

Cybersécurité bancaire : Threat intelligence, incident response et forensic

Lien : https://maroc-performance.com/formation/cybersecurite-bancaire-threat-intelligence-incident-response-et-forensic

DURÉE
8 jours (56h)

RÉFÉRENCE
FA172

CATÉGORIE
Contrôle Interne Bancaire et Conformité

Maroc Performance

OBJECTIFS DE LA FORMATION

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

- Maîtriser les fondamentaux de la cybersécurité appliquée au secteur bancaire.
- Identifier les principales cybermenaces et vulnérabilités affectant les institutions financières.
- Comprendre les principes et méthodologies de Cyber Threat Intelligence.
- Exploiter les IoC, TTP et renseignements cyber pour renforcer la détection des menaces.
- Comprendre l’architecture et le fonctionnement d’un SOC bancaire.
- Savoir qualifier, prioriser et traiter les incidents de cybersécurité.
- Maîtriser les étapes d’un processus complet d’Incident Response.
- Acquérir les fondamentaux du Digital Forensics et de l’investigation numérique.
- Savoir reconstituer la chaîne d’attaque et déterminer l’étendue d’une compromission.
- Renforcer la capacité de réponse face aux ransomwares, malwares et attaques ciblant les systèmes de paiement.
- Intégrer les enjeux de gouvernance, résilience, conformité et gestion de crise cyber.
- Être capable de concevoir, tester et améliorer un dispositif intégré de Threat Intelligence, Incident Response et Forensic adapté à une institution bancaire.

Maroc Performance

👥 POUR QUI ?

- RSSI, CISO et responsables de la cybersécurité des banques et institutions financières.
- Responsables SOC, Cyber Defense et Security Operations.
- Cyber Threat Intelligence Analysts et Cybersecurity Analysts.
- Incident Response Managers et responsables de la gestion des incidents.
- Digital Forensics Analysts et experts en investigation numérique.
- Responsables IT, infrastructures, réseaux, cloud et sécurité des systèmes d’information.
- Responsables risques opérationnels, résilience et continuité d’activité.
- Responsables conformité, LCB-FT, fraude et sécurité financière.
- Auditeurs internes, contrôleurs permanents et spécialistes du contrôle des risques IT.
- Responsables sécurité des paiements, monétique et plateformes bancaires digitales.
- Consultants, experts cybersécurité et professionnels des services financiers numériques.
- Cadres dirigeants, responsables risques et membres des équipes de crise des banques, fintechs, établissements de paiement et institutions de microfinance.

Maroc Performance



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ BANCAIRE

- Comprendre les principaux enjeux de cybersécurité propres aux banques et institutions financières.
- Identifier les menaces ciblant les systèmes bancaires, plateformes de paiement, applications digitales et infrastructures critiques.
- Évaluer l'exposition aux risques cyber et leur impact sur la confidentialité, l'intégrité et la disponibilité des données.

2 / THREAT LANDSCAPE ET TYPOLOGIE DES CYBERMENACES

- Identifier les principales menaces : ransomware, phishing, malware, compromission de comptes, DDoS et attaques par ingénierie sociale.
- Analyser les modes opératoires des groupes cybercriminels ciblant le secteur financier.
- Évaluer les vulnérabilités liées aux environnements cloud, API, mobile banking, fintechs et prestataires tiers.

3 / CYBER THREAT INTELLIGENCE

- Comprendre les principes, sources et cycles de collecte de la Cyber Threat Intelligence.
- Exploiter les renseignements relatifs aux Indicators of Compromise (IoC), Tactics, Techniques and Procedures (TTP) et acteurs malveillants.
- Transformer la Threat Intelligence en mesures concrètes de prévention, détection et réponse aux menaces.

4 / SECURITY MONITORING ET SOC BANCAIRE

- Comprendre l'architecture et les fonctions d'un Security Operations Center (SOC) bancaire.
- Exploiter les SIEM, EDR, NDR et autres outils de détection pour centraliser et corréler les événements de sécurité.

