SANS EMEA

FORMATIONS

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

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

www.sans.org
@SANSEMEA

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 140 000 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.

À travers leurs compétences, les formateurs SANS sont également des enseignants hors norme. Passionnés par leur science, ils animent les formations SANS avec dynamisme et efficacité.

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, l'ICS, 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 cœur de tout ce que nous entreprenons. Les étudiants seront en mesure de mettre en œuvre les nouvelles compétences qu'ils ont acquises, dès leur retour au bureau.

LA COMMUNAUTÉ MONDIALE

SANS Institute est un membre éminent de la communauté mondiale de la cybersécurité. Nous exploitons l'Internet Storm Centre - un système d'alerte précoce pour 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.

SANS OFFRE LE MEILLEUR EN MATIÈRE DE FORMATION ET C'EST UN INVESTISSEMENT SÛR

La formation « en immersion » SANS est intensive et pratique, et nos supports pédagogiques sont sans équivalent dans l'industrie.

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.

FORMALITÉS D'INSCRIPTION

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 et espagnol. Voir pour nos options de formation page 6, ou rendez-vous sur www.sans.org/emea.

SANS: Fournisseur de cybersécurité pour HM Government

WWW.SANS.ORG
Contacter SANS
Courriel: emea@sans.org
Tel: +44 20 33 84 34 70
Addresse: SANS EMEA, PO Box 124, Swansea, SA3 9BB, GB

UN MOT DE LA PART DE SANS

En raison de la demande croissante de formation dans le domaine de la cybersécurité, nous envisageons une forte augmentation des évènements de formation SANS qui seront organisés dans toute l'Europe et au Moyen-Orient. Nous prévoyons également plus de formations dispensées en allemand, français et espagnol. Parallèlement à notre présence établie en Europe, nous sommes fiers d'annoncer que nous allons désormais proposer des évènements à grande échelle à Zurich, Paris et Madrid.

Dans la continuité de nos efforts pour dispenser des formations dans d'autres langues, notre programme de sensibilisation à la sécurité, Securing the Human, vient d'être remanié ; une nouvelle plateforme de formation propose désormais des modules vidéo disponibles en 19 langues. L'équipe SANS qui se consacre à ce programme de sensibilisation peut vous conseiller et vous fournir une démonstration gratuite si ce sujet est d'actualité pour votre organisation.

Les gouvernements de la France et du Royaume-Uni accordent une haute priorité à la cybersécurité et se sont récemment engagés à augmenter leur budget pour prendre les dispositions nécessaires à la lutte contre le cybercrime. SANS soutient ces initiatives de grande envergure et a déjà commencé au Royaume-Uni en implémentant la Cyber Academy dans le cadre de la stratégie du gouvernement britannique, en partenariat avec HM Government. Nos Cyber Académies ont démontré dans le passé que, grâce à un enseignement intensif de haute qualité, il est possible de former des personnes même lorsqu'elles ont peu d'expérience et d'en faire des professionnels de pointe, certifiés dans le domaine de la cybersécurité, qui peuvent être affectés à des postes clés. Je m'attends à ce que cette approche soit adoptée par d'autres états pour combler le manque de personnel compétent dans ce domaine, et je suis déjà engagé dans des pourparlers à ce sujet avec les dirigeants d'État et d'entreprises privées.

C'est pour moi un immense plaisir de rencontrer autant de professionnels passionnés par leur métier et dédiés à leurs tâches. Je me réjouis de faire votre connaissance prochainement, à l'occasion de l'un de nos évènements de formation.

Jan-Pieter Spaans
MANAGING DIRECTOR, MAINLAND EUROPE, SANS INSTITUTE

CONTACTS SANS EMEA

MIDDLE EAST

NED BALTAGI
Managing Director,
ME & GCC regions
nbaltagi@sans.org

UK & NORDICS

STEPHEN M JONES
Managing Director,
UK & Nordics
sjones@sans.org

MAINLAND EUROPE

JAN-PIETER SPAANS
Managing Director,
Mainland Europe
jspaans@sans.org

Ou vous pouvez contacter l'équipe EMEA par courriel à emea@sans.org ou par tél. au +44 (0) 20 33 84 34 70

« GIAC is the only certification that proves you have hands-on technical skills. »

Christina Ford, Department of Commerce

Comment Protégez-vous vos

- DONNÉES ?
- RÉSEAUX ?
- SYSTÈMES ?
- INFRASTRUCTURES ESSENTIELLES ?

La gestion du risque est une priorité absolue. La sécurité des actifs repose sur les compétences et les connaissances de votre équipe de sécurité. Ne prenez pas de risques avec une certification générale.

GIAC teste et valide la capacité des professionnels dans les domaines de la sécurité des systèmes d'information, de l'inforensique, et de la sécurité des logiciels.

La certification GIAC atteste que les titulaires possèdent les compétences requises en matière de cybersécurité pour protéger les infrastructures informatiques critiques. Les professionnels certifiés sont recherchés dans le monde entier par les gouvernements, les institutions militaires et l'industrie.

GIAC propose plus de 30 certifications spécialisées dans la sécurité, l'inforensique, les tests d'intrusion, la sécurité des applications web, l'audit informatique, la gestion et le droit de la sécurité informatique.

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

OBTENEZ VOTRE CERTIFICATION!
RENDEZ-VOUS SUR
WWW.GIAC.ORG

CONTENU

LISTE DES COURS

CYBER DÉFENSE - FONDAMENTAUX / SÉCURITÉ RÉSEAUX & OPÉRATIONS

SEC301 Intro to Information Security ... 22
SEC401 Security Essentials: Bootcamp Style ... 23
SEC501 Advanced Security Essentials Enterprise Defender ... 24
SEC503 Intrusion Detection In-Depth ... 25
SEC505 Securing Windows with PowerShell and the Critical Security Controls ... 26
SEC506 Securing Linux/Unix ... 27
SEC511 Continuous Monitoring and Security Operations ... 28
SEC550 Active Defence, Offensive Countermeasures, and Cyber Deception ... 30
SEC579 Virtualisation and Private Cloud Security ... 31

TESTS D'INTRUSION

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling ... 32
SEC542 Web App Penetration Testing and Ethical Hacking ... 33
SEC560 Network Penetration Testing and Ethical Hacking ... 34
SEC561 Immersive Hands-On Hacking Techniques ... 35
SEC562 CyberCity Hands-On Kinetic Cyber Range Exercise ... 36
SEC567 Social Engineering for Penetration Testers ... 37
SEC573 Python for Penetration Testers ... 38
SEC575 Mobile Device Security and Ethical Hacking ... 39
SEC580 Metasploit Kung Fu for Enterprise Pen Testing ... 40
SEC617 Wireless Ethical Hacking, Penetration Testing, and Defences ... 41
SEC642 Advanced web App Penetration Testing and Ethical Hacking ... 42
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking ... 43
SEC760 Advanced Exploit Development for Penetration Testers ... 44

INFORENSIQUE & RÉPONSES AUX INCIDENTS

FOR500 Windows Forensic Analysis ... 45
FOR508 Advanced Digital Forensics and Incident Response ... 46
FOR518 Mac Forensic Analysis ... 47
FOR526 Memory Forensics In-Depth ... 48
FOR572 Advanced Network Forensics and Analysis ... 49
FOR578 Cyber Threat Intelligence ... 50
FOR585 Advanced Smartphone Forensics ... 51
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques ... 52

AUDIT

SEC440 Critical Security Controls: Planning Implementing and Auditing ... 53
AUD507 Auditing & Monitoring Networks, Perimeters and Systems ... 54
SEC566 Implementing and Auditing the Critical Security Controls – In-Depth ... 55

SYSTÈMES DE CONTRÔLES INDUSTRIELS

ICS410 ICS/SCADA Security Essentials ... 56
ICS515 ICS défense active and Incident Response ... 57

MANAGEMENT

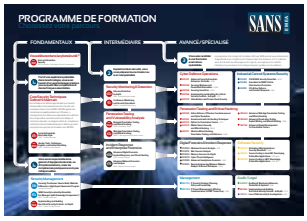
MGT414 SANS Training Program for CISSP® Certification: ... 58
MGT433 Securing The Human:
How to Build, Maintain and Measure a High-Impact Awareness Programme ... 60
MGT512 SANS Security Leadership Essentials
For Managers with Knowledge Compression™ ... 61

DÉVELOPPEUR

DEV522 Defending web Applications Security Essentials ... 62
DEV544 Secure Coding in .NET: Developing Defensible Applications ... 63

À propos de SANS ... 2
Un mot de la part de SANS ... 3
GIAC ... 4
Contenu ... 5
Options de formation SANS ... 6-7
Partenariats et solutions ... 8-9
Les formateurs SANS ... 10-13
SANS Career Roadmap ... 14-15
Programmes SANS ... 16-21
Détail des cours ... 22-63
Le Compte Portal SANS ... 29
Netwars ... 59

p14



SANS CAREER ROADMAP

ENVISAGEZ-VOUS UNE AUTRE FORMATION SANS OU UNE ÉVOLUTION / CHANGEMENT DE CARRIÈRE ? CONSULTEZ NOS PLANS DE CARRIÈRE PAGE 14.

p16

ÊTES-VOUS INSCRIT À VOTRE PREMIER STAGE DE FORMATION SANS ? CONSULTEZ NOS GUIDES DE FORMATION PAGE (16), PUIS LA DESCRIPTION DES COURS À PARTIR DE LA PAGE (22)

WWW.SANS.ORG
Contacter SANS
Courriel: emea@sans.org
Tel: +44 20 33 84 34 70
Addresse: SANS EMEA, PO Box 124, Swansea, SA3 9BB, GB

SANS TRAINING FORMATS

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 rencontrer des collègues, les formateurs et d'autres représentants de 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.

SECURITY AWARENESS TRAINING

SANS Securing the Human est une formation de sensibilisation à la sécurité de l'information, dispensée sur ordinateur et adaptée aux utilisateurs finaux, aux ingénieurs et aux développeurs ICS ; 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. STH va au-delà des questions de conformité et s'attache à changer le comportement.

www.securingthehuman.org

SANS MENTOR

Une formation dispensée par les meilleurs des postulants à la certification GIAC, dans une salle de cours, durant plusieurs semaines.

Vous étudiez à votre rythme, en vous appuyant sur des supports pédagogiques SANS et vous rencontrez votre mentor chaque semaine dans une de salle de cours.

www.sans.org/mentor

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 évènements de formations 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.

FONDÉ EN 1989, SANS EST LA RÉFÉRENCE MONDIALE EN MATIÈRE DE FORMATION POUR LA CYBERSÉCURITÉ

Les normes élevées adoptées par SANS restent constantes, quel que soit le format de la formation, et toutes nos classes adhèrent à la promesse SANS - notre engagement de vous enseigner des compétences et des techniques qui peuvent être mises en application dès votre retour au bureau.

SANS PRIVATE TRAINING

Une formation privée 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 privée permet à l'instructeur 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: emeasans.org

BESPOKE TRAINING SOLUTIONS AND CYBER ACADEMY

SANS crée des programmes de formation sur mesure pour répondre aux besoins spécifiques d'une organisation. Le contenu de la formation est sélectionné dans la liste des cours SANS et le programme inclut généralement une phase 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.

Pour en savoir plus sur les partenariats et solutions SANS, rendez-vous page 8 ou contactez-nous par courriel : emea@sans.org

SANS RESIDENCY

Un programme de formation adapté aux organisations qui auraient besoin de former toute une équipe sur une succession de cours, ou de former de nouvelles recrues.

Contactez SANS pour plus d'information : emeasans.org

SANS ONDEMAND

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

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 ».

Pour un premier entretien avec l'un des directeurs de SANS Institute, contactez-nous sur emea@sans.org ou au +44 203 384 3470

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 (voir pages 16-21,) et les offres complémentaires de SANS.

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

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

« NOUS SOMMES EN PARTICULIER À MÊME DE CONSEILLER EN MATIÈRE DE FORMATION, 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.

PROGRAMME SANS RESIDENCY

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. ●

NOS FORMATEURS SANS

Les formateurs SANS sont considérés comme la référence dans le monde.

La réputation d'excellence des formations en cybersécurité SANS est due en partie au fait que les formateur SANS sont les meilleurs dans leurs domaines respectifs.

Quelle que soit leur sphère professionnelle - que ce soit la défense, la gestion, DFIR, l'ICS, l'audit, les tests d'intrusion ou le développement de logiciels - nous pensons que les formateurs SANS sont inégalés.

Nos formateurs sont des professionnels experts du monde réel qui assument des rôles de sécurité influents au sein d'organisations importantes à travers le monde.

Les formateurs SANS sont des professionnels actifs de la cybersécurité, impliqués au quotidien et au cœur de l'action. Ils connaissent bien les dernières menaces, car leur travail consiste à y faire face au quotiden.

Armés de leurs compétences techniques et professionnelles, les formateurs SANS sont des enseignants plus que qualifiés. Ils savent comment animer leurs sujets et ce sont surtout d'excellents communicants.

Ils le doivent en partie au processus de sélection et de formation rigoureux auxquels sont soumis les formateurs SANS avant d'être accrédités et habilités à enseigner - ce processus peut s'étendre sur plusieurs années.

Nous vous présentons ici quelques-uns des formateurs SANS qui enseigneront dans la région EMEA dans les prochains mois.

www.sans.org/emea

Mouad Abouhali
INSTRUCTOR

Mouad Abouhli est actuellement chercheur dans la sécurité de l'information, testeur d'intrusion et analyste de malware chez Airbus France (Airbus Innovations Group). Il a la responsabilité des tests d'intrusion, de l'évaluation du niveau de sécurité pour l'infrastructure de réseau, des logiciels et des produits IT. Il s'occupe également de l'analyse de malwares pour Airbus CERT. Il porte un intérêt particulier à la rétro-ingénierie, la recherche de vulnérabilités et les tests d'intrusion. Il est certifié GCIH, GREM and CISSP.

Steve Armstrong
CERTIFIED INSTRUCTOR
@Nebulator

Steve a commencé à travailler dans la cybersécurité alors qu'il était en service dans la Royal Air Force. Avant de quitter ses fonctions il a dirigé pour la RAF l' équipe TEMPEST de tests d'intrusion. Aujourd'hui, Steve est consultant; il fournit des tests d'intrusion et des prestations liées à la gestion d'incident.

Benjamin Arnault
INSTRUCTOR

Benjamin travaille actuellement à l'ANSSI en tant qu'expert en sécurité de l'information. Il gère des projets abordant les audits de sécurité, les tests d'intrusion, la réponse aux incidents, la détection d'incidents de sécurité et le cloud computing. Il est impliqué dans la communauté de la sécurité de l'information et est formateur pour SANS depuis 2011. Benjamin a obtenu les certifications GCFA, GCFE, GREM, GPEN, GWAPT, GCWN, GCIH, GCIA, GSEC et CISSP.

Eric Conrad
SENIOR INSTRUCTOR
@eric_conrad

Eric Conrad, formateur chevronné est l'auteur principal de la formation SANS MGT414 : le programme de formation SANS à la certification CISSP®; il est également coauteur des deux formations SANS SEC511 : Continuous Monitoring and Security Operations et SANS SEC542: Enfin, il est l'auteur principal des livres du Guide d'étude CISSP, et Eleventh Hour CISSP : Study Guide.

Ted Demopoulos
PRINCIPAL INSTRUCTOR
@teddemop

Le premier contact significatif de Ted avec les ordinateurs remonte à 1977 quand il avait un accès illimité au PDP-11 de son lycée et le piratait sans relâche. Son cursus compte plus de 25 ans d'expérience dans la sécurité de l'information et des affaires,dont plus de 20 ans comme consultant indépendant.

Mathias Fuchs
INSTRUCTOR
@mathias_fuchs

Mathias est l'un des nos formateurs pour le cours FOR508 : Advanced Digital Forensics. En qualité de consultant spécialisé dans la réponse aux incidents chez Mandiant, une société Fireeye, il mène des investigations dans le monde entier portant sur des brèches de sécurité majeures. Professionnel à temps plein, Mathias enrichit le cours avec des cas d'étude et des scénarios tirés de sa propre expérience.

Adrien de Beaupré

CERTIFIED INSTRUCTOR

@adriendb

Adrien de Beaupré est un formateur certifié SANS et travaille comme consultant indépendant à Ottawa, Ontario. Son expérience professionnelle comprend l'enseignement technique, l'évaluation de la vulnérabilité, les tests d'intrusion, la détection d'intrusion, la gestion d'incident, et l'analyse inforensique. Il est membre du SANS Internet Storm Center (Isc.sans.edu).

Alexandre Bécholey

INSTRUCTOR

Alexandre a commencé en tant administrateur sécurité dans une institution financière majeure dans laquelle il s'est occupé de rechercher et d'implémenter des solutions de sécurités. Il a trouvé sa vraie passion quand il s'est tourné vers la sécurité offensive en 2013. Il baigne dans le développement d'exploits, l'ingénierie inverse ainsi que les tests d'intrusion sur iOS, et utilise ses compétences quotidiennement pour des clients d'industries variées. Il est nommé récemment en tant qu'expert chez Kudelski Security.

Sébastien Besson

INSTRUCTOR

Sébastien travaille dans le domaine de la sécurité des Systèmes d'information depuis plus de 10 ans et a occupé différents postes lui ayant permis de développer des compétences cyber-sécurité à la fois offensives et défensives. En 2015, Sébastien décide d'entamer une nouvelle étape dans sa carrière en travaillant au sein de l'équipe 'Cyber Security' d'un opérateur de télécommunications majeur, international. Il se spécialise alors dans la définition et dans la mise en œuvre de solutions de sécurité innovantes et dans la réalisation d'analyses post-incidents de sécurité.

Dr Eric Cole

FELLOW

@drericcole

Expert reconnu de la sécurité avec plus de 20 ans d'expérience pratique dans la technologie de l'information, Dr. Cole conseille ses clients et les aide à construire un plan de défense dynamique dans des domaines de sécurité pertinents. Dr. Cole est activement impliqué avec le SANS Technology Institute en qualité de « Fellow » et auteur de cours. Il travaille avec les élèves, enseigne, développe et aide à actualiser les supports pédagogiques.

Jason Fossen

FELLOW INSTRUCTOR

@JasonFossen

Jason Fossen est Principal Security Consultant chez Enclave Consulting LLC, un auteur publié et un orateur public qui s'exprime fréquemment sur les questions de sécurité Microsoft. Il est l'unique auteur de la formation SANS Securing Windows course (SEC505) qui se déroule sur une semaine, tient à jour la formation Windows day of Security Essentials (SEC401.5), et a été impliqué dans de nombreux autres projets SANS depuis 1998.

Bryce Galbraith

PRINCIPAL INSTRUCTOR

@brycegalbraith

En qualité d'auteur contributeur au best-seller mondial, Hacking Exposed: Network Security & Solutions, Bryce a exposé le monde secret du piratage informatique au public. Bryce a occupé des postes de sécurité chez des ISP mondiaux et pour des entreprises Fortune 500, et il a été membre de la célèbre équipe de tests d'intrusion de Foundstone.

Jess Garcia

PRINCIPAL INSTRUCTOR

@j3ssgarcia

Jess est un chercheur actif dans les domaines de DFIR et de l'analyse des malwares. Il est expert en cybersécurité, reconnu internationalement, et a dirigé l'inforensique et la gestion d'incident à l'occasion des plus graves incidents d'attaque cybernétique de ces derniers temps.

Philip Hagen

CERTIFIED INSTRUCTOR

@PhilHagen

Philip travaille dans le domaine de la sécurité de l'information depuis 1998. Actuellement, Phil est le stratégiste DFIR chez Red Canary, où il travaille avec les clients actuels et futurs du service de détection des menaces géré par Red Canary. Phil est le responsable du cours et coauteur de FOR572, Advanced Network Forensics and Analysis.

Paul A. Henry

SENIOR INSTRUCTOR

@phenrycissp

Paul A. Henry est l'un des experts les plus chevronnés de la sécurité de l'information et de l'inforensique avec plus de 30 ans d'expérience. Tout au long de sa carrière, Paul a joué un rôle stratégique clé dans le lancement de nouvelles initiatives et technologies de sécurité réseau.

David Hoelzer

FELLOW INSTRUCTOR

@it_audit

David Hoelzer est un formateur collaborateur de SANS; il est l'auteur de plus de vingt sections de programmes de formation SANS. Il est expert dans une variété de domaines de la sécurité de l'information, ayant assumé la plupart des rôles majeurs dans les industries de l'informatique et de la sécurité au cours des vingt-cinq dernières années. Actuellement, David est Principal Examiner and Director of Research pour Enclave Forensics, une société d'investigation numérique et de gestion d'incident basée à New York et Las Vegas.

