ERIC SINGER

CISO
membre du CESIN

VULNÉRABILITÉS & CYBERSÉCURITÉ

La vision du RSSI : de la gestion réactive à l'intelligence prédictive

DEPUIS TRENTE ANS, LA GESTION DES VULNÉRABILITÉS EST AU CŒUR DU MÉTIER DU RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, LE RSSI.

Recenser les failles, prioriser les correctifs, réduire la fenêtre d'exposition : un travail souvent invisible mais déterminant. Sous la pression de l'intelligence artificielle, d'un cadre réglementaire qui se durcit et d'une surface d'attaque sans cesse élargie, cette pratique entre dans une nouvelle ère.

D'UNE RÉPONSE ARTISANALE À UNE DISCIPLINE INDUSTRIELLE

Tout commence dans les années 1990, lorsque le ver Morris révèle la fragilité d'internet. Les équipes techniques réagissent au cas par cas, en appliquant manuellement les correctifs publiés par les éditeurs. Le tournant vient en 1999 avec la création du CVE, identifiant universel pour chaque faille : pour la première fois, la communauté parle un langage commun.

Mais les vagues Nimda, Code Red ou Blaster montrent vite qu'aucune réponse manuelle ne tient face à des menaces qui s'industrialisent.

>>>

>>> LES ATTAQUES QUI ONT TOUT CHANGÉ

Chaque grande crise a redessiné la pratique. WannaCry, en 2017, paralyse 200 000 systèmes dans 150 pays en exploitant une faille corrigée depuis deux mois. NotPetya frappe ensuite via une mise à jour compromise et coûte plusieurs milliards aux groupes industriels. En 2021, Log4Shell révèle la fragilité des composants open source omniprésents, tandis que SolarWinds démontre qu'une mise à jour corrompue peut compromettre 18 000 organisations. La leçon est constante : la vulnérabilité n'est pas le seul problème, c'est le délai entre sa découverte, son exploitation et sa remédiation qui fait le risque. Plus de 80 % des compromissions exploitent encore des failles connues pour lesquelles un correctif existait.

STRUCTURER, OUTILLER, SE METTRE EN CONFORMITÉ

Pour répondre à cette industrialisation, les organisations se sont structurées. Les SOC (Security Operations Centers) surveillent en continu, les CERT mutualisent la veille. Le SOC est devenu une exigence implicite de NIS2 et DORA, souvent confiée à un prestataire en mode SOC as a Service. Une règle reste non négociable : la détection peut s'externaliser, la décision reste interne. C'est le RSSI qui arbitre, dans l'urgence, entre continuité d'activité et confinement.

Côté outillage, les scanners automatisent l'inventaire et les VOC (Vulnerability Operations Centers) ajoutent une priorisation contextuelle : sur 40 000 failles publiées chaque année, seules 2 à 5 % sont effectivement exploitées. La conformité, longtemps facultative, devient structurante. ISO 27001, NIS2, DORA et la gestion des risques tiers (TPRM) imposent des processus formalisés. Des plateformes comme BitSight ou SecurityScorecard étendent cette surveillance à tout l'écosystème de partenaires.

L'IA, ET LE SEUIL FRANCHI PAR MYTHOS

Cette quête d'efficacité a trouvé dans l'IA un allié décisif. L'EPSS prédit la probabilité qu'une faille soit réellement exploitée, des outils comme Pentera ou NodeZero rendent les tests d'intrusion continus, et le DevSecOps intègre la sécurité dès l'écriture du code, où une faille coûte dix fois moins cher à corriger qu'en production.

Mais avril 2026 marque une bascule. Anthropic introduit Mythos Preview, jugé si puissant qu'il ne sera pas rendu public. Soumis à Firefox, le modèle identifie 271 vulnérabilités là où la version précédente en trouvait 22, et révèle un défaut dormant depuis 27 ans dans OpenBSD. Pour préserver l'avance des défenseurs, le Project Glasswing en restreint l'accès à un cercle d'organisations à mandat défensif. Selon Palo Alto Networks, Mythos accomplit en quelques heures l'équivalent d'une année de tests humains. La fenêtre d'exposition se mesure désormais en semaines, et la dette technique cachée des systèmes va être brutalement révélée.

LE RSSI, COURROIE DE TRANSMISSION INDISPENSABLE

Dans ce nouveau paysage, le RSSI a muté. Technicien dans les années 2000, gestionnaire de risques dans les années 2010, il est devenu en 2026 la courroie de transmission entre le monde technique et le monde métier, la ceinture de sécurité que l'entreprise numérique ne peut plus se permettre de ne pas porter. Vers la direction générale, il traduit des réalités techniques en risques business, en exposition financière, en responsabilité réglementaire. Vers les équipes, il garantit que l'innovation s'exerce dans des enveloppes de risque maîtrisées.

À l'heure où les outils détectent plus vite que l'humain ne lit, sa valeur ne réside plus dans l'opération, mais dans le jugement. Juger les priorités, les délégations, les réponses. Et construire les équipes capables d'orchestrer l'IA défensive : la comprendre, l'utiliser, la gouverner. Sa légitimité ne se décrète plus. Elle se démontre, chaque jour. ■

Plus de 80 % des compromissions exploitent encore des failles connues pour lesquelles un correctif existait.