours magistraux, des labos virtuels et des exercices pratiques, sont disponibles à tout moment et les rapports de progression vous aident à suivre votre évolution, à reprendre les points qui méritent de l'être et à planifier votre emploi du temps en conséquence.

Préparation GIAC

Les cours OnDemand constituent également une bonne méthode pour vous préparer à passer une certification GIAC. Grâce à un accès étendu au contenu de la formation, vous disposerez de tous le temps dont vous avez besoin pour réviser et maîtriser le cours... et aborder l'examen en toute sérénité.

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

DEV 522

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE

Defending Web Applications Security Essentials

Les défenseurs doivent apprendre à sécuriser les applications web en raison de l'importance croissante des données qui sont confiées à ces produits. Les défenses traditionnelles de réseau, telles que les pare-feux, sont impuissantes à protéger les applications web perito. Le cours DEV522 aborde les 10 premiers risques listés par l'OWASP pour aider les défenseurs à mieux comprendre les vulnérabilités des applications web, leur permettant ainsi de protéger correctement les actifs web de leur organisation.

Les discussions portent sur les stratégies de mitigation d'une infrastructure, d'une d'architecture, et les perspectives de codage, mais aussi sur de véritables applications web éprouvées. Le test de vulnérabilité est également abordé pour que les stagiaires puissent tester leurs propres applications par rapport aux vulnérabilités discutées en classe.

Pour optimiser les avantages pour un public élargi, les discussions se déroulent dans un langage de programmation accessible à tous. Le cours se concentre sur les stratégies de sécurité, plutôt que sur l'implémentation de niveau de codage.

Le cours DEV522: Defending Web Applications Security Essentials est conçu pour quiconque est chargé d'implémenter, de gérer et de protéger les applications web. Il est particulièrement adapté aux analystes de la sécurité des applications, aux développeurs, aux architectes d'applications, aux testeurs d'intrusion, aux auditeurs qui voudraient pouvoir faire des recommandations correctes en matière de mitigation pour les problèmes de sécurité web, aux professionnels de la sécurité des infrastructures qui ont un intérêt à mieux défendre leurs applications web.

Le cours aborde aussi d'autres problèmes, concernant les pratiques relatives au développement d'applications web, auxquels les auteurs sont confrontés quotidiennement et qu'ils jugent tout aussi importantes. Les sujets abordés incluent :

- La sécurité des infrastructures
- Les configurations de serveur
- Les mécanismes d'authentification
- La configuration du langage d'application
- Les erreurs de codage d'application, telles que les injections SQL et le script intersite
- La falsification des requêtes intersite
- Le contournement de l'authentification
- Les services web et les failles qui leur sont associées
- web 2.0 et son utilisation de services web
- Les langages et injections XPATH and XQUERY
- Les failles de la logique commerciale
- Les en-têtes protecteurs HTTP

Ce cours fait une utilisation massive d'exercices pratiques et se termine par un grand exercice défensif qui renforce les leçons apprises pendant la semaine.

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

Public visé :

- Développeurs d'application
- Analystes de la sécurité des applications web, ou responsables
- Architectes d'applications
- Les testeurs d'intrusion qui souhaitent en savoir plus sur les stratégies défensives
- Les professionnels de la sécurité qui souhaitent en savoir plus sur la sécurité des applications web
- Les auditeurs qui ont besoin de comprendre les mécanismes défensifs des applications web
- Le personnel d'organisations qualifiées PCI qui ont besoin de formation pour rester en conformité avec les exigences PCI

Vous apprendrez à...

- Comprendre les risques majeurs et les vulnérabilités les plus courantes concernant les applications web avec des exemples concrets tirés du monde réel
- Minimiser les vulnérabilités courantes des applications web en utilisant des techniques de codage correctes, des composants logiciels, des configurations et une architecture défensive
- Comprendre les meilleures pratiques dans de nombreux domaines de la sécurité des applications web, telles que l'authentification, le contrôle d'accès, et la validation de la saisie
- Satisfaire les exigences de formation requises par les normes de sécurité de l'industrie des cartes de paiement (PCI DSS 6.5)
- Déployer et consommer les services web (SOAP and REST) de façon sûre
- Déployer de façon proactive des mécanismes défensifs de pointe, tels que les en-têtes de réponses défensifs HTTP, et la politique de contenu sécurisé pour améliorer la sécurité des applications web
- Dérouler de façon stratégique un programme de sécurité web dans un vaste environnement
- Incorporer des technologies web avancées, telles que HTML5 et les requêtes cross-domain AJAX d'une façon sûre et sécurisée

GIAC
Le niveau de certification le plus élevé en matière de cybersécurité

Un ciblage spécialisé, adapté à un poste particulier

De nos jours les cyber attaques sont extrêmement sophistiquées et exploitent des failles spécifiques. Les certifications à spectre large et général ne suffisent plus. Les professionnels ont besoin de compétences spécifiques et de connaissances spécialisées essentielles pour répondre à des menaces multiples et variées. C'est la raison pour laquelle GIAC offre plus de 30 certifications, chacune d'elles étant centrée sur des compétences de travail spécifiques et nécessitant un savoir-faire unique et distinct.

