SQLI INSTITUT

400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

ANALYSTE SOC NIVEAU AVANCÉ

CODE STAGE : SOC2

OBJECTIFS

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.

DURÉE

3 jours

PUBLIC

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

PRÉ-REQUIS

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. Avoir suivi le cours Analyste SOC1

PROGRAMME

Jour 1 matin code2utf('038',0) après-midi (Threat hunting) Approfondissement
Chapitre 1 : Les sources de données à monitorer

- Indicateur Windows (processus, firewall, etc.)
- Service WEB (serveur, WAF, activité)
- IDS/IPS
- EDR, XDR
- USB
- DHCP, DNS
- Antivirus, EPP
- DLP, whitelist
- Email

Atelier pratique : cas d'usage et ligne de défense, mise en place du monitoring

Jour 2 matin code2utf('038',0) après-midi (analyse, Logstash, Elastic search) Approfondissement

Chapitre 2 : Logstash (ETL)

- Fonctionnement de Logstash
- Les fichiers input code2utf('038',0) output
- Enrichissement : Les filtres Groks et sources externes

Atelier pratique : Configuration de Logstash

Jour 3 matin (gestion des incidents)

Chapitre 3 : Réponse à incident

- État de l'art de la réponse à incident (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 une réponse à incident

Jour 3 après-midi (Conclusion)

Chapitre 4 : conclusion

- Échange des différents travaux, rapport des stagiaires lors de la formation
- Points positifs, points négatifs
- Quelle conclusion pour la méthodologie d'un analyse SOC