

CYBERSÉCURITÉ : ARRÊTONS DE NOUS RACONTER DES HISTOIRES !

Par Olivier Cristini, CTO du Groupe Squad

Il y a quelque chose d'étrange dans notre secteur : plus on investit, plus on se fait attaquer ! On le sait, on en parle, et on continue à peu près comme avant. Ce n'est pas un manque de budget. Ce n'est pas un manque d'outils. C'est un problème de lucidité.

La plupart des organisations ont aujourd'hui une posture cyber construite pour un monde qui n'existe plus : celui où l'entreprise avait un périmètre, un dedans et un dehors. Ce monde a disparu sous l'effet du cloud, de la mobilité, de l'externalisation massive et de la convergence IT/OT. Les infrastructures débordent désormais vers les prestataires, les partenaires, les objets connectés, les systèmes industriels. Mais nos réflexes défensifs, eux, sont restés en place.

La conformité nous donne bonne conscience. Rien de plus.

C'est peut-être la confusion la plus coûteuse du moment. On produit des audits, on obtient des certifications, on coche des cases pour NIS2, DORA, ISO 27001, et on en tire la conclusion implicite qu'on est protégés. Sauf qu'un audit dit ce qu'on était à la date où il a été conduit. L'attaquant, lui, n'a pas attendu.

Ce décalage n'est pas anodin : il entretient une illusion de maîtrise qui peut être plus dangereuse que l'absence de contrôle, parce qu'elle réduit la vigilance. Se conformer est nécessaire mais confondre conformité et sécurité, c'est une faute stratégique malheureusement très répandue.

L'économie de l'attaque a changé de nature

Ce qu'on sous-estime, c'est la rupture économique en cours. L'IA ne rend pas seulement les attaques plus sophistiquées, elle en effondre le coût ! Générer des exploits, personnaliser des campagnes de phishing à grande échelle, automatiser la reconnaissance : ce qui demandait hier des semaines à une équipe expérimentée s'exécute aujourd'hui en quelques heures pour quelques centaines d'euros.

Le résultat concret, c'est que le mouvement latéral (c'est-à-dire le temps qu'il faut à un attaquant pour se déplacer dans un système après y être entré) est passé de 62 minutes à moins de 30 minutes en deux ans. La fenêtre de réaction se ferme donc plus vite qu'on ne la réouvre.

Pendant ce temps, le coût de la défense reste structurellement élevé. L'asymétrie s'aggrave, et elle ne se résout pas en achetant un outil de plus.

On sécurise l'infrastructure. Rarement ce qui compte vraiment.

Voilà un angle mort qu'on ne discute pas assez : le décalage entre là où les contrôles sont denses et là où la valeur réelle se trouve. Les équipes sécurisent les endpoints, les firewalls, les accès réseau. Bref, ce qui est visible et mesurable.

Mais les données stratégiques, les processus critiques, la propriété intellectuelle (les vrais "joyaux de la couronne" !) sont souvent moins bien protégés que les serveurs de fichiers.

L'attaquant raisonne en valeur, pas en technique. Il cherche à atteindre ce qui compte, pas à vaincre l'architecture la plus solide. Ce décalage entre notre carte défensive et la réalité de ce qu'on a à protéger est systématique, et rarement nommé.

L'identité est devenue le vrai périmètre

Depuis 3 ans, les grandes compromissions s'appuient en majorité sur des identités valides - pas sur des zero-days, pas sur des exploits sophistiqués. Des comptes sur-privilegiés, des droits jamais révoqués, des accès prestataires mal gouvernés.

Quand l'attaquant entre avec des identifiants légitimes, la notion d'intérieur et d'extérieur ne veut plus rien dire. La confiance ne peut plus être un état accordé une fois pour toutes : elle doit être vérifiée en continu, contextuelle, révocable. C'est un changement de posture profond et il est encore traité comme un chantier parmi d'autres dans beaucoup d'entreprises.

Il faut arrêter de vouloir tout empêcher

C'est probablement la vérité la plus difficile à formuler dans notre métier : dans un système complexe, la compromission partielle est inévitable. La vraie question n'est pas "comment empêcher toute intrusion ?". Elle est "combien de temps entre l'entrée et la détection, entre la détection et la réponse, entre la réponse et le retour à la normale ?".

Ces délais ont un coût direct. 86 % des organisations touchées par une brèche déclarent avoir subi des perturbations opérationnelles significatives : production arrêtée, services interrompus, ventes bloquées. La résilience n'est pas un concept flou. C'est une capacité opérationnelle concrète, qui se construit, qui se teste, et qui manque encore à la plupart des organisations.

Les meilleures ne sont pas celles qui ne se font pas attaquer. Ce sont celles qui absorbent le choc sans s'effondrer.

Ce que ça change concrètement

Il ne s'agit pas de tout remettre à plat. Il s'agit de se recentrer : visibilité réelle sur ce qui est exposé, pas sur ce qui est déclaré conforme. Identité au cœur de l'architecture, pas en périphérie. Détection et réponse pensées comme des capacités qui s'entraînent, pas comme des outils qu'on installe. Et une question honnête sur ce qu'on protège vraiment, et pourquoi.

C'est ce que j'appelle la Modern Cybersecurity. Ce n'est pas un catalogue de solutions, mais un changement de regard sur ce que sécuriser veut dire quand le périmètre a disparu.

A propos du Groupe Squad

Squad est un pure player de la cybersécurité et l'une des premières forces cyber françaises. Dans un contexte d'intensification des menaces et de pression réglementaire accrue, le Groupe accompagne les grandes entreprises et institutions publiques dans la maîtrise durable de leur risque cyber. De la gouvernance à la résilience opérationnelle, de la réduction continue de la surface d'attaque à la sécurisation des identités en Zero Trust, de la protection Cloud aux SOC modernes augmentés par l'IA, Squad conçoit, intègre et opère des architectures robustes, souveraines et adaptées aux environnements les plus sensibles.

Avec plus de 1 000 experts répartis dans 14 agences en France, en Suisse, en Espagne et au Canada, Squad allie excellence technique, proximité et capacité de déploiement à grande échelle. En 2026, le Groupe recrutera 300 nouveaux talents pour accompagner sa trajectoire de croissance.

Contacts presse
Lily Magagnin
CMO Groupe Squad
lily.magagnin@squadgroup.com

Franck Tupinier
MyNTIC PR
ftupinier@myntic-pr.com