Micah Hoffman

CERTIFIED INSTRUCTOR

@WebBreacher

Micah est un professionnel du secteur de la technologie de l'information depuis 1998, aux services d'organisations diverses, notamment des clients privés, des entreprises et le gouvernement fédéral. Il les aide à identifier et à quantifier les faiblesses au sein de leur organisation en matière de sécurité de l'information. Il cumule des années d'expérience pratique et réelle dans les tests d'intrusion et la réponse aux incidents qui lui permettent de délivrer des solutions d'excellence à ses clients. Micah est certifié GIAC's GMON, GAWN, GWAPT, GPEN et CISSP.

Robert M. Lee

CERTIFIED INSTRUCTOR

@robertmlee

Rob a une passion pour l'analyse du système de contrôle du trafic, la gestion des incidents, et la recherche sur la cybermenace pour le renseignement. Il est l'auteur du cours SANS ICS515 - Active Defence and Incident Response et coauteur de SANS FOR578 – Cyber Threat Intelligence.

Justin Searle

PRINCIPAL INSTRUCTOR

@meeas

Justin Searle est Managing Partner chez UtiliSec, une entreprise spécialisée dans la conception sécurisée de l'architecture Smart Grid et les tests d'intrusion. Justin est un CISSP, diplômé de SANS et certifié GIAC en gestion des incidents (GCIH), analyste d'intrusion (AIPG), et testeur d'intrusion d'application web (GWAPT).

Dave Shackleford

SENIOR INSTRUCTOR

@daveshackleford

Dave Shackleford est chef d'entreprise et chef consultant de Voodoo Security et il est l'un des analystes SANS, et auteur de cours. Il a consulté pour des centaines d'organisations dans les domaines de la sécurité, de la conformité réglementaire, de l'architecture du réseau et de l'ingénierie. Il est un vExpert VMware.

Raul Siles

CERTIFIED INSTRUCTOR

@raulsiles

Raul est le fondateur et senior security analyst chez DinoSec. Depuis plus d'une décennie, il met en pratique son expertise en fournissant des prestations de sécurité techniques avancées et des solutions innovantes offensives et défensives pour les grandes entreprises et organisations dans diverses industries à travers le monde. Raul est l'une des rares personnes à travers le monde qui ont obtenu la désignation GIAC Security Expert (GSE), ainsi que bien d'autres certifications.

Bryan Simon

CERTIFIED INSTRUCTOR

@BryanOnSecurity

Bryan Simon est un expert internationalement reconnu en matière de cybersécurité et travaille dans la technologie de l'information et sur le terrain de la sécurité depuis 1991. Bryan est un expert spécialisé dans les capacités défensives et offensives. Il a reçu une reconnaissance pour son travail dans la sécurité, et a été plus récemment profilé par McAfee (filiale d'Intel Security) comme Hero IT.

James Lyne
CERTIFIED INSTRUCTOR
@jameslyne

James vient du milieu de la cryptographie, mais, au fil des ans, il a travaillé dans un grand nombre de domaines liés à la sécurité, y compris la lutte contre les malwares, l'inforensique, la gestion d'incident, et le hacking. James est un conseiller expert très demandé dans le monde; il participe à des commissions d'experts de l'industrie et à des groupes de décisions politiques. Il est l'un des directeurs chez SANS EMEA et Global Head of Research avec Sophos.

Heather Mahalik
SENIOR INSTRUCTOR
@HeatherMahalik

Heather Mahalik dirige la recherche inforensique en qualité de Principal Forensic Scientist pour ManTech CARD. Sa vaste expérience dans l'inforensique remonte à 2002. Elle est actuellement senior instructor pour SANS Institute et formateur principal de la formation FOR585: Advanced Smartphone Forensics.

Keith Palmgren
SENIOR INSTRUCTOR
@kpalmgren

Keith Palmgren est un professionnel de l'informatique de sécurité avec plus de 30 années d'expérience comme spécialiste de la sécurité informatique et il est l'un des instructeurs chevronnés de SANS. Au cours de sa carrière, Keith a formé plus de 10.000 professionnels de l'informatique et il est l'auteur de plus de vingt cours sur la sécurité informatique, y compris SANS SEC301.

Ian Reynolds
INSTRUCTOR

Au cours des vingt dernières années, Ian a travaillé dans plusieurs secteurs et disciplines IT et avec des entreprises de toute sorte. Il est certifié GIAC, CISSP, CISM et détient aussi plusieurs certifications de vendeurs ; il est également membre du comité consultatif de GIAC. Son objectif premier étant d'aider les entreprises à mieux comprendre les menaces auxquelles elles sont confrontées et à améliorer leur posture sécuritaire.

Stephen Sims
SENIOR INSTRUCTOR
@steph3nsims

Stephen Sims est un expert de l'industrie avec plus de 15 ans d'expérience dans la technologie et la sécurité des informations. Stephen travaille actuellement à San Francisco en qualité de consultant; ses activités incluent la rétro-ingénierie , la recherche sur l'exploitation de failles, la modélisation de menaces et les tests d'intrusion.

Lance Spitzner
CERTIFIED INSTRUCTOR
@lspitzner

Lance est reconnu à l'international comme un leader dans le domaine de la menace cybernétique, de la formation et de la sensibilisation à la sécurité. Il a contribué à développer et mettre en œuvre de nombreux programmes multi culturels de sensibilisation à la sécurité à travers le monde pour de petites et grandes organisations de 50 à 100,000 salariés.

Erik Van Buggenhout
CERTIFIED INSTRUCTOR
@erikvabu

Parallèlement à ses activités d'enseignement pour SANS, Erik est le chef des services techniques de sécurité chez nViso. Chez nViso, Erik se concentre principalement sur des évaluations de sécurité (à la fois au niveau du réseau et de l'application), mais, il conseille également les clients pour les aider à améliorer leur niveau de sécurité informatique.

Jake Williams
CERTIFIED INSTRUCTOR
@MalwareJake

Jake est le coauteur du cours SANS FOR610 (Malware Reverse Engineering) et du cours FOR526 (Memory Forensics). Il est aussi un auteur contributeur pour le cours de SEC760 (Advanced Exploit Development) qu'il enseigne également. Par ailleurs, Jake dispense d'autres cours sur la sécurité et l'investigation numérique. Il est expert dans l'inforensique du cloud et a, dans le passé, élaboré un cours sur ce sujet pour une administration américaine.

PROGRAMME DE FORMATION

Choisissez votre parcours

FONDAMENTAUX

Vous débutez dans la cybersécurité ?

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

1a

Fort d'une expérience préalable dans la technologie, vous avez besoin d'un apprentissage pratique pour acquérir des compétences et des techniques essentielles.

Core Security Techniques Defend & Maintain

Des techniques de défense approfondies qui s'avèrent indispensables à tout professionnel de la sécurité sont enseignées dans le cours SEC401. SEC504 apporte des connaissances supplémentaires sur l'offensive, le renseignement et la défense aux spécialistes de la défense. Vous comprendrez comment survient une attaque et comment y répondre. Les stagiaires dotés de compétences confirmées dans les fondamentaux de la défense peuvent commencer leur parcours de formation avec SEC504.

SEC 401 Security Essentials Bootcamp Style
GSEC - Security Essentials

SEC 504 Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH - Certified Incident Handler

1b

Vous serez responsable de la gestion d'équipes de sécurité, ou d'implémentations, mais les compétences pratiques ne sont pas indispensables.

Security Management

MGT 433 Securing The Human: How to Build, Maintain & Measure a High-Impact Awareness Program
Security Leadership

MGT 512 SANS Security Leadership Essentials For Managers (with Knowledge Compression™)
GSLC - Security Leadership

SEC 566 Implementing and Auditing the Critical Security Controls - In-Depth
GCCC - Critical Security Controls

INTERMÉDIAIRE

2

Expérimenté en sécurité, vous vous préparez à une mission ou à un rôle spécialisé.

Security Monitoring & Detection

SEC 503 Intrusion Detection In-depth
GCIA - Certified Intrusion Analyst

SEC 511 Continuous Monitoring and Security Operations
GMON - Continuation Monitoring

Penetration Testing and Vulnerability Analysis

SEC 560 Network Penetration Testing and Ethical Hacking
GPEN - Penetration Tester

SEC 542 Web App Penetration Testing and Ethical Hacking
GWAPT - Web Application Penetration Tester

Incident Response and Enterprise Forensics

FOR 508 Advanced Digital Forensics, Incident Response, and Threat Hunting
GCFA - Forensic Analyst

FOR 572 Advanced Network Forensics and Analysis
GNFA - Network Forensic Analyst

SANS EMEA

AVANCÉ/SPÉCIALISÉ

3 **Vous êtes candidat à une formation avancée ou spécialisée.**

Le programme très complet de formation offert par SANS permet aux professionnels d'approfondir leurs compétences techniques dans des domaines clés. Il s'adresse aussi directement aux développeurs de logiciels, aux ingénieurs de contrôle industriel et au personnel non technique dirigeant, juridique ou les auditeurs.

Cyber Defence Operations

- SEC501 Advanced Security Essentials Enterprise Defender - GCED
- SEC505 Securing Windows and PowerShell Automation - GCWN
- SEC506 Securing Linux/Unix - GCUX
- SEC566 Implementing and Auditing the Critical Security Controls - In-Depth - GCCC
- SEC579 Virtualization and Private Cloud Security

Industrial Control Systems Security

- ICS410 ICS/SCADA Security Essentials - GICSP
- ICS456 Essentials for NERC Critical Infrastructure Protection
- ICS515 ICS Active Defence and Incident Response - GRID

Penetration Testing and Ethical Hacking

- SEC550 Active Defence, Offensive Countermeasures and Cyber Deception
- SEC561 Immersive Hands-On Hacking Techniques
- SEC573 Python for Penetration Testers - GPYC
- SEC575 Mobile Device Security and Ethical Hacking - GMOB
- SEC617 Wireless Ethical Hacking, Penetration Testing, and Defences - GAWN
- SEC642 Advanced Web App Penetration Testing and Ethical Hacking
- SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking - GXPN
- SEC760 Advanced Exploit Development for Penetration Testers

Digital Forensics & Incident Response

- FOR500 Windows Forensic Analysis - GCFE
- FOR518 Mac Forensic Analysis
- FOR526 Memory Forensics In-Depth
- FOR578 Cyber Threat Intelligence
- FOR585 Advanced Smartphone Forensics - GASF
- FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques - GREM

Software Security

- DEV522 Defending Web Applications Security Essentials - GWEB
- DEV541 Secure Coding in Java/JEE: Developing Defensible Applications - GSSP-JAVA
- DEV544 Secure Coding in .NET: Developing Defensible Applications - GSSP-.NET

Management

- MGT514 IT Security Strategic Planning, Policy and Leadership
- MGT525 IT Project Management, Effective Communication, & PMP® Exam Prep - GCPM

Audit / Legal

- AUD507 Auditing & Monitoring Networks, Perimeters & Systems - GSNA
- SEC566 Implementing and Auditing the Critical Security Controls - In-Depth - GCCC
- LEG523 Law of Data Security & Investigations - GLEG

INDEX

LES COURS DU PROGRAMME SANS CYBER DEFENCE

CORE SECURITY

SEC301 - Intro to Information Security p. 22

SEC401 - Security Essentials Bootcamp Style p. 23

SEC501 - Advanced Security Essentials - Enterprise Defender p. 24

NETWORK & SECURITY OPERATIONS

SEC503 - Intrusion Detection In-Depth p. 25

SEC505 - Securing Windows with PowerShell & the Critical Security Controls p. 26

SEC506 - Securing Linux/Unix p. 27

SEC511 - Continuous Monitoring & Security Operations p. 28

SEC550 Active Defence, Offensive Countermeasures and Cyber Deception p. 30

SEC579 Virtualisation and Private Cloud Security p. 31

SANS CYBER DEFENCE

ACQUÉREZ DES COMPÉTENCES PRATIQUES NÉCESSAIRES POUR DÉFENDRE ET PROTÉGER LES RÉSEAUX, LES PERSONNES ET LES INFRASTRUCTURES.

SANS Cyber Defence enseigne les compétences requises en matière de cybersécurité pour prévenir, détecter et répondre aux menaces numériques. Deux cours intègrent le programme de cyberdéfense de cyberdéfense : Core Security and Network, et Security Operations.

Le programme SANS Cyber Defence explore la mise en œuvre des tâches essentielles suivantes dans le cadre de la cyberdéfense :

- Détecter, prévenir et répondre aux attaques
- Concevoir et construire des procédures sécurisées pour l'entreprise
- Identifier, évaluer et remédier aux failles de réseaux existants
- Modeler une menace et élaborer une défense
- Communiquer l'existence d'une cyberattaque - et ses ramifications - aux responsables
- Construire des solutions de sécurité évolutives
- Sécuriser et protéger la propriété intellectuelle d'une organisation

Le programme SANS Cyber Defence enseigne toutes ces compétences, et bien plus.

ARMÉ POUR DÉFENDRE

La formation SANS est pratique; plutôt que de se contenter de partager des théories bien connues, les cours SANS mettent l'accent sur l'ouverture d'une ligne de commande rapide ainsi que sur la gestion d'une situation d'attaque ou de défense.

SANS doit son succès à la qualité de ses intervenants, et en particulier leur expérience.

Les formateurs SANS sont des experts dans leurs domaines respectifs. Ce sont des professionnels qui travaillent en première ligne. Ils connaissent les menaces dominantes auxquelles les organisations doivent faire face, et comprennent les modes de défense actuels.

SANS équipe également les stagiaires avec des ressources complémentaires substantielles pour l'apprentissage. Les stagiaires, reçoivent, par exemple, une collection de manuels. Des supports de cours rédigés par les mêmes experts qui les ont conçus. Nous fournissons également aux stagiaires des affiches, des fiches de référence, et des kits d'outils logiciels. Tous nos contenus de cours sont mis à jour régulièrement.

« I GOT A REAL INSIGHT INTO THE MIND OF THE ADVERSARY. »
London
SEC401

« THIS WAS THE BEST AND MOST WELL-PRESENTED COURSE I EVER ATTENDED. »
London
SEC401

SANS FORENSICS AND INCIDENT RESPONSE

UN COURS DE PRATIQUE INTENSIVE DE L'INFORENSIQUE ET DE LA RÉPONSES AUX INCIDENTS ANIMÉ PAR DES EXPERTS RECONNUS DE LA SÉCURITÉ ET DE L'INFORENSIQUE

« INTENSE, NOTHING CAN PREPARE YOU FOR LEARNING FROM A TRUE MASTER OF THEIR ART. »
London
FOR508

Le programme Digital Forensic and Incident Response (DFIR) aide les organisations à enquêter et à répondre de façon efficace aux failles en matière de sécurité informatique.

Le programme SANS DFIR propose de nombreuses possibilités de spécialisation. SANS propose des cours spécialisés en investigation inforensique spécifiques pour Windows, les smartphones, les systèmes d'exploitation d'Apple, la mémoire, et bien plus.

Le programme SANS DFIR aide les entreprises à mettre en œuvre les bonnes réponses - des réponses conçues pour minimiser les pertes financières et les atteintes à leur réputation, et pour les aider à récupérer et à rebondir en force après une attaque.

RESSOURCES

Les formateurs du programme SANS DFIR sont des professionnels de l'industrie qui passent la majeure partie de leur vie professionnelle sur la ligne de front de la sécurité. C'est cette expérience du monde réel qu'ils apportent dans la salle de cours.

Plusieurs des formateurs SANS sont des membres éminents de la sphère inforensique et de la gestion d'incident (DFIR). Ce sont des conférenciers, ils écrivent, animent des blogs et contribuent au consensus mondial sur les questions de sécurité informatique.

Armés de leurs compétences techniques et professionnelles, les formateurs SANS sont des enseignants plus que qualifiés, qui savent tirer le meilleur de leurs stagiaires.

SANS fournit aux stagiaires les supports pédagogiques et des ressources supplémentaires. Nous fournissons à chaque élève une collection de manuels qui se rapportent directement au cours - des livres écrits par l'auteur du cours.

SANS fournit également aux stagiaires des licences pour les outils logiciels explorés en cours. Tout cela permet aux stagiaires de mettre en œuvre les compétences qu'ils ont acquises dès leur retour au bureau. ●

« MOST INTERESTING COURSE EVER. THIS COURSE BRINGS YOU THE NEXT LEVEL OF FORENSICS. THERE'S A LOT TO LEARN. »
Brussels
FOR508

INDEX

LE COURS DU PROGRAMME DE FORMATION SANS DIGITAL FORENSICS AND INCIDENT RESPONSE :

SEC504 - Hacker Tools, Techniques, Exploits & Incident Handling p. 32

FOR500 - Windows Forensic Analysis p. 45

FOR508 - Advanced Digital Forensics & Incident Response p. 46

FOR518 - Mac Forensic Analysis p. 47

FOR526 - Memory Forensics In-Depth p. 48

FOR572 - Advanced Network Forensics & Analysis p. 49

FOR578 - Cyber Threat Intelligence p. 50

FOR585 - Advanced Smartphone Forensics p. 51

FOR610 - Reverse-Engineering Malware: Malware Analysis Tools & Techniques p. 52

« EXCELLENT. THE BREADTH OF THIS COURSE IS AWE INSPIRING. »
London
FOR508

INDEX

LES COURS DU PROGRAMME SANS PENETRATION TESTING :

SEC504 - Hacker Tools, Techniques, Exploits & Incident Handling p. 32

SEC542 - web App Penetration Testing & Ethical Hacking p. 33

SEC560 - Network Penetration Testing & Ethical Hacking p. 34

SEC561 - Immersive Hands-On Hacking Techniques p. 35

SEC562 - CyberCity Hands-on Kinetic Cyber Range Exercise p. 36

SEC567 - Social Engineering for Penetration Testers p. 37

SEC573 - Python for Penetration Testers p. 38

SEC575 - Mobile Device Security & Ethical Hacking p. 39

SEC580 - Metasploit Kung Fu for Enterprise Pen Testing p. 40

SEC617 - Wireless Ethical Hacking, Penetration Testing, & Defences p. 41

SEC642 - Advanced web App Penetration Testing & Ethical Hacking p. 42

SEC660 - Advanced Penetration Testing, Exploit Writing et Ethical Hacking p. 43

SEC760 - Advanced Exploit Development for Penetration Testers p. 44

SANS PENETRATION TESTING

UNE FORMATION PRATIQUE SUR LES TESTS D'INTRUSION QUI VOUS MET DANS LA PEAU DU HACKER, VOUS ENSEIGNE SA FAÇON DE PENSER, DE TRAVAILLER ET D'ATTAQUER.

Les cours de la formation SANS Pen test ont pour vocation d'armer les stagiaires avec des compétences techniques, des connaissances et les outils qui leur permettront de faire la différence, dès leur retour au bureau.

La formation SANS Pen Test est pratique. Les stagiaires peuvent s'attendre à des exercices de laboratoire approfondis, des simulations, des défis cryptographiques et des jeux de guerre.

Nous sommes convaincus de la forte valeur ajoutée des tests d'intrusion qui sont au cœur du programme. Cette formation couvre:

- La modélisation des activités des attaquants du monde réel.
- Le repérage des vulnérabilités dans les systèmes cible.
- L'exploitation de ces vulnérabilités dans un environnement contrôlé.
- La détermination et la documentation des risques commerciaux.
- La mise en œuvre d'une excellence technique.
- Le travail en mode sécuritaire et professionnel en conformité avec un champ d'action et des règles d'engagement, soigneusement conçus.
- L'aide qu'il convient d'apporter à une organisation pour prioriser ses ressources afin d'améliorer son niveau de sécurité.

UNE EXPÉRIENCE DU MONDE RÉEL

Les formateurs de la formation SANS Penetration testing apportent une expertise ainsi qu'une expérience technique et industrielle dans la salle de cours. De nombreux formateurs occupent des postes de haut niveau auprès d'organisations mondiales. D'autres dirigent des bureaux d'études et de conseil et travaillent avec des entreprises réputées. Les formateurs SANS apportent cette richesse d'expérience dans la salle de cours.

« BEST COURSE I HAVE EVER BEEN ON. WORTH EVERYTHING REGARDLESS OF COST. »

London
SEC575

« OVERALL A WELL PRESENTED AND COMPREHENSIVE COURSE THAT I WOULD RECOMMEND TO ANY INFORMATION SECURITY PROFESSIONAL. »

London
SEC560

SANS INDUSTRIAL CONTROL SYSTEMS COURSES

APPRENEZ LES COMPÉTENCES ET LES CONNAISSANCES NÉCESSAIRES POUR DÉFENDRE LES SYSTÈMES DE CONTRÔLE INDUSTRIELS CONTRE LES CYBERATTAQUES.

