Réponse à incidents de cybersécurité (CSIRTCERT) : organisation, playbooks et gestion de crise

Lien : https://innov-systems.com/formation/reponse-a-incidents-de-cybersecurite-csirtcert-organisation-playbooks-et-gestion-de-crise

DURÉE
5 jours (35h)

RÉFÉRENCE
SI98

CATÉGORIE
Analyse Apres Incident : Analyse Forensique, Investigation Numérique et Plan de Continuité

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre le rôle et le fonctionnement d’un CSIRT/CERT
- Structurer une organisation efficace de réponse à incidents
- Mettre en place des playbooks de gestion d’incidents
- Détecter, analyser et qualifier les incidents de cybersécurité
- Réaliser des opérations de containment et remédiation
- Organiser une gestion de crise cybersécurité efficace
- Coordonner les équipes techniques et métiers en situation de crise
- Préserver les preuves et mener des analyses forensiques
- Automatiser la réponse à incident avec des outils SOAR
- Améliorer la résilience face aux cyberattaques
- Réduire l’impact opérationnel des incidents de sécurité
- Étudier des cas concrets d’incidents réels et simulations

POUR QUI ?

- Analystes SOC
- Ingénieurs cybersécurité
- Membres de CSIRT/CERT
- Incident responders
- Forensic analysts
- RSSI / CISO
- DevSecOps engineers
- Administrateurs systèmes et réseaux
- Consultants cybersécurité
- Responsables IT et infrastructure
- Risk managers
- Toute personne impliquée dans la détection et la gestion des incidents de cybersécurité

Innov Systems

Programme détaillé

1 / Introduction aux CSIRT et CERT

- Rôle des équipes de réponse à incidents (CSIRT/CERT)
- Typologie des incidents de cybersécurité
- Cycle de vie d’un incident de sécurité

2 / Organisation d’un centre de réponse à incidents

- Structure et rôles d’un CSIRT
- Gouvernance et coordination interne/externe
- Interfaces avec SOC, IT et direction

3 / Préparation et maturité de la réponse à incident

- Mise en place des capacités de détection et réponse
- Gestion des outils et de l’infrastructure CSIRT
- Indicateurs de maturité (NIST, ISO 27035)

4 / Détection et qualification des incidents

- Identification des événements suspects
- Analyse initiale et classification des incidents
- Priorisation selon l’impact métier

5 / Analyse technique des incidents

- Forensique numérique (endpoint, réseau, cloud)
- Collecte et préservation des preuves
- Analyse des malwares et comportements adverses

Innov Systems

6 / Containment, éradication et remédiation

- Stratégies de confinement rapide
- Suppression des menaces actives
- Restauration sécurisée des systèmes

7 / Playbooks de réponse à incident

- Définition et structuration des playbooks
- Scénarios types (ransomware, phishing, DDoS)
- Automatisation via SOAR

8 / Gestion de crise cybersécurité

- Organisation d’une cellule de crise
- Communication interne et externe
- Gestion de la réputation et obligations légales

9 / Coordination et communication inter-équipes

- Collaboration avec RSSI, IT et direction
- Notification des autorités et régulateurs
- Gestion des parties prenantes externes

10 / Exercices et simulations d’incidents

- Tabletop exercises et simulations réalistes
- Analyse post-incident (retour d’expérience)
- Amélioration continue des capacités CSIRT

Innov 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

04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca
16 au 20 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