SIEM Splunk : Administration, recherche et supervision de sécurité

Durée : 4 jours (28 heures)

CONNAISSANCES PREALABLES

- Connaissances de base en systèmes et réseaux.
- Connaissances générales en cybersécurité.
- Notions de journalisation et d'événements de sécurité appréciées..

PROFIL DES STAGIAIRES

- Analystes SOC N1/N2
- Administrateurs systèmes et réseaux
- Administrateurs sécurité
- Exploitants SI
- RSSI techniques
- Ingénieurs infrastructures.

OBJECTIFS

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

- Comprendre l'architecture de Splunk.
- Collecter et exploiter les données de sécurité.
- Réaliser des recherches SPL.
- Construire des tableaux de bord.
- Configurer des alertes.
- Superviser les événements de sécurité.
- Exploiter Splunk dans un contexte SOC.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Démonstrations techniques.
- Travaux pratiques sur plateforme Splunk.
- Exercices guidés de recherche SPL.
- Cas d'usage SOC.
- Ateliers de supervision.

FORMATEUR

- Consultant expert Splunk et cybersécurité disposant d'une expérience significative en déploiement SIEM, supervision de sécurité et accompagnement SOC.

METHODE D'EVALUATION DES ACQUIS

- Quiz de validation.
- Exercices SPL.
- Création de dashboards.
- Cas pratique final..

CONTENU DU COURS

Jour 1 : Découverte de Splunk et collecte des données (7h)

Module 1 : Architecture Splunk (2h)

Objectifs

- Comprendre les composants Splunk.

Contenu

- Architecture Splunk Enterprise.
- Indexers.
- Search Heads.
- Forwarders.
- Flux de données.

Mise en pratique

Atelier :

- Exploration d'une architecture Splunk.

Module 2 : Collecte et indexation des données (3h)

Objectifs

- Intégrer des sources de logs.

Contenu

- Universal Forwarder.
- Sources de données.
- Parsing.
- Indexation.
- Gestion des index.

Mise en pratique

Travaux pratiques :

- Intégration de journaux Windows et Linux.

Module 3 : Navigation et exploitation des données (2h)

Objectifs

- Rechercher efficacement dans Splunk.

Contenu

- Interface utilisateur.
- Recherche simple.
- Filtres.
- Champs.

Mise en pratique

Exercices guidés.

Jour 2 : Recherches SPL et analyse des événements (7h)

Module 4 : Langage SPL - Fondamentaux (3h)

Objectifs

- Maîtriser les recherches SPL.

Contenu

- Search.
- Stats.
- Table.
- Sort.
- Timechart.
- Eval.

Mise en pratique

Travaux pratiques SPL.

Module 5 : Analyse des événements de sécurité (2h)

Objectifs

- Identifier les événements suspects.

Contenu

- Logs systèmes.
- Logs réseau.
- Corrélations simples.

Mise en pratique

Étude de cas SOC.

Module 6 : Création de rapports (2h)

Objectifs

- Produire des rapports d'exploitation.

Mise en pratique

Création de rapports personnalisés.

Jour 3 : Dashboards et alerting (7h)

Module 7 : Création de tableaux de bord (3h)

Objectifs

- Construire des dashboards opérationnels.

Contenu

- Visualisations.
- KPI.
- Dashboards sécurité.

Mise en pratique

Travaux pratiques.

Module 8 : Alertes et supervision (2h)

Objectifs

- Mettre en place des alertes.

Contenu

- Alertes programmées.
- Alertes temps réel.
- Notifications.

Mise en pratique

Configuration d'alertes.

Module 9 : Cas d'usage SOC (2h)

Objectifs

- Exploiter Splunk dans un SOC.

Mise en pratique

Simulation d'analyse SOC.

Jour 4 : Mise en œuvre opérationnelle (7h)

Module 10 : Bonnes pratiques d'administration Splunk (2h)

Module 11 : Optimisation des recherches et performances (2h)

Module 12 : Cas pratique fil rouge (3h)

Mise en pratique

- Collecte.
- Recherche SPL.
- Dashboard.
- Alerting.
- Analyse d'incidents.

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.