FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

Cybersécurité pour Grandes Entreprises en Belgique

Guide Grand Compte

Vous avez les moyens, les équipes et la complexité. Mais les attaques qui vous visent sont d'un autre calibre, et les angles morts se cachent souvent dans l'organisation, pas dans la technique. Ce guide parle au COMEX autant qu'au CISO.

Scannez pour acceder a la version en ligne

contact@flashmodz.be | +32 471 87 87 07

https://flashmodz.be

FlashModz

L'essentiel en 5 minutes

Vous avez les moyens et les équipes. Mais les angles morts se cachent dans l'organisation, pas dans la technique.

1

La menace a changé de nature : elle vise désormais le COMEX

Les groupes APT étatiques ciblent la Belgique, siège de l'OTAN et des institutions européennes, et restent des mois dans les réseaux avant détection (IBM mesure un délai moyen de détection et confinement de plusieurs mois, année après année). Et NIS2 art. 20 engage désormais la responsabilité personnelle des dirigeants.

2

Le coût réel d'une violation va bien au-delà de la rançon

IBM chiffre le coût moyen mondial d'une violation à 4,88 M$ (Cost of a Data Breach 2024) : remédiation, notification, communication de crise, perte de clientèle, procédures. La rançon n'est qu'une fraction de la facture. S'y ajoutent les amendes : jusqu'à 10 M€ ou 2% du CA mondial sous NIS2, jusqu'à 20 M€ ou 4% sous le RGPD.

3

Vos angles morts ne sont pas techniques, ils sont organisationnels

Silos IT/métiers, dette technique, environnements hybrides (cloud, on-premise, OT, IoT), fusions mal intégrées, prestataires mal encadrés. Une part significative des violations implique un acteur interne ou un tiers de confiance (Verizon DBIR). Le PAM et le TPRM restent les parents pauvres.

4

Une équipe à taille humaine peut compléter (pas remplacer) vos équipes

Vos équipes internes sont compétentes, mais surchargées et soumises au quotidien. Un cabinet externe apporte du recul, des ressources de pointe ponctuelles (audit NIST CSF, vCISO, threat hunting), et la flexibilité d'une structure agile, sans les contraintes d'un grand cabinet.

5

La résilience opérationnelle se prouve, ne se déclare plus

NIS2 (via CyFun, ISO 27001 ou inspection CCB), DORA et bientôt l'AI Act exigent des preuves vérifiables : tests d'intrusion, exercices de crise, registre des prestataires critiques, rapports d'incidents. La transparence remplace la confiance, et les régulateurs belges (FSMA, BNB, APD, CCB) contrôlent activement depuis 2026.

Et maintenant ?

Les pages qui suivent détaillent chacun de ces points avec exemples, chiffres et actions concrètes.

Document conçu pour Grandes Entreprises & ETI · Lecture : ~15-20 min · Édition 2026

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

Le marché belge en chiffres

Chapitre 1

4,88 M$

coût moyen mondial d'une violation de données (IBM Cost of a Data Breach 2024)

Sources : textes officiels (NIS2, RGPD, DORA) et publications des éditeurs cités

277j

délai moyen pour identifier et contenir une violation de données (IBM, rapport 2023)

18/04/2026

échéance de conformité des entités essentielles NIS2 (CyFun ou ISO 27001) : elle est passée, le CCB contrôle

10 M€

amende NIS2 maximale pour une entité essentielle, ou 2% du CA mondial

Contexte & enjeux

Parlons franchement. Vous avez probablement un CISO, un SOC (interne ou externe), des budgets sécurité. Et pourtant, vous savez que ce n'est pas suffisant. Parce que le problème n'est plus technique. Il est organisationnel.

Les silos entre IT et métiers, la dette technique accumulée, les environnements hybrides (cloud, on-premise, OT, IoT), les fusions mal intégrées, les prestataires mal encadrés. Les angles morts sont partout, et les attaquants les connaissent mieux que vous.

Le CCB documente année après année des campagnes d'espionnage ciblant des entreprises belges : défense, énergie, finance, santé. La Belgique, siège de l'OTAN et des institutions européennes, est un terrain privilégié pour le cyber-espionnage d'État.

NIS2 et DORA ont changé la donne. La loi NIS2 belge est en vigueur depuis le 18 octobre 2024, l'échéance de conformité des entités essentielles (18 avril 2026) est passée, et le CCB est en phase de contrôle actif. L'article 20 rend les organes de direction personnellement responsables : un COMEX qui ignore les risques cyber s'expose à des sanctions individuelles. L'ignorance n'est plus une défense juridique.

Chez FlashModz Enterprise, on ne prétend pas remplacer vos équipes internes. On les renforce. Les ressources humaines, les connaissances pointues et les outils de niveau entreprise qu'on apporte viennent compléter ce qui existe. On a construit notre savoir-faire dans les grands comptes, c'est notre ADN. Et on le met à disposition avec l'agilité d'une structure à taille humaine, sans les contraintes d'un grand cabinet.

> *"La maturité cyber d'un grand compte se mesure à sa capacité à transformer un incident en non-événement médiatique. Le reste, c'est de la cosmétique."*
>
> — Jérémy Manet, FlashModz Enterprise

Les menaces qui pèsent sur vous

Chapitre 2

Ces risques sont réels, documentés, et touchent des entreprises belges chaque semaine.

