DOCAPOSTE Institute

Analyste SOC (Security Operation Center)

Présentation

Il s'agit d'un cours très pratique qui met en avant les techniques d'attaque les plus avancées. L'enjeu consistant à détecter (voire les anticiper), et les corriger en apportant la riposte la plus efficace et efficiente.
Le cours s'appuie sur des attaques réelles dans un environnement sandboxé (virtuel et protégé pour des questions de sécurité), à partir d'un outil dédié (un SIEM : Security Information & Event Management). Tous les composants du système d'information sont ciblés : serveurs Web, clients, réseaux, firewall, bases de données...

Cette formation est divisée en deux parties :

- La première concerne une présentation de l'organisation, les concepts, les méthodes, les techniques, les outils.
- La seconde consiste en une application au sein d'un outil de détection et de gestion de type SIEM (IBM Qradar et/ou Splunk au choix), avec introduction de malwares (entre autres) et gestion de la détection et de la correction.

Durée : 56,00 heures (8 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

- Connaître l'organisation d'un SOC
- Comprendre le métier d'analyste SOC
- Appréhender les outils utilisés par les analystes SOC
- Identifier les principales problématiques à travers des cas d'usage
- Apprendre à détecter des intrusions
- Savoir gérer différents incidents
- Optimiser la sécurité d'un système d'information

Prérequis

- Connaître le guide sécurité de l'ANSSI,
- Avoir des connaissances en réseau,

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.

Public

- Techniciens et administrateurs Systèmes et Réseaux
- Responsables informatiques
- Responsables techniques
- RSSI (responsables de la sécurité des systèmes d'information)
- Consultants en sécurité de l'information
- Architectes réseaux

Programme de la formation

1. Comprendre l'organisation et le métier d'analyste SOC : les enjeux, les méthodes, l'organisation, les rôles et responsabilités, les outils

- Qu'est-ce qu'un SOC : Security Operation Center.
- Son usage, sa fonction, ses avantages et bénéfices
- Les fonctions du SOC : Logging, Monitoring, Reporting audit et sécurité, analyses post incidents.
- L'organisation et les outils d'un SOC
- Les différents types de SOC
- Le SIM (Security Information Management).
- Le SIEM (Security Information and Event Management).
- Le SEM (Security Event Management).

Workshops :

- *Exercice pratique : définir la fiche de poste d'un analyste SOC. Sa mission, ses compétences*
- *Exercice pratique : conception d'une stratégie de monitoring sur la base de la détection d'événements et la qualification en incidents pour traitement*

2. Maîtriser les protocoles et techniques d'attaques

- Les protocoles réseaux
- Notions avancées sur IP, TCP et UDP, ARP et ICMP
- Les paquets IP, le routage, le source. routing
- La fragmentation IP et les règles de réassemblage.
- Les Access Control Lists, le filtrage

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- La sécurisation physique (sizing) et logique (système d'exploitation, application) du serveur
- Les mesures de sécurité sur l'ensemble des composants : la porte ISO 27 001, ISO 27011 ainsi que le cadre de cyber sécurité du NIST
- Les outils de renforcement de la sécurité du réseau

Exercice : analyse du trafic d'un réseau. Analyse d'une anomalie. Utilisation d'un sniffer de type Wireshark.

3. Les différents types d'attaques : réseau

- Utilisation d'ICMP et de SNMP comme un vecteur d'attaque, les covert chanels
- Le spoofing IP, ARP et DNS
- Les attaques par déni de service, Distributed DoS (Denial of Service), les Syn Flood
- Le Man in the Middle et le Meet in the Middle
- Le fraggle, le teardrop
- Le TCP
- Le TCP Hijacking

Workshops :

- *Exercice pratique : Application d'ICMP et de SNMP. Repérage ou création d'attaque sur le réseau de type déni de service, Fraggle ou Man in the Middle*
- *Exercice pratique : comment exfiltrés des informations privées et personnelles à partir d'un navigateur, à partir d'ICMP*

4. Détecter et corriger des incidents et des fuites de données

- La gestion des incidents selon ISO 27 035
- La notion d'événement et de incidents. Classification selon leur impact et leur urgence de traitement.
- Le paramétrage des paliers d'alerte
- Les backdoors (& maintenance hook)
- Virus, vers, chevaux de troie
- Les attaques de type XSS et CSRF

Workshops :

- *Exercice pratique : analyse d'un flux de type baseline d'un SIEM. Détection et traitement des événements et des anomalies.*
- *Exercice pratique : détection et traitement d'un malware de type de virus, vers ou cheval de Troie. Investigation confinement et full recovery.*
- *Exercice pratique : détecter et traiter une fuite de données*

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

5. Déploiement d'un outil de prévention et de détection d'intrusion de type SIEM

- Cette section est uniquement pratique. Elle consiste à installer, et surtout paramétrer et optimiser un outil de SIEM. Le paramétrage et l'optimisation sont deux notions clés pour gérer de manière optimale un SOC. Chaque outil doit être adapté au contexte est un processus métier qui le supporte.
- À partir de cas d'usage, les stagiaires seront encadrés pour définir des règles de paramétrage pour repérer au mieux les événements et les incidents, et surtout les corriger.

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE France
Tél : 01 56 29 70 01 - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France