Le programme SANS ICS a été créé pour aider deux catégories de professionnels : d'une part, les ingénieurs des systèmes de contrôle qui ont besoin de connaître les meilleures pratiques en matière de sécurité et de sécuriser leur infrastructure, et d'autre part les professionnels de la sécurité qui ont besoin d'une meilleure compréhension des technologies clés en matière d'ICS.

La formation SANS ICS est pratique. Les cours proposent de nombreux exercices et simulations en laboratoire. Les stagiaires peuvent, par exemple, acquérir une expérience inforensique concernant la capture de réseau, l'usurpation des signaux de commande Modbus-TCP et l'identification des mots de passe dans les décharges de l'EEPROM.

LA FORMATION SANS ICS APPORTE:

- Une formation dans un environnement réel - le cours est rédigé par un comité d'experts ayant une connaissance intime des principes de la cybersécurité et de SCADA ICS.
- La formation des ingénieurs - une formation spécialisée conçue pour aider les ingénieurs à comprendre la sécurité.
- La formation pour les professionnels de la sécurité - une formation qui aide le personnel de la sécurité à comprendre la sécurité SCADA et les systèmes intégrés, leurs fonctions et leurs limites.
- Des cours dispensés par des experts - les cours de la formation sont dispensés par des experts reconnus dans le domaine de l'ICS.
- Un support pédagogique très vaste - les stagiaires ICS sont dotés d'une collection de manuels et d'outils complémentaires. ●

« VALUABLE COURSE FOR ENGINEERS, IT AND PHYSICAL SECURITY CONSULTANTS FOR INDUSTRIAL CONTROL SYSTEMS. »
London
ICS410

INDEX

LES COURS DU PROGRAMME SANS ICS

ICS410 - ICS/SCADA Security Essentials p. 56

ICS515 - ICS Active Defense & Incident Response p. 57

« I THINK IT SECURITY PERSONNEL AND ENGINEERS FROM ANY COMPANY USING ICS SHOULD ATTEND THIS COURSE. »
London
ICS410

INDEX

LES COURS DU PROGRAMME SANS MANAGEMENT AND AUDIT

AUD507 - Auditing & Monitoring Networks, Perimeters & Systems p. 54

SEC566 - Implementing and Auditing the Critical Security Controls - niveau avancé p. 55

MGT414 - Sans Training Program for CISSP® Certification p. 58

MGT433 - Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program p. 60

MGT512 - SANS Security Leadership Essentials For Managers with Knowledge Compression™ p. 61

"THE COURSE HELPED ME TO SHARPEN UP MY AWARENESS PROGRAMME PLANNING FOR NEXT YEAR."

London
MGT433

SANS MANAGEMENT AND AUDIT

UNE FORMATION PRATIQUE CONÇUE POUR DOTER LES CADRES ET LES AUDITEURS DES COMPÉTENCES NÉCESSAIRES POUR CONSTRUIRE DE BONNES POLITIQUES ET DE BONNES PROCÉDURES, ET POUR PRENDRE LES MEILLEURES DÉCISIONS EN MATIÈRE DE SÉCURITÉ INFORMATIQUE.

Le programme de formation SANS Management Curriculum apprend aux stagiaires à gérer la sécurité. Les cours sont parfaits pour les nouvelles recrues de la sécurité, les administrateurs qualifiés qui accèdent à un grade supérieur, à un rôle de cadre dirigeant, et les responsables chevronnés qui doivent gérer un personnel technique.

LA FORMATION POUR LES AUDITEURS DE LA SÉCURITÉ INFORMATIQUE.

La formation Audit de SANS prépare les stagiaires à contrôler de nombreuses technologies déterminantes de l'entreprise, telles que les applications, les bases de données, les réseaux et les défenses de périmètre. Notre programme enseigne des méthodes fondées sur les risques et génère une sécurité accrue pour l'entreprise.

La formation d'audit SANS enseigne également les compétences pratiques et techniques nécessaires à la réalisation d'un audit informatique complet. Avec une approche pragmatique de la formation, SANS confronte les étudiants aux meilleurs outils - et aux meilleures pratiques - nécessaires pour que leurs contrôles génèrent de la valeur ajoutée pour l'entreprise.

Nos cours développent et élargissent les connaissances des stagiaires pour les contrôles critiques d'audit de la sécurité

FORMATION POUR LES RESPONSABLES DE LA SÉCURITÉ

MGT512 est un cours pratique visant à transmettre les compétences et les connaissances nécessaires pour mener un projet ou pour définir les composants de sécurité d'un produit.

Le cours permet aux gestionnaires et aux auditeurs de parler le même langage que le personnel technique, incluant les administrateurs système, sécurité et réseau.

MGT433 vise à aider les responsables à créer, mettre en oeuvre une campagne de sensibilisation efficace et convaincante.

Tous les cours de gestion SANS sont dispensés par des formateurs SANS. Nos formateurs de gestion sont, avant tout, des professionnels de la cybersécurité. C'est cette expérience du monde réel qu'ils apportent dans la salle de cours.

Les étudiants sont dotés d'une multitude de supports et de ressources pédagogiques pour compléter leur apprentissage. Nous fournissons, par exemple, une collection de manuels savamment rédigés. ●

« THIS COURSE IS EXCELLENT AS IT COVERS MOST OF THE TECHNICAL AUDITING TECHNIQUES AND TOOLS USED FOR THE AUDITING. »

Dubai UAE
AUD507

« EXCELLENT FOUNDATION FOR NEW SECURITY MANAGERS »

London
MGT512

« DEV522 REALLY COVERS THE SECURITY ASPECTS EVERY WEB DEVELOPER MUST KNOW. »
London
DEV522

« THE BEST COURSE TO TAKE YOU FROM ZERO TO HERO IN WEB PENETRATION IN SIX DAYS. »
London
SEC542

SANS SECURE SOFTWARE DEVELOPMENT

NOUS ATTACHONS UNE GRANDE IMPORTANCE AUX PRATIQUES ET PRINCIPES DE DÉVELOPPEMENT DE LOGICIELS SÉCURISÉS, ET POUR CELA SANS VOUS ENSEIGNE À CONSTRUIRE DES APPLICATIONS DÉFENDABLES.

Les cours SANS Secure Software Development sont conçus pour satisfaire deux enjeux : il faut d'une part des programmateurs équipés des compétences et des connaissances nécessaires pour écrire du code sécurisé ; d'autre part, les anciens doivent être capables de reconnaître les failles de sécurité dans le code existant.

Le programme SANS Secure Software Development couvre le codage sécurisé pour C et C#, .NET, Java/JEE et les applications web. Nous proposons également des cours en immersion intensive qui mettent l'accent sur le développement et l'architecture d'applications défendables.

Les organisations qui cherchent à améliorer la sécurité de leurs logiciels et de leurs produits peuvent également accéder au programme de formation SANS Penetration Testing. Plus précisément, SANS offre un cours conçu pour enseigner les tests d'intrusion pour applications web.

Au cœur du programme SANS de développement de logiciels sécurisés, il y a la promesse qu'en fin de formation, lorsque les stagiaires réintègrent leur équipe, ils sont en mesure de mettre immédiatement en pratique ce qu'ils ont appris.

CONCEVOIR UNE ARCHITECTURE CORRECTE

SANS Secure Software Development est conçu pour favoriser la sécurité par la conception. Nos cours de formation à la sécurité pour les développeurs apprennent aux stagiaires à:

- Construire en sécurité - Nos cours enseignent les principes de sécurité qui régissent le développement.
- Faire la chasse au défaut - Apprenez à identifier les points de vulnérabilité dans le code existant.
- Sécuriser divers langages - Les cours incluent NET, C & C ++, JAVA / JEE.
- Rester à jour - Le programme SANS Security Software illustre notre volonté de toujours garder une longueur d'avance sur les criminels.
- Concevoir autour de la sécurité- Les formateurs SANS sont des professionnels du monde réel spécialisés dans l'architecture d'applications défendables.
- Être préparé - Les stagiaires reçoivent une vaste sélection de manuels, d'outils et de ressources pédagogiques, qu'ils peuvent conserver comme références.

En dehors de la salle de cours les formateurs sont des professionnels reconnus dans le domaine de la sécurisation des logiciels, et des partisans de la programmation défensive.

La formation SANS est pratique. Attendez-vous à une longue liste d'exercices en laboratoire sur du code réel.

INDEX

LES COURS DU PROGRAMME SANS SECURE SOFTWARE DEVELOPMENT CURRICULUM :

SEC542 - web App Penetration Testing & Ethical Hacking p. 33

DEV522 - Defending web Applications Security Essentials p. 62

DEV544 - Secure Coding .NET: Developing Defensible Applications p. 63

« A VERY KNOWLEDGEABLE INSTRUCTOR WHO DEMONSTRATES VERY WELL THE ISSUES AND SOLUTIONS IN MODERN WEB APPS SECURITY. »
London
DEV522

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
- Connaître et être en mesure de discuter de diverses technologies en matière de sécurité, y compris les antimalwares, les pare-feux, et les systèmes de détection d'intrusion.
- Déterminer votre « QI Phishing » pour identifier plus facilement les messages SPAM
- Comprendre les problèmes relevant de la sécurité physique et comment celle-ci peut renforcer la cybersécurité
- Intégrer un niveau de connaissances de base concernant la gestion d'incident, la continuité des activités, le plan de reprise et de continuité d'activité
- Accéder à un certain nombre de sites web pour mieux comprendre la sécurité des mots de passe, le cryptage, le phishing, la sécurité du navigateur, etc.

PUBLIC VISÉ :

- Les nouvelles recrues dans le domaine de la sécurité de l'information qui ont besoin d'une introduction aux principes de base de la sécurité.
- Ceux qui veulent comprendre des termes complexes et techniques de sécurité.
- Les dirigeants autres que les responsables de la sécurité informatiques
- Des professionnels ayant des connaissances techniques et informatiques de base, quel que soit le domaine, qui ont besoin d'être familier avec les concepts, principes et termes basiques de la sécurité informatique.

WWW.SANS.ORG/SEC301
Formation pratique | Six Jours | Ordinateur portable requis
30 CPE / CMU Crédits | GIAC Cert: GISF

SEC 301

INTRO TO INFORMATION SECURITY

FORMATION SEC 301

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

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.

GIAC INFORMATION SECURITY FUNDAMENTALS GISF

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC401
Formation pratique | Six Jours | Ordinateur portable requis
46 CPE / CMU Crédits | GIAC Cert: GSEC

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

FORMATION SEC 401

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Le cours SEC401 met l'accent sur l'enseignement des mesures nécessaires pour prévenir les attaques et détecter les adversaires. Ce cours enseigne des techniques que les stagiaires peuvent mettre en pratique dès leur retour au bureau. Les participants côtoient des experts qui vont leur transmettre leurs connaissances, leurs astuces, et les aider à développer les compétences dont ils auront besoin pour gagner la bataille contre un grand nombre d'adversaires. Le cours est construit autour de la devise : « La prévention est idéale, mais la détection est un must. »

Au vu des menaces persistantes et sophistiquées, les organisations seront inéluctablement ciblées. La possibilité pour un attaquant de s'infiltrer avec succès dans le réseau d'une organisation dépend de l'efficacité de la défense de l'organisation.

La défense contre les attaques représente un défi permanent; de nouveaux vecteurs d'attaque émergent constamment et la prochaine génération de menaces se profile déjà. Les organisations doivent comprendre ce qui est vraiment efficace en matière de cybersécurité. Pour la cyberdéfense, il faut adopter une approche éprouvée, fondée sur le risque.

Avant même qu'une organisation dépense son budget informatique, ou alloue des ressources de temps au nom de la cybersécurité, trois questions doivent être posées:

1. Quel est le risque ?
2. Est-ce un risque prioritaire ?
3. Quel est le moyen le plus rentable de réduire ce risque ?

En matière de sécurité les entreprises doivent se concentrer sur les secteurs de défense pertinents. Dans le cours SEC401, les stagiaires apprennent le langage et la théorie sous-jacente de la sécurité informatique. Le cours enseigne les connaissances essentielles et efficaces en matière de sécurité. Il équipe également les défenseurs qui ont la responsabilité de sécuriser les systèmes avec les compétences nécessaires pour réussir.

Ce cours répond aux deux promesses clés de SANS envers les stagiaires. (1) Vous allez acquérir des compétences de pointe que vous pourrez mettre en pratique dès votre retour au travail; et (2) Vous serez encadrés par les meilleurs formateurs de l'industrie 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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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 divers outils pour inclure dumpsec et OpenVAS; une fois les vulnérabilités découvertes, configurer le système pour qu'il soit plus sécurisé.
- Déterminer les scores globaux des systèmes utilisant CIS Scoring Tools et créer une ligne de base de système pour toute l'organisation.

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...

- Identifier les menaces de réseau contre les infrastructures et construire des réseaux défendables pour minimiser l'impact des attaques
- Accéder aux outils qui peuvent être utilisés pour analyser un réseau, prévenir les attaques et détecter l'adversaire
- Décoder et analyser des paquets de données à l'aide d'outils divers pour identifier des anomalies et améliorer les défenses de réseau
- Comprendre les méthodes de l'adversaire pour compromettre les systèmes et répondre aux attaques
- Effectuer des tests d'intrusion contre une organisation afin de déterminer les vulnérabilités et les points de 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

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

« GREAT COURSE CONTENT VERY INTERESTING AND COMPREHENSIVE. »
John O'Brien
DÉFENSE AIRBUS & ESPACE

WWW.SANS.ORG/SEC501
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GCed

SEC 501

ADVANCED SECURITY ESSENTIALS ENTERPRISE DEFENDER

FORMATION SEC 501

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

La cybersécurité continue d'être un domaine critique pour les organisations et son importance augmente au fur et à mesure que les attaques deviennent plus sophistiquées, ont une plus grande incidence financière sur les entreprises, et portent atteinte à leur réputation. Le cours SEC501 établit une base solide permettant aux professionnels de la sécurité d'engager la bataille.

Un thème clé est « la prévention est idéale, mais la détection est un must ». Nous devons veiller à améliorer constamment notre sécurité pour prévenir prévautant d'attaques que possible. Cette prévention et cette protection se font sur deux fronts - interne et externe. Les attaques constituent encore une menace pour les organisations, car les données deviennent de plus en plus mobiles et les réseaux restent poreux. Par conséquent, la protection des données doit être un objectif clé; il faut sécuriser nos informations sensibles, peu importe si celles-ci résident sur un serveur, dans une architecture de réseau robuste, ou sur un appareil portable.

Malgré les efforts de l'organisation pour prévenir les attaques et protéger ses données sensibles, certaines attaques parviendront toujours à leurs fins. Par conséquent, nous devons détecter les attaques au moment opportun. Pour ce faire, il faut une bonne compréhension du trafic qui circule sur les réseaux, et savoir détecter les signes d'une attaque. Cela comprend la réalisation de tests d'intrusion envers l'organisation et l'analyse des points de vulnérabilité pour identifier les problèmes et les questions avant qu'une intrusion ne se produise.

Enfin, une fois qu'une attaque est détectée, il faut réagir à temps et effectuer une investigation numérique. La bonne compréhension des méthodes de l'assaillant permet de renforcer les mesures préventives, pour compléter le cycle sécuritaire.

SEC501 est idéal pour les nouveaux superviseurs et les cadres dirigeants qui aspirent à progresser. Le cours renforce les compétences en leadership qui améliorent l'ambiance au sein de l'organisation, ainsi que le travail d'équipe pour soutenir la mission de l'organisation, sa croissance et sa productivité, l'attitude et la satisfaction de chacun au travail et les relations avec le personnel et les clients.

« 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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC503
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GCIA

SEC 503

INTRUSION DETECTION IN-DEPTH

FORMATION SEC 503

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Le cours SEC503 : Intrusion Detection In-Depth vous transmettra le savoir technique, la perspicacité et la formation pratique qui vous permettront de défendre vos réseaux en toute confiance.

Les stagiaires apprennent la théorie sous-jacente du protocole TCP / IP et d'autres protocoles parmi les plus couramment utilisés, tels que HTTP. Les stagaires pourront ainsi surveiller intelligemment le trafic réseau pour identifier des signes d'intrusion.

Les stagaires maîtrisent les différents outils open-source comme tcpdump, Wireshark, Snort, Bro, et bien d'autres encore. Des exercices pratiques quotidiens adaptés à tous les niveaux complètent le contenu du support de cours en permettant aux stagiaires d'appliquer les connaissances acquises.

« IN ORDER TO DEFEND A NETWORK YOU NEED TO UNDERSTAND HOW IT WORKS, THIS COURSE IS BOTH ENJOYABLE AND CHALLENGING »
Houx C
MOD UK

Les exercices de base incluent des conseils et astuces; les options avancées offrent un niveau d'expérience plus complexe aux stagiaires qui sont déjà familiers avec le sujet, ou pour ceux qui ont rapidement maîtrisé les nouveaux acquis. En outre, la plupart des exercices proposent un défi supplémentaire destiné à mettre à l'épreuve les stagiaires les plus avancés.

Mike Poor, un expert de l'industrie, a créé une distribution VMware, Packetrix, spécialement pour ce cours. Comme son nom l'indique, Packetrix contient de nombreuses astuces du métier utiles pour effectuer l'analyse de trafic et de paquets. Il est enrichi par une démonstration de "pcaps", des fichiers qui contiennent le trafic réseau.

Les stagiaires ont ainsi la possibilité de suivre le cours avec la démonstration et les supports de cours sur leur ordinateur portable. Les pcaps fournissent une bonne bibliothèque de trafic réseau pouvant être utilisée lors de la révision du contenu, en particulier pour se préparer à la certification.

L'objectif de SEC503: Intrusion Detection In-Depth est d'apprendre aux stagiaires les connaissances de base, les outils et les techniques nécessaires pour défendre les réseaux. La formation vise à inculquer de nouvelles connaissances et compétences qui peuvent être immédiatement mises en pratique.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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)

PUBLIC VISÉ :

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

« GOOD INTRODUCTION TO THE FUNDAMENTALS OF HOW PACKETS ARE CONSTRUCTED, HAPPY WITH THE CONTENT AND ORGANISATION. »
Colin de Sharp
HP

VOUS APPRENDREZ À...

- Utiliser des stratégies de groupe pour renforcer Windows et les applications, déployer Microsoft EMET, créer une liste blanche AppLocker, appliquer des modèles de sécurité, et écrire vos propres scripts PowerShell
- Implémenter les autorisations de contrôle d'accès dynamique (DAC), le marquage de fichier, et faire un audit pour prévenir la perte de données (DLP)
- Utiliser les autorisations Active Directory et la politique de groupe pour déléguer en toute sécurité une autorité administrative au sein d'une grande entreprise, afin de mieux faire face aux diverses attaques sophistiquées notamment, l'abus de token, pass-the --hash, service/task account et autres
- Installer et gérer Windows PKI dans sa totalité, notamment les cartes à puce, le certificat d'inscription automatique, et détecter une éventuelle usurpation de certificat d'authentification
- Renforcer les SSL, RDP, DNS, et autres protocoles dangereux
- Déployer les règles du pare-feu Windows et IPSec par la politique de groupe et PowerShell
- Apprendre à automatiser les tâches de sécurité sur les systèmes locaux et distants avec le langage de script PowerShell et remoting framework

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

« I HAVE BEEN TO OTHER WINDOWS TRAINING, BUT NEVER ONE WITH A FOCUS ON SECURITY. THIS HAS BEEN EYE-OPENING EXPERIENCE. I HOPE TO ATTEND MORE EVENTS LIKE THIS IN THE FUTURE. »

Dewayne Wasson
KELLOGG COMPANY

WWW.SANS.ORG/SEC505
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GCWN

SEC 505

SECURING WINDOWS WITH POWERSHELL AND THE CRITICAL SECURITY CONTROLS

FORMATION SEC505

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Qu'est-ce que Windows Hello dans Windows 10 ? Que peuvent faire les défenseurs contre les attaques pass-the-hash, la compromission de comptes administrateur, et le mouvement latéral des hackers à l'intérieur des réseaux ? Comment implémenter les contrôles critiques de sécurité dans un vaste environnement Windows ? Le cours SEC505 aborde ces problèmes complexes, et bien plus.

Comprendre comment les testeurs d'intrusion et les hackers s'infiltrent dans les réseaux est une chose; comprendre la conception de défenses contre ces intrusions en est une autre, surtout lorsque l'on fonctionne dans un environnement Active Directory vaste et complexe. Connaitre les outils comme Metasploit, Netcat et Poison Ivy est utile, mais il n'existe pas de remède simple contre l'usage abusif de ces outils.