Des États dans votre réseau

APT28 (Russie), APT41 (Chine), Lazarus (Corée du Nord) : ces groupes ciblent activement les entreprises et institutions belges. IBM mesure chaque année un délai de détection et de confinement qui se compte en mois. Largement le temps de copier tout ce qui a de la valeur.

Ransomware + chantage à la publication

Les groupes comme LockBit pratiquent la double extorsion : ils chiffrent VOS données et menacent de les publier si vous ne payez pas. La rançon n'est qu'une fraction de la facture réelle : remédiation, notification, communication de crise, perte de clients, procédures. IBM chiffre le coût moyen mondial d'une violation à 4,88 M$ (rapport 2024).

Un seul fournisseur compromis, et tout s'effondre

L'affaire MOVEit en 2023 : un seul logiciel de transfert de fichiers compromis, plus de 2.500 organisations impactées dans le monde. Votre surface d'attaque, ce n'est pas juste votre réseau. C'est chaque fournisseur, chaque SaaS, chaque API.

Vos usines et vos infrastructures physiques

L'IT et l'OT convergent, et les attaquants l'ont compris. Colonial Pipeline a montré en 2021 qu'un ransomware sur le réseau IT peut paralyser des infrastructures physiques. En Belgique, le port d'Anvers a déjà été la cible d'intrusions informatiques documentées.

Le CA est désormais responsable. Personnellement.

NIS2, article 20 : les organes de direction doivent approuver et superviser les mesures de cybersécurité, et peuvent être tenus personnellement responsables des manquements, jusqu'à l'interdiction temporaire d'exercer des fonctions dirigeantes. Ce n'est pas de la théorie, c'est du droit belge en vigueur depuis le 18 octobre 2024.

La menace vient aussi de l'intérieur

Un employé mécontent, un compte admin compromis, un prestataire avec trop d'accès. Le Verizon DBIR documente chaque année une part significative de violations impliquant un acteur interne. Et la gestion des accès privilégiés (PAM) reste le parent pauvre de la plupart des grandes organisations.

Mythes vs Réalité

Chapitre 3

Six idées reçues qui empêchent d'agir — et ce qu'en disent les chiffres.

01

ON ENTEND SOUVENT

Notre SOC tourne 24/7, on détecte toutes les attaques.

EN RÉALITÉ — *Use cases > outils*

Un SOC mal calibré génère des milliers d'alertes par jour, dont l'écrasante majorité est du bruit. Sans threat intelligence contextualisée et sans use cases métier, les vraies attaques (slow & low) passent inaperçues. Ce qui compte, ce n'est pas d'avoir un SOC : c'est qu'il détecte vraiment les comportements anormaux.

02

ON ENTEND SOUVENT

On est victime du même bruit de fond que tout le monde.

EN RÉALITÉ — *CCB · Threat reports*

Les grandes entreprises belges sont ciblées spécifiquement : OTAN et institutions européennes à Bruxelles, énergie, défense, santé, finance. Le CCB documente régulièrement des campagnes d'espionnage visant des organisations belges. Les attaquants connaissent vos noms de domaine, vos employés clés, vos prestataires.

03

ON ENTEND SOUVENT

On commande des audits annuels au Big Four, on a une roadmap.

EN RÉALITÉ — *Complémentarité*

Les rapports des grands cabinets sont utiles pour le board, mais souvent génériques et déconnectés de vos opérations, donc inutilisables au niveau tactique. Une approche complémentaire, avec un cabinet à taille humaine qui accompagne la mise en œuvre, apporte des résultats opérationnels, pas seulement de la conformité documentaire.

04

ON ENTEND SOUVENT

En migrant vers Azure / AWS, on a délégué la sécurité.

EN RÉALITÉ — *Responsabilité partagée*

Le modèle de responsabilité partagée signifie que VOUS restez responsable de la configuration, des accès, des données. Gartner estime que la quasi-totalité des défaillances de sécurité cloud relèvent de la responsabilité du client, pas du fournisseur. Une migration cloud sans Cloud Security Posture Management (CSPM) est un transfert de risque, pas une réduction.

05

ON ENTEND SOUVENT

On a des SLA cyber dans nos contrats, c'est suffisant.

EN RÉALITÉ — *ENISA · MOVEit 2023*

L'affaire MOVEit en 2023 a montré qu'un seul prestataire compromis impacte des milliers d'organisations. Les SLA contractuels ne remplacent pas un programme de Third-Party Risk Management : audits réguliers, droit d'audit exercé, right-to-know sur les sous-traitants, plan de sortie en cas de défaillance. NIS2 (art. 21) et DORA l'exigent d'ailleurs explicitement.

06

ON ENTEND SOUVENT

Notre réseau OT n'est pas connecté à Internet, donc protégé.

EN RÉALITÉ — *Dragos · rapports OT*

La convergence IT/OT est généralisée : remote maintenance, IIoT, supervision centralisée. L'isolation totale n'existe quasiment plus. L'attaque sur Colonial Pipeline a montré qu'un ransomware sur le SI bureautique peut paralyser l'OT par effet de bord. Une segmentation IT/OT stricte avec data diodes reste indispensable.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

CAS 1 // Énergéticien belge — 4 mois d'intrusion dans le réseau OT

Contexte: Un groupe APT exploite une faille connue dans un VPN Fortinet. Pendant 4 mois, les attaquants se déplacent latéralement dans le réseau jusqu'à atteindre les systèmes SCADA contrôlant des sous-stations électriques. Personne ne voit rien, jusqu'au jour où ils commencent à tester des commandes.

