

## Ransomware – Détection et gestion de la menace

2 jours (14 heures)

Initiation

Présentiel ou classe à distance

à partir de

**2 000 € HT** par personne (TVA en vigueur)

Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 02/10/2026.

### Objectifs

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

- Décrire l'écosystème et les tendances récentes des ransomwares (RaaS, double extorsion et data-only)
- Identifier les principales techniques d'intrusion et de mouvement latéral utilisées par les opérateurs de ransomware
- Mettre en oeuvre des stratégies de détection multi-couches (EDR / XDR, NDR, Threat Intelligence et logs)
- Concevoir et appliquer un playbook de réponse à incident ransomware aligné sur les bonnes pratiques (NIST et CSF ransomware profile)
- Mettre en place les activités de remédiation, de reprise et de durcissement post-incident
- Mettre en oeuvre une amélioration continue de la posture de sécurité face aux ransomwares au sein de l'organisation.

Les compétences visées par cette formation font l'objet d'une évaluation.

### À qui s'adresse cette formation ?

Ingénieurs et administrateurs systèmes / réseaux, analystes SOC, analystes détection et réponse (EDR / XDR / NDR), consultants et experts en cybersécurité offensive et défensive ainsi que les responsables techniques impliqués dans la réponse à incident et la gestion de crise cyber.

## Prérequis

Avoir des connaissances de base en réseaux (TCP / IP, segmentation, services) et systèmes (Windows/Linux) ainsi que des connaissances de base en sécurité des systèmes d'information (authentification, journalisation et vulnérabilités). Etre familier avec au moins un SIEM ou une solution EDR / XDR et avoir des notions de base en procédures de réponse à incident ou gestion de crise cybersécurité.

# Programme

## 1 Pendant votre formation

## Ransomware – Détection et gestion de la menace

Jour 1 – Matin

### Panorama de la menace ransomware

- Définitions et typologie des ransomwares
  - Ransomware "classique" vs data-only extortion
  - Double et triple extorsion
  - Chiffrement, vol de données et déni de service ciblé
- Evolution récente de l'écosystème
  - Ransomware as a Service (RaaS) et économie des affiliés
  - Fragmentation, rebranding et nouveaux groupes
  - Cibles privilégiées : supply chain, MSP et secteurs critiques
- Tendances techniques modernes
  - Ciblage des environnements hybrides, Linux et ESXi
  - Automatisation, scripts, Living-off-the-Land et fileless
  - Intelligence Artificielle (IA), deepfakes et ingénierie sociale avancée
- Impacts métier, réglementaires et assurantiels
  - Interruption d'activité et coûts indirects
  - Fuite de données, RGPD et implications légales
  - Pressions des régulateurs, cyberassurance et reporting

### Kill chain ransomware et scénarios d'attaque

- Chaîne d'attaque type d'un ransomware moderne
  - Reconnaissance, initial access et prise de pied
  - Escalade de privilèges, persistance et mouvement latéral

- Data staging, exfiltration, chiffrement et extorsion
- Vecteurs d'intrusion dominants
  - Phishing ciblé et compromission d'identifiants
  - Exploitation de vulnérabilités exposées (VPN, ESXi et appliances)
  - Compromission de fournisseurs, MSP et prestataires externes
- Techniques de furtivité et évaison
  - Living-off-the-Land (PsExec, PowerShell, WMI et outils natifs)
  - Evasion EDR / AV, chiffrement du trafic C2 et LOLBins
  - Désactivation des sauvegardes, Shadow Copies et services sécurité
- Etude de cas récents
  - Attaques sur secteurs finance et industrie
  - Attaques supply chain / MSP
  - Enseignements techniques pour la détection et la réponse

#### *Exemples de travaux pratiques (à titre indicatif)*

- *Analyse guidée d'un scénario d'attaque ransomware de bout en bout (diagramme kill chain, mapping tactiques / techniques MITRE)*
- *Identification des moments clés de détection possible et des indicateurs à collecter sur chaque étape*

