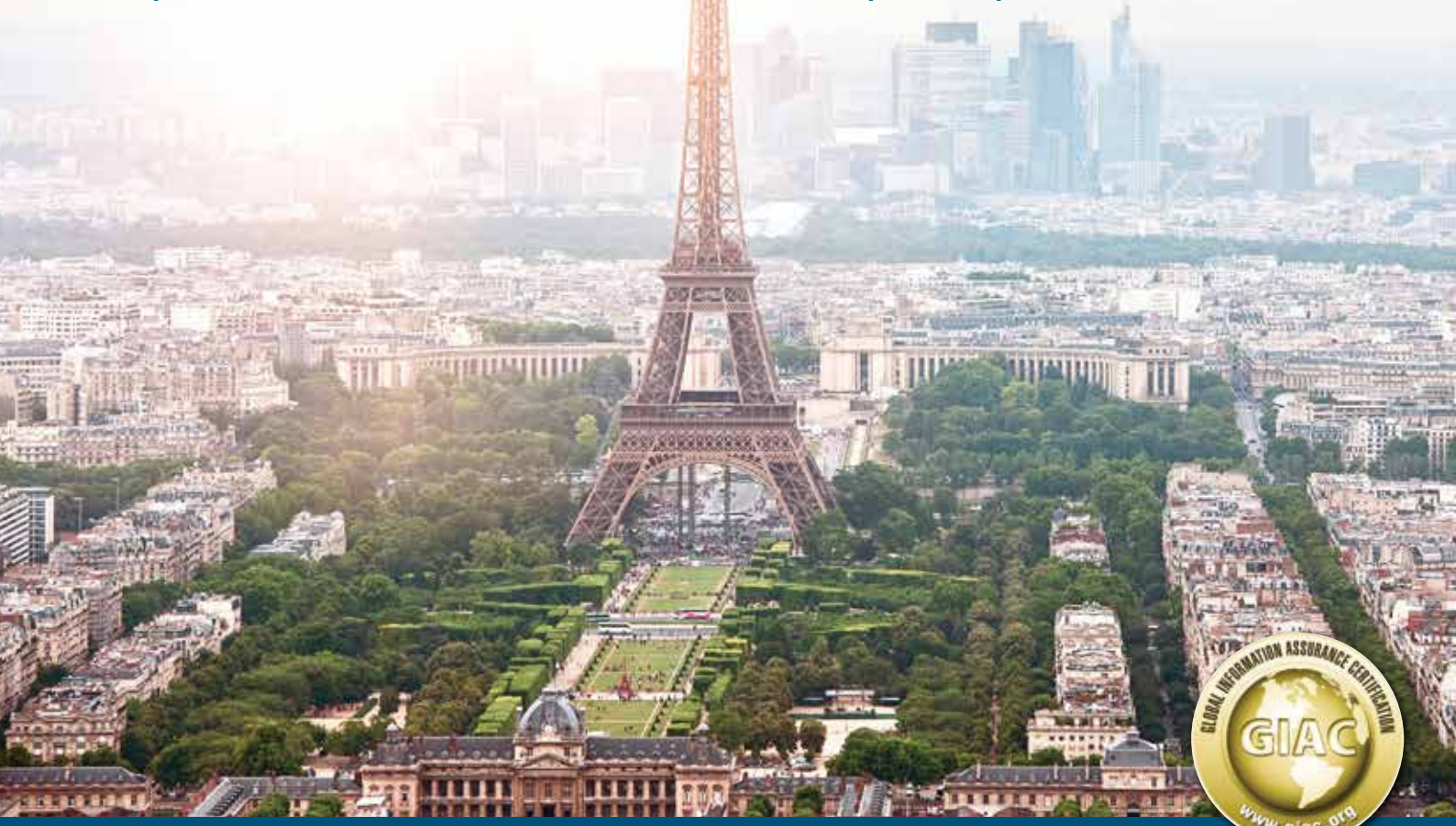
★ LA RÉFÉRENCE MONDIALE EN MATIÈRE DE FORMATION, RECHERCHE ET CERTIFICATION, ★
À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

SANS EMEA

26 JUIN – 1 JUILLET, 2017 #SANSPARIS

SANS PARIS 2017

Préparez-vous à la certification GIAC – Formations dispensées par nos formateurs SANS



INSCRIVEZ-VOUS EN LIGNE ET VOIR LES DESCRIPTIONS DETAILLÉES DES COURS SUR
WWW.SANS.ORG/PARIS-2017

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.
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

BIENVENUE À SANS PARIS 2017

SANS PARIS 2017 DU LUNDI 26 JUIN AU SAMEDI 1ER JUILLET À PARIS MARRIOTT RIVE GAUCHE HÔTEL 6 COURS DU PROGRAMME SANS SONT PROPOSÉS.

