Comprendre la gestion des incidents et le rôle du centre d'opérations de sécurité SOC

Détecter, analyser et traiter efficacement les incidents de sécurité

Stage pratique
Sécurité

Code :
GISOC

Durée :
1 jour(s) (7,00 heures)

Exposés : **60 %**
Cas pratiques : **20 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 990,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

DESCRIPTION

Face à la montée des cyberattaques, la capacité à détecter et à gérer efficacement les incidents de sécurité constitue aujourd'hui un enjeu majeur pour les organisations.

Cette formation propose une immersion rapide dans le fonctionnement d'un Security Operations Center (SOC), en abordant les processus clés de détection, d'analyse et de réponse aux incidents, ainsi que les outils associés.

Les participants développent les compétences essentielles pour analyser des alertes, qualifier des incidents et contribuer à une réponse adaptée, en lien avec les équipes sécurité et les métiers.

OBJECTIFS PEDAGOGIQUES

- Comprendre les concepts fondamentaux de la détection/gestion des incidents
- Expliquer le rôle, les missions et l'organisation d'un SOC (niveaux d'analyse, interactions IT/RSSI/métiers, principes d'escalade)
- Identifier les principaux outils et données d'un SOC (SIEM, EDR, Threat Intelligence, logs)
- Décrire et appliquer les étapes clés du cycle de vie d'un incident : détection, triage/qualification, analyse, confinement, éradication, restauration et retour d'expérience

PUBLIC CIBLE

- Collaborateurs et Managers IT et SSI

PRE-REQUIS

- Connaissances de base en IT et en sécurité des systèmes d'information (SSI) nécessaires
- Notions de code et de requêtage

METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés

de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

1) ***COMPRÉHENSION DES CONCEPTS CLÉS***

- Définir ce qu'est un incident de sécurité et comprendre ses impacts sur l'organisation
- Expliquer le rôle et les missions d'un Security Operations Center (SOC) dans la détection et la réponse aux incidents
- Identifier les principaux outils et technologies utilisés (SIEM, SOAR, EDR, Threat Intelligence)

2) ***ORGANISATION ET RÔLES AU SEIN DU SOC***

- Décrire les différents rôles au sein du SOC : analystes niveaux 1, 2, 3, responsable SOC, coordinateur de crise
- Comprendre les interactions avec les autres départements (IT, gouvernance, RSSI, autres équipes Sécurité)

3) ***PROCESSUS DE GESTION DES INCIDENTS***

- Décrire les différentes étapes du cycle de vie d'un incident : détection, analyse, confinement, éradication, récupération
- Expliquer les procédures d'escalade ainsi que la coordination avec les équipes internes et externes
- Présenter les principaux standards et référentiels (ISO 27035, NIST Incident Response)

4) ***ANALYSE, INVESTIGATION ET DOCUMENTATION DES ALERTES***

- Analyser une alerte et distinguer les faux positifs des incidents avérés
- Identifier les vecteurs d'attaque et les indicateurs de compromission (IoC)
- Documenter les actions menées et produire les rapports post-incident clairs et exploitables

5) ***MISES EN PRATIQUE***

- Création d'une règle de détection (identification des sources adéquates, composition de la logique de détection)
- Simulation d'un exercice d'incident

6) ***AMÉLIORATION CONTINUE***

- Importance des exercices « Post-Mortem » et comment les intégrer dans un processus d'amélioration de la résilience de l'IT
- Identification des indicateurs clés pertinents pour le suivi de performance d'un SOC

7) ***CONCLUSION***

- Questions/Réponses
- Synthèse de la journée et rappel des messages clés : détecter, analyser et traiter efficacement les incidents de sécurité
- Évaluation finale

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com