Des connaissances approfondies du monde réel

La connaissance théorique est l'ultime risque en matière de sécurité. Des compétences approfondies du monde réel mises en pratique sont les seuls moyens fiables qui permettent de réduire les risques sécuritaires. Aucune certification n'arrive à la hauteur d'une certification GIAC pour garantir un niveau inégalé de maitrise des connaissances et des compétences requises dans le monde réel.

La certification dont le concept est réputé être le plus fiable

La conception d'un examen de certification impacte la qualité et l'intégrité de la certification. Le contenu et le format des questions de l'examen GIAC sont développés au cours d'un processus rigoureux mené par un personnel formé en psychologie et aux métriques, puis revus par des experts dans chaque domaine. Plus de 78 000 certifications ont été décernées depuis 1999. Les certifications GIAC répondent aux normes ANSI.

"I think the exam was both fair and practical. These are the kind of real-world problems I expect to see in the field."

– Carl Hallberg, Wells Fargo, GIAC Reverse Engineering Malware (GREM)

"GIAC made the testing process much better than other organizations. The material is spot on with what I do at work, daily."

Jason Pfister, EWEB,
GIAC Continuous Monitoring
(GMON)

GIAC
DEEPER KNOWLEDGE. ADVANCED SECURITY.
www.giac.org

ICS 410

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

CINQ JOURS • ORDINATEUR PORTABLE REQUIS

ICS/SCADA Security Essentials

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

Parmi les thèmes traités :

- Identifier les défauts de sécurité dans votre code
- Corriger les bogues de sécurité en utilisant des techniques de codage sécurisé Utiliser des en-têtes HTTP de protection pour prévenir les attaques
- Sécuriser vos services sensibles de Representational State Transfer (REST) Intégrer la sécurité dans vos processus de développement
- Utiliser les outils de sécurité disponibles gratuitement pour tester vos applications

> **"Every IT security professional and others within support and projects around ICS should take this course."**
>
> Simon Poole, *SHELL*

Concernant les risques les plus élevés et les besoins dans les secteurs dotés d'infrastructures critiques, les auteurs de ce cours se sont penchés attentivement sur les principes de sécurité essentiels aux diverses tâches qui relèvent du contrôle des systèmes.

En raison de la nature dynamique des systèmes de contrôle industriels, grand nombre d'ingénieurs n'ont pas une bonne compréhension des caractéristiques et des 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 opérationnelles 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 savoir maintenir ces systèmes pour qu'ils restent disponibles et intègres. Parallèlement, le cours répond au besoin d'aider les ingénieurs des systèmes de contrôle et les opérateurs à mieux comprendre le rôle important qu'ils jouent en matière de 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.

Lorsque les stagiaires quittent le cours, ils apprécient, comprennent et partagent un langage commun qui leur permettra de travailler ensemble pour sécuriser les environnements des systèmes de contrôle industriels. Le cours encourage le développement de pratiques d'ingénierie sensibilisées à 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.

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

Public visé :

Ce cours a été conçu pour toutes celles et ceux qui travaillent dans des environnements de systèmes de contrôles industriels, qui peuvent interagir avec ces environnements ou même les affecter. Sont également inclus les propriétaires ressources, les vendeurs, les personnes en charge d'intégration et toute autre tierce partie. Ces individus appartiennent principalement à quatre domaines :

- Personnel IT (y compris les services qui soutiennent la technologie opérationnelle)
- Personnel de la sécurité IT (y compris la sécurité de la technologie opérationnelle)
- Ingénieurs
- Tout personnel concerné par les 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 pour automatiser le fonctionnement de programmes afin d'effectuer une surveillance continue de divers outils
- Installer VMWare et créer des machines virtuelles pour fabriquer un laboratoire virtuel où les outils / sécurité des systèmes seront testés et validés
- Mieux comprendre divers systèmes de contrôle industriels, leur but, leur usage, leur fonction, et leur corrélation avec les IP de réseau, ainsi qu'avec les communications industrielles
- Travailler avec des systèmes d'exploitation (les concepts d'administration de systèmes Unix/Linux et/ou Windows)
- Travailler avec la conception des infrastructures de réseau (concept d'architecture de réseau, y compris la topologie, les protocoles, et les composants)
- Mieux comprendre le cycle de vie de la sécurité des systèmes

ICS 456

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

Essentials for NERC Critical Infrastructure Protection

Le cours Essentials for NERC Critical Infrastructure Protection est une formation de 5 jours qui permet d'étudier en détail les standards des versions 5/6. Ce cours traite du rôle de la FERC, de la NERC et des Entités régionales. Il aborde également l'identification et la catégorisation des Systèmes cyber BES sous différentes approches et il aide les propriétaires ressources 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 avec une approche professionnelle qui prend aussi bien en compte l'aspect cybersécurité que le respect des normes.

