Guide **SecOps** : Enjeux, mise en œuvre et apport des solutions Palo Alto Networks

Les organisations évoluent aujourd'hui dans un environnement numérique marqué par l'augmentation des cybermenaces, la complexité des infrastructures et l'adoption du cloud. Les attaques sont plus ciblées, rapides et automatisées, notamment grâce à l'usage de l'IA par les acteurs malveillants, permettant d'industrialiser les attaques et de contourner les mécanismes de défense traditionnels. Dans ce contexte, la sécurité ne peut plus être uniquement préventive et doit être intégrée aux opérations pour détecter et limiter rapidement les incidents, donnant naissance au SecOps, une approche de sécurité opérationnelle. L'IA est aujourd'hui au cœur de la sophistication des cyberattaques, mais constitue également la seule réponse efficace pour les détecter, les analyser et y répondre à grande échelle.

Par ailleurs, l'augmentation du volume de données, la généralisation du cloud et la multiplication des outils rendent les modèles de sécurité traditionnels plus complexes à opérer. Les organisations doivent donc s'appuyer sur des capacités d'analyse avancées, souvent basées sur l'IA, pour identifier les menaces en temps réel et y répondre efficacement. Le SecOps s'inscrit dans cette évolution en rapprochant les capacités de détection, d'investigation et de réponse aux incidents, en s'appuyant sur l'automatisation et l'intelligence pour faire face à des menaces toujours plus sophistiquées.

Le SecOps : Une réponse aux défis modernes

Le SecOps est une approche organisationnelle et technique qui rapproche les équipes sécurité et les équipes opérationnelles IT. Son objectif est d'améliorer la coordination, la visibilité et la capacité de réaction face aux incidents. Plutôt que de considérer la sécurité comme une fonction isolée, le SecOps l'intègre dans le fonctionnement quotidien du système d'information.

Objectifs principaux du SecOps :

- **Réduire le temps moyen de détection (MTTD)**
- **Réduire le temps moyen de réponse (MTTR)**
- **Améliorer la priorisation des incidents**
- **Automatiser les tâches répétitives**
- **Renforcer la résilience globale du SI**

Dans un modèle SecOps mature, les équipes SOC s'appuient sur des plateformes capables de centraliser les données de sécurité, d'analyser les comportements suspects et d'automatiser les réponses aux incidents. Cette approche permet d'améliorer la visibilité sur l'infrastructure et d'optimiser les opérations de sécurité.

Du concept à l'opérationnel : Fonctionnement d'un SecOps

SURVEILLANCE ET COLLECTE

Les événements issus du réseau, des endpoints, des applications et des environnements cloud sont centralisés. Cette consolidation permet d'obtenir une vision unifiée de l'activité du système d'information.

CORRÉLATION ET ANALYSE

Les événements isolés sont analysés dans leur contexte. Une tentative de connexion suspecte, associée à un comportement anormal sur un poste de travail, peut ainsi révéler une compromission plus large. Les plateformes modernes utilisent aussi des capacités d'analyse avancées (Machine Learning, Threat Intelligence) afin d'identifier des menaces complexes et de réduire le nombre de faux positifs générés par les outils de sécurité.

RÉPONSE AUX INCIDENTS

Une fois un incident confirmé, des actions sont déclenchées :

- Isolement d'un poste compromis
- Blocage d'un flux réseau malveillant
- Réinitialisation d'identifiants
- Notification des équipes concernées

AUTOMATISATION

L'automatisation permet d'exécuter des scénarios prédéfinis sans intervention humaine systématique. Cela garantit :

