Mise en place d’un SIEM

Lien : https://innov-systems.com/formation/mise-en-place-dun-siem

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC150

CATÉGORIE
SIEM, SOC et LogPoint

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Connaitre les problématiques liées à la détection d’intrusion ainsi que leurs limites
- Découvrir les principes technologiques derrière l'acronyme SIEM
- Apprendre à mettre en place un SIM avec implémentation de sonde SNORT et d’agent HIDS dans un réseau existant
- Prendre les bonnes décisions suite à l'analyse des remontées d'informations et à leur corrélation

POUR QUI ?

- Consultants en sécurité
- Ingénieurs / Techniciens
- Responsables techniques

Programme détaillé

1 / Vue d'ensemble de la cybersécurité

- Histoire de la cybersécurité
- Présentation du programme Creeper
- Présentation du projet Rabbit
- La cybersécurité aujourd'hui et ses risques
- La dangerosité des données numériques
- Les différents hackers et leurs motivations
- Classification des risques

2 / Prévention et détection d’intrusion

- Les divers IDS
- Les méthodes de détection
- La détection par analyse scénaristique
- L’analyse comportementale

3 / La technologie SIEM (Security Information and Event Management)

- Architecture et fonctionnalités
- Comprendre le fonctionnement d'un SIEM
- Les objectifs d'un SIEM et de la corrélation des données

4 / Mise en place de Windows Server

- Installer Windows server R2
- Configurer le serveur
- Activer et configurer le domaine
- Activer et configurer le service Active Directory (AD)

5 / ElasticSearch

- Découvrir Elasticsearch
- Approche théorique : terminologie
- Application Full REST et utilisation

6 / Logstash

- Découvrir Logstash
- Approche théorique : fonctionnement de logstash

7 / Kibana

- Découvrir Kibana
- Installer et configurer Kibana
- Utiliser l'interface Discover
- Visualisation des résultats
- Créer des alertes
- Exporter en PDF les données Dashboard
- Sécuriser Kibana

8 / Détection d'intrusion et remontée d'alertes sur l'Active Directory (AD)

- Présentation du scénario et de l'objectif
- Approche théorique sur l'agent WinlogBeat

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

20 au 24 Juil. 2026	Présentiel - Casablanca
14 au 18 Sep. 2026	Distanciel
09 au 13 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com