SIEM Splunk Avancé : Détection, Threat Hunting et ingénierie SOC

Durée : 4 jours (28 heures)

CONNAISSANCES PREALABLES

- Maîtrise des fondamentaux Splunk.
- Connaissance du langage SPL.
- Expérience SOC ou cybersécurité opérationnelle.

PROFIL DES STAGIAIRES

- Analystes SOC N2/N3
- Ingénieurs cybersécurité
- Threat Hunters
- Ingénieurs détection
- Responsables SOC.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Développer des cas d'usage de détection.
- Exploiter Splunk Enterprise Security.
- Réaliser du Threat Hunting.
- Construire des corrélations avancées.
- Développer des tableaux de bord SOC avancés.
- Optimiser les performances du SIEM.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Laboratoires avancés.
- Études de cas SOC réelles.
- Exercices de Threat Hunting.
- Simulations d'attaques.

FORMATEUR

- Consultant expert Splunk Enterprise Security, SOC et Threat Hunting disposant d'une expérience significative en détection avancée, réponse à incident et ingénierie SOC.

METHODE D'EVALUATION DES ACQUIS

- Exercices avancés SPL.
- Développement de règles de détection.

- Cas pratique final.

CONTENU DU COURS

Jour 1 : SPL avancé et corrélations (7h)

Module 1 : SPL avancé (3h)

Contenu

- Rex.
- Transaction.
- Join.
- Lookup.
- Subsearch.
- Macros.

Mise en pratique

Laboratoires SPL avancés.

Module 2 : Développement de corrélations (2h)

Objectifs

- Construire des règles de détection.

Mise en pratique

Création de cas d'usage SOC.

Module 3 : MITRE ATT&CK et détection (2h)

Mise en pratique

- Mapping ATT&CK.

Jour 2 : Splunk Enterprise Security (7h)

Module 4 : Architecture Enterprise Security (2h)

Module 5 : Risk Based Alerting (2h)

Module 6 : Notable Events et Incident Review (3h)

Mise en pratique

- Gestion d'incidents SOC.

Jour 3 : Threat Hunting et investigation (7h)

Module 7 : Méthodologies de Threat Hunting (2h)

Module 8 : Investigation avancée (3h)

Module 9 : IOC et Threat Intelligence (2h)

Mise en pratique

- Chasse aux menaces sur données réelles.

Jour 4 : Ingénierie SOC et optimisation (7h)

Module 10 : Développement de contenus de détection (2h)

Module 11 : Optimisation des performances (2h)

Module 12 : Cas pratique SOC avancé (3h)

Mise en pratique

- Détection d'une compromission complète.
- Investigation.
- Corrélations.

- Threat Hunting.
- Restitution SOC.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.