Nos 25 labos pratiques couvrent des aspects divers et variés, de la sécurisation des stations de travail à l'investigation numérique en passant par le lock-picking.

Le mot de l'auteur

Le cours SANS ICS456: NERC Critical Infrastructure Protection Essentials a été élaboré par des membres de l'équipe SANS ICS ayant une expérience approfondie de l'industrie de l'électricité, dont des anciens contacts primaires d'organismes enregistrés, un ancien responsable NERC et un coprésident de la NERC CIP Interpretation Drafting Team. Ensemble, les auteurs viennent transmettre l'expérience professionnelle qu'ils ont acquise en développant les programmes de conformité NERC CIP et NERC 693 et en participant activement aux processus de développement des standards.

Public visé :

- Architectes sécurité
- Ingénieurs réseaux
- Architectes réseaux
- Analystes sécurité
- Ingénieurs sécurité seniors
- Administrateurs systèmes
- Responsables sécurité techniques
- Analystes CND
- Spécialistes surveillance sécurité
- Enquêteurs cybermenace

Vous apprendrez à...

- Analyser une architecture sécurité à la recherche de défaillance
- Appliquer les principes appris en cours pour concevoir une architecture sécurité défendable
- Déterminer les besoins précis en surveillance sécurité pour des organisations de toutes tailles
- Tirer au maximum profit des investissements existant en architecture sécurité en reconfigurant les ressources existantes
- Déterminer les capacités requises pour supporter la surveillance continue des Contrôles critiques de sécurité clés
- Configurer un logging et un monitorage appropriés afin d'assister un Centre d'opérations de sécurité et un programme de surveillance continue

CERT. GIAC : GCIP
31 CRÉDITS CPE/CMU
WWW.GIAC.ORG/GICSP

ICS 515

TRAINING EVENTS | PRIVATE TRAINING

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

ICS Active Defense and Incident Response

Le cours ICS515 (Industrial Control Systems) apprend aux stagiaires à comprendre l'environnement de leurs systèmes de contrôle industriels en réseau. Ils apprennent à surveiller les menaces qui visent leurs infrastructures ICS, à gérer des incidents contre 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 industriels - des menaces, telles que Stuxnet, Havex, et BlackEnergy2.

Les stagiaires quittent ce cours avec la capacité de déconstruire des attaques ICS ciblées et de combattre ces adversaires. Ce cours utilise une approche pratique et utilise des malwares réels pour craquer les cyberattaques contre les infrastructures ICS. Les stagiaires acquièrent une compréhension technique et pratique pour optimiser les concepts de défense active. Ces derniers utilisent la « threat intelligence », la mise en place d'une surveillance 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.

Vous saurez :

- Mettre en place une gestion d'incident focalisée sur la sécurité des opérations qui hiérarchise la sécurité et la fiabilité des opérations
- Comment la "threat intelligence" ICS est générée et utiliser les ressources de la communauté pour soutenir les environnements ICS.
- Identifier les actifs ICS et les topologies de leur réseau, et surveiller les points sensibles des ICS pour détecter des anomalies et des menaces.
- Analyser les malwares qui visent les ICS et en extraire les informations qui vont permettre d'évaluer rapidement leur portée et de comprendre la nature de la menace.
- Gérer une attaque et obtenir les informations nécessaires pour instruire les équipes et les décideurs afin qu'ils sachent quand mettre les opérations à l'arrêt, ou quand il est possible de gérer la menace de façon sécurisée tout en poursuivant les opérations.
- Tirer parti de plusieurs disciplines de sécurité conjointement, pour optimiser la défense active et sauvegarder les ICS, en s'appuyant sur des exercices pratiques et des concepts techniques.

"This course is the missing piece to get companies to take threats seriously, pursue the truth, and share their findings."

Rob Cantu,
DOE

Public visé :

- Responsables et les membres d'équipes de réponse aux incidents ICS
- Personnel des services de sécurité OT et ICS
- Professionnels de la sécurité IT
- Membres d'équipes de la sécurité opérationnelle (SOC)
- Testeurs d'intrusion et les "Red Team" ICS
- Chargés de défense active

Vous apprendrez à...

