Sécurité Technique

Maîtriser l’analyse des journaux systèmes avec Splunk : Visualisation, Corrélation et Surveillance Active

Vous allez apprendre à

- Installer, configurer et prendre en main Splunk dans un contexte professionnel.
- Comprendre la structuration et l’indexation des journaux issus des systèmes et réseaux.
- Construire des requêtes efficaces avec le Search Processing Language (SPL).
- Créer des tableaux de bord opérationnels pour le suivi de la sécurité, du réseau et des applications.
- Mettre en œuvre un système de surveillance proactive via alertes et rapports automatisés.
- Corréler les événements issus de multiples sources pour une analyse avancée de la posture IT.

Public visé

- Administrateurs systèmes, ingénieurs réseaux, analystes sécurité.
- Toute personne impliquée dans la surveillance ou l’exploitation des infrastructures IT.
- Techniciens souhaitant monter en compétence sur un outil SIEM accessible et puissant.

Les objectifs de la formation

- Obtenez les bases nécessaires pour la réalisation d’audits de sécurité avancés sur les applications iOS.

Les prérequis de la formation

- Connaissances de base des systèmes (Windows/Linux) et des réseaux.
- Expérience en exploitation ou supervision IT (niveau intermédiaire).

Programme de la formation

Jour 1

- Fondamentaux et premières analyses

Jour 2

- Visualisation, corrélation, alertes