Intégration d’un SOC (Security Operation Center)

Lien : https://innov-systems.com/formation/integration-dun-soc-security-operation-center

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SEC153**	**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
- Etre en mesure d'implémenter et de manipuler un SOC (Security Operation Center) dans un environnement complet

POUR QUI ?

- Ingénieurs / Techniciens
- Responsables techniques

Innov Systems

Programme détaillé

1 / Vue d'ensemble de la cybersécurité

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

2 / Prévention et détection d’intrusion

- Présentation des différents IDS
- Présentation des méthodes de détection
- La détection par analyse scénaristique
- L’analyse comportementale

3 / Définition et approche stratégique

- Terminologie du monde SOC
- Définition et environnement
- Les objectifs et missions
- Les services actifs au sein du SOC
- Les processus du SOC
- Les composantes au sein du SOC
- Les rôles et tâches au sein des équipes
- La génération et le traitement des données
- La structuration SOC selon le CLUSIF

Inov Systems

4 / Le déploiement d'un SOC

- La définition du projet de déploiement
- L'approche constructive entreprise
- La délimitation des besoins
- La phase de "Build"
- La phase de "Run"
- Premier bilan et retour d'expériences
- La poursuite du déploiement

5 / La technologie SIEM (Security Information Management System)

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

6 / 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)

7 / Le pare-feu

- Vue d'ensemble des firewalls
- Fonctionnement d'un firewall
- Les types de filtrages
- Les types de firewalls
- Vue d'ensemble de pfSense

8 / Mise en place du firewall

Innov Systems

- Rappel sur le protocole DHCP (Dynamic Host Configuration Protocol)
- Vue d'ensemble du portail d'authentification
- Vue d'ensemble du protocole SNMP
- Les différents modules SNMP avec pfSense

9 / Vue d'ensemble des types de détections systèmes

- Définitions
- Intrusion Detection System (IDS)
- Network IDS
- Wireless IDS
- Hybride IDS

10 / Mettre en place son IDS Suricata

- Présentation de l'IDS Suricata
- Les différents modes d'exécution
- Approche théorique : les formats de règles Suricata
- Les options de règles

11 / ElasticSearch

- Présentation de Elasticsearch
- Approche théorique : terminologie
- Application Full REST et utilisation

12 / Logstash

- Présentation de Logstash
- Approche théorique : fonctionnement de logstash

13 / Kibana

Innov Systems

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

13 / Détection d'intrusion et remontée d'alertes sur l'Active Directory

- 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

25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	Présentiel - Casablanca
06 au 10 Sep. 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

Innov Systems