SOC nouvelle génération : IA et open source pour une cybersécurité plus accessible

Fayçal Ehlali, Intelcia IT Solutions

le 19-06-2025
Par La rédaction

Dans un contexte où les cybermenaces deviennent de plus en plus sophistiquées, la cybersécurité est devenue un enjeu vital pour toutes les entreprises, y compris les PME. Or ces dernières sont souvent moins armées face aux risques (ressources humaines, budget…). Longtemps réservés aux grandes structures, des SOC (Security Operation Center) de nouvelle génération, plus agiles, et plus automatisés, leur sont désormais accessibles. Une nouvelle approche qui démocratise enfin un haut niveau de protection. Parmi les éléments essentiels de cette révolution : l'adoption de technologies open source et de l'IA.

La vitesse de détection et la capacité d'adaptation conditionnent aujourd'hui la résilience des organisations. Il devient indispensable de repenser les modèles traditionnels de cybersécurité. Le SOC nouvelle génération (SOC NG) s'impose ainsi comme une réponse pragmatique aux exigences actuelles. Grâce à un recours rationnel à l'IA et à des technologies open source, il devient accessible aux PME.

Un SOC nouvelle génération plus sensible aux signaux faibles

Contrairement au SOC traditionnel, où la gestion des alertes repose souvent sur une organisation pyramidale et manuelle, le SOC nouvelle génération est capable d'**automatiser les étapes les plus chronophages et à moindre valeur ajoutée de ses processus**. Il permet aux équipes de **se concentrer sur les alertes complexes**. Pour cela, il tire parti de technologies telles que l'intelligence artificielle, le machine learning et l'automatisation.

Cette capacité à **traiter et à corréler des données à une vitesse accrue** permet aussi d'identifier des **signaux faibles**, de détecter des **comportements anormaux** et des **menaces potentielles** que des solutions classiques n'auraient jamais perçues. De plus, l'intégration de systèmes d'automatisation via des **« playbooks »** améliore la pertinence des réponses face aux incidents de sécurité.

Surtout, il fonctionne sans nécessiter de matériel spécifique du côté du client, ce qui en fait une solution plus souple et économiquement viable, en particulier pour les PME et ETI.

Aujourd'hui, **46 % des attaques par ransomware ciblent les TPE/PME**, mettant en lumière leur vulnérabilité accrue. Les SOC nouvelle génération permettent à ces structures de bénéficier d'un haut niveau de protection jusque-là réservé aux grandes organisations.

L'open source pour un SOC NG accessible

Si l'innovation dans le SOC NG est indéniable, une question fondamentale demeure : comment les entreprises, notamment les PME, peuvent-elles en bénéficier avec un budget contraint ? C'est là que l'open source prend tout son sens. En s'appuyant sur des briques technologiques open source pour concevoir leur architecture, les SOC NG contournent les contraintes budgétaires des solutions propriétaires. Ils deviennent ainsi accessibles à un plus grand nombre d'entreprises.

Les technologies open source offrent plusieurs avantages :

* **Indépendance vis-à-vis des éditeurs** : Contrairement aux solutions propriétaires, qui sont souvent soumises à des augmentations de prix annuelles ou à des cycles de renouvellement complexes, l'open source permet une **totale indépendance**. Le prestataire de services SOC maîtrise pleinement ses coûts et peut proposer des solutions à ses clients, sans surprises liées à la politique tarifaire d'un éditeur tiers.

* **Scalabilité et flexibilité** : L'open source offre la possibilité d'**adapter les solutions en fonction des besoins du client final**. Plutôt que d'être limité par des solutions fermées, l'entreprise peut faire évoluer ses systèmes au fur et à mesure de sa croissance, et ce, sans coûts excessifs ou investissements imprévus.

* **Accessibilité économique** : Les solutions open source, bien qu'**offrant des fonctionnalités équivalentes à des solutions propriétaires, sont bien plus abordable** Ce modèle permet à des entreprises de taille intermédiaire, ou même des PME, d'accéder à des **solutions de cybersécurité performantes, autrefois réservées aux grandes entreprises disposant de budgets conséquents**.

* **Communauté et évolution continue** : L'un des plus grands avantages de l'open source est la communauté qui l'entoure. En étant **auditable et constamment mise à jour par une large communauté de développeurs**, les solutions open source bénéficient d'une évolution continue, renforçant ainsi leur sécurité et leur fiabilité. **Contrairement aux solutions SOC traditionnelles, souvent rigides et dépendantes d'un seul éditeur, le SOC NG s'appuie sur une base ouverte, en perpétuelle amélioration, et intégrée nativement à des logiques de sécurité proactives.**

Parmi les technologies open source les plus utilisées dans les SOC NG figurent **Wazuh** (détection des intrusions), **TheHive** (gestion des incidents), **MISP** (partage d'indicateurs de compromission) ou encore **Suricata** (analyse réseau). Ces outils modulaires, **combinés à des orchestrateurs comme Shuffle, permettent de bâtir des environnements de détection et de réponse performants et personnalisables**.

Le recours à ces technologies permet aussi de mettre en place une **facturation forfaitaire basée sur le nombre d'assets, déconnectée du nombre d'événements traités**, offrant aux clients une meilleure **prévisibilité des coûts** et évitant les mauvaises surprises en cas de pic d'activité ou d'évolution du périmètre

Une Interopérabilité renforcée

L'un des défis majeurs auxquels sont confrontées les entreprises lorsqu'elles mettent en place un SOC NG est l'intégration avec leurs systèmes existants. Ici encore, l'open source se distingue en offrant une **interopérabilité supérieure**. En effet, les outils sont conçus pour être **flexibles et facilement intégrables à des environnements technologiques différents,** qu'ils soient propriétaires ou open source. Grâce aux API et à la capacité de développer des intégrations sur mesure, les organisations peuvent enrichir leur dispositif de détection en connectant facilement de nouvelles sources de logs ou d'alertes, telles que les solutions EDR, WAF, NDR ou les environnements cloud. Cette interopérabilité permet de centraliser les données au sein d'une tour de contrôle unifiée, renforçant la corrélation des événements et la réactivité face aux menaces.

Cela permet aussi de garantir une solution sur mesure qui évolue avec les besoins de l'entreprise.

La cybersécurité ne devrait jamais être un choix dicté par les contraintes budgétaires. La protection des systèmes d'information peut être accessible à tous, sans compromis sur l'efficacité ou la réactivité. Grâce au SOC nouvelle génération et aux technologies open source, il est aujourd'hui possible d'offrir aux PME comme aux ETI un niveau de sécurité autrefois réservé aux grandes entreprises. Celles qui investissent aujourd'hui dans une cybersécurité agile et ouverte se donnent une longueur d'avance décisive sur un terrain où l'inaction ne sera plus une option.

Par **Fayçal Ehlali**, Directeur Services Managés chez **Intelcia IT Solutions**