Les frais d'inscription incluent des pauses et le déjeuner, mais n'incluent pas l'hébergement.

Visitez: **www.sans.org/event/paris-2017**

LIEU

HOTEL
Paris Marriott Rive Gauche
Hotel and Conference Centre
17 Boulevard Saint Jacques
Paris,
75014 FR

FORMATIONS

		LUN 26	MAR 27	MER 28	JEU 29	VEN 30	SAM 01
FOR 408	WINDOWS FORENSIC ANALYSIS (In English)	●	●	●	●	●	●
FOR 508	ADVANCED DIGITAL FORENSICS, INCIDENT RESPONSE, AND THREAT HUNTING (In English)	●	●	●	●	●	●
ICS 515	ICS ACTIVE DEFENSE AND INCIDENT RESPONSE (In English)	●	●	●	●	●	●
SEC 401	SECURITY ESSENTIALS BOOTCAMP STYLE (In English)	●	●	●	●	●	●
SEC 504	HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING (Dispensée en français*)	●	●	●	●	●	●
SEC 560	NETWORK PENETRATION TESTING AND ETHICAL HACKING (In English)	●	●	●	●	●	●

*CETTE FORMATION SERA DISPENSÉE EN FRANÇAIS ET LES SUPPORTS DE COURS SERONT EN ANGLAIS

VOUS ALLEZ APPRENDRE À

- Utiliser toute une méthodologie et une panoplie d'outils d'expertise inforensique permettant d'analyser la moindre action accomplie par un suspect sur un système Windows dans le détail, notamment: Déterminer qui a placé un artefact sur le système et comment, 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 grâce à l'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 grâce à l'analyse des artefacts Windows tels que le registre et les fichiers journaux.

PUBLIC VISÉ

- Les professionnels de la sécurité de l'information
- Membres d'une équipe de réponse aux incidents
- Les représentants des forces de l'ordre, les agents du renseignement, de la justice et d'autres administrations de l'État chargés d'enquêtes
- Les analystes spécialisés dans l'exploitation des médias
- Toute personne souhaitant approfondir sa compréhension de l'inforensique pour Windows

REGISTER NOW:
www.sans.org/paris-2017

WWW.SANS.ORG/FOR408
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GCFE

FOR 408

WINDOWS FORENSIC ANALYSIS

DISPENSÉE EN ANGLAIS

DÉTAILS DU COURS

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. SEC408 vous apprend à exploiter cette source de données.

Une bonne analyse exige des données réelles. Le cours FOR408 complètement actualisé forme les analystes inforensique à l'aide de nouveaux exercices pratiques réalisés en laboratoire,qui intègrent 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 qui soient. Les participants apprennent à faire une analyse exhaustive sur les systèmes hérites Windows XP afin de découvrir les artefacts de Windows 10.

FOR408 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 gratuite, open-source, et des outils commerciaux fournis dans le 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

WWW.SANS.ORG/FOR508
Hands On | Six Days | Laptop Required
36 CPE/CMU Credits | GIAC Cert: GCFA

FOR 508

ADVANCED DIGITAL FORENSICS AND INCIDENT RESPONSE

DISPENSÉE EN ANGLAIS

DÉTAILS 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 ont fouillé le réseau sans être détectés pendant des mois, voire des années.

Les tactiques et les procédures de réponse aux incidents ont rapidement évolué au cours des dernières années. Les brèches 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 chasser, contrer et réparer un large éventail de menaces contre les réseaux d'entreprise. Les situations étudiées incluent des adversaires 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 kit à outils SANS SIFT Workstation.