L'objectif du cours SEC505 est d'enseigner comment se défendre non seulement contre les techniques d'attaque actuelles à l'encontre de Windows, mais aussi contre les attaques auxquelles nous serons vraisemblablement confrontés dans le futur. Plus qu'une simple gestion de solutions réactives - nous devons agir de façon proactive pour concevoir la sécurité des systèmes et des réseaux.

Les adversaires cherchent à élever leurs capacités pour gagner le contrôle des serveurs et des contrôleurs de domaine. Pour cette raison, le contrôle des pouvoirs administratifs à l'aide de scripts Group Policy et PowerShell est un thème majeur de ce cours.

L'apprentissage de PowerShell est probablement la nouvelle compétence la plus essentielle pour les administrateurs système, particulièrement au vu de la tendance croissante de l'informatique cloud. La première journée est consacrée à PowerShell, puis des exercices PowerShell supplémentaires seront proposés tout au long de la semaine. Il n'est pas nécessaire d'avoir une expérience préalable du script.

« THE TRAINING COURSE IS VERY PRACTICAL AND INTERESTING. SUPERIOR TO COMPARABLE MICROSOFT COURSE TITLES. VERY REAL-WORLD ORIENTATED. »

Paul Bendall
FIL

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC506
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GCUX

SEC 506

SECURING LINUX / UNIX

FORMATION SEC506

PRIVATE TRAINING*

ONDEMAND

DÉTAILS DU COURS

Le cours SEC506 couvre de façon approfondie les problèmes de sécurité avec Linux et Unix. Il inclut notamment des directives spécifiques de configuration, des conseils pratiques, des exemples concrets, des conseils et des astuces.

Vous apprendrez à atténuer ou éliminer les problèmes généraux applicables à tous les systèmes d'exploitation de type Unix. La liste comprend les vulnérabilités dans le système d'authentification par mot de passe, le système de fichiers, le système de mémoire virtuelle, ainsi que dans les applications qui fonctionnent généralement sous Linux et Unix.

Le cours enseigne les compétences et apporte les outils nécessaires pour gérer les questions de sécurité. Les outils logiciels explorés sont librement disponibles et comprennent SSH, AIDE, sudo, lsof, et bien d'autres encore.

Les cours SANS sont très pragmatiques pour permettre aux stagiaires d'utiliser les outils et les techniques qu'ils ont appris dès leur retour au travail. Des exercices pratiques sont faits quotidiennement. Le cours SEC506 utilise aussi ces outils dans une section spéciale dédiée aux techniques inforensiques de base pour enquêter sur les systèmes compromis.

LE COURS SEC506 ENSEIGNE LES COMPÉTENCES, LES TECHNIQUES ET LES OUTILS SUIVANTS :

- Attaques de la mémoire, débordement de mémoire
- Attaques des systèmes de fichiers, race conditions
- Chevaux de Troie et rootkits
- Surveillance et outils d'alerte
- Journalisation Unix et audit au niveau du noyau
- Construction d'une infrastructure de journalisation centralisée
- Outils de sécurité réseau
- SSH pour l'administration sécurisée
- Verrouillage de serveur pour Linux et Unix
- Contrôle de l'accès root avec sudo
- SELinux et chroot() pour la sécurité des applications
- Déploiement de DNSSEC et automatisation
- Mod security et applications pare-feu pour le web
- Configuration sécurisée de BIND et Apache
- Investigation inforensique des systèmes Linux

GIAC CERTIFIED UNIX SECURITY ADMINISTRATOR GCUX

« 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.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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

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

WWW.SANS.ORG/SEC511
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GMON

SEC 511

CONTINUOUS MONITORING AND SECURITY OPERATIONS

FORMATION SEC511

ONDEMAND

DÉTAIL DU COURS

Les organisations investissent beaucoup de temps et de ressources pour lutter contre les cyberattaques. Malgré ces immenses efforts, des organisations sont encore compromises. Ni l'approche traditionnelle axée périmètre, ni l'approche dominante préventive de l'architecture de sécurité, ne parviennent pas à empêcher les intrusions.

Aucun réseau n'est impénétrable, une réalité que les dirigeants d'entreprises et les professionnels de la sécurité se doivent d'accepter. La prévention est cruciale, et nous ne pouvons pas perdre de vue l'objectif principal. Cependant, une nouvelle approche proactive de la sécurité est nécessaire pour renforcer les capacités des organisations à détecter les menaces qui vont inévitablement s'infiltrer dans leurs défenses.

La détection des incidents à temps reste le défi implicite des organisations. Les données de l'industrie suggèrent que la plupart des violations de sécurité restent indécelables durant une moyenne de sept mois. Les assaillants savent que le manque de visibilité et le manque de contrôles de sécurité internes leur permettent de mener méthodiquement leur mission et d'atteindre leurs objectifs.

« VERY COMPREHENSIVE, HANDS-ON AND CAN BE APPLIED TO WORKING ENVIRONMENT. »
Ewa Konkolska
PRUDENTIAL, PGDS

L'architecture de sécurité défendable, la surveillance pour la sécurité des réseaux / les diagnostics continus et la mitigation / la surveillance continue en matière de sécurité, sont autant de sujets enseignés dans ce cours qui permettront à une organisation ou au centre d'opérations sécuritaires (SOC) d'être en position optimale pour analyser les menaces et détecter les anomalies qui pourraient signaler un comportement cybercriminel.

L'avantage de cette nouvelle approche proactive est la détection précoce d'une intrusion, et la possibilité de contrecarrer avec succès les efforts des attaquants. Le National Institute of Standards and Technology a développé les lignes directrices décrites dans NIST SP 800-137 pour la surveillance continue, et au cinquième jour, les stagiaires auront acquis des compétences et une bien meilleure compréhension qui leur permettront d'implémenter des systèmes de surveillance continue en utilisant le cadre NIST framework.

« THE INSTRUCTOR'S EXPERIENCE AND EXPERTISE IN THE SUBJECT DOMAIN ARE ESPECIALLY USEFUL FOR ME, HELPING ME TO UNDERSTAND THE CUSTOMER'S REQUIREMENTS AND, THEREAFTER, DEPLOY AN APPROPRIATE MONITORING ENVIRONMENT TO ADDRESS THE NEEDS OF SECURITY OPERATIONS. »
Ryan Wong
ACCEL

Pour ouvrir votre compte portail SANS inscrivez-vous sur **www.sans.org/account/login**

LE FREE COMPTE PORTAIL SANS

Inscrivez-vous pour ouvrir votre compte portail SANS et pour recevoir :

- Les webcasts gratuits
- Les bulletins d'information
- Les dernières nouvelles en matière de cybersécurité et les mises à jour

Inscrivez-vous aujourd'hui pour rester à jour et recevoir une perspective pointue sur les toutes dernières nouvelles en matière de sécurité.

SANS **News**Bites

SANS NewsBites est une revue de haut niveau publié deux fois par semaine qui résume les articles les plus importants publiés sur la sécurité informatique au cours de la semaine précédente. Chaque élément d'actualité est brièvement résumé et inclut une référence sur le web pour plus d'informations, lorsqu'elles sont disponibles.

Inscrivez-vous et soyez à jour avec une perspective de haut niveau sur toutes les dernières nouvelles en matière de sécurité. De nouvelles éditions sont publiées chaque mardi et vendredi.

@RISK: The Consensus Security Alert

@RISK fournit un résumé hebdomadaire fiable sur :

1. les nouveaux vecteurs d'attaque récemment découverts
2. les vulnérabilités avec de nouvelles exploitations de failles actives
3. des explications éclairées sur le déroulement des attaques récentes, et d'autres informations précieuses

Un objectif clé du @RISK est de fournir des données qui feront en sorte que les 20 contrôles critiques (la référence US et UK pour une protection efficace des systèmes en réseau) restent les défenses les plus efficaces contre tous les vecteurs d'attaque connus.

OUCH !

OUCH ! est un rapport de consensus mensuel sur la sensibilisation à la sécurité pour les utilisateurs finaux. Il explique ce à quoi il faut être attentif pour éviter le phishing et d'autres pratiques frauduleuses, les virus et d'autres malwares– en prenant les toutes dernières attaques comme exemples. Il vous aiguille également vers des ressources spécialisées et très utiles comme l'étonnant Phishing Self-Test. Ce service a bénéficié des contributions de 460 organisations, de toutes tailles.

Si vous souhaitez distribuer OUCH! à tous vos utilisateurs, vous pouvez le faire suivre, ou vous y abonner à l'aide d'une seule adresse qui correspond à une liste de distribution.

Webcasts

les webcasts d'information sur la sécurité SANS sont diffusés en direct sur le web; ils associent des diaporamas et des interventions réalisées par des conférenciers expérimentés. SANS propose plusieurs types de webcasts conçus pour apporter des informations précieuses et améliorer vos connaissances en matière de sécurité.

Posez des questions aux experts du webcast: Les experts SANS apportent des informations actuelles et opportunes sur des sujets de sécurité informatique pertinents. Les webcasts ATE sont le format en ligne permettant d'obtenir des informations exploitables pour vous aider dans vos objectifs de sécurité.

- Webcasts des analystes: Une extension du programme des analystes SANS, les Analysts webcasts fournissent des informations essentielles de nos livres blancs et de nos enquêtes.
- WhatWorks webcasts: Les WhatWorks webcasts SANS regroupent des expériences client puissantes qui montrent comment les utilisateurs finaux ont résolu des problèmes spécifiques de sécurité informatique.
- Tool talks: Les Tool Talks sont conçus pour vous apporter une solide compréhension d'un problème donné, et ils vous expliquent comment mettre à profit l'outil commercial d'un fournisseur pour résoudre ou atténuer ce problème.

VOUS APPRENDREZ À...

- Suivre les hackers à la trace avec les rappels de documents Word (callback Word documents)
- Utiliser Honeybadger pour suivre les assaillants du web
- Bloquer les assaillants pour les empêcher d'attaquer les serveurs avec Honeyports
- Bloquer les assaillants du web pour les empêcher de découvrir des pages automatiquement et d'y insérer des champs
- Comprendre les limites légales et les restrictions relatives à la défense active
- Masquer les entrées DNS
- Créer des serveurs de défense active non attribuables
- Combiner la géolocalisation avec des applications Java existantes
- Créer des profils destinés à la cyberdéception sur les médias sociaux en ligne
- Créer et déployer avec facilité des honeypots

PUBLIC VISÉ :

- Professionnels de la sécurité en général
- Penetration Testers
- Hackers éthiques
- Développeurs d'application web
- Concepteurs de sites web et architectes

WWW.SANS.ORG/SEC550
Formation pratique | Cinq Jours | Ordinateur portable requis
30 CPE / Crédits CMU

SEC 550

ACTIVE DEFENCE, OFFENSIVE COUNTER-MEASURES, AND CYBER DECEPTION

FORMATION SEC550

PRIVATE TRAINING

DÉTAIL DU COURS

Les formes de menaces évoluent, et les défenses traditionnelles échouent. Les organisations ont besoin de développer de nouvelles stratégies pour se défendre. Plus important encore, les professionnels de la cybersécurité ont besoin de mieux comprendre l'assaillant et ses motifs.

Les stagiaires pourront appliquer immédiatement certaines des mesures discutées dans ce cours, alors que d'autres prendront un peu plus de temps. Quoi qu'il en soit, tout ce qui est couvert dans le cours SEC550 constitue une boîte à outils que les stagiaires pourront utiliser pour déterminer qui est l'assaillant, le gêner et contre-attaquer.

SEC550: La défense active, les contre-mesures offensives et la cyberimposture sont basées sur l'ADHD (Active Defence Harbinger Distribution) dans un environnement Linux. La distribution Linux est financée par la Defence Advanced Research Projects Agency (DARPA).

Cette machine virtuelle est construite de toutes pièces pour que les défenseurs puissent rapidement mettre en œuvre la défense active dans leurs environnements. Le cours SEC550 met l'accent sur les activités pratiques - il n'aborde pas seulement la défense active, il intègre des exercices pratiques qui permettent aux défenseurs de mettre en œuvre rapidement et facilement ce qu'ils ont appris dans leur propre environnement de travail.

« REAL WORLD, AND BLUE TEAMS NEED THESE TYPES OF TOOLS AND PROCESSES, NOT ONLY WILL THIS HELP THEM DEFEND BUT GOOD FOR ALERTING-METRICS. »

Bryon Mangler
MANDIANT

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC579
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / Crédits CMU

SEC 579

VIRTUALISATION AND PRIVATE CLOUD SECURITY

FORMATION SEC579

PRIVATE TRAINING

DÉTAIL DU COURS

La virtualisation des serveurs est l'une des technologies qui évoluent le plus rapidement. De nombreuses organisations réalisent déjà des économies de coûts grâce aux serveurs virtualisés. En outre, les administrateurs aiment la facilité de déploiement et de gestion des systèmes virtualisés.

Tous ces avantages ont aussi une face cachée. La technologie de virtualisation fait l'objet de nombreuses menaces et exploits d'un nouveau genre, et présente de nouvelles vulnérabilités qui doivent être gérées. Il existe par ailleurs un grand nombre d'options de configuration que les administrateurs système et sécurité doivent comprendre, avec un niveau supplémentaire de complexité qui doit être géré par les équipes opérationnelles.

Les deux premiers jours du cours SEC579 sont dédiés à l'architecture et à la conception de la sécurité pour les infrastructures cloud, virtuelles et privées. L'ensemble des composants est couvert, des plateformes d'hyperviseur au réseau virtuel, la sécurité du stockage, et le verrouillage des fichiers individuels de la machine virtuelle.

Les troisième et quatrième jours, le cours SEC579 détaille l'attaque et la défense - comment évaluer les environnements virtualisés à l'aide d'outils et de techniques de scan et de tests d'intrusion. Le cours explore également le changement qui s'opère lorsque nous migrons vers un modèle cloud.

Une fois que la violation a été traitée, le cours SEC579 change d'approche et explore en détail la détection d'intrusion et la connexion dans un environnement virtuel. Il couvre aussi les avancées des malwares et les changements au sein de l'infrastructure virtuelle.

Au cinquième jour, les stagiaires apprennent à adapter les politiques et les pratiques de sécurité existantes à la nouvelle infrastructure virtualisée ou reposant sur le cloud. Le cours SEC579 montre comment concevoir un programme d'évaluation de risque de base pour élaborer ensuite, à partir de celui-ci, les politiques, la gouvernance, et la mise en place de normes de conformité au sein d'un environnement.

Les configurations de virtualisation les mieux cotées et les guides de durcissement de la Defense Information Security Agency (DISA), Center for Internet Security (CIS), Microsoft et VMware sont abordés au sixième jour. Le cours porte sur les leçons essentielles et les instructions fournies par ces guides. Les stagiaires effectuent ensuite un audit concret de la technologie scriptée VMware à l'aide des commandes utiles du guide de durcissement VMware.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea (nombre minimum de participants requis)

VOUS APPRENDREZ À...

- Verrouiller et maintenir une configuration sécurisée pour tous les composants d'un environnement de virtualisation
- Concevoir une architecture sécurisée de réseau virtuel
- Évaluer les pare-feux virtuels, la détection d'intrusion et les systèmes de prévention, ainsi que d'autres infrastructures de sécurité
- Évaluer la sécurité pour les environnements de cloud privé
- Effectuer des évaluations de vulnérabilité et des tests d'intrusion dans des environnements cloud et virtuels privés, et obtenir des preuves inforensiques
- Effectuer des audits et des évaluations de risque dans des environnements cloud virtuels ou privés

PUBLIC VISÉ :

- Personnel de sécurité chargé de sécuriser les infrastructures cloud virtuelles et privées
- Les administrateurs système et réseau qui ont besoin de comprendre comment concevoir, sécuriser et maintenir les technologies de virtualisation et de cloud computing
- Les auditeurs techniques et les consultants qui ont besoin d'acquérir une compréhension plus approfondie de VMware virtualisation du point de vue de la sécurité et de la conformité

« EVERY SINGLE VIRTUALISATION ADMIN (IN OUR ORGANISATION) SHOULD TAKE THIS COURSE. I AM GOING TO PROMOTE THIS COURSE! «
Cory Verboom
DMO

« EXCELLENT COURSE, VERY RELEVANT TO MY OWN DUTIES. SO I WILL BE ABLE TO APPLY SKILLS TO THIS. A LOT OF INFO TO TAKE IN BUT WILL USE THE GOOD BOOKS TO REFRESH! »
Mike Costello
QUALCOMM

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.
- Exécuter un scanner des ports à l'aide des scans Nmap et Nessus pour rechercher les failles sur les systèmes ciblés et utiliser des outils tels que tcpdump ou netstat pour détecter les intrusions et analyser les résultats des scans.

PUBLIC VISÉ :

- Membres et responsables d'équipe de gestion d'incident, testeurs d'intrusion, hackers éthiques
- 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

WWW.SANS.ORG/SEC504
Formation pratique | Six Jours | Ordinateur portable requis
37 CPE / CMU Crédits | GIAC Cert: GCIH

SEC 504

HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING

FORMATION SEC504

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

La probabilité d'une infiltration malveillante des systèmes d'une organisation est élevée. Un ou deux salariés mécontents et une connexion Internet suffisent. Qu'il s'agisse de cinq, dix ou cent intrusions au niveau de l'infrastructure Internet d'une entreprise ou d'un seul salarié malveillant qui s'infiltre progressivement dans le système pour exfiltrer des informations, le constat reste le même : les assaillants ne cessent d'innover pour augmenter leur force de frappe tout en restant discrets, voire indétectables.

Le cours SEC504 aide les défenseurs à comprendre les tactiques et les stratégies des assaillants de façon détaillée et leur apporte une expérience pratique dans la recherche de points de vulnérabilité et la découverte d'intrusion. Le cours dote les stagiaires d'un plan de gestion d'incident exhaustif qui va inverser le rapport de force.

Les vecteurs d'attaque les plus récents et les plus sophistiqués et les attaques les plus élémentaires qui n'en restent pas moins toujours d'actualité, ainsi que diverses méthodes criminelles entre ces deux extrêmes seront abordés. Au-delà de l'enseignement basique de quelques astuces de piratage, la formation intègre tout un processus éprouvé de réponses aux incidents, étape par étape. Les stagiaires auront une description détaillée du mode d'attaque des assaillants et comment ils déstabilisent et exploitent les systèmes. Les responsables de la sécurité sont ainsi en mesure de se préparer en amont, de détecter les attaques et d'y répondre de manière efficace. Le cours comprend des ateliers pratiques pour découvrir les failles et devancer les adversaires.

La formation SEC504 couvre également les questions juridiques liées aux réponses à des attaques informatiques, notamment la surveillance des employés, la collaboration avec les forces de l'ordre, et la gestion des preuves.

Cette formation de haut niveau est particulièrement adaptée aux responsables et aux membres d'équipe de gestion d'incident. Les experts en sécurité générale, les administrateurs système et les architectes de sécurité pourront également en tirer profit pour mieux concevoir et faire fonctionner 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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC542
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GWAPT

SEC 542

WEB APP PENETRATION TESTING AND ETHICAL HACKING

FORMATION SEC542

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Le cours SEC542 prépare les étudiants à devenir des testeurs professionnels capables d'aller au-delà du simple scan et d'effectuer des tests complets à forte valeur ajoutée sur des applications web.

Les clients attendent beaucoup des applications web en matière de fonctionnalités et d'accès aux données. Aux côtés des applications web conçues pour le client, les applications web d'usage interne sont maintenant des outils commerciaux de plus en plus utilisés au sein de toute organisation et revêtent une importance toute particulière. Malheureusement, il n'existe pas de "Patch Tuesday" pour les applications web personnalisées. Par conséquent, les grandes études de l'industrie constatent que les défauts des applications web jouent un rôle majeur dans les violations et intrusions. Les adversaires se concentrent de plus en plus sur ces cibles de grande valeur soit en abusant directement des applications conçues pour le public, soit en ciblant des applications web après une effraction initiale.

Le cours SEC542 permet aux stagiaires d'évaluer la posture de sécurité d'une application web
et démontre de façon convaincante les conséquences d'une sécurité insuffisante, hélas constatée dans la plupart des organisations.

Les stagiaires viennent pour comprendre les défauts majeurs des applications web et leur exploitation. Plus important encore, les stagiaires apprennent un processus testé sur le terrain et réutilisable permettant de découvrir systématiquement des failles, et ils vont pouvoir transmettre leur savoir à leurs organisations.