- Rapidité
- Cohérence
- Traçabilité

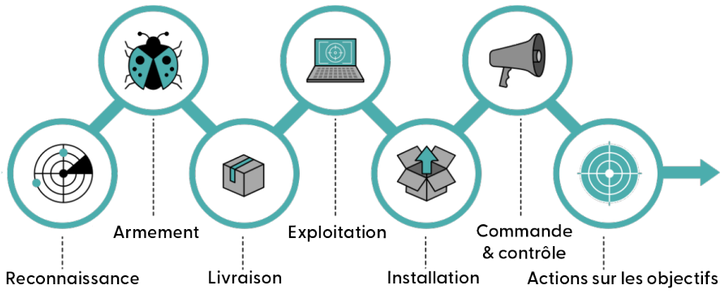
SecOps et chaîne de cyberattaques

Une cyberattaque suit généralement une progression structurée : reconnaissance, compromission initiale, mouvement latéral, élévation de privilèges, puis exfiltration ou sabotage. Sans dispositif SecOps efficace, un attaquant peut rester présent dans le système d'information pendant plusieurs semaines avant d'être détecté. La capacité à détecter rapidement ces différentes étapes est essentielle pour limiter l'impact d'une attaque. Les plateformes SecOps modernes permettent d'identifier ces comportements grâce à la corrélation d'événements provenant de multiples sources de données.

L'approche SecOps permet d'intervenir à **différents niveaux** de cette chaîne :

- **Détection précoce** des comportements anormaux
- **Corrélation d'événements multi-sources**
- **Containment rapide** pour éviter la propagation
- **Analyse post-incident** pour éviter la récurrence

LES ÉTAPES DE LA CYBER KILL CHAIN



Mise en œuvre du SecOps en entreprise

La réussite d'un projet SecOps repose sur une combinaison de gouvernance, d'outils et de compétences.

Bonnes pratiques organisationnelles :

- Définition claire des rôles et responsabilités
- Mise en place de procédures de gestion d'incident
- Collaboration entre SOC, IT et équipes métiers
- Exploitation des retours d'expérience

Bonnes pratiques techniques :

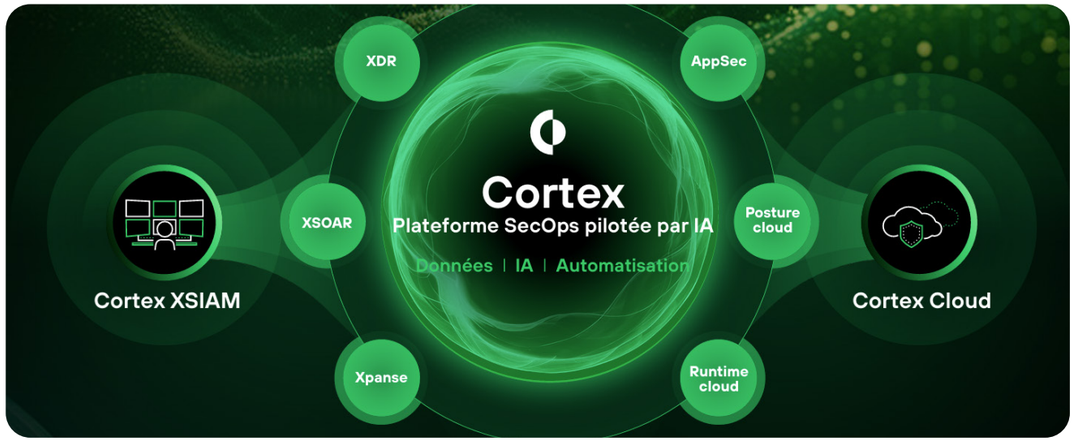
- Centralisation des logs et événements de sécurité
- Corrélation automatique des alertes
- Supervision en temps réel
- Automatisation des réponses simples et répétitives

SecOps et solutions industrielles : L'exemple Palo Alto Networks

La mise en œuvre du SecOps s'appuie sur des solutions capables de fournir v**isibilité, corrélation et automatisation.** Dans ce contexte, Palo Alto Networks propose une plateforme couvrant les principaux domaines de la sécurité d'entreprise.

Les solutions de Palo Alto Networks permettent de collecter des événements issus du réseau, des endpoints et du cloud, puis de les corréler afin de détecter plus efficacement les incidents. L'automatisation des réponses contribue à réduire les délais de réaction et à améliorer l'efficacité opérationnelle des équipes SecOps. Cette approche intégrée permet aux entreprises de transformer les principes du SecOps en **processus concrets et mesurables**, adaptés aux environnements hybrides modernes.

L'approche SecOps de Palo Alto Networks repose sur la plateforme Cortex, qui centralise la télémétrie de sécurité et automatise les opérations du SOC. Cette plateforme permet de collecter les données issues du réseau, des endpoints et du cloud afin de détecter plus rapidement les menaces et de coordonner la réponse aux incidents.