Impact: 8,2 millions d'euros de remédiation. Intervention du CCB et de la Défense. 6 mois de reconstruction IT/OT. Notification au régulateur et aux clients. Enquête AIPD toujours en cours.

Leçon: Une segmentation IT/OT stricte et un SOC avec détection d'anomalies réseau auraient identifié l'intrusion en jours, pas en mois. Le patch Fortinet était disponible depuis 3 mois au moment de l'attaque.

CAS 2 // Institution financière à Bruxelles — double extorsion

Contexte: Un employé tombe dans un piège de spear-phishing ultra-ciblé. LockBit entre, exfiltre 2,3 To de données clients et financières, puis chiffre les systèmes. La double peine : payer la rançon OU voir les données publiées.

Impact: Rançon demandée : 4 millions d'euros. Coût total (arrêt, remédiation, régulateur, communication de crise, risque de class action) : 12 millions d'euros. La confiance des clients est durablement entamée.

Leçon: Un EDR/XDR sur tous les endpoints aurait détecté l'exfiltration en cours. Une stratégie DLP aurait bloqué la sortie des 2,3 To. Des sauvegardes immuables auraient rendu le chiffrement inopérant.

CAS 3 // Groupe hospitalier — retour au papier pendant 5 semaines

Contexte: Trois sites hospitaliers. Un ransomware entre et chiffre tout : dossiers patients, imagerie médicale, planning opératoire, pharmacie. Les sauvegardes ? Sur le même réseau. Chiffrées elles aussi.

Impact: 5 semaines sans système informatique. 2.800 consultations reportées, 340 opérations annulées. Des patients transférés d'urgence. Un décès lors d'un transfert (enquête en cours). Coût : 15 millions d'euros.

Leçon: Des sauvegardes air-gapped et un PRA testé auraient permis une reprise en 48-72h. L'architecture Zero Trust aurait limité la propagation. Personne n'avait testé le plan de reprise : il n'existait que sur le papier.

Avant / Après — la différence concrète

Chapitre 5

Ce qui change quand on passe d'une posture artisanale à une posture maîtrisée.

Maturité cyber traditionnelle	Posture moderne et résiliente
01 GOUVERNANCE	
Politique cyber dans un classeur, jamais relue. CISO sans accès direct au COMEX. Pas de KPI cyber au board.	Comité cyber trimestriel au COMEX. Tableau de bord avec KPI alignés sur le business. Politique vivante mise à jour.
02 DÉTECTION	
SOC submergé d'alertes, MTTD > 200 jours. Threat intelligence générique. Pas de threat hunting proactif.	SOC + Threat Hunting actif, MTTD < 24h. TI contextualisée Belgique/secteur. Use cases métier opérationnels.
03 ARCHITECTURE	
Approche château fort : périmètre fort, intérieur faible. VPN sans zero trust. Réseau plat IT/OT.	Architecture Zero Trust : vérification continue. Micro-segmentation. Séparation IT/OT stricte avec data diodes.
04 IDENTITÉS	
AD obsolète, comptes admin trop nombreux, MFA partiel. Pas de PAM. Anciens employés actifs.	IAM moderne (Entra ID/Okta), MFA généralisé, PAM avec session recording, Just-in-Time access, deprovisioning automatisé.
05 TIERS / SUPPLY CHAIN	
Questionnaires sécurité envoyés une fois à la signature. Pas de droit d'audit exercé. SBOM inexistant.	Programme TPRM continu. Audits annuels des tiers critiques. SBOM exigé. Plans de sortie testés.

06 RÉPONSE AUX INCIDENTS

- Plan rédigé, jamais testé. Communication de crise improvisée. Pas de coordination COMEX/legal/comm.
- Plan testé en exercice tabletop semestriel. Cellule de crise pré-définie. Communication pré-rédigée. Coordination CCB/régulateurs.

07 CONFORMITÉ

- Logique de checkbox annuelle. Auditeurs externes vérifient la documentation, pas la réalité.
- Conformité by design : NIS2, DORA, RGPD intégrés dans l'architecture et les processus. Preuves vivantes.

Auto-évaluation de maturité

Chapitre 6

Faites le point en 5 minutes : où en êtes-vous vraiment ?

Pour chaque question, cochez la case qui correspond le mieux à votre situation actuelle.

SITUATION	NON	PARTIEL	OUI
1. Notre stratégie cybersécurité est validée annuellement par le COMEX et alignée sur la stratégie business.	☐	☐	☐
2. Le CISO a un accès direct au COMEX et un mandat clair (budget, autorité, indicateurs).	☐	☐	☐
3. Nous avons cartographié notre exposition aux référentiels NIS2, DORA, RGPD, ISO 27001 et NIST CSF.	☐	☐	☐
4. Notre posture sécurité est mesurée par des KPI cyber présentés au board (MTTD, MTTR, couverture EDR, etc.).	☐	☐	☐
5. Une architecture Zero Trust est en cours de déploiement (vérification continue, micro-segmentation).	☐	☐	☐
6. Le PAM gère les comptes à privilèges avec session recording, JIT access et rotation automatique.	☐	☐	☐
7. Notre SOC dispose de threat intelligence contextualisée Belgique et secteur, avec use cases métier.	☐	☐	☐
8. Le threat hunting proactif fait partie de nos opérations sécurité (pas seulement la détection réactive).	☐	☐	☐
9. Nous avons un programme TPRM avec audits réguliers des prestataires critiques et droit d'audit exercé.	☐	☐	☐
10. Le plan de réponse aux incidents est testé en exercice tabletop au moins 2 fois par an, avec le COMEX.	☐	☐	☐
11. Nos sauvegardes critiques sont immuables, air-gapped, et la restauration est testée trimestriellement.	☐	☐	☐
12. La séparation IT/OT (si applicable) est stricte avec data diodes et flux unidirectionnels documentés.	☐	☐	☐
13. Nos environnements cloud disposent d'un CSPM et d'une politique IAM mature (least privilege).	☐	☐	☐
14. Nous formons et faisons signer un engagement cyber au conseil d'administration (obligation NIS2 art. 20).	☐	☐	☐

