



RÉPONSE À INCIDENT CYBER ET GESTION DE CRISE

Compte piraté, virement détourné, serveurs chiffrés : contenir, restaurer, déclarer, puis renforcer. À distance dès le premier appel, sur site en Martinique et en Guadeloupe depuis Sainte-Marie.

LES PREMIÈRES HEURES DÉCIDENT DE TOUT

Une cyberattaque ne se gère pas dans la panique. Débrancher au mauvais moment détruit les preuves ; restaurer trop vite réinstalle l'attaquant ; payer la rançon ne garantit rien. L'incident est devenu ordinaire : c'est la réponse qui fait la différence.

128 ²

compromissions par rançongiciel signalées à l'ANSSI en 2025, dont 48 % de TPE, PME et ETI

+93 % ¹

de fraudes au virement visant les entreprises en 2025 — le délai de réaction conditionne le rappel des fonds

+45 % ¹

de piratages de comptes chez les professionnels : la porte d'entrée la plus fréquente d'une intrusion

72 h

pour déposer plainte (LOPMI) afin d'être indemnisé, et pour notifier une violation de données à la CNIL



En Martinique et aux Antilles : la CTM paralysée par le rançongiciel Rhysida et Le Robert touché (2023), une attaque DDoS contre Dauphin Telecom et Coral Telecom (2023), des cabinets d'avocats visés, et en 2026 le vol revendiqué de 43 Go de données de l'Éducation nationale ³. TAVITA CYBERSECURITY, implantée à Sainte-Marie, est intervenue 11 fois après une cyberattaque en cinq ans.

Sources — ¹ Cybermalveillance.gouv.fr, *Rapport d'activité et état de la menace 2025* • ² ANSSI, *Panorama de la cybermenace 2025*, CERTFR-2026-CTI-002 • ³ Presse locale : Le Pélican, Journal de Saint-Barth, Bondamanjak, RCI, ETV.

LES BONS RÉFLEXES EN ATTENDANT NOTRE APPEL

1

Isoler, ne pas éteindre

Débranchez le réseau des machines suspectes mais laissez-les allumées : la mémoire vive contient des preuves qui disparaissent à l'extinction.

3

Changer les accès critiques

Depuis un appareil sain : mots de passe administrateurs, messagerie et banque en ligne ; activez la double authentification.

5

Nous appeler

+33 6 99 63 17 11. Désignez un interlocuteur unique, réunissez direction, informatique et prestataires.

2

Préserver

Ne restaurez pas, ne réinstallez pas, ne payez pas. Photographiez les écrans de rançon et notez l'heure de chaque constat.

4

Alerter la banque

En cas de virement suspect, appelez immédiatement votre banque pour tenter un rappel de fonds.

6

Ne pas communiquer seul

Ni sur les réseaux sociaux, ni avec l'attaquant : la communication se prépare avec nous.

PLAINTÉ

Sous 72 h en gendarmerie ou au commissariat, condition de l'indemnisation par l'assureur.

CNIL

Notification sous 72 h dès qu'une donnée personnelle est exposée, information des personnes si le risque est élevé.

ANSSI • ASSUREUR

Signalement ANSSI (24 h en NIS 2), déclaration à l'assureur, parcours 17Cyber, délais préfectoraux possibles.

Choisir TAVITA CYBERSECURITY, c'est faire le choix d'un partenaire de confiance, expert, réactif et engagé pour la protection durable de votre système d'information.

NOTRE INTERVENTION AU VERSO →

NOTRE INTERVENTION, DE L'ALERTE AU RETOUR À LA NORMALE



Une réponse à incident est une course contre l'attaquant et contre l'horloge réglementaire. TAVITA CYBERSECURITY prend la main dès le premier appel et conduit les six phases ci-dessous avec vos équipes et vos prestataires, jusqu'à un système d'information restauré et durci.

SIX PHASES, UNE SEULE CHAÎNE DE COMMANDEMENT

1 • Qualifier

Premières heures

Cadrage, périmètre touché, criticité, hypothèse d'attaque. Cellule de crise : direction, informatique, prestataires, un interlocuteur unique.

2 • Contenir

Jour 1

Isolement des segments et comptes compromis, blocage des accès distants, préservation des journaux et images mémoire pour l'enquête.

3 • Comprendre

Jours 1 à 3

Analyse forensique : point d'entrée, mouvements latéraux, données exfiltrées, persistance. Indicateurs de compromission partagés avec vos outils et l'ANSSI.

4 • Restaurer

Jours 2 à 10

Reconstruction depuis des sauvegardes vérifiées saines, réinitialisation de l'Active Directory et des secrets, remise en service par priorité métier.

5 • Déclarer

En parallèle

Plainte, notification CNIL, signalement ANSSI, dossier assureur ; éléments de langage pour vos équipes, clients, partenaires et, si besoin, la presse.

6 • Durcir et apprendre

Semaines suivantes

Rapport d'incident, plan de remédiation priorisé (MFA, EDR, sauvegardes hors ligne, supervision), retour d'expérience et exercice de crise.

CE QUE VOUS RECEVEZ

- 1 Un pilote unique de la crise**
Un interlocuteur qui coordonne informatique, prestataires, assureur, autorités et direction, et décide avec vous, pas à votre place.
- 2 Des preuves exploitables**
Journaux, images disque et mémoire, chronologie de l'attaque : recevables pour la plainte, l'assureur et une éventuelle procédure.
- 3 Un rapport d'incident**
Ce qui s'est passé, ce qui a été touché, ce qui a été fait, ce qui reste à faire : lisible par un dirigeant comme par un DSI.
- 4 Les déclarations rédigées**
Plainte, notification CNIL, signalement ANSSI, déclaration de sinistre : préparés dans les délais, avec les pièces attendues.
- 5 Un SI restauré et durci**
Pas un simple retour à l'état d'avant : les failles exploitées sont fermées avant la remise en service.
- 6 Un plan « la prochaine fois »**
Plan de réponse en une page, contacts, procédures, et un exercice sur table avec votre direction.

DEUX FAÇONS DE NOUS SOLLICITER

En urgence, sans contrat préalable

Un appel, un cadrage de 30 minutes, une intervention à distance dans la foulée, un devis transmis dans la journée. Déplacement sur site en Martinique le jour même, en Guadeloupe et en Guyane sous 24 à 48 h.

Avant l'incident : contrat de réponse à incident

Engagement de prise en charge, plan de réponse et contacts en place, connaissance préalable de votre SI, exercice de crise annuel. Attendu par les assureurs et NIS 2 ; intégrable au RSSI externalisé.



VOTRE INTERLOCUTEUR EN CAS DE CRISE

David TOUCHE Gérant et consultant en cybersécurité

Ancien des forces armées, 23 ans au Ministère des Armées, 28 ans en SI dont 17 en cybersécurité ; ISO/IEC 27005 Risk Manager, label ExpertCyber. Originaire de Sainte-Marie et installé en Martinique, 11 crises cyber gérées en cinq ans, membre de la Cybersecurity Flying Squad Paris 2024. Il conduit personnellement chaque intervention.

VOUS ÊTES ATTAQUÉ ? APPELEZ.

Un premier échange n'engage à rien et évite les erreurs irréversibles des premières heures.

contact@tavita-cybersecurity.com

+33 6 99 63 17 11 • +689 87 30 41 25

www.tavita-cybersecurity.com

Nous suivre : linktr.ee/TAVITACYBERSECURITY

SIRET 798 544 722 00035 • N° Tahiti E31755 • RCS 211712A