CORTEX XDR®
BY PALO ALTO NETWORKS

Cortex XDR détecte les menaces venant des endpoints, du réseau et du Cloud, en s'appuyant sur des mécanismes avancés d'analyse comportementale, pilotés par l'IA et le machine learning. **L'eXtended Detection & Response** permet de répondre aux attaques avec précision.

- Découverte des menaces par un Machine Learning continu
- Management unifié dans une seule console
- Reprise les informations venant des NGFW Palo Alto Networks et autres
- Nativement Intégré à Cortex XSOAR

Cette corrélation multi-sources, combinée à l'intelligence artificielle, permet d'identifier les attaques complexes et les mouvements latéraux au sein du système d'information.

CORTEX XSOAR®
BY PALO ALTO NETWORKS

Cortex XSOAR analyse les alertes venant de Cortex XDR et des autres outils de sécurité, pour réduire les incidents et répondre automatiquement aux attaques. Cette plateforme d'orchestration, d'automatisation et de réponse de sécurité (SOAR) permet aux équipes de sécurité opérationnelles de piloter de manière unifiée la gestion d'incidents, l'automatisation, la collaboration temps réel et la gestion des sources de Threat Intelligence. La réponse est coordonnée avec plus de 850 éditeurs de sécurité différents. La plateforme permet également de standardiser les processus d'investigation grâce à des playbooks automatisés capables de coordonner les actions entre différents outils de sécurité.

CORTEX XPANSE
BY PALO ALTO NETWORKS

Cortex XPANSE scanne Internet pour découvrir l'exposition de l'entreprise, réduire et protéger sa surface d'attaque.

- Découverte de tous les systèmes connectés et les services exposés relatif à l'entreprise
- Attribution des actifs basée sur le Machine Learning et hiérarchisation automatisée des risques pour une réponse immédiate
- Création des playbooks automatisés alimentés par l'IA pour identifier les propriétaires de services et remédier au problème en temps réels

Cette visibilité permet aux équipes de sécurité d'identifier les actifs exposés, les services non maîtrisés et les mauvaises configurations pouvant représenter un risque pour l'organisation.

CORTEX XSIAM
BY PALO ALTO NETWORKS

Cortex XSIAM est **une plateforme unifiée regroupant les capacités Cortex,** le tout **alimenté par l'IA.** Ce modèle permet de traiter **un volume de données** et **un nombre de sources inégalés, renforçant** ainsi **la performance des capacités d'analyse et d'automatisation basées sur l'IA.** Cortex XSIAM est une solution qui centralise **la télémétrie** de l'infrastructure, la **Threat Intelligence** et **les données ASM** dans une base de données unifiée, permettant une détection et une réponse largement automatisées. Cortex XSIAM permet d'**automatiser le traitement des tâches répétitives et des volumes importants de données**. Les analystes gagnent ainsi en productivité et peuvent se concentrer sur des activités à plus forte valeur ajoutée. Cette approche permet d'évoluer vers **un SOC autonome** capable d'automatiser la détection, l'investigation et la réponse à grande échelle.

Le SecOps s'impose aujourd'hui comme **une approche incontournable de la cybersécurité en entreprise**. En combinant collaboration, surveillance continue et automatisation, il permet de réduire l'impact des incidents et d'améliorer la résilience du système d'information. Grâce à l'analyse de données à grande échelle et à l'automatisation des opérations de sécurité, les plateformes modernes permettent aujourd'hui d'améliorer significativement l'efficacité des équipes SecOps. Plus qu'un ensemble d'outils, le SecOps représente **une évolution des pratiques**, indispensable pour faire face aux menaces actuelles et futures.

Palo Alto Networks propose une solution cohérente pour répondre aux enjeux SecOps actuels. Grâce à une approche combinant **prévention, visibilité, automatisation et Zero Trust**, la plateforme permet d'améliorer la sécurité tout en optimisant les opérations quotidiennes des équipes.

Contactez-nous

Appelez le +33 1 60 19 34 52

reseausecu@miel.fr

Voir la page produit

MIEL

www.miel.fr/palo-alto-networks