15. Nous disposons d'un plan de continuité d'activité (PCA/PRA) testé sur scénario ransomware réaliste.	☐	☐	☐

SCORING : Non = 0 pt • Partiel = 1 pt • Oui = 2 pts

< 40% : Critique • 40-70% : À renforcer • > 70% : Bonne posture

Ce qu'on fait concrètement pour vous

Chapitre 7

Des ressources de grand compte, enfin accessibles — Humaines, Connaissances & Outils.

Audit de maturité — on vous dit où vous en êtes vraiment

On évalue votre posture selon NIST CSF, ISO 27001 et CIS Controls. On identifie les gaps NIS2 et DORA. Et on vous rend un rapport que votre COMEX peut lire et comprendre : pas 200 pages de technique, mais une roadmap 24 mois avec des priorités claires.

Architecture Zero Trust — on redesigne vos fondations

Micro-segmentation, IAM/PAM, chiffrement end-to-end. On ne vous vend pas un produit. On conçoit et implémente une architecture qui correspond à votre réalité : vos contraintes legacy, vos environnements hybrides, vos obligations sectorielles.

vCISO — un CISO qui connaît votre métier

Nos profils viennent des grands comptes et connaissent les réalités d'une organisation complexe : reporting au board, conformité multi-cadres, gestion de prestataires, incidents à grande échelle. On ne fait pas de la sécurité en chambre, on la pilote sur le terrain.

Red Team — on vous attaque pour de vrai

Ingénierie sociale, exploitation de failles, mouvement latéral, escalade de privilèges. On simule ce que ferait un vrai attaquant sur vos environnements IT, OT et cloud. Pas un scan automatique avec un rapport générique : une vraie mise à l'épreuve par des humains.

Détection & réponse — le dispositif qui détecte vraiment

Un SOC qui génère des milliers d'alertes ignorées ne protège personne. On conçoit vos use cases de détection, on sélectionne et pilote le partenaire SOC/MDR adapté à votre secteur, on intègre une threat intelligence contextualisée Belgique. Notre rôle : que la détection serve la décision, pas le reporting.

NIS2 & conformité — on vous accompagne de A à Z

Applicabilité, gap analysis, choix de la voie de démonstration (CyFun, ISO 27001 ou inspection CCB), remédiation, documentation, formation du management, préparation aux audits. On sait ce que le régulateur attend, et ce qui sert vraiment votre sécurité au-delà de la case à cocher.

Notre façon de travailler

Une méthode en 4 étapes, progressive, pensée pour votre réalité. Pas de slides : des livrables concrets à chaque étape.

1

VOIR CLAIR

AUDIT

On commence par comprendre votre contexte : cartographie de l'existant, entretiens avec les équipes, identification des vrais risques. Pas de diagnostic à distance, pas d'hypothèses. On part de ce qui existe chez vous.

2

PRIORISER ENSEMBLE

PLAN

Qu'est-ce qui est urgent, qu'est-ce qui peut attendre ? On construit le plan avec vous, pas à votre place. Chaque action est pondérée par son impact, son effort et votre budget. Vous gardez la main sur les décisions.

3

STABILISER

ACTION

On corrige, on durcit, on protège. Des actions concrètes et mesurables, livrées par jalons. À chaque étape, vous validez avant qu'on avance. Pas de surprise, pas de dérive budgétaire.

4

TRANSMETTRE

AUTONOMIE

On documente tout ce qu'on fait, on forme vos équipes, on vous laisse les clés. Notre succès se mesure à votre capacité à continuer sans nous. Pas de dépendance, du transfert de compétences.

Feuille de route en phases

Chapitre 8

Un chemin balisé, du diagnostic à la maturité — étape par étape.

1	2	3	4	5
1-2 MOIS	MOIS 3	MOIS 4-9	MOIS 10-15	CONTINU
Diagnostic	**Stratégie**	**Fondations**	**Résilience**	**Maturité continue**
• Audit NIST CSF • Pentest red team • Cartographie risques • Gap NIS2/DORA	• Roadmap 24 mois • Validation COMEX • Budget pluriannuel • KPI cyber board	• Zero Trust • PAM/IAM modernes • EDR/XDR généralisé • SOC renforcé	• Sauvegardes immuables • Exercices crise • TPRM programme • PRA testé	• Threat hunting • Veille TI Belgique • Audits semestriels • Évolution NIS2/DORA

Conseil méthodo

Chaque phase est un livrable autonome. Vous pouvez vous arrêter à n'importe quelle étape ou ralentir le rythme selon votre budget et votre charge interne. L'important n'est pas la vitesse — c'est de ne pas reculer.

Obligations oubliées & bénéfices cachés

Chapitre 9

Des cadres réglementaires sous-estimés qui sont pourtant des leviers de valeur.