Jour 1 – Après-midi

### **Hygiène de sécurité et mesures préventives**

- Gestion des surfaces d'attaque
  - Cartographie des actifs critiques et chemins d'accès
  - Exposition internet, Shadow IT et services exposés
  - Gestion des vulnérabilités et patch management
- Gestion des identités et des privilèges
  - MFA, gestion des comptes à privilèges et segmentation des droits
  - Durcissement AD / Azure AD et comptes de service
  - Politiques de mots de passe et détection d'abus d'identifiants
- Sauvegardes et résilience
  - Stratégies de sauvegarde (3-2-1, offline et immutable)
  - Tests de restauration et RTO / RPO
  - Protection des sauvegardes contre les ransomwares
- Sensibilisation et procédures internes
  - Formation utilisateurs aux signaux faibles (phishing et comportements anormaux)
  - Procédures de remontée d'alerte et de signalement
  - Coordination IT / Sécurité / Métiers

*Exemples de travaux pratiques (à titre indicatif)*

- *Atelier de revue d'une architecture existante : identification des points de durcissement prioritaires contre les ransomwares*
- *Exercice de revue de stratégie de sauvegarde et validation des hypothèses de restauration*

**Détection sur endpoints (EDR / XDR)**

- Principes de détection sur endpoints
  - Signatures et détection comportementale
  - Indicators of Compromise (IoC) et Indicators of Behavior (IoB)
  - Cas d'usage spécifiques aux ransomwares
- Règles et politiques de détection ransomware
  - Surveillance des processus de chiffrement massif
  - Détection de patterns de déplacement latéral et exfiltration
  - Blocage automatique, isolation machine et kill process
- Intégration EDR / XDR avec Threat Intelligence
  - Matching de campagnes connues et enrichissement de contexte
  - Gestion des faux positifs et tuning des règles
  - Suivi des groupes et familles actifs
- Investigation initiale côté endpoint
  - Timeline des événements et pivot sur artefacts
  - Analyses de dump mémoire, fichiers et artefacts persistants
  - Collecte de preuves pour la suite de la réponse

*Exemples de travaux pratiques (à titre indicatif)*

- *Analyse de télémétrie EDR simulée pour identifier un scénario de ransomware en cours (kill chain sur endpoints)*
- *Construction d'un ensemble de règles de détection ciblant plusieurs comportements ransomware typiques*

Jour 2 – Matin

**Détection réseau (NDR) et logs**

- Détection réseau et NDR
  - Visibilité réseau, flux, paquets et métadonnées
  - Détection d'anomalies, C2, exfiltration et mouvement latéral
  - Positionnement de NDR dans l'architecture de sécurité
- Intégration NDR / EDR / SIEM
  - Corrélation des alertes réseau et endpoint
  - Use cases SOC spécifiques aux ransomwares
  - Gestion des alertes, runbooks et priorisation
- Détection via SIEM, journaux applicatifs et systèmes

- Sources de logs pertinentes (AD, VPN, proxy, FW, mail...)
- Règles de corrélation et détection de patterns anormaux
- Détection de signaux faibles précurseurs d'une attaque
- Exemples d'alertes et de tableaux de bord ransomware
  - Tableaux de bord IOC / IOA
  - KPI de détection, MTTR et couverture use cases
  - Reporting technique vers le management

#### *Exemples de travaux pratiques (à titre indicatif)*

- *Analyse d'un jeu de logs / SIEM simulés pour identifier une campagne de ransomware (focalisation sur signaux réseau)*
- *Conception d'un jeu minimal de règles SIEM orientées détection précoce ransomware*