Pen testing est une discipline technique. Cependant, un test d'intrusion de grande valeur va au-delà de simples découvertes sécuritaires. Les meilleurs testeurs d'intrusion sont en mesure d'expliquer ce que leurs découvertes signifient aux chefs d'entreprise et aux responsables budgétaires. Les organisations ont besoin de comprendre les failles de sécurité et se doivent de les prendre au sérieux.

Le cours SEC542 met l'accent sur des travaux pratiques exhaustifs, pour que les stagiaires puissent appliquer immédiatement tout ce qu'ils ont appris. Le cours comporte plus de 30 exercices pratiques, et culmine avec un tournoi de tests d'intrusion sur une application web, conçue et alimentée par SANS NetWars Cyber Range. Le tournoi Capture the Flag consiste à former des équipes de stagiaires qui doivent mettre en pratique les techniques acquises de tests d'intrusion pour applications web et montrer qu'ils les maîtrisent.

« CTF IS A GREAT WAY TO PRACTICE THE COURSE CONTENT, REALLY ENJOYED IT. »
Chris Campbell
RBS

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.

PUBLIC VISÉ :

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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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 éffectuer 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.
- Configurer l'outil d'exploitation Metasploit pour analyser, exploiter, puis pivoter de façon intensive dans un environnement cible.

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
- Membres « Red Team »
- Membres « Blue Team »

WWW.SANS.ORG/SEC560
Formation pratique | Six Jours | Ordinateur portable requis
37 CPE / CMU Crédits | GIAC Cert: GPEN

SEC 560

NETWORK PENETRATION TESTING AND ETHICAL HACKING

FORMATION SEC560

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Les professionnels de la sécurité ont des responsabilités cruciales : rechercher et comprendre les vulnérabilités d'une organisation, puis travailler avec diligence pour minimiser ces risques avant que les criminels n'exploitent les failles. Le cours SEC560 prépare les professionnels à ces fonctions, et plus encore.

Le cours SEC560 débute avec la planification, la détermination du champ d'application et la reconnaissance, puis se poursuit avec le scan, l'exploitation de la cible, les attaques de mots de passe, et les applications web et wifi. Le cours comporte plus de 30 exercices pratiques détaillés.

Le cours SEC560 prépare les stagiaires à effectuer une reconnaissance détaillée en examinant les infrastructures d'une cible et en exploitant les blogs, les moteurs de recherche, les sites de réseaux sociaux et autres infrastructures Internet et intranet. Le cours est riche en exemples et astuces pratiques, puisés dans le monde réel.

Les stagiaires apprennent à scanner les réseaux cible en utilisant les meilleurs outils de l'industrie. Les options et configurations ordinaires de ces outils sont explorées. Les capacités plus avancées de ces outils sont aussi abordées et discutées en groupe.

« THANKS FOR THE QUALITY (TECHNICAL AND RELATIONSHIP)... IT WAS GREAT! »
Guillame Durand
NEOLASE

Après le scan, les stagiaires apprennent de nombreuses méthodes permettant d'exploiter des systèmes cibles. Le cours SEC560 explore l'accès à ces systèmes et l'évaluation du risque commercial réel. Les stagiaires examinent les situations post-exploitation, les attaques de mot de passe, les applications web et wifi. Le cours SEC560 évolue dans l'environnement cible pour modéliser aussi les attaques du monde réel.

Après l'acquisition et la consolidation de compétences durant cinq jours de travaux pratiques, le cours se termine par une journée complète dédiée à un scénario réel de test d'intrusion. Les stagiaires effectuent un test d'intrusion du début à la fin, en appliquant les connaissances, les outils et les principes appris pendant le cours SEC560. Les stagiaires découvrent et exploitent les vulnérabilités dans un échantillon réaliste d'un organisation cible.

« IT INTRODUCES THE WHOLE PROCESS OF PEN TESTING FROM START OF ENGAGEMENT TO END. »
Barry Tsang
DELOITTE

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC561
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / Crédits CMU

SEC 561

IMMERSIVE HANDS-ON HACKING TECHNIQUES

FORMATION SEC561

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Les professionnels des tests d'intrusion ont des compétences pratiques. Ils savent trouver, exploiter, et résoudre les vulnérabilités. Pour aider les stagaires à atteindre ce niveau de compétences rapidement, SANS a conçu le cours SEC561 : Immersive Hands-On Hacking Techniques.

Plus de 80% du cours repose sur des exercices pratiques pour acquérir des capacités exhaustives en matière de sécurité. Le cours privilégie les exercices pratiques pour optimiser le temps des stagiaires. Le cours SEC561 est le plus pragmatique des cours proposés par SANS Avec plus de 30 heures d'ateliers pratiques, les stagiaires verront leurs capacités techniques faire un grand bond en avant. Les stagiaires quittent ce cours armés de compétences pratiques nécessaires pour gérer des tests d'intrusion et d'évaluation de vulnérabilité très stricts, dans un environnement d'entreprise.

Tout au long du cours, un formateur expert SANS guide les stagiaires pendant qu'ils s'entraînent sur des scénarios concrets, complexes et de plus en plus exigeants, basés sur des exemples du monde réel. Les compétences acquises sont immédiatement applicables sur le lieu de travail.

Les sujets abordés dans le cours incluent:

- L'application des outils d'analyse de réseau et d'évaluation de vulnérabilité pour cartographier efficacement des réseaux et hiérarchiser les vulnérabilités afin d'y apporter une solution efficace.
- La manipulation de protocoles réseau courants pour reconfigurer les modèles de trafic réseau interne, ainsi que des moyens de défense contre de telles attaques.
- L'analyse des systèmes Windows et Linux pour en identifier les faiblesses en utilisant les dernières capacités de gestion d'entreprise des systèmes d'exploitation, notamment le superpuissant outil Windows Remote Management (WinRM).
- L'application d'outils de pointe pour analyser les mots de passe et identifier les contrôles d'authentification faibles pouvant conduire à un accès au serveur non autorisé.
- L'examen des applications web et des systèmes mobiles pour identifier et exploiter des failles de développement pouvant avoir des conséquences dévastatrices.
- L'évitement d'outils anti-virus et le contournement de Windows User Account Control pour comprendre ces techniques avancées et être en mesure de se défendre.
- Le perfectionnement des compétences en matière de phishing permettant d'évaluer l'efficacité des initiatives de sensibilisation du personnel qui ont été prises.

Le cours porte sur des leçons pratiques et des conseils innovants, immédiatement applicables. Le cours SEC561 met également les nouvelles compétences des stagiaires à l'épreuve avec NetWars. Les scénarios NetWars sont nouveaux et élaborés sur mesure.

« 80% HANDS-ON IS INTENSE AND AWESOME. BEST WAY TO BUILD ON PREVIOUS PEN-TESTING -FOCUSSED SANS COURSES. »
Timothy McKenzie
DELL / SECURE-WORKS

« THE AMOUNT OF TOOLS AND INFORMATION PROVIDED IS EXTREMELY VALUABLE. »
Roger Szulc
MDA

VOUS APPRENDREZ À...

- Utiliser des outils d'analyse de réseau et d'évaluation de la vulnérabilité permettant de cartographier efficacement les réseaux et de prioriser les vulnérabilités découvertes afin d'appliquer des solutions efficaces
- Utiliser des outils d'analyse de mots de passe pour identifier la faiblesse des contrôles d'authentification pouvant donner lieu à un accès non autorisé au serveur
- Évaluer des applications web pour identifier des défauts courants de développement susceptibles de produire des conditions non négligeables de perte de données
- Manipuler des protocoles réseau courants pour reconfigurer intentionnellement les modèles internes de trafic réseau
- Identifier les faiblesses des signatures anti-virus modernes et des systèmes d'analyse heuristiques
- Inspecter les lacunes de configuration et les menaces de divulgation d'informations présentes sur les serveurs Windows et Linux
- Contourner les systèmes d'authentification pour l'implémentation des applications web courantes
- Exploiter les lacunes des systèmes cryptographiques courants
- Contourner les systémes de surveillance en tirant parti de la IPv6 scan et de l'exploitation des outils
- Exfiltrer des données sensibles des appareils mobiles de cibles iOS et Android

PUBLIC VISÉ :

- Les professionnels de la sécurité souhaitant élargir leurs compétences techniques dans de nouveaux domaines d'analyse tels que l'analyse de paquets, l'inforensique, l'évaluation de la vulnérabilité, le durcissement d'un système et les tests d'intrusion
- Les administrateurs système et réseau souhaitant développer une expérience pratique pour acquérir des compétences en matière de sécurité de l'information, dans le but de devenir de meilleurs administrateurs
- Les analystes de réponse aux incidents qui veulent mieux comprendre les techniques d'attaque et de défense d'un système
- Les analystes inforensiques qui ont besoin d'améliorer leurs compétences analytiques en expérimentant des situations d'attaque réalistes
- Les testeurs d'intrusion cherchant à développer une expérience pratique qu'ils pourront appliquer à leurs propres évaluations

VOUS APPRENDREZ À...

- Scan et découvrir les détails associés aux actifs informatiques, réseau et ICS
- Analyser et manipuler des protocoles couramment utilisés, très puissants, mais généralement moins bien maîtrisés, tels que Profinet, DNP3, Modbus, et d'autres encore.
- Travailler dans le cadre d'une équipe d'analyse des actions de l'attaquant et de la prévention des impacts cinétiques contre les systèmes de contrôle industriel
- Rechercher des vulnérabilités dans les systèmes liés à la distribution électrique de puissance, les systèmes d'eau, les systèmes de circulation, et autres infrastructures
- Utiliser une variété d'outils pratiques permettant d'analyser et d'interagir avec les systèmes cible, notamment Wireshark, tcpdump, Nmap, Metasploit, et autres.
- Contrôler diverses interfaces personne-machine et les terminaux d'interface opérateur largement utilisés par le système SCADA, ainsi que d'autres systèmes de contrôle industriels (ICS)
- Empêcher les attaquants de faire des ravages en manipulant les ordinateurs qui contrôlent les infrastructures physiques

PUBLIC VISÉ :

- Membres "Red Team" et "Blue Team"
- Cybercombattants
- Gestionnaires d'incident
- Penetration Testers
- Hackers éthiques
- Tout autre personnel de la sécurité en première ligne lorsque les systèmes sont attaqués

« THIS COURSE IS THE GREATEST. I HAVE BEEN WAITING FOR THIS KIND OF COURSE CTF FOREVER. I LEARNT MANY THINGS FROM THIS COURSE. »

Masashi Fujimara
HITACHI LTD

WWW.SANS.ORG/SEC562
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / Crédits CMU

SEC 562

CYBERCITY HANDS-ON KINETIC CYBER RANGE EXERCISE

FORMATION SEC562

PRIVATE TRAINING*

DÉTAIL DU COURS

Les ordinateurs, les réseaux et les contrôleurs logiques programmables font fonctionner la plupart des infrastructures physiques de notre monde moderne. Des systèmes comprenant les réseaux électriques, les systèmes d'approvisionnement en eau et les systèmes de circulation sans oublier les systèmes CVC et l'automatisation industrielle.

De plus en plus, les professionnels de la sécurité doivent posséder les compétences pour évaluer et défendre ces infrastructures importantes. SEC562 est basé sur la gamme cinétique SANS CyberCity. Les stagiaires apprennent à analyser et évaluer la sécurité des systèmes de contrôle et d'infrastructures connexes, en découvrant des vulnérabilités qui pourraient avoir un impact cinétique substantiel.

VOUS APPRENDREZ :

- Comment analyser les infrastructures cybernétiques qui contrôlent et affectent les infrastructures cinétiques.
- Comment manipuler une variété de protocoles industriels clés, notamment Modbus, CIP, DNP3, Profinet, et autres protocoles liés SCADA.
- Comment créer rapidement un prototype des outils d'attaque informatiques contre des vulnérabilités spécifiques
- Comment découvrir des failles de sécurité dans une variété de systèmes de contrôle SCADA et de systèmes de contrôle industriels (ICS) afin d'enrayer les attaques contre ces systèmes.
- Comment effectuer des tests d'intrusion et des évaluations associées aux infrastructures cinétiques.

UN MOT DE L'AUTEUR :

Le monde est confronté à une pénurie critique de professionnels ayant les compétences nécessaires pour défendre les systèmes informatiques et les infrastructures réseau qui contrôlent notre monde physique.

SANS a conçu le cours SEC562 pour aider à combler cette lacune, en enseignant aux professionnels comment analyser, contrôler et défendre d'innombrables systèmes de contrôle, de protocoles et d'autres infrastructures cinétiques auxquels ils seront confrontés à l'avenir.

Le cours SEC562 présente SANS CyberCity, un éventail cybernétique, permettant aux stagiaires de constater l'impact de leurs travaux pratiques sur un prototype de ville, grâce au streaming vidéo en temps réel. Par exemple, lorsque les stagiaires restaurent le réseau électrique, ils voient les lumières de la ville s'allumer à nouveau (et un bulletin est publié en temps réel pour annoncer la résolution de la panne). Presque chaque mission du cours est associée à des impacts visuels, qui inspirent et motivent autant les stagiaires que les formateurs SANS. *(Ed Skoudis, Josh Wright, et Tim Medin)*

« BEST CLASS EVER! »
Timothy McKenzie
DELL/SECUREWORKS

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea (nombre minimum de participants requis)

WWW.SANS.ORG/SEC567
Formation pratique | Deux Jours | Ordinateur portable requis
12 CPE / Crédits CMU

SEC 567

SOCIAL ENGINEERING FOR PENETRATION TESTERS

FORMATION SEC567

DÉTAIL DU COURS

SEC567 : Social Engineering for Penetration Testers apporte tout ce qu'il faut en matière de connaissances en ingénierie sociale pour compléter la panoplie de compétences des testeurs d'intrusion.

L'ingénierie sociale réussie utilise des principes psychologiques et des techniques permettant de mesurer le succès et de gérer le risque.

Le cours SEC567 couvre les principes de la persuasion et les fondements de la psychologie indispensables pour élaborer des attaques efficaces. Il illustre ces principes par de nombreux exemples de ce qui fonctionne tant du point de vue du cybercriminel que de celui de l'auteur compte tenu de ses propres expériences et ses engagements.

Au-delà des principes, le cours SEC567 fournit un certain nombre d'outils et d'exercices pratiques centrés sur les compétences techniques clés utiles pour mesurer le succès de l'ingénierie sociale. Les stagiaires apprennent également à faire un rapport correct à une entreprise ou un client.

Au fur et à mesure que le cours progresse, les stagiaires apprennent à effectuer des reconnaissances sur des cibles en utilisant une grande variété de sites et d'outils, créer et à suivre des campagnes de phishing et développer des charges utiles de médias qui démontrent avec efficacité des scénarios de compromis.

Le cours SEC567 poursuit en explorant comment manœuvrer pour soutirer des informations et se termine par un exercice « Capture the Human » qui met en pratique tout ce qui a été appris

C'est le cours idéal pour ouvrir de nouvelles possibilités d'attaque, pour mieux comprendre la vulnérabilité humaine lors des attaques; il permet aux stagiaires de poser des pièges testés à maintes reprises.

VOUS APPRENDREZ À...

- Participer à un premier test d'ingénierie sociale dans une entreprise, ou intervenir en qualité de consultant
- Améliorer le savoir-faire de l'ingénierie sociale pour développer de nouvelles variantes, ou pour augmenter le taux de pièges
- Gérer quelques-uns des défis éthiques et des risques associés aux engagements d'ingénierie sociale
- Améliorer les autres disciplines de tests d'intrusion par une meilleure compréhension du comportement humain dont il faut apprendre à tirer parti.

PUBLIC VISÉ :

- Le personnel ou les consultants testeurs d'intrusion qui cherchent à accroître l'ampleur et l'efficacité de leurs tests
- Les défenseurs de la sécurité qui cherchent à améliorer leur compréhension des techniques d'attaque pour améliorer leurs défenses
- Le personnel de sécurité responsable des campagnes de sensibilisation et d'éducation qui souhaite comprendre comment les cybercriminels se frayent un chemin au travers des défenses

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea (nombre minimum de participants requis)

VOUS APPRENDREZ À...

- Écrire une porte dérobée qui utilise la gestion des exceptions, les sockets, l'exécution de processus, et le cryptage pour un ancrage initial dans un environnement cible. La porte dérobée comprendra des caractéristiques telles qu'un scanner de port pour trouver un port de sortie ouvert, des techniques pour se soustraire à un logiciel antivirus, la surveillance de réseau; elle aura aussi la capacité d'intégrer la charge utile d'outils tels que Metasploit.
- Écrire un outil d'injection SQL qui utilise des bibliothèques Python classiques afin d'interagir sur les sites web ciblés Utiliser différentes techniques d'attaque SQL pour extraire des données à partir d'un système cible vulnérable
- Développer un outil d'attaque permettant de deviner les mots de passe avec des fonctionnalités comme le multi-threading, les gestionnaires de cookies, des supports pour proxys d'application tels que Burp, et bien plus encore
- Écrire un outil de reconnaissance de réseau qui utilise SCAPY, StringsIO et PIL pour réassembler des flux de paquets TCP, extraire des charges utiles de données telles que des images, des images d'affichage, extraire des métadonnées telles que des coordonnées GPS, et relier ces images avec des coordonnées GPS à Google Map

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

« GREAT COMBINATION OF PRACTICE AND THEORY. FUN CHALLENGES. »
Marek Kuczynski
SHELL

WWW.SANS.ORG/SEC573
Formation pratique | Cinq Jours | Ordinateur portable requis
30 CPE / CMU Crédits | GIAC Cert: GPYC

SEC 573

PYTHON POUR PENETRATION TESTERS

FORMATION SEC573

PRIVATE TRAINING*

« EXCELLENT CLASS FOR BEGINNERS AND ADVANCED ALIKE. IT HAS SOMETHING FOR EVERYONE »
Mike Perez
DISNEY

DÉTAIL DU COURS

SEC573: Python for Penetration Testers enseigne les compétences nécessaires pour adapter et personnaliser les outils existants. Le cours explore également comment développer des outils originaux en partant de peu. Le cours SEC573 est conçu pour différents niveaux de compétences et attire des profils variés et très différents. Que les stagiaires n'aient aucune expérience de programmation, ou qu'ils soient des développeurs Python expérimentés souhaitant appliquer leurs compétences aux tests d'intrusion, ce cours profitera à tous.

Les professionnels ne peuvent pas devenir des concepteurs d'outils de première classe en se contentant de cours magistraux; ce cours comprend donc un grand nombre de travaux pratiques. Chaque jour nous enseignons les compétences nécessaires pour développer des programmes Python très sophistiqués, et nous vous montrons comment appliquer ces compétences à vos missions de test d'intrusion.

Le cours commence par une introduction à SANS pyWars : une compétition "Capture the Flag" de quatre jours qui se déroule parallèlement au cours. Il défie les compétences de programmation existantes et aide à développer de nouvelles compétences. Les programmateurs expérimentés vont rapidement progresser vers des concepts avancés, alors que les novices prendront le temps de construire des bases solides.

Les stagiaires exploreront ensuite les compétences essentielles permettant de tirer le meilleur parti du langage Python. L'atelier pratique qui couvre les fondamentaux, enseigne les concepts et les techniques pour développer des outils originaux. L'atelier se concentre sur les compétences de programmation essentielles et leur application dans des scénarios concrets.

Le cours présente aussi les raccourcis qui transformeront les développeurs les plus expérimentés en redoutables programmateurs. Une fois que les fondamentaux sont acquis, les nouvelles compétences sont appliquées au développement d'outils qui amélioreront votre prochain test d'intrusion.

Pendant le cours, vous développerez une porte dérobée, capable d'analyser les ports, d'éviter les antivirus et d'infecter la cible, que vous implantez dans le système ciblé; vous développerez aussi un outil d'injection SQL résistant aux outils de protection ordinaires afin d'exfiltrer des données de sites web.

Les stagiaires apprennent les concepts nécessaires à la construction d'un outil multitâches permettant de deviner les mots de passe et d'un outil de reconnaissance de réseau d'assemblage de paquets. Le dernier jour, le cours se conclut par une compétition "Capture the Flag" qui complète le défi pyWars. Ainsi votre capacité à appliquer les nouveaux outils et les nouvelles compétences de programmation sera testée.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC575
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GMOB

SEC 575

MOBILE DEVICE SECURITY AND ETHICAL HACKING

FORMATION SEC575

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Pour la plupart des organisations les dispositifs mobiles représentent le plus gros terrain d'attaque. Pourtant, peu de professionnels ont les compétences nécessaires pour les évaluer. Le cours SEC575 enseigne ces compétences, et bien d'autres encore. Le cours aborde aussi Android Marshmallow, iOS 9, Apple Watch and Android Ware.