NIS2 — Le CA engage sa responsabilité personnelle

Nouveau 2024

Article 20 : les organes de direction doivent approuver les mesures cyber ET superviser leur application. En cas de manquement, sanctions personnelles, y compris l'interdiction temporaire d'exercer des fonctions dirigeantes.

BÉNÉFICE CACHÉ :

Une gouvernance cyber formalisée au niveau du board pèse aussi dans la négociation des primes d'assurance : les assureurs la demandent. Mais l'effet le plus puissant est interne. Quand la direction s'implique visiblement, la culture de sécurité percole dans toute l'organisation. Les équipes IT se sentent soutenues, restent plus longtemps, et sont plus efficaces.

DORA — Vos fournisseurs IT sont dans le périmètre

Entrée en vigueur jan. 2025

DORA impose aux entités financières ET à leurs fournisseurs IT critiques des tests de résilience, une gestion formalisée des risques tiers, et un reporting au régulateur.

BÉNÉFICE CACHÉ :

La mise en conformité DORA force à cartographier tous vos fournisseurs IT critiques et à automatiser le suivi de leurs risques. Les organisations qui le font découvrent presque toujours des dépendances et des vulnérabilités qu'elles ignoraient, et sortent des fichiers Excel dispersés et des relances manuelles. C'est un gain opérationnel autant que sécuritaire.

NIS2 — Documenter la sécurité de la supply chain

Souvent ignoré

Article 21§2d : évaluation formelle de la sécurité de vos fournisseurs. Clauses cyber, audits réguliers, suivi des incidents chez vos tiers. La plupart des grandes entreprises belges n'ont pas encore formalisé ce processus.

BÉNÉFICE CACHÉ :

En structurant votre Third-Party Risk Management, vous centralisez et automatisez la gestion fournisseurs. Fini les fichiers Excel dispersés et les relances manuelles. Vous réduisez une exposition bien réelle (MOVEit l'a rappelé à des milliers d'organisations) tout en libérant vos équipes procurement et sécurité de tâches répétitives à faible valeur ajoutée.

Rétention des talents cyber — un enjeu réglementaire indirect

Angle mort

NIS2 exige des compétences cyber documentées au sein de l'organisation. Or la pénurie de profils cyber est structurelle en Belgique comme ailleurs : l'étude mondiale ISC² sur la main-d'œuvre cyber documente chaque année un déficit de plusieurs millions de professionnels. Chaque départ coûte des mois de recrutement et de montée en compétence.

BÉNÉFICE CACHÉ :

Les organisations qui investissent dans la formation continue, des parcours de carrière clairs et des outils modernes retiennent nettement mieux leurs profils cyber. La conformité NIS2 est le prétexte parfait pour structurer ça : budget formation, certifications, droit à l'expérimentation. Vos meilleurs éléments restent parce qu'ils apprennent et grandissent.

RGPD — Votre DPO a-t-il vraiment les moyens ?

Sous-dimensionné

L'APD constate que beaucoup de DPO n'ont ni les ressources, ni l'indépendance, ni l'accès au board nécessaires. C'est une non-conformité de fait.

BÉNÉFICE CACHÉ :

Un DPO outillé avec des solutions de data discovery et de classification automatisée identifie des risques invisibles et répond beaucoup plus vite aux demandes RGPD (accès, suppression, portabilité). C'est un investissement qui libère du temps juridique, réduit le risque d'amende, et montre au marché que vous prenez la protection des données au sérieux.

Checklist détachable — vos actions prioritaires

Imprimez cette page, cochez au fur et à mesure. Les colonnes EFFORT et IMPACT vous aident à séquencer.

		EFFORT	IMPACT	DÉLAI
☐	Audit de maturité NIST CSF + gap analysis NIS2/DORA, restitué au COMEX.	🟢🟢🟠⚪⚪	🟢🟢🟠🔴🔴	2 mois
☐	Roadmap cyber 24 mois validée par le COMEX, avec budget et KPI alignés business.	🟢🟢🟠⚪⚪	🟢🟢🟠🔴🔴	3 mois
☐	Pentest red team avec scénarios TTP réalistes (4-8 semaines, MITRE ATT&CK).	🟢🟢🟠🔴⚪	🟢🟢🟠🔴🔴	6 mois
☐	Architecture Zero Trust (vérification continue, micro-segmentation, ZTNA).	🟢🟢🟠🔴🔴	🟢🟢🟠🔴🔴	12 mois
☐	PAM moderne avec session recording, JIT access, rotation automatique.	🟢🟢🟠🔴⚪	🟢🟢🟠🔴🔴	6 mois
☐	EDR/XDR généralisé, y compris postes COMEX (souvent oubliés).	🟢🟢🟠⚪⚪	🟢🟢🟠🔴🔴	3 mois
☐	Threat intelligence contextualisée Belgique + threat hunting proactif.	🟢🟢🟠🔴⚪	🟢🟢🟠🔴⚪	6 mois
☐	Programme TPRM structuré : audits annuels des prestataires critiques.	🟢🟢🟠🔴⚪	🟢🟢🟠🔴⚪	9 mois
☐	Sauvegardes immuables + air-gapped, avec restauration testée trimestriellement.	🟢🟢🟠⚪⚪	🟢🟢🟠🔴🔴	3 mois
☐	Plan de réponse aux incidents testé en exercice tabletop avec COMEX (2× par an).	🟢🟢🟠⚪⚪	🟢🟢🟠🔴🔴	6 mois
☐	Programme de formation du conseil d'administration (NIS2 art. 20).	🟢🟢⚪⚪⚪	🟢🟢🟠🔴⚪	4 mois