- À mener une réponse aux incidents SCI en vous concentrant sur les opérations de sécurité et en dressant la liste des priorités relatives quant aux opérations de sécurité et de fiabilité
- Comment les renseignements sur les menaces SCI sont générés et comment utiliser les informations disponibles dans la communauté pour développer les environnements SCI. Les compétences d'analyse que vous développerez vous permettront d'analyser de manière critique les informations obtenues des rapports de renseignements sur les menaces SCI
- Comment identifier les ressources SCI et leurs topologies réseaux et comment surveiller les zones sensibles des SCI pour détecter les anomalies et les menaces. Vous vous familiariserez avec des méthodologies comme la surveillance de la sécurité des réseaux SCI et avec des approches visant à réduire le paysage des menaces qui pèsent sur les systèmes de contrôles
- Comment analyser des malwares SCI et comment extraire les informations critiques dont vous avez besoin pour mesurer rapidement l'étendue de l'environnement et comprendre la nature de la menace
- Comment faire face à une attaque et comment obtenir les informations dont vous avez besoin pour informer les équipes et les responsables soit lorsqu'il est nécessaire d'interrompre les opérations, soit lorsque les opérations peuvent continuer et qu'il est possible de répondre à la menace
- Comment utiliser différentes disciplines de la sécurité en les articulant de manière à déployer la meilleure des défenses actives et sauvegarder le SCI, le tout grâce à des labos pratiques et des concepts techniques

GIAC RESPONSE AND INDUSTRIAL DEFENSE — GRID

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

ICS 612

TRAINING EVENTS | PRIVATE TRAINING | ON-DEMAND

FORMATION PRATIQUE • CINQ JOURS • ORDINATEUR PORTABLE REQUIS

ICS Cybersecurity In-Depth | NOUVEAU

LES LOGICIELS MALVEILLANTS VISANT LES SYSTÈMES ICS, AINSI QUE LES ATTAQUES PERPÉTRÉES CONTRE LES INFRASTRUCTURES STRATÉGIQUES, AUGMENTENT AUSSI BIEN EN TERMES DE FRÉQUENCE QUE DE SOPHISTICATION. LA SÉCURISATION DE VOTRE ENVIRONNEMENT ICS PASSE PAR UNE IDENTIFICATION DES MENACES, VULNÉRABILITÉS ET MÉTHODES DE DÉFENSE APPROPRIÉES. NOS FORMATIONS SONT LÀ POUR VOUS Y AIDER.!

Le cours ICS612 : vous aidera à :

- *Apprendre des méthodes actives et passives permettant de recueillir en toute sécurité des informations concernant un environnement ICS*
- *Identifier les vulnérabilités au sein des environnements ICS*
- *Identifier la manière dont les attaquants interrompent et prennent le contrôle des processus avec une intention malveillante, ainsi que les moyens d'y faire face*
- *Mettre en œuvre des mesures proactives pour prévenir, détecter, ralentir ou stopper les attaques*
- *Comprendre les opérations ICS et les attributs caractéristiques d'une opération « normale »*
- *Créer des points d'étranglement dans une architecture et apprendre à les exploiter pour détecter et contrer les incidents de sécurité*
- *Gérer des environnements ICS complexes et développer des capacités de détection et de réaction face aux événements de sécurité*

Les concepts du cours et les objectifs d'apprentissage reposent principalement sur des exercices pratiques en labo. La configuration en salle de classe vise à reproduire un environnement réel dans lequel un contrôleur surveille et gère des dispositifs déployés sur le terrain, avec l'assistance d'une interface homme-machine (IHM) à écran tactile également présente sur site, qui est mise à la disposition du personnel local pour apporter aux processus les modifications nécessaires. Grâce à des postes de travail situés dans un centre de commande à distance, les opérateurs surveillent et contrôlent les équipements de terrain au moyen d'un système SCADA. La configuration de la salle de classe, qui vise à recréer un environnement ICS réel, inclut une connexion à l'entreprise permettant le transfert de données (de type Historian), l'accès à distance et d'autres fonctions internes caractéristiques.
Les labos mettent les stagiaires aux prises avec une diversité de situations expérimentales au cours desquelles un attaquant infiltre un système ICS architecturé de façon défaillante (ce qui, malheureusement, est souvent le cas), en enseignant aux défenseurs les moyens de sécuriser et gérer l'environnement.

