Détection de Cyberattaques avec SIEM Prelude couplé aux sondes SNORT

Lien : https://innov-systems.com/formation/detection-de-cyberattaques-avec-siem-prelude-couple-aux-sondes-snort

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SEC151**	**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
- Apprendre à mettre en place un SIM avec implémentation de sonde 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

Innov Systems

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 / Prévention et détection d'intrusion

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

3 / Le SIEM

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

4 / Le SIEM Prelude

- Le traitement des événements et des alertes
- Gestion et stockage des journaux
- Les modules techniques Prelude : Parsing, Correlator, Manager, Prewikka, etc.
- Les fonctions : Détection / Corrélation / Agrégation / Notification
- Les modules fonctionnels : ALERTE, ARCHIVE, ANALYSE & ADMIN
- La documentation Prelude

Innov Systems

5 / Les IDS

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

6 / Les agents IDS ET HIDS

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

7 / Présentation de SNORT

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

8 / 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

9 / Configuration de SNORT

- Snort.conf
- Les variables
- Aperçu sur les Pré-processeurs et les Décodeurs

Inov Systems

- Aperçu sur les Règles avancée (cas de PCRE)
- Les Différents Outputs

10 / Implémentation de SNORT

- Implémenter SNORT dans Prelude
- 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

12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca
23 au 27 Août 2027	Présentiel - Casablanca

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

Innov Systems

Réservation & Renseignements

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

Innov Systems — Tous droits réservés