TRIBUNE

Clichy, le 17 novembre 2025

LE PARADOXE DU SOC MODERNE : TROP D'ALERTES, PAS ASSEZ DE VISION

Par Xavier Gruau, CTO, Squad Cybersolutions

Les SOC se sont imposés comme le coeur de la cybersécurité. Pourtant, beaucoup d'entre eux sont submergés par le volume alertes. L'enjeu n'est plus de détecter davantage mais de voir mieux.

Face à cette saturation, l'avenir du SOC repose sur trois leviers indissociables : le CTEM, l'IA et l'automatisation.

En théorie, le Security Operations Center (SOC) est le bouclier de l'entreprise, toutefois, en pratique, il devient souvent son point de fragilité.
Chaque jour, les équipes doivent traiter des milliers d'alertes.
Résultat : la majorité du temps est consacrée à trier, pas à analyser.

Ce phénomène, l'*alert fatigue*, diminue drastiquement la réactivité des équipes et réduit leur capacité à identifier les signaux faibles.
La technologie commence à apporter une réponse au travers de l'avènement de l'IA et de l'automatisation qui tendent à améliorer la situation.
Néanmoins, tant que le SOC se concentrera sur la détection en aval, il continuera à subir le flot d'alertes.

Il faut passer d'une défense opérationnellement réactive à stratégiquement préventive.
C'est précisément le rôle du CTEM (Continuous Threat Exposure Management).
Son objectif est simple, transformer la cybersécurité en un processus continu qui mesure et réduit l'exposition au risque.
Au lieu d'attendre qu'une menace déclenche une alerte, le CTEM permet d'identifier, valider et prioriser les vulnérabilités ou mauvaises configurations avant qu'elles ne soient exploitées.

Adossé à un VOC (Vulnerability Operating Center), ce modèle complète le SOC en le déchargeant préventivement d'une partie de la pression opérationnelle en surveillant en continu les surfaces d'exposition, en suivant les correctifs et en orchestrant les remédiations avec les équipes IT.
Cette approche dynamique réduit mécaniquement le bruit de fond des alertes : moins de vulnérabilités actives qui sont exploitées en priorité par les attaquants, c'est moins d'événements déclenchés, et donc un SOC plus focalisé sur les vraies menaces.

Le dernier pilier de cette transformation, c'est l'automatisation.
À mesure que les environnements se complexifient (cloud, IoT, identités multiples, chaînes logicielles étendues), la vitesse de propagation des attaques dépasse largement la capacité d'intervention humaine.

L'automatisation, nourrie par la corrélation, la télémétrie et l'intelligence artificielle, permet de prioriser et d'enrichir les alertes avant qu'elles n'atteignent les analystes. Toutefois, elle pourrait générer des effets de bord dangereux. L'enjeu n'est donc pas d'automatiser plus, mais d'automatiser mieux, en associant l'expertise contextuelle des analystes à la puissance du machine learning pour créer un SOC augmenté.

En conclusion, le SOC de demain ne sera pas plus bruyant, il sera plus ciblé en réduisant l'exposition avant qu'elle ne devienne exploitable.

Son objectif ne sera plus de détecter ce qui se passe mais d'empêcher ce qui pourrait arriver, se transformant ainsi en un centre de maîtrise des expositions.

A propos de Squad Cybersolutions

Squad Cybersolutions, ex Newlode, est intégrateur et Managed Security Service Provider (MSSP), expert des enjeux de cybersécurité. Filiale du Groupe Squad depuis fin 2023, Squad Cybersolutions accompagne la sécurisation des infrastructures IT & OT de ses clients, de la phase conseil au pilotage automatisé multi-éditeurs de leurs architectures. Sa force, c'est sa capacité à construire et déployer des environnements intelligents capables d'optimiser leur défense face aux menaces. Opérant pour la moitié du CAC 40 et du SBF 120, Squad Cybersolutions pilote des projets Build/Run d'envergure internationale et dispose d'un Operation Center parisien qui officie en 24x7 et repose sur une équipe d'experts, capables de s'engager sur des SLA clients exigeants. Avec 1000 collaborateurs en France et à l'International, le Groupe Squad réalise 125 millions d'euros de chiffre d'affaires.

Contacts presse
Franck Tupinier
MyNTIC PR
ftupinier@myntic-pr.com

Lily Magagnin
CMO Squad Group
lily.magagnin@squadgroup.com