" Truly understanding the devices we are charged with defending is imperative to effectively implementing security measures."
Crystal B.,
U.S. ARMY

Public visé :

- *Les anciens stagiaires du cours ICS410 ayant achevé avec succès la formation ICS410 : ICS/SCADA Security Essentials possèdent les connaissances de base considérées comme une condition préalable à ce cours Process control engineers*
- *Ingénieurs en contrôle des processus*
- *Ingénieurs de systèmes ou de sécurité des systèmes*
- *Défenseurs actifs d'environnements ICS*
- *Toute personne possédant une expérience significative des systèmes de contrôle et souhaitant comprendre les processus et méthodes de sécurisation de l'environnement ICS*

Vous apprendrez á :

- *Acquisition d'une expérience pratique au moyen de ressources typiques d'un environnement industriel, telles qu'un contrôleur logique programmable (PLC), des interfaces opérateur (OI) pour le contrôle local, des serveurs d'interface homme-machine (IHM), un serveur Historian, ainsi que des commutateurs, routeurs et dispositifs pare-feu*
- *Meilleure compréhension de l'exécution des contrôleurs PLC par le biais d'exercices pratiques*
- *Identification des méthodes de sécurité applicables aux systèmes de contrôle et d'entrée/sortie en temps réel*
- *Connaissance des avantages et inconvénients présentés par les diverses architectures PLC/IHM et recommandations visant à améliorer les postures de sécurité sur ces systèmes de contrôle en temps réel*
- *Localisation des ressources essentielles au sein d'un environnement industriel.*
- *Approche du rôle des services de réseau informatique au sein d'un système ICS et identification des méthodes de sécurité applicables*

30 CRÉDITS CPE/CMU

SANS EMEA

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 qui leur permet de sélectionner et suivre la formation dont ils ont besoin quand ils en ont besoin
- approuver et gérer facilement les inscriptions
- suivre les employés dans leur progression ainsi que leurs notes afin de garantir un résultat satisfaisant
- vérifier les investissements, les débits et les soldes de comptes pour élaborer un budget optimal

Les fonds Voucher peuvent être utilisés quelle que soit la formation SANS suivie (aussi bien en classe et qu'en ligne), mais aussi pour tous les événements SANS Summit, les certifications GIAC, ou les renouvellements de la certification.* Les fonds Voucher doivent être utilisés dans les 12 mois, avec la possibilité d'étendre cette durée grâce à des investissements supplémentaires.

Se lancer

Rendez-vous sur www.sans.org/vouchers et remplissez le formulaire de contact pour être mis en relation avec un représentant de SANS par message électronique ou par téléphone au cours des 24 heures ouvrables qui suivent. Le personnel concerné et éligible pourra alors commencer sa formation dans la semaine qui suit.

*Sont actuellement exclus du programme SANS Voucher : le programme Partnership, la formation Security Awareness et les ateliers SANS workshop tenus lors d'événements organisés par d'autres organisations.

www.sans.org/vouchers

SANS Cyber Defence formations de 2 jours

FORMATION PRATIQUE

SEC440: Critical Security Controls: Planning, Implementing, and Auditing

TRAINING EVENTS
PRIVATE TRAINING
ON-DEMAND

Ce cours vous aide à maîtriser les techniques et outils spécifiques et éprouvés par la pratique 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, dont vous retrouverez la liste ci-dessous, font de plus en plus l'objet d'un consensus général et constituent la première des listes des priorités à contrôler avant tout le reste pour toute organisation dont les activités revêtent un caractère sensible.

Ces contrôles ont été sélectionnés et définis par l'armée américaine, par d'autres gouvernements et par des organisations privées (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 défini ces contrôles de manière collégiale pour en faire la meilleure défense possible contre les attaques connues et le meilleur moyen de parer et d'atténuer les dommages causés par les attaques réussies. Pour les professionnels de la sécurité, ce cours permet de voir comment mettre en place ces contrôles dans un réseau existant grâce à une utilisation efficace et étendue de l'automatisation. Pour les chargés d'audit, les CIO 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. SEC 440 ne contient aucun labo. Si les stagiaires cherchent un cours sur les Critical Controls avec des labos pratiques, il leur est conseillé de s'orienter vers SEC566.

Un des principaux avantages de ce cours réside dans sa manière d'exploiter l'aspect offensif pour développer l'aspect défensif. En d'autres termes, vous disséquerez les attaques actuelles que vous aurez à bloquer ou à atténuer. L'idée étant de donner un caractère concret à vos défenses pour faire de vous un meilleur professionnel de la sécurité.

> **"Great teacher; very knowledgeable, passionate, entertaining, and informative"**
> Mike Mayers
> *RIM*

FORMATION PRATIQUE

SEC455: SIEM Design & Implementation

TRAINING EVENTS
PRIVATE TRAINING
ON-DEMAND

Security Information and Event Management (Information de sécurité et gestion des incidents, SIEM) peut se révéler être un atout extraordinaire pour la sécurité d'une organisation, mais comprendre et conserver cet atout s'avère parfois difficile. 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'utilisation de services professionnels peut laisser aux équipes de sécurité l'impression de ne pas parfaitement comprendre le fonctionnement de leur SIEM, ni de ne pas en avoir un parfait 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 facilitent 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, mais encore faut-il qu'il soit exploité à son plein potentiel. Ce cours a été 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 simple et à maintenir.