Pendant les exercices pratiques d'intrusion, 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

VOUS ALLEZ APPRENDRE 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 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.
- Utiliser la mémoire du système et le kit d'outils Volatility pour trouver les malwares actifs sur un système, déterminer comment le malware a été placé, le récupérer pour en tirer la « threat intelligence » dans le but de délimiter un champ d'action lors d'une réponse à un incident.
- Détecter des capacités avancées, telles que Stuxnet, TDSS, ou les commandes APT ; neutraliser immédiatement les malwares 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 l'organisation, et de déterminer la véritable portée d'une violation de données.
- Suivre les empreintes digitales précises d'un assaillant sur de multiples systèmes et analyser les données collectées.
- Suivre les mouvements d'un adversaire sur un réseau via l'analyse historique « timeline » en utilisant les outils log2timeline.
- Procéder à la récupération et la réparation de la compromission à l'aide aux indicateurs de compromission (IOC) et aux techniques IR/Forensics essentielles permettant d'identifier les malwares actifs et tous les systèmes de l'entreprise qui ont été compromis.
- Effectuer une réparation des système de fichiers à l'aide de l'outil Sleuth Kit pour découvrir leur fonctionnement , ainsi que des artefacts puissants tels que les index de répertoire de fichiers NTFS $130, « journal parsing », et l'analyse de Master File Table.

PUBLIC VISÉ

- Membres d'une équipe de réponse aux incidents
- 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 « Red Team », les testeurs d'intrusion, et les développeurs d'exploits

REGISTER NOW:
www.sans.org/paris-2017

VOUS ALLEZ APPRENDRE À

- Examiner les réseaux ICS et identifier les actifs et leurs flux de données afin de comprendre les données de référence du réseau pour identifer 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

- Membres d'équipes de réponse aux incidents ICS
- Le personnel des services de sécurité OT et ICS
- Les professionnels de la sécurité IT
- Membres d'une équipe de sécurité opérationnelle (SOC)
- Membres d'une équipe « Red Team » ICS et Testeurs d'intrusion

REGISTER NOW:
www.sans.org/paris-2017

WWW.SANS.ORG/ICS515
Hands On | Five Days | Laptop Required
30 CPE/CMU Credits

ICS 515

ICS ACTIVE DEFENCE AND INCIDENT RESPONSE

DISPENSÉE EN ANGLAIS

DÉTAILS 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 incluent la « threat intelligence » la mise en place d'une surveillance de la sécurité des réseaux, ainsi que l'analyse de malwares et la réponse d'incident pour assurer la sécurité et la fiabilité des opérations.

Vous saurez :

- Mettre en place une gestion d'incident focalisée sur la sécurité des opérations et qui hiérarchise la sécurité et la fiabilité des opérations
- Comment la "threat intelligence" ICS est générée et comment 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 anormalités 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

WWW.SANS.ORG/SEC401
Hands On | Six Days | Laptop Required
46 CPE/CMU Credits | GIAC Cert: GSEC

SEC 401

SECURITY ESSENTIALS BOOTCAMP STYLE

DISPENSÉE EN ANGLAIS

DÉTAILS DE LA FORMATION

SEC401 met l'accent sur l'enseignement des mesures nécessaires pour prévenir les attaques et détecter les adversaires. Ce cours enseigne des techniques applicables 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, il est pratiquement inévitable que les organisations soient 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 défense, 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 immédiatement 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

VOUS ALLEZ APPRENDRE 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 inclurent 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 informatique
- 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 de connaître les fondamentaux de la sécurité pour être aussi performants que possible dans leur travail
- Toute personne nouvelle dans le domaine de la sécurité informatique ayant une certaine expérience des systèmes d'information et des réseaux

REGISTER NOW:
www.sans.org/paris-2017

VOUS ALLEZ APPRENDRE 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 les 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 d'équipe de gestion d'incident, les testeurs d'intrusion, les hackers éthiques,
- Les administrateurs système en première ligne de réponse et de défense
- Les architectes de sécurité
- Tout autre personnel de sécurité intervenant en premier lieu lors de l'attaque d'un système

REGISTER NOW:
www.sans.org/paris-2017

WWW.SANS.ORG/SEC504
Hands On | Six Days | Laptop Required
37 CPE/CMU Credits | GIAC Cert: GCIH

SEC 504

HACKER TOOLS, TECHNIQUES, EXPLOITS AND INCIDENT HANDLING

CETTE FORMATION SERA DISPENSÉE EN FRANÇAIS ET LES SUPPORTS DE COURS SERONT EN ANGLAIS

DÉTAILS DU COURS

La probabilité d'un piratage 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 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, ainsi que les attaques les plus élémentaires qui n'en restent pas moins toujours d'actualité, et entre ces deux extrêmes, diverses méthodes criminelles seront abordées. 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 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 comprendre et comment concevoir, créer et se servir de leurs systèmes pour éviter les attaques, les détecter et y répondre de manière efficace.

