Ref. formation 202003079976

# Exploitation du SIEM OSSIM couplé aux sondes SNORT

### Financement

Formation professionnelle continue
**Non conventionnée / sans dispositif**

### Organisme responsable et contact

M2I FORMATION MERIGNAC
**Agnès RICHIR**
05.57.19.07.65
a.richir@m2iformation.fr

### Accès à la formation

**Publics visés :**

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

**Sélection :**

Tests

**Niveau d'entrée requis :**

Sans niveau spécifique

**Conditions d'accès :**

Aucune

**Prérequis pédagogiques :**

Avoir des connaissances en TCP/IP, la sécurité, les réseaux, Linux administration et SNORT.

**Contrat de professionnalisation possible ?**

Non

## Objectif de la formation

**Traiter des incidents et leur management Aborder les problématiques liées à la détection d'intrusion ainsi que leurs limites 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.**

## Contenu et modalités d'organisation

**Introduction Les incidents de sécurité La gestion des risques Réagir à un incident de sécurité Principe d'un NSM Bonnes pratiques Le SIEM Présentation Fonctionnement d'un SIEM Limites d'utilisation Le SIEM OSSIM Fonctionnement et mise en oeuvre Les IDS Avantages Limites Attaques et contournement d'un IDS Précautions à prendre Les agents IDS et HIDS Panorama des agents Implémenter un agent sur Windows Implémenter un agent sur Linux SNORT Présentation Implémenter SNORT dans OSSIM Paramétrage de base Configuration avancée**

Parcours de formation personnalisable ? **Oui** Type de parcours **Individualisé**

## Validation(s) Visée(s)

**> Attestation de fin de formation**

## Et après ?

**Suite de parcours**

***Non renseigné***

## Calendrier des sessions

| Numéro Carif | Dates de formation | Ville | Organisme de formation | Type d'entrée | CPF | Modalités |
|---|---|---|---|---|---|---|
| 00188994 | du 01/01/2019 au 31/12/2022 | Mérignac (33) | M2I FORMATION MERIGNAC | | Non éligible | FPC |