Le cours SEC575 permet aux stagiaires de comprendre les forces et les faiblesses des systèmes d'exploitation mobiles les plus connus. Avec ces compétences, les stagiaires peuvent évaluer les vulnérabilités d'applications tierces ou intégrées.

Au fur et à mesure que le cours progresse, les stagiaires apprennent à contourner le cryptage de plateforme et à manipuler les applications Android pour déjouer les techniques d'occultation. Le cours SEC575 explore également comment tirer parti des outils d'analyse pour applications mobiles, manuelles et automatisées, afin d'identifier les lacunes du trafic réseau d'une application mobile, le stockage de systèmes de fichiers, les chaînes de communication entre applications.

Les stagiaires apprennent à travailler de façon sécurisée avec des échantillons, afin de comprendre le risque de divulgation de données sensibles - dans les systèmes d'exploitation Android et iOS. Le cours SEC575 aborde aussi l'exploitation de dispositifs mobiles perdus ou volés et explique comment les données sensibles d'applications mobiles peuvent être exfiltrées.

Il est utile de comprendre et d'identifier les vulnérabilités et les menaces, mais cette compétence doit être associée à la capacité de faire connaître les risques encourus. Pendant le cours, les stagiaires apprennent à rapporter les menaces de façon efficace aux parties concernées. Ce processus inclut des outils d'optimisation tels que Mobile App Report Cards qui permettent de rapporter et de décrire les menaces aux responsables et aux décideurs; il identifie aussi un échantillon de code et des bibliothèques que les développeurs pourront exploiter pour répondre aux risques posés par des applications internes.

En utilisant leurs nouvelles compétences, les stagiaires apprennent à mettre en œuvre un test d'intrusion pour dispositif mobile, étape par étape, en commençant par l'accès à des réseaux sans fil, pour implémenter des attaques dites « homme au milieu », et en terminant par l'exploitation de dispositifs mobiles et l'exfiltration de données. Les stagiaires examinent chaque étape de la réalisation de ce test en atelier pratique. Ils reçoivent des instructions détaillées, des astuces et des « tuyaux » transmis par des centaines de testeurs d'intrusion reconnus. Armés de ces compétences, les stagiaires retournent au travail, prêts à effectuer leurs propres tests; mieux informés et plus attentifs à ce qu'ils doivent rechercher; ils savent comment analyser les résultats d'un test d'intrusion réalisé par un tiers.

GIAC MOBILE DEVICE SECURITY ANALYST
GMOB

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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

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

« 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

PUBLIC VISÉ :

- Cette formation est essentielle pour toute entreprise qui doit régulièrement procéder à des tests pour satisfaire des exigences de conformité ou tester son infrastructure de sécurité dans le cadre d'une politique de sécurité saine et préventive.
- Testeurs d'intrusion
- Personnel chargé d'évaluer les vulnérabilités
- Auditeurs
- Ingénieurs de sécurité générale
- Chercheurs dans le domaine de la sécurité

WWW.SANS.ORG/SEC580
Formation pratique | Deux Jours | Ordinateur portable requis
12 CPE / Crédits CMU

SEC 580

METASPLOIT KUNG FU FOR ENTERPRISE PEN TESTING

FORMATION SEC580

PRIVATE TRAINING*

DÉTAIL DU COURS

De nombreuses entreprises sont aujourd'hui confrontées à des exigences de conformité et de réglementation qui nécessitent des tests d'intrusion et des évaluations de vulnérabilité. Les coûts des outils commerciaux et des prestations pour ces tests sont élevés. Bien que des outils très robustes, comme Metasploit, soient disponibles, nombre de testeurs ne comprennent pas, dans leur ensemble, le caractère exhaustif des fonctionnalités de ces outils ou ne savent pas comment les appliquer à une méthodologie de tests de niveau professionnel. Metasploit a été conçu pour aider les testeurs à confirmer les vulnérabilités à l'aide d'une structure open source facile à utiliser. Ce cours va aider les stagiaires à tirer parti de cet outil gratuit.

Il fera découvrir aux stagiaires les capacités incroyables de Metasploit dans le cadre d'un test d'intrusion complet et d'une évaluation de vulnérabilité, en appliquant une méthodologie exhaustive à ces tests. Les stagiaires auront une compréhension solide de ce que Metasploit peut apporter à leurs tests d'intrusion et à leurs activités d'évaluation au quotidien. Le cours apporte une compréhension détaillée de Metasploit qui va bien au-delà de la simple démonstration de l'exploitation d'un système à distance. Le cours couvre l'exploitation et la reconnaissance post – exploitation, la manipulation de jetons, le spear-phishing, et l'ensemble très riche des fonctionnalités de Meterpreter, un environnement shell personnalisé, créé spécifiquement pour exploiter et analyser les failles de sécurité.

« I HAVE TAKEN THE 560 AND 504 COURSES AND THIS COURSE DEFINITELY COVERS WHAT I NEEDED TO HAVE, MY METASPLOIT SKILLS. »
Vincent Bartsch
CUBIC TRANSPORTATION SYSTEMS

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC617
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GAWN

SEC 617

WIRELESS ETHICAL HACKING, PENETRATION TESTING, AND DEFENCES

FORMATION SEC617

PRIVATE TRAINING*

DÉTAIL DU COURS

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.

GIAC ASSESSING AND AUDITING WIRELESS NETWORKS
GAWN

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea (nombre minimum de participants requis)

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.

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

« GOOD COURSE. I WOULD RECOMMEND IT INTENSELY IN MY COMPANY. LARRY WAS GREAT. »

Yaacon Apelbaum
AGT INT

VOUS APPRENDREZ À...

- Évaluer et attaquer les applications modernes complexes
- Comprendre les tests et les exploits spéciaux disponibles contre les systèmes de gestion de contenu tels que Sharepoint et WordPress
- Utiliser des techniques pour identifier et attaquer l'encryption dans les applications
- 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

PUBLIC VISÉ :

- Testeurs d'intrusion
- Consultants de la sécurité
- Développeurs
- Testeurs QA
- Administrateurs système
- Responsables IT
- Architectes système

« HANDS-ON AND TO THE POINT! »
Frans Kollée
MADISON GUIRKHA B.V.

WWW.SANS.ORG/SEC642
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / Crédits CMU

SEC 642

ADVANCED WEB APP PENETRATION TESTING AND ETHICAL HACKING

FORMATION SEC642

PRIVATE TRAINING*

DÉTAIL DU COURS

Le cours SEC642 enseigne des compétences et des techniques avancées pour tester les applications web. Ce cours de haut niveau concerne les tests d'intrusion pour applications web; il associe un cours magistral, des expériences réelles et des exercices pratiques pour inculquer les techniques permettant de tester la sécurité des applications d'entreprise. Le cours se termine avec une compétition "Capture the Flag".

Le cours commence par explorer des techniques et des attaques spécifiques auxquelles les applications sont vulnérables. Ces techniques et ces attaques utilisent des concepts et des compétences de haut niveau pour exploiter un système en utilisant des contrôles et des protections variés.

Le cours SEC642 explore l'encryption relative aux applications web. Les stagiaires apprennent comment fonctionne l'encryption ainsi que les techniques permettant d'identifier le type d'encryption utilisé dans l'application. De surcroît, les stagiaires apprennent, en cours et en travaux pratiques, des méthodes pour exploiter ou détourner cette encryption.

Au fur et à mesure que les stagiaires progressent dans le cours, ils apprennent à identifier les pare-feux d'application web, le filtrage, et d'autres techniques de protection. Les stagiaires explorent des méthodes pour contourner ces contrôles. Pour aller plus loin dans l'évaluation de la sécurité d'une application, les stagiaires acquièrent des compétences leur permettant d'exploiter le contrôle lui-même.

Après avoir réalisé ces exploits classiques, les stagiaires étudient des techniques qui ciblent des applications spécifiques d'une entreprise. Les participants attaquent des systèmes tels que des systèmes de gestion de contenu et d'émission de billets.

Nous explorons les risques et les failles trouvés dans ces systèmes et apprenons à mieux les exploiter. En raison de leur fréquence dans les organisations modernes, cette partie du cours inclut les applications de service web et les applications mobiles.

Le cours SEC642 se termine par une journée de compétition "Capture the Flag". La compétition cible les applications web d'une organisation imaginaire, comprenant à la fois des applications Internet et Intranet et des technologies diverses.

Pour résumer, le cours SEC642 améliore l'ensemble des compétences des stagiaires en matière d'exploitation et de défense. Il répond aussi à la nécessité d'enseigner plus de techniques avancées, telles que celles qui sont couvertes dans le cours SEC642 portant sur les fondamentaux. web Application Penetration Testing and Ethical Hacking.

« VERY GOOD TECHNIQUES AND METHODS COVERED WHICH WILL BE USEFUL TO ANY NEW APP TESTER. »
Vivek Veerappan
GEMALTO

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC660
Formation pratique | Six Jours | Ordinateur portable requis
46 CPE / CMU Crédits | GIAC Cert: GXPN

SEC 660

ADVANCED PENETRATION TESTING, EXPLOIT WRITING, AND ETHICAL HACKING

FORMATION SEC660

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Dans ce cours, les stagiaires seront exposés à des dizaines d'attaques réelles, utilisées par les testeurs d'intrusion les plus chevronnés. Nous étudierons la méthodologie d'une attaque donnée, puis nous procèderons à des exercices de laboratoire dans un environnement réel. Cette approche renforce les concepts avancés acquis durant le cours et vous permettra de mettre en œuvre les techniques apprises, dès votre retour au bureau.

Chaque journée de classe inclut un entraînement intensif de deux heures en soirée permettant aux stagiaires de maîtriser encore mieux les techniques abordées.

Les sujets abordés dans le cours incluent : L'armement de Python pour les testeurs d'intrusion, les attaques contre des contrôles d'accès réseau (NAC) et la manipulation VLAN, l'exploitation de dispositifs de réseau, l'émancipation des environnements restrictifs de Linux et Windows, l'élévation de privilèges IPv6 et Linux, et l'écriture d'exploits, les tests d'implémentations cryptographiques, les tests fuzz, le renversement des contrôles modernes OS tels que ASLR et DEP, Return Oriented Programming (ROP), l'écriture d'exploits pour Windows, et plus.

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 ».

GIAC EXPLOIT RESEARCHER AND ADVANCED PENETRATION TESTER
GXPN

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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
- Appliquer de la rétro ingénierie aux codes vulnérables pour écrire des exploits personnalisés

PUBLIC VISÉ :

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

« 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 CORPORATION

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

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

« THIS COURSE IS THE CHALLENGE I WAS LOOKING FOR. IT WILL BE OVERWHELMING, BUT WELL WORTH IT. »

William Stott
RAYTHEON

WWW.SANS.ORG/SEC760
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / Crédits CMU

SEC 760

ADVANCED EXPLOIT DEVELOPMENT FOR PENETRATION TESTERS

FORMATION SEC760

PRIVATE TRAINING*

DÉTAIL DU COURS

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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/FOR500
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GCFE

FOR 500

WINDOWS FORENSIC ANALYSIS

FORMATION FOR500

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

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.

FOR500 Windows Forensic Analysis vous apprend à:

1. Mener une investigation numérique détaillée des systèmes d'exploitation et médias Windows avec une attention particulière pour Windows 7, Windows 8 /8.1, Windows 10, et Windows Server 2008/2012.
2. Identifier les artefacts et mettre en évidence les sources permettant de répondre à des questions essentielles notamment : l'exécution d'une l'application, l'accès aux fichiers, le vol de données, l'utilisation d'un appareil externe, les services cloud, la géolocalisation, le téléchargement de fichiers, l'anti-inforensique, et l'utilisation détaillée du système.
3. Concentrer vos capacités sur l'analyse, plutôt que sur la façon d'utiliser un outil spécifique.
4. Extraire des réponses clés et construire une capacité inforensique interne via une variété d'outils gratuits, open source, et des outils commerciaux fournis par la SANS Windows SIFT Workstation.

« COURSE IS VERY UP-TO-DATE AND CHALLENGES EXISTING IDEAS TO HELP BECOME A BETTER INVESTIGATOR. COURSE IS WELL PREPARED. »
Frank Visser
PWL

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

VOUS APPRENDREZ À...

- Utiliser toute une méthodologie et une panoplie d'outils d'expertise numérique permettant d'analyser la moindre action accomplie par un suspect sur un système Windows, notamment : Déterminer comment un artefact a été placé sur le système et par qui; ainsi que : l'exécution de programme, l'ouverture de dossiers et de fichiers, la géolocalisation, l'historique du navigateur, l'utilisation d'un dispositif externe USB, et bien plus.
- Examiner le registre et les artefacts Windows et collecter des indicateurs tels que la date et l'heure exactes de l'exécution d'un programme par un utilisateur spécifique et comprendre ce que ces informations peuvent apporter dans des enquêtes concernant des activités criminelles, entre autres le vol de propriété intellectuelle et l'espionnage industriel.
- Déterminer combien de fois un fichier a été ouvert par un suspect à l'aide d'une analyse inforensique du navigateur, l'examen des fichiers de raccourcis (LNK), l'analyse des courriels et l'analyse des registres Windows.
- Identifier des mots de passe recherchés par un utilisateur spécifique sur un système Windows afin de repérer les fichiers et les informations ciblés par le suspect, puis faire un inventaire détaillé des dommages.
- Utiliser l'analyse des clés de registre Windows pour articuler chaque dossier et chaque répertoire ouvert par un utilisateur lors de sa navigation sur des disques durs internes et externes et des lecteurs réseau.
- Déterminer combien de fois un dispositif USB unique et spécifique a été connecté sur le système Windows, les fichiers et les dossiers auxquels le suspect a eu accès, et qui a connecté le dispositif à l'aide de l'analyse des artefacts Windows tels que le registre et les fichiers journaux.

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...

- Découvrir chaque système compromis d'une entreprise en utilisant les outils de gestion d'incident, tels que F-Response et les capacités d'analyse inforensique de la machine virtuelle SIFT Workstation pour identifier les mécanismes de spear-phishing et d'attaque de type APT beach head, les mouvements latéraux et les techniques d'exfiltration de données.
- Analyser la mémoire du système en utilisant l'outil Volatility pour identifier les codes malveillants actifs sur un système, déterminer comment celui-ci a été implanté, le récupérer pour en extraire des indicateurs de compromission dans le but de délimiter le champ d'action de l'attaquant lors d'une réponse à incident.
- Détecter des capacités avancées, telles que celles employées par Stuxnet ou TDSS ; identifier rapidement les codes malveillants par une analyse de la mémoire, en utilisant l'index d'évaluation Redline Malware Risk Index (MRI) qui permet de déterminer rapidement la menace qui pèse sur le système d'information de l'organisation ciblée, et de déterminer la véritable portée d'une intrusion.
- Suivre les empreintes digitales d'un assaillant sur de multiples systèmes et analyser les artefacts collectées.
- Suivre les mouvements d'un adversaire sur un réseau via l'analyse historique « timeline » en utilisant les outils log2timeline et plaso.
- Procéder à la remédiation de la compromission à l'aide aux indicateurs de compromission (IOC) et aux techniques inforensiques essentielles permettant d'identifier les codes malveillants actifs et tous les systèmes de l'entreprise qui ont été compromis.
- Effectuer une réparation des systèmes de fichiers à l'aide de l'ensemble d'outils Sleuth Kit pour découvrir leur fonctionnement, ainsi que des artefacts puissants tels que les index de répertoire de fichiers NTFS $I30, USN journal et l'analyse de la Master File Table.

PUBLIC VISÉ :

- Les membres d'une équipe de réponse aux incidents
- Les membres d'une équipe de sécurité des opérationnelle (SOC) et les professionnels de la sécurité de l'information.
- Les administrateurs système
- Les agents du renseignement, les représentants des forces de l'ordre, de la justice et d'autres administrations chargés d'enquêtes
- Les membres d'une « Red Team », les testeurs d'intrusion, et les développeurs d'exploits

WWW.SANS.ORG/FOR508
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GCFA

FOR 508

ADVANCED DIGITAL FORENSICS AND INCIDENT RESPONSE

FORMATION FOR508

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Plus de 80% des victimes d'un piratage sont informées de la compromission par un tiers, et non par les équipes de sécurité internes. Dans la majeure partie des cas, les adversaires se sont maintenus dans le réseau sans être détectés pendant des mois, voire des années.

Les techniques et les méthodes de réponse aux incidents ont rapidement évolué au cours des dernières années. Les fuites de données et les intrusions sont devenues plus complexes. Les adversaires ne s'attaquent plus à un ou deux systèmes d'une entreprise, mais à des centaines. Une équipe ne peut plus se permettre d'utiliser des techniques dépassées en matière de réponse à l'incident - des techniques qui sont incapables d'identifier les systèmes compromis, de contenir une brèche et, in fine, ne peuvent plus remédier rapidement aux incidents.

Ce cours approfondi en réponse aux incidents apporte aux défenseurs des compétences pointues pour identifier, lutter et remédier à un large éventail de menaces contre les réseaux d'entreprise. Les situations étudiées incluent des APT, des syndicats de crime organisé et des hackeurs activistes. Le cours FOR508, constamment actualisé, traite les incidents d'aujourd'hui en apportant des réponses pratiques relatives à la tactique et la technique que les intervenants de haut niveau utilisent avec succès dans des incidents concrets.

Un exercice pratique d'intrusion (développé à partir d'une véritable attaque APT ciblée sur le réseau d'une entreprise et basée sur les méthodes employées par un groupe APT pour cibler les réseaux) amène les stagiaires à relever les défis et à trouver des solutions grâce à l'utilisation intensive de la boîte à outils SANS SIFT Workstation.

Pendant les exercices pratiques, les stagiaires identifient le point d'intrusion initial de l'attaque ciblée ainsi que les mouvements latéraux entre de multiples systèmes compromis. Les participants extraient des informations puis créent une source de « threat intelligence » qui permet d'estimer correctement la portée de la compromission et de détecter de futures menaces.

« 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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/FOR518
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / Crédits CMU

FOR 518

MAC FORENSIC ANALYSIS

FORMATION FOR518

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

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 cours FOR518: Mac Forensic Analysis vise à former de bons investigateurs en présentant l'inforensique pour le Mac dans un environnement inforensique basé sur Windows. Ce cours porte sur des sujets tels que les systèmes de fichiers HFS+, les fichiers de données spécifiques au Mac, le suivi de l'activité d'un utilisateur, la configuration du système, l'analyse et la corrélation des journaux Mac, des applications Mac, et des technologies Mac exclusives. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

« 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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

VOUS APPRENDREZ À...

- Analyser et décrypter manuellement le système de fichiers hiérarchique (HFS+), et reconnaître les domaines spécifiques du système de fichiers logique et les types de fichiers spécifiques au Mac
- Comprendre et profiler des utilisateurs à partir de leurs fichiers de données et de la configuration de leurs préférences.
- Déterminer comment un système a été utilisé ou compromis grâce aux fichiers système et aux fichiers de données de l'utilisateur en corrélation avec les fichiers de journal du système
- Comprendre et analyser de nombreuses technologies spécifiques au Mac, notamment Time machine, Spotlight, iCloud, Versions, FireVault, Airdrop,et Facetime

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...

- Bien maîtriser la mémoire : capturer une mémoire ciblée pour vérifier l'intégrité des données et démontrer des techniques de combat anti-capture
- Identifier un vice dans la mémoire : détecter des processus malfaisants, cachés et injectés, les rootkits au niveau du noyau, le piratage DLL (Dynamic Link Libraries), les processus d'évidement, et les mécanismes de persistance
- Maîtriser, étape par étape, de techniques efficaces pour l'analyse de mémoire : utiliser un processus chronologique, l'analyse de haut et bas niveau, et naviguer dans l'arbre VAD pour détecter les comportements anormaux.
- Acquérir les techniques relevant des meilleures pratiques : apprendre le bon moment pour implémenter le triage, l'analyse de système en direct, les techniques d'acquisition alternatives, mais aussi élaborer des scripts d'analyse personnalisés pour examiner une mémoire ciblée

PUBLIC VISÉ :

- Les membres d'équipe de réponse aux incidents qui interviennent régulièrement sur des incidents de sécurité / intrusions et souhaitent comprendre l'investigation numérique de mémoire pour élargir leur champ d'action
- Les investigateurs expérimentés qui souhaitent consolider et élargir leur compréhension de l'inforensique de mémoire
- Les membres « Red Team » et les développeurs d'exploits qui souhaitent comprendre comment leurs adversaires identifient leurs actions, découvrir comment des erreurs courantes peuvent compromettre les opérations sur des systèmes distants, et comment les éviter. Ce cours porte sur l'investigation à distance de systèmes et les techniques de collection de données qui peuvent être facilement intégrées dans des procédures opérationnelles "post-exploit" et des batteries de tests d'exploit.
- Les forces de l'ordre, les agents du renseignement ou enquêteurs qui veulent devenir experts dans le domaine de l'inforensique de mémoire
- Les stagiaires qui ont déjà suivi les cours FOR508 et SEC504 et qui veulent élever leurs compétences de l'inforensique de mémoire au niveau supérieur

WWW.SANS.ORG/FOR526
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / Crédits CMU

FOR 526

MEMORY FORENSICS IN-DEPTH

FORMATION FOR526

PRIVATE TRAINING*

DÉTAIL DU COURS

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.