"VERY STRUCTURED AND WELL PREPARED COURSE. INTERESTING AND ENGAGING FOR PEOPLE NEW TO THE FIELD AS WELL AS EXPERIENCED PROFESSIONALS"
Ewe Konkolska
PRUDENTIAL

WWW.SANS.ORG/SEC560
Hands On | Six Days | Laptop Required
37 CPE/CMU Credits | GIAC Cert: GPEN

SEC 560

NETWORK PENETRATION TESTING AND ETHICAL HACKING

DISPENSÉE EN ANGLAIS

DÉTAILS 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 ces 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 il se poursuit avec 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, puisées dans le monde réel.

Les stagiaires apprennent à scanner les réseaux cibles 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.

Après le scan, les stagiaires apprennent des dizaines de méthodes pour exploiter des systèmes cibles. Le cours SEC560 explore comment accéder à ces systèmes et mesurer le 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'une organisation cible.

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

VOUS ALLEZ APPRENDRE 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 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 représnter le risque commercial que court l'organisation.
- Analyser les résultats produits par les outils d'analyse pour effectuer une vérification manuelle et réduire les faux positifs à l'aide des outils Netcat et Scapy packet.
- Pousser les tests d'intrusion plus loin en utilisant les lignes de commande Windows et Linux pour exploiter les systèmes cible afin d'en extraire des informations capitales, établir des pivots permettant de démultiplier les atteintes, et aider l'entreprise à déterminer les risques.
- 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
- Auditeurs qui ont besoin d'acquérir des compétences techniques plus approfondies
- Membres « Red Team »
- Membres « Blue Team »

REGISTER NOW:
www.sans.org/paris-2017

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

CORE COURSES

FUNCTION: INFORMATION SECURITY

Les professionnels de la sécurité informatique sont chargés de faire la recherche et l'analyse des menaces de sécurité qui peuvent mettre en danger les actifs, les produits ou les spécificités techniques d'une organisation.

Grâce à une formation pointue, ces professionnels de la sécurité vont explorer, de façon bien plus approfondie que la plupart de leurs collègues, les protocoles et les spécificités techniques liés aux menaces afin de déterminer des stratégies de défense contre les attaques.

EXEMPLES:
Cyber Security Analyst , Cyber Security Engineer, Cyber Security Architect

- **SEC301** Intro to Information Security GISF
- **SEC401** Security Essentials Bootcamp Style GSEC
- **SEC501** Advanced Security Essentials Enterprise Defender GCED

FUNCTION: NETWORK OPERATIONS CENTRE, SYSTEM ADMIN, SECURITY ARCHITECTURE

Un Network Operations Center (NOC) est un centre opérationnel où des professionnels de l'informatique encadrent, surveillent et mettent à jour les réseaux d'une entreprise. Ils effectuent des diagnostics de réseau en cas de problème, des mises à jour et la distribution de logiciels, la gestion des systèmes et des routeurs ; ils veillent au bon fonctionnement et à la coordination de réseaux liés. Les analystes NOC travaillent en liaison étroite avec le Security Operations Center (SOC) qui est chargé de la protection de l'entreprise et assure une surveillance en continu contre les menaces.

EXEMPLES:
Security Analyst / Engineer, SOC Analyst, Cyber Threat Analyst, CERT Member, Malware Analyst

CORE COURSES
SEC301 GISF › SEC401 GSEC › SEC501 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** Virtualisation and Private Cloud Security

FUNCTION: SECURITY OPERATIONS CENTRE/ INTRUSION DETECTION

Le SOC est un centre opérationnel chargé de la détection d'intrusions, de la protection contre les incidents liés à une cyberattaque, de la veille sécuritaire, et de la protection des actifs du réseau de l'organisation et de ses terminaux. Les analystes SOC sont chargés de la sensibiliser l'entreprise aux situations, et de la surveillance continue, notamment la surveillance du trafic, le blocage de trafic Internet indésirable entrant et sortant, et la détection de tout type d'attaque. Les technologies de solution de sécurité sont le point de départ pour rendre les réseaux plus résistants aux tentatives d'intrusion potentielles.