> **"The course is amazing. You get to build a SIEM from the ground up which helps you understand a lot more about what SIEM does in the background."**
> Billy Davis
> *AWS*

SEC402: Cybersecurity Writing: Hack the Reader

TRAINING EVENTS
ON-DEMAND

Want to write better? Learn to hack the reader! Discover how to find an opening, break down your readers' defenses, and capture their attention to deliver your message—even if they're too busy or indifferent to others' writing. This unique course, built exclusively for cybersecurity professionals, will strengthen your writing skills and boost your security career. You will:

- *Uncover the five "golden elements" of effective reports, briefings, emails, and other cybersecurity writing.*
- *Make these elements part of your arsenal through hands-on exercises that draw upon common security scenarios.*
- *Learn the key topics you need to address in security reports and other written communications.*
- *Understand how to pick the best words, structure, look, and tone.*
- *Begin improving your skills at once by spotting and fixing weaknesses in security samples.*
- *Receive practical checklists to ensure you'll write clearly and effectively right away.*

SEC546: IPv6 Essentials

TRAINING EVENTS

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

Penetration Testing formations de 2 jours

FORMATION PRATIQUE

SEC564: Red Team Operations and Threat Emulation

TRAINING EVENTS
PRIVATE TRAINING
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 utilisées pour protéger les environnements. Utilisant les fondamentaux du test de pénétration, la Red Team déploie une approche globale pour obtenir des informations sur la sécurité générale d'une organisation de façon à tester sa capacité à détecter une attaque, à y répondre et à s'en relever. Lorsqu'elles sont correctement conduites, les activités d'une Red Team améliorent de manière significative les contrôles de sécurité d'une organisation, peaufinent ses capacités défensives et mesurent l'efficacité de ses opérations de sécurité.

Le concept de Red Team nécessite une approche différente des tests de sécurité classiques et repose fortement sur des TTP bien définies, sans lesquelles il est impossible d'obtenir une simulation réaliste de menaces ou d'adversaires concrets. Les résultats produits par une Red Team dépassent la liste classique des vulnérabilités détectées au cours d'un test de pénétration, procurent une compréhension plus approfondie de la réaction potentielle d'une organisation contre une menace actuelle et identifient les forces et les faiblesses de sécurité.

Si vous occupez un rôle défensif ou offensif dans la sécurité, comprendre l'intérêt d'une Red Team et les améliorations qu'elle peut apporter à la sécurité s'avérera particulièrement intéressant pour vous. Les organisations consacrent beaucoup de temps et d'argent à la sécurité de leurs systèmes, et il est indispensable pour elles 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, en définir les engagements et en comprendre le rôle et l'importance en matière de test de sécurité. Ce cours de deux jours aborde 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.

> **" The content from SEC564 is great and I will be able to implement it in my organization right away!"**
> Kirk Hayes
> *Rapid 7*

FORMATION PRATIQUE

SEC580: Metasploit Kung Fu for Enterprise Pen Testing

TRAINING EVENTS
PRIVATE TRAINING
ON-DEMAND

Nombre d'entreprises doivent aujourd'hui gérer les normes légales et sectorielles qui régissent le test de pénétration et les évaluations de vulnérabilité. Les outils et services commerciaux permettant de réaliser ces tests peuvent s'avérer onéreux. S'il existe des outils gratuits comme Metasploit qui font très bien le travail, peu de testeurs en comprennent toutes les fonctionnalités et savent comment les appliquer dans une méthodologie de test professionnelle.

Metasploit a été conçu pour aider les testeurs à confirmer des vulnérabilités en utilisant un cadre de travail open source et simple d'utilisation.

Ce cours aidera les étudiants à tirer le plein potentiel de cet outil gratuit et leur montrera comment appliquer les incroyables capacités du cadre de travail de Metasploit dans un protocole complet de test de pénétration et d'évaluation des vulnérabilités grâce à une méthodologie précise. Les étudiants qui suivent ce cours disposent en sortie d'une solide compréhension de Metasploit et de l'intérêt que présente son intégration dans leurs activités quotidiennes de test de pénétration et d'évaluation. Ce cours vous procurera une compréhension approfondie du cadre de travail de Metasploit qui dépasse de loin la simple présentation de l'exploitation d'un système à distance.

Les étudiants découvriront l'exploitation, la reconnaissance post exploitation, la manipulation de token, les attaques par hameçonnage 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 le cadre de travail de Metasploit, ainsi que la manière de les éviter et de les contourner, pour des tests plus sûrs et plus efficaces.

