Fondamentaux de la Cybersécurité et des Opérations en Centre SOC

Lien : https://innov-systems.com/formation/fondamentaux-de-la-cybersecurite-et-des-operations-en-centre-soc

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**RST313**	**Cisco Entreprise**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre le rôle, la structure et les missions d'un centre d'opérations de sécurité (SOC).
- Acquérir une maîtrise des outils de surveillance et d'investigation en cybersécurité.
- Identifier et analyser les vecteurs d'attaque, activités malveillantes et comportements suspects.
- Appliquer des méthodes d'investigation et de réponse adaptées aux incidents de sécurité.
- Mettre en œuvre des procédures d'automatisation et d'optimisation du SOC.
- Se préparer à occuper efficacement un poste d'analyste SOC de premier niveau

POUR QUI ?

- Professionnels de l'informatique, ingénieurs et techniciens système/réseau souhaitant évoluer vers la cybersécurité.
- Administrateurs réseau et sécurité en charge de la surveillance et de la protection des infrastructures
- Responsables techniques souhaitant approfondir la gestion des incidents et des opérations SOC

Programme détaillé

1 / RÔLE ET ORGANISATION DU SOC

- Définition et missions du centre d’opérations de sécurité
- Typologie des services fournis par un SOC
- Rôles et responsabilités des analystes de niveau 1

2 / INFRASTRUCTURE ET ENVIRONNEMENT TECHNIQUE

- Architecture type d’un SOC et composants essentiels
- Outils de monitoring et collecte d’événements (SIEM, NSM)
- Flux de données et points de collecte

3 / BASES DE LA SÉCURITÉ RÉSEAU ET SYSTÈMES

- Principes du modèle TCP/IP et ses vulnérabilités
- Technologies de sécurité réseau essentielles (pare-feu, IDS/IPS)
- Premières notions sur la sécurité des systèmes Windows et Linux

4 / TYPES ET CATEGORIES DE DONNÉES POUR L’ANALYSTE SOC

- Journaux systèmes, fichiers de log et captures réseau
- Événements applicatifs et traces d’activité utilisateur
- Normalisation et corrélation des données

5 / INTRODUCTION À LA CRYPTOGRAPHIE

- Concepts fondamentaux (chiffrement, hachage, clés symétriques et asymétriques)
- Applications pratiques dans la cybersécurité (TLS, VPN, signatures numériques)
- Détection et investigation d’activités liées à la cryptographie

Innov Systems

6 / TECHNOLOGIES DE SÉCURITÉ DES TERMINAUX

- Solutions antivirus, EDR et contrôle d’accès
- Surveillance des postes de travail et mobiles
- Détection d’anomalies sur les terminaux

7 / VECTEURS D’ATTAQUE COURANTS

- Techniques d’exploitation des protocoles TCP/IP
- Attaques basées sur le Web et les navigateurs
- Abus de protocoles applicatifs (DNS, HTTP, SMTP)

8 / ACTIVITÉS MALVEILLANTES ET COMPORTEMENTS SUSPECTS

- Reconnaissance, exploitation et persistance des menaces
- Indicateurs de compromission (IOC) et comportements anormaux
- Étude de cas d’incidents connus

9 / MÉTHODOLOGIE D’INVESTIGATION

- Chaîne de destruction et modèle en diamant
- Analyse de logs et corrélation multi-sources
- Enquêtes guidées avec outils spécialisés (Security Onion, Wireshark, Splunk)

10 / PROCESSUS DE RÉPONSE AUX INCIDENTS

- Élaboration d’un plan de réponse adapté au SOC
- Rôles et responsabilités d’une équipe CSIRT
- Documentation des incidents avec le standard VERIS

11 / AUTOMATISATION ET ORCHESTRATION DU SOC

- Utilisation des playbooks de sécurité
- Outils SOAR (Security Orchestration, Automation and Response)

Inov Systems

- Amélioration de l’efficacité et réduction du temps de réaction

12 / MESURES ET INDICATEURS SOC

- Définition des métriques de performance
- Tableaux de bord et reporting
- Amélioration continue du SOC

13 / LABORATOIRE PRATIQUE SUR LES DONNÉES ET MENACES

- Analyse de captures PCAP et de journaux systèmes
- Détection et investigation d’attaques TCP/IP
- Exploration des comportements suspects DNS

14 / SIMULATION D’UNE ENQUÊTE SOC

- Mise en œuvre d’un scénario d’incident complet
- Identification des indicateurs de compromission
- Application d’un plan de réponse et rédaction d’un rapport

15 / SYNTHÈSE ET ÉVALUATION FINALE

- Retour sur les concepts clés de la formation
- Évaluation pratique et théorique des acquis
- Plan d’action individuel pour une montée en compétence en cybersécurité

Inov Systems

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

16 au 20 Nov. 2026	Distanciel
15 au 19 Fév. 2027	Présentiel - Casablanca
12 au 16 Avr. 2027	Présentiel - Casablanca
07 au 11 Juin 2027	Présentiel - Casablanca
02 au 06 Août 2027	Présentiel - Casablanca

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

Innov Systems — Tous droits réservés