	EFFORT	IMPACT	DÉLAI
☐ Cloud Security Posture Management (CSPM) sur tous les environnements cloud.	●●●○○	●●●●○	6 mois
☐ Séparation IT/OT stricte avec data diodes (si applicable au métier).	●●●●●	●●●●●	18 mois
☐ Cellule de crise cyber pré-définie : COMEX, IT, legal, comms, RH.	●●○○○	●●●●●	3 mois
☐ KPI cyber au board : MTTD, MTTR, couverture EDR, conformité, incidents critiques.	●●○○○	●●●●○	4 mois

CONSEIL : Commencez par les actions à fort impact ET faible effort (les "quick wins").

Si vous bloquez sur une action, contactez-nous : on vous oriente gratuitement.

Questions fréquentes

Chapitre 10

Les questions que nos clients posent le plus souvent — et nos réponses sans détour.

Q1. Pourquoi faire appel à un cabinet à taille humaine plutôt qu'à un Big Four ?

Pas en remplacement, en complément. Les Big Four excellent sur les audits formels et la conformité documentaire. Un cabinet à taille humaine apporte de l'agilité opérationnelle : on s'assoit avec vos équipes, on comprend vos contraintes spécifiques, on livre du concret. La complémentarité est la règle. Plusieurs grands comptes belges combinent les deux approches avec succès.

Q2. Combien de jours de vCISO faut-il pour piloter notre stratégie cyber ?

Pour une grande entreprise (>1000 employés), comptez 6 à 10 jours/mois pour un vCISO senior qui anime le comité cyber, pilote la roadmap, gère les incidents majeurs et représente la cybersécurité au COMEX. Pour une ETI, 4 à 6 jours/mois suffisent souvent. C'est une fraction du coût d'un CISO interne, avec une expérience multi-organisationnelle en prime.

Q3. Comment se conformer à NIS2 et DORA en parallèle ?

Les deux cadres se recouvrent largement : gestion des risques, gouvernance, gestion des incidents, résilience opérationnelle, risques tiers. On bâtit un framework unifié : un seul système de management, des contrôles mappés sur NIS2 + DORA + ISO 27001, des audits combinés. C'est nettement plus efficient que de gérer chaque réglementation séparément, en coût comme en charge pour les équipes. Bonus : ISO 27001 est aussi l'une des voies de démonstration NIS2 reconnues par le CCB.

Q4. Quelle est la valeur réelle d'un Red Team exercise pour un grand compte ?

Un Red Team va au-delà du pentest : il simule un attaquant motivé pendant 4 à 8 semaines, avec une approche TTP réaliste (Initial Access > Lateral Movement > Exfiltration). Le résultat n'est pas une liste de vulnérabilités, mais une démonstration de scénarios d'attaque end-to-end. Indispensable pour valider votre Blue Team et identifier les angles morts détectionnels.

Q5. Comment piloter la cybersécurité de notre supply chain (TPRM) ?

Cinq piliers : (1) Inventaire exhaustif des prestataires avec criticité business. (2) Tiering : audits approfondis pour les prestataires critiques, questionnaires pour les autres. (3) Droit d'audit contractualisé ET exercé annuellement. (4) Monitoring continu de la posture (BitSight, SecurityScorecard). (5) Plans de sortie testés. Un programme TPRM mature réduit fortement les incidents liés aux tiers, et répond directement aux exigences supply chain de NIS2 (art. 21) et DORA.

Q6. Comment mesurer le ROI de la cybersécurité au COMEX ?

Trois angles complémentaires : (1) Risk reduction : valeur attendue des pertes évitées (FAIR methodology). (2) Conformité : coût des amendes évitées + coût de l'audit conforme vs non-conforme. (3) Business enablement : contrats gagnés grâce à la maturité (ISO 27001, SOC 2, CyFun). Le ROI cyber n'est jamais "le coût d'un incident évité" : c'est la combinaison des trois.

Q7. Comment intégrer la cybersécurité dans une fusion-acquisition (M&A) ?

Trois temps : (1) Cyber due diligence avant la signature : audit de la posture cyber de la cible, identification des passifs cyber latents (incidents non révélés, dette technique). (2) Day 1 readiness : isolation des SI, RBAC, monitoring renforcé. (3) Intégration progressive sur 12-24 mois avec roadmap dédiée. Un cabinet expert peut intervenir sur les trois phases.

Q8. Comment préparer notre conseil d'administration aux obligations NIS2 art. 20 ?

NIS2 exige que les organes de direction approuvent les mesures cyber et suivent une formation. On organise un programme dédié : (1) Briefing initial 4h sur le panorama des menaces. (2) Sessions trimestrielles 1h sur l'évolution des risques. (3) Exercice tabletop annuel avec le COMEX. (4) Reporting cyber structuré (KPI alignés board). Cela transforme la cyber d'un sujet technique en un sujet de gouvernance.

Glossaire

Chapitre 11

Tous les termes techniques de ce guide, expliqués en français clair.

2FA / MFA (Authentification à deux facteurs)

Méthode qui combine deux preuves d'identité pour se connecter : un mot de passe + un code reçu sur le téléphone, ou une empreinte. Selon les mesures publiées par Microsoft, bloque la grande majorité des piratages de compte. C'est gratuit, ça prend 5 minutes à activer, et ça change tout.