CORE COURSES
SEC301 › SEC401

- **SEC504** Hacker Tools, Techniques, Exploits, & Incident Handling GCIH

EXEMPLES:
Intrusion Detection Analyst, Security Operations Centre Analyst / Engineer, CERT Member, Cyber Threat Analyst

Endpoint Monitoring
- **SEC501** Advanced Security Essentials - Enterprise Defender GCED
- **FOR508** Advanced Digital Forensics and Incident Response GCFA

Network Monitoring
- **SEC503** Intrusion Detection In-Depth GCIA
- **FOR572** Advanced Network Forensics and Analysis GNFA
- **SEC511** Continuous Monitoring and Security Operations GMON
- **SEC550** Active Defense, Offensive Countermeasurers, & Cyber Deception

Threat Intelligence
- **FOR578** Cyber Threat Intelligence

FUNCTION: RISK & COMPLIANCE/AUDITING/ GOVERNANCE

Ces experts évaluent et font des rapports de risque pour l'organisation en mesurant la conformité aux politiques, procédures et normes. Ils font des recommandations d'amélioration pour rendre l'organisation plus efficace et plus rentable à l'aide de contrôles permanents de la gestion du risque.

EXEMPLES:
Auditor, Compliance Officer

- **MGT433** Securing The Human: Building and Deploying an Effective Security Awareness Programme
- **SEC566** Implementing & Auditing the Critical Security Controls - In-Depth GCCC
- **AUD507** Auditing & Monitoring Networks, Perimeters, and Systems GSNA
- **LEG523** Law of Data Security and Investigations GLEG

FUNCTION: INCIDENT RESPONSE AND THREAT HUNTING

Lorsque la sécurité d'un système ou d'un réseau est compromise, la personne chargée de répondre aux incidents est en première ligne de défense pendant la brèche. Celui qui répond n'est pas seulement ingénieux sur le plan technique, il doit aussi gérer le stress généré par l'incident, s'occuper des personnes, des processus et des technologies afin de répondre de façon rapide et efficace et de minimiser les dommages causés par l'incident.

EXEMPLES:
Security analyst/engineer, SOC analyst, Cyber threat analyst, CERT member, Malware analyst

CORE COURSES
SEC301 GISF › SEC401 GSEC

- **SEC504** Hacker Tools, Techniques, Exploits and Incident Handling GCIH

Network Analysis
- **SEC503** Intrusion Detection In-Depth GCIA
- **FOR572** Advanced Network Forensics and Analysis GNFA

Endpoint Analysis
- **FOR408** Windows Forensic Analysis GCFE
- **FOR508** Advanced Digital Forensics and Incident Response GCFA

Malware Analysis
- **FOR610** Reverse Engineering Malware: Malware Analysis Tools & Techniques GREM

- **FOR578** Cyber Threat Intelligence

Specialisations
- **FOR526** Windows Memory Forensics In-Depth
- **MGT535** Incident Response Team Management

FUNCTION: PENETRATION TESTING/ VULNERABILITY ASSESSMENT

Parce que la meilleure défense consiste à connaître ses adversaires et ses propres faiblesses, ces experts apportent une énorme valeur ajoutée à l'organisation. Ils appliquent diverses techniques d'attaque leur permettant de trouver les points de vulnérabilité, évaluent le risque encouru par l'organisation, et recommandent des solutions de protection avant que ces failles ne soient exploitées par de véritables hackers.

EXEMPLES:
Penetration tester, Vulnerability assessor, Ethical hacker, Red/Blue team member, Cyberspace engineer

CORE COURSES
SEC301 GISF › SEC401 GSEC

- **SEC504** Hacker Tools, Techniques, Exploits and Incident Handling GCIH
- **SEC550** Active Defense, Offensive Countermeas-ures & Cyber Deception

Network & Exploits
- **SEC560** Network Penetration Testing and Ethical Hacking GPEN
- **SEC660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking GXPN
- **SEC760** Advanced Exploit Development for Penetration Testers

Web
- **SEC542** Web App Penetration Testing and Ethical Hacking GWAPT
- **SEC642** Advanced Web App Penetration Testing and Ethical Hacking

Mobile / Wireless
- **SEC575** Mobile Device Security and Ethical Hacking GMOB
- **SEC617** Wireless Ethical Hacking, Penetration Testing, and Defenses GAWN

Lab Centred
- **SEC561** Immersive Hands-on Hacking Techniques
- **SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise

Specialisations
- **SEC567** Social Engineering for Penetration Testers
- **SEC580** Metasploit Kung Fu for Enterprise Pen Testing
- **SEC573** Python for Penetration Testers GPYC

FUNCTION: SECURE DEVELOPMENT

Le développeur, expert en matière de sécurisation des logiciels, encourage naturellement tous ses collègues développeurs à concevoir des logiciels sécurisés et à implémenter des techniques de programmation sécurisées ne comportant pas de faille du point de vue de la conception et de la mise en application technique. L'expert a l'ultime responsabilité d'assurer que le logiciel de son client ne comporte aucune vulnérabilité pouvant être exploitée par un assaillant.

EXEMPLES:
Developer, Software Architect, QA Tester, Development Manager

Core
- **Securing the Human for Developers STH. Developer** Application Security Awareness Modules
- **DEV522** Defending Web Applications Security Essentials GWEB
- **DEV531** Defending Mobile Applications Security Essentials
- **DEV534** Secure DevOps: A Practical Introduction

Secure Coding
- **DEV541** Secure Coding in Java/JEE GSSP-JAVA
- **DEV544** Secure Coding in .NET GSSP-.NET
- **DEV543** Secure Coding in C/C++

Specialisations
- **SEC542** Web App Penetration Testing & Ethical Hacking GWAPT
- **SEC642** Advanced Web App Penetration Testing & Ethical Hacking

FUNCTION: CYBER OR IT SECURITY MANAGEMENT

La gestion du personnel, des processus et des technologies est essentielle pour maintenir de façon proactive une sensibilisation à la sécurité dans l'organisation et pour assurer une surveillance continue efficace. Ces dirigeants doivent avoir des connaissances actualisées et des compétences en matière de leadership ; ils se doivent d'être exemplaires, en appliquant des pratiques exemplaires, et capables de prendre des décisions au bon moment, des décisions efficaces qui profiteront à la totalité de l'infrastructure de l'information de l'entreprise.

EXEMPLES:
CISO, Cyber Security Manager / Officer, Security Director

Foundational
- **MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ GSLC
- **MGT525** IT Project Management, Effective Communica-tion, and PMP® Exam Prep GCPM
- **MGT414** SANS Training Programme for CISSP® Certification GISP

Core
- **MGT514** IT Security Strategic Planning, Policy & Leadership
- **MGT535** Incident Response Team Management
- **LEG523** Law of Data Security and Investigations GLEG
- **MGT415** A practical Introduction to Cybersecurity Risk Management

Specialisation
- **MGT433** Securing The Human: Building and Deploying an Effective Security Awareness Programme
- **AUD507** Auditing & Monitoring Networks, Perimeters, and Systems GSNA
- **SEC566** Implementing and Auditing the Critical Security Controls - In-depth GCCC

FUNCTION: DIGITAL FORENSIC INVESTIGATIONS & MEDIA EXPLOITATION

De nos jours, en raison de l'évolution perpétuelle des technologies et des environnements, il est inévitable que toute organisation doive faire face à la cybercriminalité, notamment en matière de fraude, de menaces internes, d'espionnage industriel et d'hameçonnage (phishing). Pour relever ces défis, les organisations recrutent des professionnels de l'investigation inforensique et elles s'appuient aussi sur des agents de lutte contre la cybercriminalité pour reconstituer dans le détail l'attaque qui a été commise.

EXEMPLES:
Computer Crime Investigator, Law Enforcement, Digital Investigations Analyst, Media Exploitation Analyst, Information Technology Litigation Support & Consultant, Insider Threat Analyst

- **FOR408** Windows Forensic Analysis GCFE
- **SEC504** Hacker Tools, Techniques, Exploits and Incident Handling GCIH
- **FOR508** Advanced Digital Forensics and Incident Response GCFA
- **FOR585** Advanced Smartphone Forensics GASF
- **FOR518** MAC Forensic Analysis
- **FOR526** Memory Forensics In-Depth

FUNCTION: INDUSTRIAL CONTROL SYSTEMS

ICS-focused courses are designed to equip both security professionals and control system engineers with the knowledge & skills they need to safeguard critical infrastructure.

- **ICS410** ICS/SCADA Security Essentials GICSP
- **ICS515** ICS Active Response and Defense & Response GRID

EXEMPLES:
IT & OT Support, IT & OT Cyber Security, ICS Engineer