



Mise en place de SIEM OSSIM couplé aux sondes SNORT

Lien :

<https://innov-systems.com/formation/mise-en-place-de-siem-ossim-couple-aux-sondes-snort>

 DURÉE
5 jours (35h)

 RÉFÉRENCE
SEC152

 CATÉGORIE
SIEM, SOC et LogPoint

OBJECTIFS DE LA FORMATION

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

- ✓ Connaître les problématiques liées à la détection d'intrusion ainsi que leurs limites
- ✓ Apprendre à mettre en place le SIEM OSSIM avec implémentation de sondes SNORT et d'agents HIDS dans un réseau existant
- ✓ Prendre les bonnes décisions suite à l'analyse des remontées d'informations et à leur corrélation

POUR QUI ?

- ✓ Administrateurs
- ✓ Architectes réseaux
- ✓ Chefs de projets



Programme détaillé

1 / Introduction

- Les incidents de sécurité
- La gestion des risques
- Réagir à un incident de sécurité
- Principe d'un NSM
- Bonnes pratiques

2 / Le SIEM

- Présentation
- Fonctionnement d'un SIEM
- Limites d'utilisation

3 / Le SIEM OSSIM

- Fonctionnement et mise en œuvre

4 / Les IDS

- Avantages des IDS
- Limites
- Attaques et contournement d'un IDS
- Précautions à prendre

5 / Les agents IDS et HIDS

- Panorama des agents
- Implémenter un agent sur Windows
- Implémenter un agent sur Linux

6 / Présentation de SNORT

- Histoire et Introduction à Snort
- Fonctionnalité de Snort
- Architecture de Snort
- Les Scénarios de Déploiement de Snort

7 / Installation et Mise en Marche de Snort en mode NIDS

- Versions, Packages et modules divers
- Installation de Snort en mode NIDS
- Les Options de Démarrage de Snort
- Les Modules d'output de Snort
- Premier pas avec les règles Snort

8 / Configuration de SNORT

- Snort.conf
- Les variables
- Aperçu sur les Pré-processeurs et les Décodeurs
- Aperçu sur les Règles avancée (cas de PCRE)
- Les Différents Outputs

9 / Implémentation de SNORT

- Implémenter SNORT dans OSSIM
- Configuration avancée

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>