APD (Autorité de Protection des Données)

Le régulateur belge du RGPD. C'est l'organisme qui contrôle, conseille et sanctionne en cas de non-respect des règles sur les données personnelles. Site : autoriteprotectiondonnees.be.

APT (Advanced Persistent Threat)

Groupe d'attaquants très organisé (souvent étatique : Russie, Chine, Corée du Nord) qui s'infiltre lentement dans un réseau et y reste des mois pour espionner ou voler. Cible plutôt les grandes entreprises et les administrations.

Backup 3-2-1

Règle d'or des sauvegardes : 3 copies de vos données, sur 2 supports différents (disque + cloud par exemple), dont 1 hors site et déconnectée. Si un ransomware frappe, la copie déconnectée reste intacte.

BitLocker / FileVault

Outils intégrés gratuitement à Windows (BitLocker) et macOS (FileVault) pour chiffrer le disque dur. Si votre laptop est volé, le voleur ne peut rien lire. À activer dès aujourd'hui — c'est en 10 minutes.

CCB (Centre for Cybersecurity Belgium)

L'autorité belge de cybersécurité. Publie des alertes, accompagne les victimes d'incidents, et signale les attaques en cours. C'est aussi à eux qu'on notifie les incidents NIS2 sous 24h.

CISO / RSSI

Chief Information Security Officer / Responsable de la Sécurité des SI. La personne (interne ou externe / fractionnelle) qui pilote la stratégie cybersécurité d'une organisation.

Conditional Access

Mécanisme Microsoft (Entra ID) qui décide si un utilisateur peut se connecter selon le contexte : depuis quel appareil, quelle localisation, à quelle heure. Empêche un attaquant de se connecter même avec votre mot de passe.

DLP (Data Loss Prevention)

Technologie qui empêche la fuite de données sensibles : un employé qui essaie d'envoyer un fichier client par email perso, ou de le mettre sur une clé USB, est bloqué automatiquement.

DORA (Digital Operational Resilience Act)

Règlement européen entré en vigueur en janvier 2025. Impose au secteur financier (banques, assurances, fintechs) des règles strictes sur la résilience IT. Sanctions jusqu'à 1% du CA quotidien.

EDR / XDR

Endpoint Detection & Response : un antivirus "intelligent" qui détecte les comportements suspects sur un poste (un ransomware qui chiffre des fichiers, par exemple) et le bloque en temps réel. XDR = même chose mais étendu au réseau et au cloud.

Entra ID (anciennement Azure AD)

Le service d'identité Microsoft dans le cloud. C'est lui qui gère qui peut se connecter à quoi (Microsoft 365, applications métier, Azure). Le "trousseau de clés" central de votre IT.

Hameçonnage / Phishing

Email frauduleux qui se fait passer pour un fournisseur, un client, votre banque ou votre patron, pour vous voler vos identifiants ou vous faire cliquer sur un lien malveillant. Cause #1 des piratages.

IAM / PAM

Identity Access Management / Privileged Access Management. Outils qui gèrent qui a accès à quoi, et surtout qui contrôlent les comptes "admin" très puissants (avec validation, traces, sessions enregistrées).

ISO 27001

Norme internationale qui définit comment organiser la sécurité de l'information. Une certification ISO 27001 prouve à vos clients et partenaires que vous avez mis en place une vraie démarche structurée.

NIS2

Directive européenne transposée en droit belge en 2024. Oblige certains secteurs (santé, énergie, transport, fabrication, numérique…) à mettre en place une gouvernance cybersécurité, sous peine de 10M€ d'amende. Voir notre guide dédié.

NIST CSF

Framework de cybersécurité publié par le NIST (institut américain). Structure la sécurité en 5 fonctions : Identifier, Protéger, Détecter, Répondre, Récupérer. Référence mondiale, gratuit.

Patch / Patch management

Mise à jour de sécurité d'un logiciel ou système. Les hackers exploitent les failles connues en quelques heures après publication d'un patch. La gestion de patches consiste à appliquer ces correctifs systématiquement et rapidement.

PRA / PCA

Plan de Reprise d'Activité / Plan de Continuité d'Activité. Document qui décrit comment redémarrer l'IT après une catastrophe (incendie, ransomware, panne majeure). Sans plan testé, on improvise — et on perd plus.

Ransomware

Logiciel malveillant qui chiffre tous vos fichiers et exige une rançon en cryptomonnaie pour les déchiffrer. Le CCB traite ce type d'incident en continu en Belgique, PME et indépendants compris.

RGPD / GDPR

Règlement européen sur la protection des données personnelles (Règlement Général sur la Protection des Données). En vigueur depuis 2018. S'applique à toute organisation qui traite des données de citoyens européens. Sanctions jusqu'à 20M€ ou 4% du CA mondial.

SIEM / SOAR

Security Information & Event Management : centralise les logs de tous vos systèmes et détecte les anomalies. SOAR ajoute l'automatisation des réponses aux incidents.

SOC (Security Operations Center)

Équipe (interne ou externe) qui surveille en continu les systèmes IT pour détecter et répondre aux attaques. Un SOC externalisé permet à une PME d'avoir une protection 24/7 sans recruter.

VPN

Virtual Private Network : tunnel chiffré entre votre poste et un réseau d'entreprise. Indispensable en télétravail, MAIS doit absolument être protégé par 2FA, sinon un mot de passe volé ouvre tout votre SI.