> **"SEC580 is a great course – right audience size, right pace, good labs, and excellent instruction."**
> Robert Lockwood
> *Fusion Cell Consulting*

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

SEC699: Purple Team Tactics Adversary Emulation for BreachPrevention &Detection | VERSION BÊTA

TRAINING EVENTS

Le cours SEC699 de SANS, spécialement conçu pour les équipes Purple Team de haut niveau, s'articule autour de l'émulation d'adversaires dans le cadre de la prévention et de la détection du vol de données. Tout au long de ce cours, les stagiaires apprendront à émuler les auteurs de menaces réelles dans un environnement d'entreprise réaliste. S'inscrivant dans le plus pur esprit "purple", ce cours a pour but d'enseigner aux stagiaires la manière dont des techniques contradictoires peuvent être imitées et détectées..

Cours de formation par équipe

FORMATION PRATIQUE • SIX JOURS • ORDINATEUR PORTABLE REQUIS

TBT570: Team-Based Training – Blue Team & Red Team Dynamic Workshop

TRAINING EVENTS
PRIVATE TRAINING
ON-DEMAND

Dire que la composition d'une équipe de sécurité puissante relève parfois du défi est un pur euphémisme. C'est précisément la raison pour laquelle SANS a introduit la formation par équipe TBT570, un cours unique durant lequel des équipes de trois à cinq stagiaires travaillent ensemble en mode Blue Team pour combattre un adversaire en temps réel. Cette formation est conçue pour permettre aux stagiaires d'acquérir des compétences en équipe, des capacités de leadership, des techniques de communication et une expertise technique, tout en étant exposés à des salves de scénarios de plus en plus complexes à résoudre.

Durant cet exercice réparti sur six journées, les stagiaires recevront un enseignement dispensé par les meilleurs instructeurs praticiens de SANS. Ils bénéficieront en outre d'un exposé des mesures prises par d'autres organisations de grand renom, ainsi que du mode de collaboration déployé par celles-ci pour protéger leur activité.

Secure DevOps formations de 2 jours

FORMATION PRATIQUE • DEUX JOURS • ORDINATEUR PORTABLE REQUIS

SEC534: Secure DevOps: A Practical Introduction

TRAINING EVENTS
PRIVATE TRAINING
ON-DEMAND

Ce cours aborde les fondamentaux de DevOps et la manière dont les équipes DevOps peuvent concevoir et livrer des logiciels sécurisés. Vous apprendrez les principes et les pratiques DevOps ainsi que les outils associés et comment les exploiter au mieux pour améliorer la fiabilité, l'intégrité et la sécurité des systèmes. Vous vous construirez une expérience pratique en utilisant des outils open-source populaires comme Puppet, Jenkins, GitLab, Vault, Grafana, et Docker pour automatiser la Gestion de la configuration (« infrastructure comme code »), l'Intégration continue (IC), la Livraison continue (LC), la compartimentation, la micro-segmentation et la conformité automatisée (« conformité comme code ») et la Surveillance continue. En exploitant les chaînes de compilation Secure DevOps, les étudiants mèneront une série de labos de sécurisation de projet CI/CD, avec toute une variété d'outils, de protocoles et de techniques de sécurité.

Management formations de 2 jours

FORMATION PRATIQUE • ORDINATEUR PORTABLE REQUIS

MGT415: A Practical Introduction to Cyber Security Risk Management

TRAINING EVENTS
PRIVATE TRAINING
ON-DEMAND

Pendant ce cours, les stagiaires développent les compétences pratiques dont ils ont besoin pour mener à bien des évaluations de risque régulières pour le compte de leurs organisations. 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, trop de vulnérabilités potentielles et pas assez de ressources. Les organisations doivent donc prioriser, de manière organisée ou non, les décisions à prendre pour défendre au mieux leurs données et leurs biens. La gestion de risque se doit d'être un outil fondamental qui facilite les stratégies de défense réfléchies et ciblées.

MGT433: Securing The Human: How to build, maintain, and measure a high-impact awareness programme

TRAINING EVENTS
PRIVATE TRAINING
ON-DEMAND

Les organisations investissent des quantités astronomiques d'argent et de ressources 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. La manière la plus efficace de sécuriser le facteur humain consiste à établir un programme de sensibilisation à la sécurité ayant un fort impact, ce programme visant à changer les comportements plutôt que la conformité.

MGT433 est un cours intensif de deux jours qui aborde les concepts et compétences clés nécessaires pour construire, maintenir et mesurer un programme de sensibilisation à la sécurité. L'intégralité du contenu du cours repose sur les enseignements tirés de centaines de programmes de sensibilisation à la sécurité dans le monde entier.