Maroc Performance

- Mettre en place des mécanismes de surveillance, de corrélation et d’escalade des alertes cyber.

5 / DÉTECTION ET QUALIFICATION DES INCIDENTS

- Identifier les signaux permettant de distinguer une anomalie, une alerte de sécurité et un incident confirmé.
- Analyser les logs, événements systèmes, traces réseau et comportements inhabituels.
- Prioriser les incidents selon leur criticité, leur périmètre, leur impact potentiel et le niveau d’urgence.

6 / INCIDENT RESPONSE ET GESTION DE CRISE CYBER

- Maîtriser les étapes du cycle de réponse : préparation, identification, containment, éradication, récupération et retour d’expérience.
- Organiser les rôles et responsabilités des équipes techniques, métiers, conformité, juridique et direction générale.
- Élaborer des procédures d’escalade et de communication adaptées aux incidents majeurs affectant une institution financière.

7 / DIGITAL FORENSICS ET COLLECTE DES PREUVES

- Comprendre les principes de l’investigation numérique appliquée aux incidents bancaires.
- Collecter, préserver et analyser les preuves numériques dans le respect de leur intégrité et de leur traçabilité.
- Examiner les systèmes, postes, serveurs, environnements cloud, journaux et supports numériques compromis.

8 / ANALYSE FORENSIQUE DES CYBERATTAQUES

- Reconstituer la chronologie d’une compromission à partir des artefacts et traces disponibles.
- Identifier le vecteur d’attaque, les mécanismes de persistance, les mouvements latéraux et les actions de l’attaquant.
- Déterminer l’étendue de la compromission et les systèmes, comptes ou données potentiellement affectés.

9 / MALWARE, RANSOMWARE ET ANALYSE DES INDICATEURS DE COMPROMISSION

- Identifier les caractéristiques et comportements des malwares et ransomwares ciblant les institutions financières.

Maroc Performance

- Analyser les IoC et TTP afin d’identifier les infrastructures et activités malveillantes.
- Mettre en place des mécanismes permettant d’améliorer la détection et la réponse face aux attaques persistantes.

10 / CYBERSÉCURITÉ DES PAIEMENTS ET FRAUDE NUMÉRIQUE

- Identifier les menaces affectant les systèmes de paiement, cartes bancaires, virements, wallets et plateformes de paiement digital.
- Analyser les interactions entre cyberattaque, fraude financière, compromission de comptes et usurpation d’identité.
- Renforcer la coordination entre équipes cybersécurité, fraude, conformité et opérations bancaires.

11 / GOUVERNANCE, RÉSILIENCE ET CONFORMITÉ CYBER

- Mettre en place une gouvernance permettant de piloter les risques cyber, les incidents et la résilience opérationnelle.
- Intégrer les exigences de sécurité dans la gestion des fournisseurs, prestataires cloud et partenaires technologiques.
- Organiser la documentation, le reporting, les exercices de crise et l’amélioration continue du dispositif de cybersécurité.

12 / SIMULATION D’INCIDENT ET PLAN DE RÉPONSE BANCAIRE

- Concevoir et exécuter des scénarios de simulation d’incidents cyber affectant une institution financière.
- Tester la capacité des équipes à détecter, contenir, investiguer et remédier à une compromission.
- Construire un plan d’amélioration intégrant les enseignements du retour d’expérience et les mesures correctives prioritaires.

Maroc Performance

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Mises en Situation pour faciliter l'assimilation
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

12 au 21 Jan. 2027	Présentiel - Casablanca
08 au 17 Mars 2027	Présentiel - Casablanca
03 au 12 Mai 2027	Présentiel - Casablanca
28 Juin au 07 Juil. 2027	Présentiel - Casablanca
23 Août au 01 Sep. 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@maroc-performance.com
Web : https//www.maroc-performance.com

Maroc Performance — Tous droits réservés

Maroc Performance