Sécurité défensive

Parcours Analyste SOC (Security Operation Center)

8 jours (56h00) | ★★★★½ 4,6/5 | SEC-ANASOC | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Formations Informatique › Cybersécurité › Sécurité défensive

Document mis à jour le 26/04/2024

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Expliquer l'état de l'art du SOC (Security Operation Center)
- Répondre aux besoins des enjeux cybers et des menaces par le métier d'analyste SOC.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir des connaissances générales en sécurité offensive et défensive et des notions sur le fonctionnement des systèmes d'exploitation. Il est également recommandé d'avoir une capacité de recherche et de restitution (prospecter l'actualité cyber afin d'en comprendre les enjeux).

Public concerné

Etudiant en sécurité informatique, administrateurs système et/ou réseaux, consultants en sécurité de l'information (sécurité offensive, défensive ou organisationnelle) et/ou contractuels des systèmes d'information (développeurs, ingénieurs Big Data, architectes...).

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Phase 1 : SOC et métier d'analyste

Jour 1 - Matin

Etat de l'art du Security Operation Center

- Définition du SOC
- Les avantages, l'évolution du SOC
- Les services intégrés au SOC, les données collectées, playbook
- Le modèle de gouvernance du SOC (approche SSI, type de SOC, CERT, CSIRT)
- PDIS (Prestataires de Détection d'Incidents de Sécurité) de l'ANSSI
- Prérequis et rôles d'un analyste SOC (techniques, soft skills, rôles, modèles)
- Les référentiels (ATT&CK, DeTT&CT, Sigma, MISP)
- Exemple de démonstration : utilisation du Framework ATT&CK via Navigator (attaque et défense)

Phase 2 : Découverte et mise en place du SIEM

Jour 1 - Après-midi

Focus sur l'analyste SOC

- Quel travail au quotidien ?
- Triage des alertes
- Révision et état de sécurité
- Identification et rapport
- Threat Hunting
- Exemple de démonstration : utilisation de l'outil Sysmon

Phase 3 : Threat Hunting

Jour 2 - Matin et après-midi

Les sources de données à monitorer

- Indicateur Windows (processus, firewall...)
- Service Web (serveur, WAF, activité)
- IDS / IPS
- EDR, XDR
- USB

- DHCP, DNS
- Antivirus, EPP
- DLP, whitelist
- Email

Exemple de travaux pratiques (à titre indicatif)

- *Cas d'usage et ligne de défense*

Phase 4 : Analyse, Logstash, Elasticsearch

Jour 3 - Matin

Tour d'horizon du SIEM

- Contexte du SIEM
- Solution existante
- Principe de fonctionnement d'un SIEM
- Les objectifs d'un SIEM
- Solution de SIEM

Jour 3 - Après-midi

Présentation de la suite Elastic

- Les agents BEATS et Sysmon
- Découverte de Logstash
- Découverte d'Elasticsearch
- Découverte de Kibana

Exemple de travaux pratiques (à titre indicatif)

- *Mise en place d'ELK et première remontée de log*

Jour 4 - Matin et après-midi

Logstash (ETL)

- Fonctionnement de Logstash
- Les fichiers Input et Output
- Enrichissement : les filtres Groks et sources externes

Jour 5 - Matin

Elasticsearch

- Terminologie
- Syntax Lucene
- Alerte avec ElastAlert et Sigma
- Exemple de démonstration : utilisation d'ElastAlert et Sigma

Exemple de travaux pratiques (à titre indicatif)

- *Création d'alertes, alarmes*

Phase 5 : Kibana

Jour 5 - Après-midi

Kibana

- Recherche d'événements
- Visualisation des données
- Exemple de démonstration :

- Création d'un filtre sur Kibana
- Ajout de règles de détection, IoC
- Allez plus loin dans l'architecture ELK avec HELK

Phase 6 : Cyber-entraînement et rapport

Jour 6 - Matin

Mise en situation

- L'analyste SOC est en situation et doit identifier plusieurs scénarios d'attaque lancés par le formateur

Exemple de travaux pratiques (à titre indicatif)

- *Configurer un SIEM et l'exploiter*

Jour 6 - Après-midi

Exemple de travaux pratiques (à titre indicatif)

- *Détecter une cyber attaque simple*

Jour 7 - Matin

Exemple de travaux pratiques (à titre indicatif)

- *Détecter une cyber attaque complexe (APT MITRE ATT&CK)*

Jour 7 - Après-midi

Rapport

- L'analyste SOC doit rapporter les attaques, détecter et identifier les menaces, impacts et vérifier si son système d'information est touché

Exemple de travaux pratiques (à titre indicatif)

- *Créer un rapport des attaques interceptées et évaluer l'impact*

Phase 7 : Initiation à la gestion des incidents

Jour 8 - Matin

Réponse aux incidents

- Etat de l'art de la réponse aux incidents (CSIRT, CERT, FIRST, CERT-FR)
- Les différents métiers du CSIRT
- Quelle méthode, quel framework pour un CSIRT ?
- PRIS (Prestataires de Réponse aux Incidents de Sécurité) de l'ANSSI
- Communication avec le CSIRT
- Alerter le CSIRT lors d'une détection
- Comment le CSIRT procède lors d'une crise et quelle réponse apporte-t-il aux incidents ?

Phase 8 : Synthèse

Jour 8 - Après-midi

Echange autour des différents travaux / rapport des stagiaires lors de la formation : points positifs / points négatifs

Quelle conclusion pour la méthodologie d'un analyse SOC

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.