Parcours Analyste SOC (Security Operations Center)

Cycle de 8 jours - 56h
Réf : ASR - Prix 2024 : 5 190CHF HT

A l'issue de la formation, l'apprenant 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.

Ce cycle est composé de :

- Analyste SOC, le métier (Réf. ASH, 2 jours)
- Collecte et analyse des logs, un SIEM pour optimiser la sécurité de votre SI (Réf. LCA, 3 jours)
- Analyse Forensic (Réf. AFB, 3 jours)

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

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

TRAVAUX PRATIQUES

Nombreux travaux pratiques sur la mise en place et l'utilisation des outils de l'analyste SOC, la détection d'intrusion, les problématiques les plus courantes, l'analyse post-incident.

LE PROGRAMME

dernière mise à jour : 07/2022

1) Le SOC (Security Operation Center)

- Qu'est-ce qu'un SOC ?
- A quoi sert-il ? Pourquoi de plus en plus d'entreprises l'utilisent ?
- Les fonctions du SOC : Logging, Monitoring, Reporting audit et sécurité, analyses post incidents.
- Les bénéfices d'un SOC.
- Les solutions pour un SOC.
- Le SIM (Security Information Management).
- Le SIEM (Security Information and Event Management).
- Le SEM (Security Event Management).
- Exemple d'une stratégie de monitoring.

2) Le métier de l'analyste SOC

- En quoi consiste le métier de l'analyste SOC ?
- Quelles sont ses compétences ?
- Monitorer et trier les alertes et les événements.
- Savoir prioriser les alertes.

PARTICIPANTS

Techniciens et administrateurs systèmes et réseaux, responsables informatiques, consultants en sécurité, ingénieurs, responsables techniques, architectes réseaux, chefs de projets…

PRÉREQUIS

Connaître le guide sécurité de l'ANSSI, avoir des connaissances en réseau, avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

3) La collecte des informations

- L'hétérogénéité des sources. Qu'est-ce qu'un événement de sécurité ?
- Le Security Event Information Management (SIEM). Les événements collectés du SI.
- Les journaux système des équipements (firewalls, routeurs, serveurs, bases de données, etc.).
- La collecte passive en mode écoute et la collecte active.

4) Optimiser la sécurité du SI : outils, bonnes pratiques, pièges à éviter

- Panorama des solutions et des produits.
- Syslog.
- Le programme SEC.
- Le logiciel Splunk.
- La législation française.

5) La détection d'intrusion, principales problématiques

- Bien comprendre les protocoles réseaux (TCP, UDP, ARP, ICMP, routeurs, firewall, proxy…).
- Les attaques sur TCP/IP (spoofing, déni de service, vol de session, attaque SNMP…).
- Intelligence Gathering, recherche de traces, scans de réseaux.
- Les trojans, les backdoors, bugs des navigateurs, les « Covert Channels », les agents de déni de service distribués...
- Attaques et exploitation des failles (prise de contrôle, DDoS, buffer overflow, RootKits...).

6) Comment gérer un incident ?

- Les signes d'une intrusion réussie dans un SI.
- Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
- Comment réagir face à une intrusion réussie ?
- Quels serveurs sont concernés ?
- Savoir retrouver le point d'entrée et le combler.
- La boîte à outils Unix/Windows pour la recherche de preuves.
- Nettoyage et remise en production de serveurs compromis.

7) Analyser les incidents pour mieux se protéger : l'analyse forensic

- Informatique judiciaire : types de crimes informatiques, rôle de l'enquêteur informatique.
- La cybercriminalité moderne.
- La preuve numérique.

8) Analyse forensic d'un système d'exploitation Windows

- Acquisition, analyse et réponse.
- Compréhension des processus de démarrage.
- Collecter les données volatiles et non volatiles.
- Fonctionnement du système de mot de passe, du registre Windows.
- Analyse des données contenues dans la mémoire vive, des fichiers Windows.
- Analyse du cache, cookie et historique de navigation, historique des événements.

LES DATES

Ce parcours est composé d'un ensemble de modules. Les dates indiquées ci-dessous correspondent aux premières sessions possibles du parcours.

CLASSE À DISTANCE
2024 : 13 mai, 27 mai, 24 juin, 09 sept., 18 nov.