TAVITA CYBERSECURITY
GARDIEN CYBER DES TERRITOIRES

PME · ETI · GROUPES

ACCOMPAGNEMENT CYBER SUR MESURE DES PME, ETI ET GROUPES

Structurer, gouverner, superviser : un accompagnement proportionné à votre taille, votre exposition et vos obligations réglementaires, de la PME au groupe multi-sites.

LES ENTREPRISES, PREMIÈRES VICTIMES

ERP, messagerie, données clients et RH, sites de production, prestataires interconnectés : plus l'entreprise grandit, plus sa surface d'attaque s'étend. Les PME et ETI sont la première cible des cybercriminels, et les bilans 2025 de Cybermalveillance.gouv.fr, de l'ANSSI et de la CNIL le confirment.

+73 % [1]
de demandes d'assistance d'entreprises et d'associations sur le 17Cyber en 2025

48 % [2]
des 128 victimes de rançongiciel signalées à l'ANSSI en 2025 sont des TPE, PME et ETI, catégorie la plus touchée

+93 % [1]
de fraudes au virement visant les entreprises en 2025 : un faux fournisseur ou un faux dirigeant, et la trésorerie part

+45 % [1]
de piratages de comptes chez les professionnels en 2025, première menace : Microsoft 365, VPN, comptes à privilèges

Concrètement : un compte à privilèges compromis ouvre l'Active Directory ; un rançongiciel chiffre les serveurs et exfiltre les données avant de les publier ; un prestataire mal sécurisé sert de rebond. Aux Antilles, opérateurs télécoms, cabinets d'avocats et collectivités ont déjà été touchés (2023) [4]. TAVITA CYBERSECURITY est intervenue 11 fois après une cyberattaque auprès de PME, ETI et groupes.

Sources — [1] Cybermalveillance.gouv.fr, *Rapport d'activité et état de la menace 2025* (cybermalveillance.gouv.fr) · [2] ANSSI, *Panorama de la cybermenace 2025*, CERTFR-2026-CTI-002 (cyber.gouv.fr) · [4] Presse locale : Le Pélican, Journal de Saint-Barth, Bondamanjak, RCI.

SE METTRE EN CONFORMITÉ N'EST PLUS UNE OPTION

RGPD Mesures de sécurité adaptées (art. 32), registre, analyses d'impact, DPO selon l'activité, notification d'une violation à la CNIL sous **72 h**.

NIS 2 Entités essentielles et importantes de 18 secteurs (dès 50 salariés ou 10 M€ de CA) : gestion des risques, notification des incidents sous 24 h, chaîne d'approvisionnement, responsabilité des dirigeants.

ASSURANCE Indemnisation conditionnée à un dépôt de plainte sous **72 h** (LOPMI) ; les assureurs exigent MFA, EDR, sauvegardes hors ligne, PCA/PRA et audits documentés.

DORA · CRA Résilience numérique du secteur financier (DORA) et sécurité des produits connectés (Cyber Resilience Act) : des exigences que vos clients et donneurs d'ordre répercutent dans leurs contrats et appels d'offres.

SANCTIONS
486,8 M€ d'amendes CNIL en 2025 ; NIS 2 : jusqu'à 2 % du CA et responsabilité des dirigeants.

ACTIVITÉ
Arrêt de production, perte de clients, exclusion des appels d'offres et des chaînes de sous-traitance exigeant des garanties cyber.

ASSURANCE & AIDES
Refus ou surprime d'assurance cyber ; aides (Diag Cybersécurité Bpifrance) conditionnées à une démarche structurée.

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 RÉPONSE AU VERSO →

UN ACCOMPAGNEMENT SUR MESURE, DIMENSIONNÉ À VOTRE TAILLE

Une PME de 60 personnes et un groupe multi-sites n'ont ni les mêmes obligations ni les mêmes moyens. TAVITA CYBERSECURITY refuse toute approche standardisée : après un diagnostic préalable, nous dimensionnons le dispositif à votre taille, votre exposition et vos obligations, par paliers activables un par un, chacun chiffré sur devis.