Zero Trust

Philosophie de sécurité moderne : "ne jamais faire confiance, toujours vérifier". Chaque accès est validé en continu, même quand l'utilisateur est à l'intérieur du réseau. Remplace le modèle "château fort" obsolète.

Ressources externes

Chapitre 12

Sites officiels, outils gratuits et lectures recommandées pour aller plus loin.

CCB — Centre for Cybersecurity Belgium

ccb.belgium.be

L'autorité belge officielle de la cybersécurité. Alertes en temps réel, fiches pratiques en français, signalement d'incidents, accompagnement gratuit pour les victimes (Safeonweb).

APD — Autorité de Protection des Données

autoriteprotectiondonnees.be

Le régulateur belge RGPD. Modèles de registre, guides sectoriels, formulaire de notification des fuites de données sous 72h.

Safeonweb (CCB)

safeonweb.be

Plateforme grand public du CCB. Alertes phishing en cours en Belgique, conseils simples, formation gratuite "Citizen Cybersafe".

Have I Been Pwned

haveibeenpwned.com

Service gratuit pour vérifier si votre adresse email ou un mot de passe a fuité dans une cyberattaque connue. À consulter au moins une fois par trimestre.

ENISA — European Cybersecurity Agency

enisa.europa.eu

Agence européenne de la cybersécurité. Publications de référence sur NIS2, DORA, supply chain, gestion d'incidents — gratuites.

NIST Cybersecurity Framework

nist.gov/cyberframework

Le référentiel mondial de gouvernance cyber. Gratuit, structurant, utilisé pour cadrer les audits internes et les feuilles de route.

CIS Controls v8

cisecurity.org/controls

18 contrôles de sécurité priorisés et concrets, conçus par la communauté. Idéal pour les PME qui veulent une checklist actionnable plutôt qu'un référentiel théorique.

Bitwarden (gestionnaire de mots de passe)

bitwarden.com

Outil open-source, gratuit pour usage personnel et abordable pour les équipes. Élimine la réutilisation des mots de passe — la première cause de piratage.

KeePassXC (alternative locale) keepassxc.org

Gestionnaire de mots de passe 100% local, gratuit, open-source. Pour ceux qui ne veulent rien stocker dans le cloud.

FlashModz Enterprise — Documents & guides flashmodz.be/documents

Notre bibliothèque complète de guides cybersécurité, conformité, infrastructure et automatisation pour les PME et indépendants belges. Gratuit.

À propos de FlashModz Enterprise

FlashModz Enterprise est un cabinet d'expertise IT opérationnelle, fondé par Jérémy Manet et basé à Farciennes, dans la région de Charleroi. Conseil et mise en œuvre concrète : sécurité, audit et pentest, automatisation Linux/DevOps et formations — pour les particuliers comme pour les entreprises, en Belgique et à l'international. Notre conviction : les ressources, les connaissances pointues et les outils des grandes entreprises doivent être accessibles aux PME et aux indépendants. À leur échelle. À leur budget. Avec la même rigueur.

CE QUE NOUS FAISONS

- Audit sécurité
- Pentest & rapport
- Sprint de stabilisation
- Team Lead fractionnel
- Formations Linux / DevOps

CERTIFICATIONS & RÉFÉRENTIELS

- CWNA · Ruckus
- Cisco Meraki
- Fortinet NSE
- Veeam
- Jamf · Apple
- OWASP / PTES
- NIS2
- ISO 27001
- RGPD

Jérémy Manet

Fondateur · Ingénieur & architecte système/réseau

Plus de 15 ans en architecture et ingénierie système/réseau : infrastructure, Wi-Fi d'entreprise, sécurité et virtualisation. Également management (people & technique) et gouvernance IT en tant que Process Owner COBIT, DORA et NIS2. Certifié CWNA, Cisco Meraki, Fortinet, Veeam, Jamf, Apple. Technologies : Aruba, HPE, Cisco, FortiGate, Nutanix.

Spécialités : Architecture · Réseau · Wi-Fi · Sécurité · Virtualisation · Gouvernance · NIS2 · DORA

De l’expertise IT pour ce qui compte vraiment.

contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

LinkedIn Facebook TikTok Avis Google

IDENTITÉ LÉGALE

FlashModz Enterprise

DÉNOMINATION	FlashModz Enterprise
FONDATEUR	Jérémy Manet
SIÈGE SOCIAL	Rue du Wainage 18, 6240 Farciennes (Belgique)
BCE / TVA	1035.510.038 · BE 1035.510.038
EU VAT	2.386.268.987
ZONES DESSERVIES	Charleroi et alentours (B2C) · Belgique & international (B2B)
CONTACT	contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

FlashModz

Structurez votre gouvernance cyber

Chaque entreprise est unique. Chaque idée a ses contraintes,
son contexte et ses priorités.

C'est pourquoi nous ne proposons pas de grille tarifaire figée.
Nous préférons échanger avec vous, comprendre votre situation
et construire une réponse adaptée à vos vrais besoins.

Parlons de votre situation

EMAIL

contact@flashmodz.be

TELEPHONE

+32 471 87 87 07

WEB

flashmodz.be

RETROUVEZ-NOUS

LinkedIn · Facebook · TikTok · Avis Google

Scannez pour accéder à ce document

BCE 1035.510.038 | Charleroi · Belgique & international