« 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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/FOR572
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GNFA

FOR 572

ADVANCED NETWORK FORENSICS AND ANALYSIS

FORMATION FOR572

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Lorsqu'il s'agit de gérer un incident d'intrusion, de vol de données ou d'abus de la part d'un salarié, le réseau offre souvent une vue sans pareil de l'incident. Les renseignements issus d'un réseau apportent la preuve nécessaire pour démontrer l'intention et prouver définitivement qu'un crime a été commis.

Le cours FOR572 est entièrement construit pour inculquer les compétences clés permettant de mener des investigations véritables et efficaces en réponse à un incident. Le cours se concentre sur les connaissances nécessaires pour faire progresser la mentalité inforensique, depuis les données résiduelles sur les médias d'enregistrement (systèmes ou dispositifs) jusqu'aux communications transitoires qui se sont produites dans le passé ou continuent à faire des apparitions. Même si le plus malin des assaillants a compromis un système à l'aide d'un exploit indétectable, le système doit malgré tout communiquer sur le réseau.

Ce cours enseigne les outils, la technologie, et les processus requis pour intégrer les sources de preuves d'un réseau dans vos investigations. Les stagiaires sont ainsi équipés d'une boîte à outils bien remplie, et d'un savoir-faire qu'ils pourront utiliser dès leur retour au bureau.

Les leçons couvrent un vaste éventail de preuves provenant des réseaux, notamment l'analyse de haut niveau NetFlow, l'exploration basique pcap, l'examen de journaux auxiliaires de réseau, et bien plus encore. Nous enseignons comment tirer parti des dispositifs d'infrastructure existants qui peuvent contenir des mois, voire des années, de données de grande valeur, mais aussi comment installer de nouvelles plateformes de collection alors qu'un incident est déjà en cours.

Les travaux pratiques en classe font appel à une gamme d'outils étendue, notamment, les très respectables tcpdump et Wireshark pour la saisie de paquets et l'analyse, les outils commerciaux comme Splunk, NetworkMiner et SolarWinds. Les outils open source incluent nfdump, tcpxtract, ELSA, et bien d'autres encore. À travers tous ces exercices, les capacités d'écriture de scripts shell sont utiles pour extraire des milliers d'enregistrements de données.

« FANTASTIC COURSE, VERY WELL TAUGHT WITH GREAT LABS THAT REINFORCE THE TAUGHT MATERIAL. »
A. Honey
NCA

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

VOUS APPRENDREZ À...

- Extraire des fichiers de saisies de paquets de réseau et des fichiers proxy cache, vous permettant une analyse continue de malware ou des déterminations de perte définitive de données
- Utiliser les données historiques NetFlow pour identifier les occurrences passées et pertinentes du réseau qui permettent d'évaluer correctement la portée de l'incident
- Appliquer une rétro-ingénierie personnalisée aux protocoles de réseau pour identifier les actions et les capacités de commande et de contrôle de l'adversaire
- Décrypter le trafic SSL saisi pour identifier les actions d'un assaillant et identifier les données volées à la victime
- Utiliser les données typiques de protocoles de réseau pour accroître la fiabilité des découvertes d'une investigation
- Examiner le trafic en utilisant des protocoles de réseau courants afin d'identifier des modèles d'activité ou des actions spécifiques qui justifient une investigation plus poussée
- Incorporer les données de journaux dans un processus exhaustif d'analyse
- Apprendre comment les assaillants tirent parti d'outils du « milieu » pour intercepter des communications - en apparence - sécurisées
- Examiner les protocoles de réseaux privés pour déterminer quelles actions ont eu lieu sur les terminaux des systèmes
- Analyser le trafic de réseau sans fil pour trouver des preuves d'activité malveillante
- Utiliser les outils et les techniques de virtualisation pour distiller des sources de données complexes dans des rapports aisément lisibles pour les dirigeants
- Apprendre à modifier la configuration de dispositifs de réseau typiques afin d'accroître la valeur du renseignement de leurs journaux et de leurs alertes pendant l'investigation

PUBLIC VISÉ :

- Membres d'équipe de réponse aux incidents
- Forces de l'ordre, agents, et enquêteurs
- Responsables de la sécurité informatique
- Défenseurs de réseaux
- Professionnels IT
- Ingénieurs réseau
- Avocats spécialisés en droit numérique et juristes
- Toute personne intéressée par les intrusions de réseaux informatiques et les investigations

WWW.SANS.ORG/FOR578
Formation pratique | Cinq Jours | Ordinateur portable requis
30 CPE / Crédits CMU

FOR 578

CYBER THREAT INTELLIGENCE

FORMATION FOR578

PRIVATE TRAINING*

VOUS APPRENDREZ À...

- Construire et exploiter la « threat intelligence » concernant les menaces afin de détecter des menaces APT, d'y répondre et de les combattre
- Analyser les intrusions réussies ou ratées, perpétrées par des assaillants expérimentés
- Établir des corrélations entre les incidents d'intrusion, les auteurs des menaces et les organisations d'État
- Gérer, partager et collecter des renseignements sur les groupes d'attaques APT
- Générer du renseignement à partir des propres données de ces groupes pour les partager comme il se doit
- Identifier, extraire et optimiser le renseignement à partir des intrusions APT
- Exploiter le renseignement existant pour construire le profil des groupes adversaires
- Optimiser le renseignement acquis pour mieux se défendre et répondre à de futures intrusions

PUBLIC VISÉ :

- Les membres d'équipe de réponse aux incidents qui interviennent régulièrement sur des intrusions/incidents complexes venant d'adversaires APT et ayant besoin de détecter, enquêter, remédier et réparer les systèmes compromis d'une entreprise
- Le personnel des centres d'opérations sécuritaires et les professionnels de la sécurité informatique qui interviennent dans des opérations de chasse pour identifier les assaillants dans leur environnement de réseau
- Les investigateurs numériques expérimentés qui veulent consolider et élargir leur compréhension de l'inforensique des systémes de fichiers, des investigations concernant des adversaires dotés de compétences techniques avancées; des tactiques de réponse aux incidents et des investigations d'intrusion avancées
- Les forces de l'ordre et les agents du renseignement qui veulent maîtriser l'investigation d'intrusion et la réponse aux incidents, ainsi qu'élargir leurs compétences en matière d'investigation au-delà de l'investigation numérique traditionnelle basée sur l'hôte
- Les stagiaires ayant suivi les cours SANS FOR408, FOR572, FOR508, ou FOR610 souhaitant pousser leurs compétences à un niveau supérieur

DÉTAIL DU COURS

Les défenses de réseau traditionnelles telles que les systèmes de détection d'intrusion et les outils antivirus sont centrées sur la composante de vulnérabilité du risque, et les méthodologies traditionnelles pour la gestion d'incident présupposent une intrusion réussie. Cependant, la sophistication croissante des intrusions sur les réseaux informatiques a rendu ces approches insuffisantes pour parer aux menaces que doivent affronter les organisations sur réseau de nos jours. Les adversaires d'aujourd'hui réalisent leurs objectifs en utilisant des outils et des techniques de pointe, conçus pour contourner la plupart des mécanismes traditionnels de défense des réseaux informatiques. Ils peuvent être indétectables pendant l'intrusion, et le rester longtemps après.

La science qui consiste à collecter, organiser et exploiter des informations concernant les adversaires - généralement connue sous le nom de « cyber threat intelligence » apporte une supériorité aux défenseurs des réseaux. Elle peut être utilisée pour réduire les chances de réussite des adversaires à chaque tentative subséquente d'intrusion. Ceux qui répondent aux incidents ont besoin d'informations correctes et détaillées au moment opportun pour surveiller les nouvelles attaques ou celles qui évoluent. Ils ont également besoin de méthodes pour exploiter ces informations afin d'améliorer leur posture de défense. La « threat intelligence » concernant la menace cybernétique représente une force exponentielle pour les organisations qui cherchent à actualiser leurs programmes de détection et de réponse. Elle leur permet également de traiter des menaces persistantes de plus en plus sophistiquées et avancées.

« FANTASTIC CLASS! I LOVE THE WAY THE TERMINOLOGY WAS COVERED. I WILL BE MAKING INDEX CARDS TO ENSURE I HAVE THEM MEMORISED. »
Nate DeWitt
EBAY

Lors d'une attaque ciblée, une organisation doit pouvoir apporter une réponse de pointe; pour ce faire, elle doit d'être armée de renseignements essentiels pour comprendre le modus operandi de l'adversaire et pour riposter. Le cours FOR578 : Cyber Threat Intelligence enseigne au défenseur comment détecter, évaluer et sélectionner un plan d'action souple en réponse à ces intrusions et violations des données.

« 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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/FOR585
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / Crédits CMU

FOR 585

ADVANCED SMARTPHONE FORENSICS

FORMATION FOR585

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

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.

Le cours FOR585: Advanced Smartphone Forensics apprend aux stagiaires à:

- Localiser les preuves clés sur le smartphone
- Expliquer de quelle façon les données sont arrivées sur le smartphone
- Récupérer des données supprimées d'un dispositif mobile, alors que la plupart des outils inforensiques n'en sont pas capables
- Décoder des preuves enregistrées dans des applications de tiers
- Détecter, décompresser, et analyser des malwares et des spywares mobiles
- Gérer des dispositifs, des applications, et des containers verrouillés ou cryptés

« 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

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
- Récupérer des communications cachées ou brouillées à partir d'applications sur les smartphones
- Décrypter ou déchiffrer des données d'application qui ne sont pas analysées par vos outils inforensiques
- Détecter des smartphones compromis par un malware ou un spyware en utilisant des méthodes d'investigation inforensiques
- Décompresser et analyser les malwares mobiles à l'aide d'outils open source
- Gérer l'encryption sur les smartphones et éviter, craquer, et/ou décoder des codes de verrouillage récupérés manuellement sur des smartphones, notamment craquer des fichiers de sauvegarde qui étaient chiffrés par iTunes

PUBLIC VISÉ :

- Les investigateurs numériques expérimentés qui veulent élargir leurs connaissances et faire l'expérience de l'analyse numérique des dispositifs mobiles, en particulier les smartphones
- Les analystes de l'exploitation des médias qui ont besoin de maîtriser l'exploitation tactique ou les opérations d'exploitation de documents et de médias (DOMEX) sur des smartphones et dispositifs mobiles en apprenant comment des individus utilisent leurs smartphones, avec qui communiquent-ils et quels sont les fichiers auxquels ils accèdent

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

VOUS APPRENDREZ À...

- Construire un environnement de laboratoire isolé pour analyser le code et les comportements de programmes malveillants
- Utiliser des outils de réseau et de surveillance de système pour analyser comment le malware interagit avec le système de fichier, le registre, le réseau, et d'autres processus sur Microsoft Windows
- Découvrir et analyser des composants malveillants de JavaScript, VB Script et ActionScript sur des pages web qui sont souvent utilisés pour des attaques lors d'un passage rapide sur celles-ci.
- Contrôler certains aspects du comportement de programmes malveillants par l'interception de trafic sur le réseau et la correction de code
- Utiliser un désassembleur et un débogueur pour analyser le fonctionnement interne de logiciels malveillants Windows
- Éviter divers mécanismes de défense conçus par les auteurs de malware pour rediriger, embrouiller ou tout au moins ralentir l'analyste
- Reconnaître et comprendre des modèles de langage d'assemblage courants dans des codes malveillants, tels que l'injection DLL
- Accéder à la menace associée à des documents malveillants, tels que des PDF et des fichiers Microsoft Office dans le contexte d'attaques ciblées
- Dériver des indicateurs de compromis (IOC) à partir de logiciels malveillants pour contenir et rebondir après l'attaque
- Utiliser des techniques inforensiques de mémoire pratiques pour examiner la capacité des rootkits

PUBLIC VISÉ :

- Les professionnels et les responsables dans les domaines suivants : la réponse aux 'incidents, l'investigation numérique, la sécurité Windows, et l'administration des systèmes
- Les professionnels qui gèrent des incidents impliquant des malwares et voudraient mieux comprendre certains aspects clés des programmes malveillants
- Toute personne ayant une expérience préalable de l'analyse de malwares et souhaitant formaliser et élargir son expertise inforensique en ce domaine

WWW.SANS.ORG/FOR610
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GREM

FOR 610

REVERSE-ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES

FORMATION FOR610

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Comprendre les capacités des malwares est essentiel pour permettre à une organisation de dériver des renseignements sur la menace, de répondre aux incidents, et de renforcer ses défenses. Ce cours donne une fondation solide pour la rétro-ingénierie de logiciels malveillants. Il explore une variété de fonctionnalités de surveillance des systèmes et des réseaux, des désassembleurs, des débogueurs et d'autres outils utiles pour examiner le malware de fond en comble.

Le cours commence par les aspects fondamentaux de l'analyse des malwares. Les stagiaires apprennent comment installer un laboratoire modulable et peu coûteux. Le cours FOR610 enseigne ensuite comment analyser le fonctionnement interne d'un logiciel malveillant et utiliser le laboratoire pour disséquer des échantillons réels. Les stagiaires analysent des échantillons de codes et de modèles de comportement. Le cours se poursuit par une discussion des concepts essentiels de langage d'assemblée x86.

Les stagiaires examinent aussi du code malveillant pour en comprendre les composants clés et le flux d'exécution. Par ailleurs, le cours explore comment identifier les caractéristiques courantes des malwares en examinant des modèles Windows API suspects, utilisés par les bots, rootkits, keyloggers, downloaders, et autres types de malwares.

Puis, les stagiaires apprennent à gérer les malwares autodéfensifs, en contournant la protection offerte par les packers et autres procédés antianalytiques. Étant donné l'usage fréquent des malwares de navigateur pour cibler les systèmes, les stagiaires explorent des approches pratiques pour analyser des scripts malveillants de navigateur, débusquer du JavaScript et du VBscript afin de comprendre la nature de l'attaque.

Le cours FOR606 enseigne aussi aux stagiaires à analyser des documents malveillants tels que des fichiers Microsoft Office et des fichiers PDF Adobe. Ces documents agissent comme des vecteurs d'infection courants et peuvent avoir besoin d'être analysés aussi bien pour des infections à grande échelle que pour des attaques ciblées.

« IT REALLY GIVES A NICE REALISTIC GUIDANCE ON HOW TO APPROACH COMPLEX PROBLEMS IN MALWARE ANALYSIS. »
Markus Jeckeln
LUFTHANSA

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC440
Formation pratique | Deux jours | Ordinateur portable non requis
12 CPE / Crédits CMU

SEC 440

CRITICAL SECURITY CONTROLS: PLANNING, IMPLEMENTING AND AUDITING

FORMATION SEC440

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Ce cours va vous aider à maîtriser des techniques et des outils spécifiques et éprouvés pour implémenter des contrôles de sécurité critiques et pour les auditer selon les directives du CIS (Center for Internet Security). Ces contrôles de sécurité critiques, détaillés ci-dessous, sont reconnus par les plus grandes et les plus sérieuses des organisations comme étant la référence absolue en matière de mesures et contrôle de sécurité qui doivent être mis en place, suivis et faire l'objet de tests. Ces contrôles ont été sélectionnés et définis par l'armée des États-Unis ainsi que d'autres gouvernements et organisations privées (dont la NSA; DHS, GAO et autres) qui détiennent une expertise absolue et reconnue sur le mode d'opération des assaillants et des solutions pour les arrêter. Ces contrôles représentent un consensus sur la meilleure façon de bloquer des attaques connues, d'identifier et de limiter les dommages occasionnés. Le cours montre aux professionnels de la sécurité comment mettre en place des contrôles sur leurs réseaux existants à l'aide d'un système d'automatisation efficace, largement répandu et rentable. Pour les auditeurs, hauts responsables du secteur informatique (CIO) et responsables de la gestion du risque, ce cours permet de comprendre comment mesurer l'efficacité des contrôles en place.

« Quelles sont les mesures les plus importantes que nous devons prendre protéger nos systèmes ? » Voici la question que le CIO de la base de défense industrielle a posée au Département de la Défense lorsqu'il a appris que ses systèmes avaient été infiltrés et que des secrets militaires de la plus haute importance avaient été dérobés pour le compte d'autres nations. C'est aussi la question que les responsables des opérations informatiques à tous les niveaux du gouvernement se sont posée lorsqu'ils ont appris, au cours d'une enquête menée par le Congrès américain que les contrôles, institués par la loi FISMA, n'étaient pas capables d'évaluer les mesures de sécurité correctement. C'est exactement la même question que se posent les dirigeants des entreprises d'énergie, des banques, des compagnies pétrolières, et des organisations de santé. Si vous pouvez répondre à cette question, mettre en place les contrôles et en réaliser l'audit, vous changerez la donne. Les résultats ne seront peut ne pas immédiats, mais ils seront au rendez-vous.

ORDINATEUR PORTABLE NON REQUIS

Un ordinateur n'est pas nécessaire pour ce cours. Cependant pendant le cours, l'instructeur distribuera des échantillons d'outils aux stagiaires sur une clé USB. Si les stagiaires souhaitent accéder à ces outils pendant le cours, ils devront apporter un ordinateur capable d'accéder aux fichiers sur la clé USB. L'accès à ces fichiers est optionnel et n'est pas nécessaire pour participer aux activités du cours.
Pour toutes autres questions concernant les spécificités d'ordinateur portable, veuillez contacter laptop_prep@sans.org.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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
- Utiliser le script pour élaborer un système de référence de base afin d'effectuer des contrôles automatiques de répertoire actif et de tous les systèmes d'un domaine Windows

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

WWW.SANS.ORG/AUD507
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: GSNA

AUD 507

AUDITING & MONITORING NETWORKS, PERIMETERS & SYSTEMS

FORMATION AUD507

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

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.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/SEC566
Formation pratique | Cinq Jours | Ordinateur portable requis
30 CPE / CMU Crédits | GIAC Cert: GCCC

SEC 566

IMPLEMENTING AND AUDITING THE CRITICAL SECURITY CONTROLS IN-DEPTH

FORMATION SEC566

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

Les attaques en matière de cybersécurité augmentent et évoluent à une telle vitesse qu'il est plus difficile que jamais de les prévenir et de se défendre. Existe t-il au sein de l'organisation une méthode efficace pour détecter, déjouer et surveiller des menaces externes ou internes afin de prévenir les violations de sécurité ? Ce cours aide les stagiaires à maîtriser des techniques et des outils spécifiques et éprouvés pour implémenter et auditer les contrôles de sécurité critiques - tels qu'ils sont décrits par le CIS (Center for Internet Security).

Au fur et à mesure que les menaces évoluent, la sécurité d'une organisation doit elle aussi évoluer. Pour permettre à une organisation de rester au-dessus de ce scénario de menace en mouvement perpétuel, SANS a conçu un cours intensif et exhaustif qui enseigne comment implémenter les contrôles de sécurité critiques selon une approche hiérarchisée et basée sur le risque. Les contrôles, conçus par des experts du secteur privé et public du monde entier, représentent le meilleur moyen de bloquer des attaques connues et, le cas échéant, minimiser les dommages. Ils ont été adoptés par le Department of Homeland Security aux États-Unis, par des gouvernements d'État, des universités, et de nombreuses entreprises privées

Les contrôles sont des directives spécifiques pouvant être utilisées par les responsables de la sécurité informatique (CISO), les responsables de l'information (CIO), les généralistes informatiques, les administrateurs système et tout personnel de la sécurité informatique, pour gérer et mesurer l'efficacité de leurs défenses. Ils sont conçus en complément des normes, des cadres, et des plans de conformité existants; ils hiérarchisent les menaces les plus critiques et les défenses les plus rentables tout en apportant une référence de base pour mener des actions contre les risques auxquels nous sommes tous confrontés.

Les contrôles constituent un cadre de sécurité efficace parce qu'ils sont basés sur de véritables attaques perpétrées régulièrement contre des réseaux. La priorité est accordée aux contrôles qui (1) minimisent les attaques connues (2) répondent à une grande variété d'attaques, et (3) identifient et arrêtent les attaquants tôt dans le cycle de compromission.