Les stagiaires apprennent auprès de leur formateur SANS et au travers d'interactions étendues avec leurs pairs. De fait, les candidats doivent donc apporter des exemples issus de leur propre programme de sensibilisation à la sécurité.

Pour finir, une série de labos et d'exercices amène les stagiaires à développer un plan personnalisé de sensibilisation à la sécurité pouvant être mis en œuvre dès leur retour auprès de leur organisation.

> **"Good course whether you are developing training and awareness or improving your current system."**
> Tina Baker
> *AWE PLC*

MGT521: Driving Cybersecurity Change – Establishing a Culture of Protect, Detect and Respond | BETA

Cybersecurity is no longer just about technology it is ultimately about organizational change. Change in not only how people think about security but what they prioritize and how they act, from the Board of Directors on down. Organizational change is a field of management study that enables organizations to analyze, plan, and then improve their operations and structures by focusing on people and culture. SANS course MGT521 will teach leaders how to leverage the principles of organizational change, enabling them to develop, maintain and measure a security-driven culture. Through hands-on, real-world instruction and a series of interactive labs and exercises in which you will apply the concepts of organizational change to a variety of different security initiatives, you will quickly learn how to embed cybersecurity into your organizational culture.

SANS EMEA

Créez un **compte SANS** dès aujourd'hui sur **www.sans.org/account** pour profiter des ressources gratuites suivantes

Newsletters

NewsBites

Synthèse bi-hebdomadaire et de haut-vol de l'actualité pour les professionnels de la cybersécurité.

OUCH !

La lettre d'information mensuelle et gratuite, à la pointe de la cybersécurité et à destination de tous ceux qui utilisent un ordinateur.

Webcasts

Ask the Experts Webcasts

Les experts de SANS apportent des informations récentes et précises sur des sujets actuels dans le domaine de la Sécurité informatique.

Analyst Webcasts

Suivi du SANS Analyst Program, les Analyst Webcasts apportent des informations cruciales issues de nos livres blancs et de sondages.

Autres ressources gratuites

(Aucun compte portail requis)

- InfoSec Reading Room
- Top 25 des erreurs logicielles
- 20 Critical Controls
- Règles de sécurité
- Détection d'intrusion : FAQ
- Astuce du jour

@RISK: The Consensus Security Alert

Un résumé hebdomadaire fiable qui aborde
(1) les vecteurs d'attaque nouvellement découverts,
(2) les vulnérabilités avec exploits nouvellement actifs,
(3) le déroulement des attaques récentes, et
(4) d'autres informations récentes et importantes.

WhatWorks Webcasts

Les webcasts SANS WhatWork mettent en lumière des expériences client riches d'enseignement : comment des utilisateurs finaux ont résolu des problèmes spécifiques de sécurité informatique.

Tool Talks

Les Tool Talks ont été conçus pour vous décrire un problème et vous faire découvrir des outils commerciaux à même de résoudre ou limiter ce problème.

- Poster de sécurité
- Leaders d'opinion
- 20 carrières qui font rêver
- Glossaire sécurité
- SCORE
  (Security Consensus Operational Readiness Evaluation)

Suivez-nous sur les réseaux sociaux pour rester au courant des derniers développements et annonces dans le monde de la cybersécurité autour des événements SANS EMEA.

SANS EMEA

The World's Largest and Most Trusted Cyber Security Training and Certification Provider

SANS Training Events France 2020

SANS LILLE SEC401 2020
16-21 MARCH
IN FRENCH

SANS LYON SEC560 2020
23-28 MARCH
IN FRENCH

SANS NANTES SEC504 2020
16-21 MARCH
IN FRENCH

SANS RENNES SEC660 & FOR610 2020
5-10 OCT
IN FRENCH

SANS PARIS MARCH 2020
9 - 14 MARCH
IN ENGLISH

SANS PARIS NOVEMBER 2020
2 - 7 NOV
IN ENGLISH

SANS PARIS JUNE 2020
8 - 13 JUNE
IN ENGLISH

SANS PARIS DECEMBER 2020
7 - 12 DEC
IN ENGLISH

SANS PARIS SEPTEMBER 2020
21 - 26 SEPT
IN ENGLISH

To book your place, visit **www.sans.org/emea**

+44 203 384 3470 www.sans.org/emea emea@sans.org @sansemea

SANS EMEA

LEVEL UP

DÉVELOPPEZ VOS COMPÉTENCES ET PASSEZ AU NIVEAU SUIVANT

PASSER LE TEST SUR

SANS.ORG/LEVEL-UP

Pour les nouvelles, les défis et les mises à jour du roadshow, suivez @SANSEMEA, #LevelUp