TROIS APPROCHES SELON VOTRE TAILLE

PME — structurer

Audit complet puis pilotage à temps partagé

Audit technique et organisationnel, remédiation des points critiques, sensibilisation des équipes, PSSI et charte, PCA/PRA, conformité RGPD et dossier assureur ; RSSI à temps partagé quelques jours par mois.

ETI — gouverner

Gouvernance SSI et supervision continue

Analyse de risques EBIOS RM, conformité NIS 2, ISO 27001, DORA, comité SSI et tableau de bord, SOC/EDR/SIEM, tests d'intrusion, gestion des risques tiers, exercices de crise avec la direction.

Groupe — industrialiser

Multi-sites, filiales et chaîne d'approvisionnement

Schéma directeur cyber groupe, politiques communes et déclinaison par site, SMSI ISO 27001, supervision centralisée, audits des filiales et des prestataires, exercices de crise inter-sites, reporting au comité de direction.

DES MODULES À ACTIVER SELON VOS PRIORITÉS

1 — Audit et sécurisation du SI
Active Directory, Microsoft 365, pare-feu, EDR, réseau et Wi-Fi, sauvegardes, applications métier, scan web, test d'intrusion ; puis remédiation.

2 — Audit organisationnel et risques
Cartographie des processus, rôles, dépendances (prestataires, cloud), analyse de risques EBIOS RM et plan d'amélioration priorisé.

3 — Sensibilisation et formation
Comité de direction, comptabilité, métiers, équipes IT : hygiène numérique, fraude au virement, campagnes de phishing simulées, formation des administrateurs.

4 — Gouvernance SSI et conformité
PSSI, charte, comité SSI, cartographie des exigences RGPD, NIS 2, DORA, ISO 27001 et plan de conformité opposable à vos assureurs et donneurs d'ordre.

5 — Gestion de crise et réponse à incident
PCA/PRA, plan de réponse, exercices sur table ; en cas d'attaque : contenir, restaurer, forensique, déclarations (plainte sous 72 h, CNIL, assureur).

6 — Supervision et maintien en condition de sécurité
SOC/EDR (Wazuh), veille darkweb, gestion des vulnérabilités, durcissement continu, infogérance sécurisée, reporting mensuel.

TROIS MODALITÉS D'INTERVENTION, COMBINABLES

RSSI / DSI externalisé

Pilotage SSI et IT à temps partagé, de quelques heures par mois à plusieurs jours, conseil à la direction, interface avec prestataires, assureurs et autorités.

Conseil et intervention ponctuels

Diagnostic flash, audit, test d'intrusion, remédiation, sensibilisation, schéma directeur cyber ou volet sécurité de vos projets, à la journée.

Réponse à incident

Compte à privilèges compromis, virement détourné, serveurs chiffrés : contenir, restaurer, analyser, déclarer, et renforcer pour que cela ne se reproduise pas.

VOTRE INTERLOCUTEUR

David TOUCHE — Gérant et consultant en cybersécurité

Architecte système, réseau et sécurité, ancien des forces armées : 23 ans au Ministère des Armées, 28 ans d'expérience en SI dont 17 en cybersécurité. Master 2, certifié ISO/IEC 27005 Risk Manager, membre de la Cybersecurity Flying Squad Paris 2024. Il intervient personnellement sur chaque mission.

Ils nous font déjà confiance : Solari Mobility Group, hôtels Maitai, Pacific Beachcomber, SOPADEP · 57 projets d'audit et de sécurisation · 5 entreprises supervisées (SOC) · 11 interventions après cyberattaque · 234 personnes formées.

SUR MESURE, SUR DEVIS

Un premier échange et un diagnostic de votre exposition suffisent pour bâtir une proposition adaptée à votre taille, vos priorités et votre budget.

contact@tavita-cybersecurity.com
+33 6 99 63 17 11 · +689 87 30 41 25
www.tavita-cybersecurity.com
Nous suivre : linktr.ee/TAVITACYBERSECURITY