Le Centre pour la protection des infrastructures nationales du Royaume-Uni décrit les contrôles comme étant "la référence en matière de mesures et de contrôles hautement prioritaires qui peuvent être appliqués à travers une organisation afin d'en améliorer la cyberdéfense".

VOUS APPRENDREZ À...

- Appliquer un cadre de sécurité basé sur des menaces réelles qui peut être mesuré, mis à l'échelle et sur lequel on pourra se fier pour stopper les attaques connues et pour protéger les informations et les systèmes cruciaux d'une organisation
- Comprendre l'importance de chaque contrôle, comment il peut être compromis s'il est ignoré; expliquer les objectifs de défense qui peuvent apporter des solutions rapides et augmenter la visibilité des systèmes et des réseaux
- Identifier et utiliser des outils qui implémentent les contrôles à l'aide de l'automatisation
- Apprendre comment créer un outil pour mesurer l'efficacité de chaque contrôle
- Utiliser des métriques spécifiques pour établir une ligne de base et mesurer l'efficacité des contrôles de sécurité
- Comprendre comment des contrôles critiques s'alignent sur des normes tels que NIST 800-53, ISO 27002, Top 35, et d'autres encore
- Auditer chacun des contrôles de sécurité critiques avec des modèles spécifiques éprouvés, des listes de contrôle, et des scripts fournis pour faciliter le processus d'audit

PUBLIC VISÉ :

- Commissaires aux comptes
- Concepteurs système ou administrateurs
- Ingénieurs de sécurité réseau
- Administrateurs IT
- Administrations d'État ou clients
- Secteur privé

« PROVIDES GREATER STRUCTURE TO THE BASIC CONTROLS. GOOD METHODOLOGY PROVIDED IN IMPLEMENTING CONTROLS. »
Jalal Moloo
DB SCHENKER

« I AM A NEW EMPLOYEE IN THIS FIELD. THIS COURSE GIVES ME REALLY GOOD KNOWLEDGE FOR MY WORK. »
Wafa Al Raisi

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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
- Mieux comprendre les principes et les fondements de la sûreté des renseignements (confidentialité, intégrité, disponibilité, authentification, non —répudiation)
- Utiliser vos compétences pour défendre les réseaux informatiques (détection de l'hôte et d'intrusions basées sur le réseau à l'aide des technologies de détection)
- Implémenter la gestion d'incident et des méthodologies de gestion

PUBLIC VISÉ :

- 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

« EVERY IT SECURITY PROFESSIONAL AND OTHERS WITHIN SUPPORT AND PROJECTS AROUND ICS SHOULD TAKE THIS COURSE. »

Simon Poole
SHELL

WWW.SANS.ORG/ICS410
Formation pratique | Cinq Jours | Ordinateur portable requis
30 CPE / CMU Crédits | GIAC Cert: GISCP

ICS 410

ICS/SCADA SECURITY ESSENTIALS

FORMATION ICS410

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

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.

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.

« GREAT INTRODUCTION INTO ICS LANDSCAPE AND ASSOCIATED SECURITY CONCERNS. THE ICS MATERIAL PRESENTED WILL PROVIDE IMMEDIATE VALUE RELATIVE TO HELPING SECURE MY COMPANY. »

Mike Poulos
COCA-COLA ENTERPRISES

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/ICS515
Formation pratique | Cinq Jours | Ordinateur portable requis
30 CPE / Crédits CMU

ICS 515

ICS ACTIVE DEFENCE AND INCIDENT RESPONSE

FORMATION ICS515

PRIVATE TRAINING*

DÉTAIL DU COURS

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

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

VOUS APPRENDREZ À...

- Examiner les réseaux ICS et identifier les actifs et leurs flux de données afin de comprendre les données de référence du réseau pour identifier des menaces avancées.
- Utiliser les concepts de défense active tels que l'utilisation de renseignements sur les menaces, la surveillance de la sécurité des réseaux, l'analyse des malwares et la gestion d'incident pour sauvegarder les ICS.
- Construire votre propre Programmable Logic Controller en utilisant un kit CYBATIworks
- Acquérir une expérience pratique sur des échantillons Havex, BlackEnergy2, et Stuxnet en déconstruisant ces menaces, et d'autres, dans un environnement contrôlé
- Optimiser des outils techniques, tels que Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analysers, malware sandboxes, et d'autres
- Créer des indicateurs de compromis (IOC) dans OpenIOC et YARA tout en comprenant les normes de partage d'information, telles que STIX et TAXII
- Tirer parti de modèles, tels que Sliding Scale of Cybersecurity, Active Cyber Defense Cycle, et ICS Cyber Kill Chain pour extraire des informations à partir des menaces et les utiliser pour garantir le succès à long terme de la sécurité des ICS

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

VOUS POURREZ...

- 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

PUBLIC VISÉ :

- Professionnels de la sécurité souhaitant se préparer à l'examen pour obtenir la certification CISSP®
- Tout professionnel, responsable et dirigeant soucieux de comprendre les concepts issus des huit domaines de connaissance et les secteurs 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

WWW.SANS.ORG/MGT414
Formation pratique | Deux Jours | Ordinateur portable requis
12 CPE / Crédits CMU

MGT 414

SANS TRAINING PROGRAM FOR CISSP® CERTIFICATION

FORMATION MGT414

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

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.

Après avoir complété ce cours, les élèves auront acquis:

- Une compréhension détaillée des 8 domaines de connaissance
- Les compétences analytiques nécessaires pour réussir l'examen CISSP®
- Les fondamentaux requis pour devenir un professionnel de la sécurité informatique certifié CISSP®.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

DEVANCEZ L'ENNEMI
RELEVEZ LE DÉFI !

NETWARS

NetWars propose une série de défis pratiques sur la sécurité des réseaux et des systèmes - des défis conçus pour tester les compétences et l'expérience des participants. Deux compétitions NetWars sont proposées: Core NetWars et DFIR Netwars; l'une porte sur les fondamentaux de la sécurité, l'autre sur l'inforensique et la gestion d'incident.

Core NetWars

Le tournoi SANS Netwars Fondamentaux est une suite de scénarios d'apprentissage pratiques et interactifs qui permettent aux professionnels de la sécurité de développer et de maîtriser les compétences concrètes dont ils auront besoin pour se surpasser dans leur domaine. Les cours SANS sont conçus par des experts; les participants témoignent de la haute valeur ajoutée des exercices pratiques qui accompagnent le cours. Core NetWars a élevé la barre, en mettant les participants en situation dans un environnement virtuel. Des équipes doivent surmonter différents niveaux de difficulté; tous les défis sont des exercices pratiques centrés sur la maîtrise des compétences que les professionnels de la sécurité informatique doivent appliquer tous les jours dans leur travail.

Public visé :

- Professionnels de la sécurité
- Administrateurs système
- Administrateurs réseau
- Hackers éthiques
- Penetration Testers
- Gestionnaires d'incident
- Auditeurs de sécurité
- Tout personnel impliqué dans l'évaluation des vulnérabilités
- Tout personnel des centres d'opérations sécuritaires (SOC)

DFIR NetWars

Le tournoi SANS DFIR NetWars est un simulateur d'incidents qui propose de nombreux défis faisant appel à l'investigation numérique et à la gestion d'incident. Le tournoi DFIR NetWars contient de nombreux défis qui nécessitent de conduire des investigations numériques sur l'hôte et sur les réseaux, ainsi que d'analyser la mémoire et les malwares. Ce tournoi a été élaboré par des gestionnaires d'incident et des analystes qui utilisent leurs compétences tous les jours pour enquêter sur des intrusions, réparer des failles et stopper le vol de données. Commencez par aiguiser vos compétences en équipe avant d'être confronté à un véritable incident.

Public visé :

- Analystes inforensiques
- Analystes de rétro-ingénierie et de malwares
- Personnel chargé de répondre aux incidents
- Forces de l'ordre, les agents du renseignement ou les enquêteurs
- Analystes et investigateurs numériques des centres d'opérations sécuritaires (SOC)
- Enquêteurs de cybercrimes
- Analystes d'exploitation de médias

sans.org/netwars

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

WWW.SANS.ORG/MGT433
Formation pratique | Deux Jours | Ordinateur portable requis
12 CPE / Crédits CMU

MGT 433

SECURING THE HUMAN:

COMMENT CONSTRUIRE, MAINTENIR ET MESURER UN PROGRAMME DE SENSIBILISATION À FORT IMPACT

FORMATION MGT433

PRIVATE TRAINING*

VOUS APPRENDREZ À...

- Identifier le degré de maturité des programmes de sensibilisation existants et décider dans quelle direction s'orienter par la suite
- Expliquer la différence entre la prise de conscience, l'éducation, et la formation
- Expliquer les trois variables différentes du risque et comment les appliquer au risque humain et aux programmes de sensibilisation à la sécurité
- Expliquer pourquoi les personnes sont vulnérables et comment les criminels exploitent ces vulnérabilités
- Élaborer une charte de projet et obtenir l'aval et le soutien de la direction pour un programme de sensibilisation à la sécurité
- Identifier les différents objectifs d'un programme de sensibilisation
- Caractériser la culture d'une organisation et déterminer les moyens de communication les plus efficaces pour cette culture
- Identifier, mesurer et hiérarchiser les risques humains
- Concevoir et implémenter des métriques clés pour mesurer l'impact d'un programme de sensibilisation
- Créer un programme efficace d'évaluation du phishing

PUBLIC VISÉ :

- Responsables de la sensibilisation à la sécurité
- Cadres dirigeants de la sécurité et représentants de la gestion de la sécurité
- Auditeurs de la sécurité et responsables de la bonne gouvernance et de la conformité
- Ressources humaines et personnel communicant
- Représentants d'organisations réglementées par des industries, telles que HIPAA, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, ou toute autre norme de conformité
- Toute personne impliquée dans la planification, le déploiement, ou le maintien d'un programme de sensibilisation à la sécurité

DÉTAIL DU COURS

Les organisations investissent des ressources énormes, tant matérielles que financières pour sécuriser la technologie, et paradoxalement peu, voire rien, pour sécuriser le personnel.

Par conséquent, les personnes, et non la technologie, sont devenues le maillon faible de la cybersécurité. Le moyen le plus efficace pour sécuriser le facteur humain est d'établir un programme à fort impact de sensibilisation à la sécurité - un programme qui va changer le comportement plutôt que se limiter à la simple mise en conformité

MGT433 est un cours intensif sur deux jours. Il enseigne les concepts clés et les compétences pour construire entretenir et mesurer un programme de sensibilisation à la sécurité. Tout le contenu du cours est fondé sur les leçons tirées par de centaines de programmes de sensibilisation à la sécurité dans le monde entier.

« GOOD COURSE WHETHER YOU ARE DEVELOPING TRAINING AND AWARENESS OR IMPROVING YOUR CURRENT SYSTEM. »
Tina Baker
AWE PLC

Les stagiaires acquièrent un savoir non seulement de leur formateur SANS, mais aussi des échanges intensifs qu'ils ont avec leurs collègues. De ce fait, les participants sont encouragés à apporter des exemples où des échantillons puisés dans leur propre programme de sensibilisation à la sécurité.

Finalement, en réalisant une série d'exercices pratiques, les stagiaires élaborent un plan de sensibilisation à la sécurité personnalisé qu'ils pourront mettre en pratique dès qu'ils seront de retour dans leur organisation.

« VALUABLE SKILLS LEARNT TO TAKE BACK AND APPLY IN MY SECURITY AWARENESS PROGRAMME. »
Cornelius Thiart
CONTRARIUS INVESTMENT ADVISORY

« THE COURSE PROVIDES AN EXCELLENT FRAMEWORK WITHIN WHICH ANY TYPE OF ORGANISATION CAN DEVELOP A SECURITY AWARENESS PROGRAMME THAT FITS IN WITH NEEDS. »
Mark James
UNIVERSITY OF BRISTOL

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

WWW.SANS.ORG/MGT512
Formation pratique | Cinq Jours | Ordinateur portable requis
30 CPE / CMU Crédits | GIAC Cert: GSLC

MGT 512

SECURITY LEADERSHIP ESSENTIALS FOR MANAGERS

WITH KNOWLEDGE COMPRESSION™

FORMATION MGT512

PRIVATE TRAINING*

DÉTAIL DU COURS

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

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.

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

« 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

« WAS ABLE TO MERGE MANAGEMENT SKILLS AND TECHNICAL MATERIALS IN ONE A SIMPLE FORMAT. »
Abdulaziz Al-Sultan
SAUDI ELECTRIC COMPANY

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea
(nombre minimum de participants requis)

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
- Développer des stratégies pour évaluer la posture de sécurité de multiples applications web

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

WWW.SANS.ORG/DEV522
Formation pratique | Six Jours | Ordinateur portable requis
36 CPE / CMU Crédits | GIAC Cert: Gweb

DEV 522

DEFENDING WEB APPLICATIONS SECURITY ESSENTIALS

FORMATION DEV522

PRIVATE TRAINING*

ONDEMAND

« GIVES A GOOD LEVEL OF TRAINING FOR DEFENDING WEB APPS »
Kar Hopkinson -Turrell QA

« DEV522 REALLY COVERS THE SECURITY ASPECTS EVERY WEB DEVELOPER MUST KNOW »
Daniel Abrahamsson KLARNA AB

DÉTAIL DU COURS

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.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea (nombre minimum de participants requis)

WWW.SANS.ORG/DEV544
Mains | Cinq Jours | Ordinateur portable requis
30 CPE / CMU Crédits | GIAC Cert: GSSP-.NET

DEV 544

SECURE CODING IN .NET : DEVELOPING DEFENSIBLE APPLICATIONS

FORMATION DEV544

PRIVATE TRAINING*

ONDEMAND

DÉTAIL DU COURS

ASP.NET et .NET Framework ont fournit aux développeurs web des outils leur apportant un degré de flexibilité et de productivité sans précédent. Cependant, ces outils sophistiqués génèrent aussi des problèmes. Il est plus facile que jamais d'oublier de petits détails qui vont se transformer en vulnérabilités. Depuis ASP.NET 2.0, Microsoft a fait un travail gigantesque pour intégrer la sécurité dans ASP.NET, mais l'ultime responsabilité d'assurer que le code est sécurisé repose toujours sur les développeurs d'applications qui doivent comprendre les limites de Framework.

Vous êtes-vous déjà demandé si la validation intégrée ASP.NET était efficace? Vous êtes-vous déjà senti concerné par la possibilité que les services web puissent introduire des problèmes de sécurité non détectés dans votre application? Ne devriez-vous pas vous sentir mal à l'aise si vous vous fiez uniquement aux contrôles de sécurité intégrés dans ASP.NET Framework? Le cours Secure Coding in .Net va apprendre aux stagiaires à tirer parti des technologies intégrées et des technologies défensives adaptables, qu'ils pourront intégrer dans leurs propres applications.

LE CONTENU DU COURS :

Ce cours est exhaustif car il aborde un vaste ensemble de connaissances et de compétences. Il s'agit non pas d'un cours de théorie de haut niveau, mais de véritable programmation. Dans ce cours vous allez analyser du code réel, travailler avec de vrais outils, construire des applications, et gagner en confiance, car vous allez être équipé de ressources qui vous accompagneront tout au long de votre parcours pour améliorer la sécurité des applications .NET.

Nous préférons enseigner aux stagiaires les concepts de la programmation sécurisée plutôt que de limiter notre intervention à l'enseignement du simple usage d'une boîte à outils. Le cours consiste à examiner un morceau de code spécifique, à identifier une faille de sécurité, et à implémenter une correction pour les failles résultant des erreurs de programmation les plus dangereuses, listées dans OWASP Top 10 et CWE/SANS Top 25.
Le cours se termine par l'analyse de la sécurité d'une application réelle en open source. Vous allez examiner un code, lire un rapport de test d'intrusion, tester la sécurité en exploitant de réelles vulnérabilités, et enfin utiliser des techniques de codage sécurisées, apprises en classe pour corriger ces problèmes.

PCI COMPLIANCE

La section 6.5 des normes de l'industrie des cartes de paiement concernant la sécurité des données (PCI DSS) demande aux auditeurs de vérifier que des processus sont en place - des processus qui exigent que les développeurs soient formés aux techniques de codage sécurisées. Si votre application traite les données d'un détenteur de carte de paiement et vous devez répondre aux normes de conformité PCI, alors ce cours est pour vous.

Pour connaître les dates de formation, rendez-vous sur www.sans.org/emea (nombre minimum de participants requis)

PUBLIC VISÉ :

Ce cours est conçu pour :

- Les développeurs ASP.NET qui veulent construire des applications web plus sûres
- Développeurs .NET Framework
- Ingénieurs logiciel
- Architectes logiciel
- Les développeurs qui ont besoin de se former à des techniques de codage sécurisées afin d'être conformes aux normes PCI

Ce cours est centré spécifiquement sur le développement de logiciel, mais il est relativement accessible à quiconque est capable de travailler avec du code et a un intérêt à comprendre le point de vue du développeur. Peuvent être inclus:

- Les auditeurs de la sécurité des applications
- Les chefs de projet technique
- Les spécialistes QA des logiciels seniors
- Les testeurs d'intrusion qui veulent une meilleure compréhension des méthodes de ciblage ASP.NET des applications web ou qui souhaitent apporter des solutions plus exhaustives pour corriger les vulnérabilités

FORMATION DE SENSIBILISATION À LA SÉCURITÉ

Changez le comportement humain • Gérez le risque
Opérez en toute conformité • Protégez votre marque

La formation SANS Securing The Human est conçue pour sensibiliser vos salariés à la cybersécurité et les transformer en défenseurs actifs.

Securing The Human est une formation web qui prépare vos salariés à reconnaître et à réagir correctement aux cybermenaces prédominantes d'aujourd'hui. Le programme de formation comporte des solutions globales pour éduquer les utilisateurs finaux, les développeurs, les ingénieurs ICS, le personnel des secteurs de l'énergie, et les professionnels du monde médical.

La formation se présente sous forme de vidéos interactives et utilise des quizz pour vérifier que le salarié a bien retenu ce qu'il a appris. Securing The Human se décline en plus de 20 langues.

Securing The Human Key Benefits offre de nombreux avantages:

- **Adapté aux fonctions** – construisez des programmes de formation sur mesure pour des groupes de salariés spécifiques
- **Une plateforme d'accueil fiable et sûre** – l'infrastructure SANS garantit que la formation est toujours disponible et dispensée de façon sécurisée
- **Un côté pratique** – une formation condensée, disponible en modules vidéo de courte durée qui permettent aux salariés de suivre la formation à leur rythme
- **Une formation de sensibilisation à la sécurité, tout-en-un** - la solution de formation clés-en-main pour les organisations qui cherchent un programme préétabli
- **Une formation à votre image** – les programmes de formation peuvent être personnalisés avec votre logo d'entreprise et intégrer des documents et des liens pertinents
- **Des fonctionnalités claires et instructives** – des tableaux de bord et des rapports générés en arrière-plan permettent aux dirigeants de suivre et d'évaluer l'efficacité du programme de sensibilisation
- **Production automatique de rapports et émission de rappels** – les dirigeants sont assurés que tout le personnel est incité à suivre la formation et que des rappels sont envoyés, si nécessaire

Que vous soyez une PME qui veut être en conformité, ou une entreprise d'envergure qui cherche à sensibiliser ses salariés à la sécurité, SANS vous propose un niveau de service adapté.

Nos concepteurs du programme SANS offrent la vision et le soutien nécessaires aux organisations qui veulent élaborer un programme de sensibilisation, le déployer, puis en mesurer l'impact.

Pourquoi faire appel à SANS?

Nous aidons les entreprises à mettre en place un programme de sensibilisation à fort impact ; SANS organise des évènements de formation en cybersécurité et propose des ressources expertes, des outils de formation, ainsi que l'accès à notre plateforme communautaire de sensibilisation à l'échelle mondiale. Rendez-vous sur www.securingthehuman.org/resources/getting-support

« SANS SECURING THE HUMAN IS A BLESSING. WE ARE THANKFUL FOR THE SYSTEM'S EASY USE AND ACCESS. THE FACT THAT EMPLOYEES CAN TAKE THE TRAINING 24/7 IS A PLUS. »

Nic Lee
NORTHROP GRUMMAN IS

www.securingthehuman.org

Pour plus d'informations sur le programme, regarder une démo, ou pour obtenir des conseils sur la mise en place d'un programme de sensibilisation, n'hésitez pas à faire appel à notre équipe d'experts:
Tel: +44 203 33 84 34 70, Courriel : awarenesstraining@sans.org