Formation Analyste SOC (Security Operation Center)

Présentation

Ce parcours intensif de 8 jours forme les participants aux missions essentielles d'un analyste SOC dans un environnement de cybersécurité opérationnelle. À travers des ateliers pratiques, ils apprendront à détecter, analyser et gérer des incidents de sécurité en s'appuyant sur les outils clés du SOC (SIEM, EDR, CTI).
Ce programme permet de maîtriser les fondamentaux techniques, les méthodes de supervision, et les bonnes pratiques d'investigation.

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

Objectifs de la formation

A l'issue de la formation, le stagiaire sera capable d'assurer les fonctions d'analyste d'un Security Operations Center (SOC), principalement la détection et l'analyse des intrusions, l'anticipation et la mise en place des protections nécessaires.

- Connaître le rôle et les missions d'un analyste SOC
- Maîtriser les fondamentaux de la cybersécurité défensive
- Utiliser les outils et technologies du SOC
- Analyser et corréler les événements de sécurité
- Gérer les incidents de sécurité
- Rédiger des rapports techniques
- Travailler en coordination avec les autres équipes de cybersécurité
- Faire de la veille (cybermenaces, techniques d'attaques)

Prérequis

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

Public

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - 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

Techniciens et administrateurs Systèmes et Réseaux, responsables informatiques, consultants en sécurité, ingénieurs, responsables techniques, architectes réseaux, chefs de projets...

Programme de la formation

Jour 1
Objectifs :
- Connaître l'organisation d'un SOC
- Comprendre le métier d'analyste SOC

Introduction à la cybersécurité et au métier d'analyste SOC
- Panorama des menaces actuelles (malware, phishing, ransomware)
- Notions clés : vulnérabilités, risques, événements, incidents
- Qu'est-ce qu'un SOC ? Missions, rôles, types d'organisation
- Acteurs du SOC : analyste L1/L2, SOC Manager, Threat Hunter
- Outils principaux : SIEM, EDR, SOAR, ticketing

Exercice : identifier les rôles dans un organigramme SOC fictif

Jour 2
Objectifs :
- Appréhender les outils utilisés par les analystes SOC

Bases réseau pour la cybersécurité
- Modèle OSI et protocoles essentiels (TCP/IP, HTTP, DNS, ICMP)
- Ports et services : reconnaissance d'un trafic légitime
- Introduction aux logs système, réseau et applicatifs
- Outils de base : Wireshark, tcpdump

Travaux pratiques : analyse de trafic simple avec Wireshark

Jour 3
Objectifs :
- Identifier les principales problématiques à travers des cas d'usage

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - 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

Introduction aux attaques informatiques

- Techniques d'attaque classiques :
- IP/ARP Spoofing, DoS/DDoS, Man-in-the-middle
- Introduction aux malwares (virus, vers, chevaux de Troie)
- Typologie des attaques selon le MITRE ATT&CK

Atelier : simulation d'une attaque simple de type reconnaissance réseau

Jour 4

Objectifs :

- Identifier les principales problématiques à travers des cas d'usage

Gestion des incidents de sécurité

- Différence entre alerte, événement et incident
- Cycle de gestion des incidents (ISO 27035)
- Classification : gravité, criticité, temps de traitement
- Méthodes de confinement, remédiation et restauration

Exercice pratique : étude d'un incident et rédaction d'un rapport d'investigation

Jour 5

Objectifs :

- Apprendre à détecter des intrusions

Initiation à la supervision avec un SIEM

- Fonction d'un SIEM : collecte, corrélation, détection, visualisation
- Architecture d'un SIEM (source de logs, parseurs, règles)
- Démonstration : Splunk / Wazuh ou QRadar (au choix selon outil disponible)

Travaux pratiques : visualiser une alerte de type login suspect dans un SIEM

Jour 6

Objectifs :

- Apprendre à détecter des intrusions

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - 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

Détection d'anomalies et fuites de données

- Fuites d'informations : causes, détection, impact
- Signatures comportementales (baseline, UEBA simple)
- Exemples : détection d'une exfiltration via DNS ou ICMP

Travaux pratiques : détecter un comportement anormal à l'aide de logs

Jour 7

Objectifs :

- Savoir gérer différents incidents

Exercices pratiques de corrélation et d'enrichissement

- Corrélation d'événements dans un SIEM
- Alertes croisées : multi-sources (ex. EDR + SIEM)
- Enrichissement de logs avec CTI (threat intelligence)
- Préparer une alerte enrichie (source, gravité, type de menace)

Travaux pratiques : investigation d'une alerte multi-source dans un SIEM

Jour 8

Objectifs :

- Optimiser la sécurité d'un système d'information

Bilan, mini-projet et préparation à l'autonomie

- Restitution d'un incident : détection ? analyse ? réponse
- Présentation de tableaux de bord (KPI simples : MTTD, MTTR)
- Rappel des bonnes pratiques d'un analyste SOC débutant
- Conseils pour intégrer une équipe SOC (veille, rigueur, méthode)

Projet final : étude de cas complet « Réagir à une attaque type et produire un rapport »

Organisation

Formateur

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - 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

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.

Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétence.

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.
- Équilibre 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

- 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.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - 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

- 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.

NB : dans le cadre d'une Action collective, chaque stagiaire bénéficiaire sera également contacté par un prestataire choisi par l'Opco Atlas afin d'évaluer « à chaud » la qualité de la formation suivie.

Accessibilité

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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - 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