

TIP 2.12

Réagir face à un poste suspect ou compromis

Fiche de révision - Équipements numériques

1. Signes d'alerte à reconnaître

Indice	Exemple
Antivirus	Détection, quarantaine ou protection désactivée sans raison.
Système	Processus inconnu, ralentissement brutal, fenêtre PowerShell inattendue.
Navigateur	Pop-ups, redirections, extension inconnue.
Données	Fichiers renommés, chiffrés ou inaccessibles.
Compte	Demandes MFA non sollicitées, messages envoyés à l'insu de l'utilisateur.

Méthode à retenir :
Identifier → Contenir → Préserver → Alerter → Analyser → Remédier → Valider

2. Première réaction : contenir l'incident

Si une compromission active est fortement suspectée, la priorité est de limiter son impact. Selon la procédure, cela peut consister à isoler le poste du réseau : câble Ethernet débranché, Wi-Fi désactivé ou fonction d'isolation d'une solution de sécurité centralisée.

Attention : isoler ne signifie pas forcément éteindre. Un arrêt ou un redémarrage peut faire disparaître des informations utiles présentes en mémoire. Suivre la procédure d'incident et escalader rapidement.

3. Préserver les informations utiles

À relever	Pourquoi
Date / heure	Reconstituer la chronologie.
Poste / utilisateur	Identifier précisément le périmètre.
Message / alerte	Conserver le texte exact de la détection.
Fichier / chemin	Identifier l'élément concerné.
Actions réalisées	Éviter les doublons et comprendre ce qui a déjà modifié l'état du poste.

4. Outils Windows utiles

Outil / commande	Usage
Get-MpComputerStatus	État de Microsoft Defender et de plusieurs protections.
Get-MpThreatDetection	Consulte des détections Defender.
Get-Process	Liste les processus actifs.
Get-NetTCPConnection	Affiche des connexions TCP actives.
eventvwr.msc	Observateur d'événements Windows.
perfmon /rel	Moniteur de fiabilité et chronologie des incidents.
Get-FileHash	Calcule une empreinte permettant d'identifier précisément un fichier.

5. Compte potentiellement compromis

Situation	Réaction adaptée
Phishing avec mot de passe saisi	Traiter le compte comme potentiellement compromis.
Demandes MFA inattendues	Refuser les demandes et signaler immédiatement.
Changement de mot de passe	Le faire depuis un équipement considéré comme sain, selon la procédure.
Sessions actives	Peuvent nécessiter une révocation par l'équipe compétente.

6. Ransomware

Indices possibles : fichiers chiffrés ou renommés, note de rançon, activité inhabituelle et accès aux partages réseau. La priorité est l'isolement du poste, l'alerte et la protection du reste du SI. Ne pas restaurer immédiatement une sauvegarde sur un système encore compromis.

À éviter : payer ou négocier, supprimer les traces au hasard, connecter d'autres supports, continuer à utiliser le poste ou copier des fichiers vers un partage réseau.

7. Support USB ou fichier suspect

Ne pas brancher une clé USB suspecte sur d'autres machines et ne pas ouvrir un fichier douteux sur son propre poste pour « voir ce qu'il fait ». L'analyse doit être réalisée avec les outils et environnements prévus par l'organisation.

8. Escalader au bon moment

Escalade nécessaire si...	Informations à transmettre
Compromission confirmée ou fortement suspectée.	Utilisateur, poste, date et heure.
Plusieurs postes ou comptes concernés.	Symptômes, messages et chronologie.
Ransomware ou compte privilégié touché.	Fichiers concernés et alertes de sécurité.
Données sensibles potentiellement exposées.	Actions déjà réalisées et état actuel du poste.

9. Ce qu'il faut éviter

Mauvaise action	Risque
Éteindre / redémarrer systématiquement	Perte d'informations volatiles utiles à l'analyse.
Supprimer les fichiers suspects	Destruction d'éléments utiles à l'investigation.
Nettoyer les journaux	Suppression de traces importantes.
Réinstaller immédiatement Windows	Effacement d'indices avant décision de remédiation.
Changer le mot de passe depuis le poste suspect	Le nouveau secret pourrait être intercepté.

10. Validation du retour en service

Contrôle	État attendu
Incident	Traité selon la procédure.
Système	Considéré comme sain ou reconstruit.
Protections	Antivirus, pare-feu et mises à jour opérationnels.
Comptes	Identifiants renouvelés et MFA contrôlé si nécessaire.
Données	Restaurées depuis une source considérée comme fiable.
Utilisateur	Informé des actions à retenir et des bons réflexes.
Traçabilité	Incident et actions documentés.

11. À retenir

Face à un poste suspect : ne pas improviser. Identifier les symptômes, contenir l'incident, préserver les informations utiles, alerter l'équipe compétente, puis analyser, remédier et valider le retour en service selon la procédure.