### **Threat Intelligence et veille ransomware**

- Rôle de la Threat Intelligence dans la détection ransomware
  - Flux de TI (IoC, TTP et bulletins sectoriels)
  - Cartographie des groupes et familles de ransomwares
  - Priorisation des menaces et focalisation sur les plus probables
- Sources et plateformes de veille
  - Sources publiques, sectorielles et communautés de partage
  - Plateformes TIP et intégration avec SIEM et EDR / XDR
  - Bonnes pratiques d'opérationnalisation de la TI
- Alignement sur MITRE ATT&CK et CSF ransomware
  - Mapping des TTP par groupe de menace
  - Utilisation du profile ransomware NIST CSF pour prioriser
  - Identification des gaps de détection par TTP
- Processus de veille continue et gestion des campagnes
  - Détection des nouvelles campagnes, lenteurs et réutilisation de TTP
  - Mises à jour des règles, playbooks et use cases SOC
  - Communication régulière des risques aux équipes internes

#### *Exemples de travaux pratiques (à titre indicatif)*

- *Atelier de construction d'une fiche de menace pour un groupe ransomware (profil, TTP, IoC et vecteurs privilégiés)*
- *Mise à jour d'un use case SOC et d'un runbook à partir de nouvelles informations de Threat Intelligence*

Jour 2 – Après-midi

### **Playbook de réponse à incident ransomware**

- Référentiels et cadres de réponse
  - NIST CSF 2.0 et profil ransomware

- NIST 800-61 (incident handling)
- Intégration dans la gouvernance globale cybersécurité
- Détection et déclenchement du playbook
  - Critères de qualification de l'incident ransomware
  - Notification interne, escalade et mobilisation de l'équipe de réponse
  - Premières mesures de confinement rapide
- Containment, eradication et recovery
  - Segmentation et isolement des systèmes compromis
  - Suppression des artefacts malveillants et backdoors
  - Organisation de la restauration (priorisation, tests et contrôles)
- Communication, juridique et parties prenantes externes
  - Communication interne, direction et métiers
  - Relations avec autorités, CNIL, régulateurs et forces de l'ordre
  - Gestion des prestataires, assureurs et partenaires

#### *Exemples de travaux pratiques (à titre indicatif)*

- *Elaboration collective d'un playbook ransomware pour l'organisation type (étapes, rôles et décisions clés)*
- *Exercice table-top sur la mise en oeuvre du playbook (jeu de rôles, décisions et arbitrages techniques)*

#### **Remédiation, durcissement post-incident et amélioration continue**

- Analyse post-incident et leçons apprises
  - Reconstitution détaillée de la chronologie
  - Analyse des causes racines techniques et organisationnelles
  - Plan d'action correctif et préventif
- Durcissement de l'infrastructure
  - Renforcement des contrôles d'accès et segmentation
  - Amélioration de la surveillance et de la détection
  - Renforcement des sauvegardes et tests de restauration
- Mise à jour des playbooks et use cases
  - Intégration des nouveaux IOC / TTP dans les outils de détection
  - Ajustement des playbooks de réponse et procédures crise
  - Mise à jour des formations utilisateurs et des exercices
- Indicateurs de maturité et reporting
  - Indicateurs clés liés à la menace ransomware
  - Suivi de la maturité par rapport au profil NIST CSF ransomware
  - Intégration dans les tableaux de bord de gouvernance cyber

#### *Exemples de travaux pratiques (à titre indicatif)*

- *Elaboration d'un plan d'amélioration continue post-incident pour une organisation type (technique, processus et humain)*
- *Définition d'un set d'indicateurs de suivi spécifique à la menace ransomware pour le COMEX et l'IT*

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel\* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode\*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

\* nous consulter pour la faisabilité en distanciel

\*\* ratio variable selon le cours suivi

### Accessibilité aux personnes en situation de handicap

## Détails de la session

Du 7 octobre 2026 au 8 octobre 2026 (2 jours / 14 heures)

À distance

Du 7 octobre 2026 au 8 octobre 2026

À distance

- 7 octobre 2026 ..... 9h00 – 16h30
- 8 octobre 2026 ..... 9h00 – 16h30