Cortex : Secure the Future

Identifier et répondre aux attaques les plus sophistiquées, combler les failles de sécurité nécessitent toujours plus de produits à gérer, plus de sources de données à corréler et plus d'actions répétitives.

Face à une telle quantité d'évènements à gérer et de solutions à synchroniser, les équipes de sécurité opérationnelles n'ont pas d'autre choix que d'avoir recours à l'automatisation, appuyée par de l'intelligence artificielle, pour accélérer la détection, l'investigation et la réponse.

L'approche de Palo Alto Networks, appuyée par la suite de produits Cortex, a la réponse la plus cohérente et la plus pertinente du marché dans ce domaine.

REINVENTER LA SECURITE OPERATIONNELLE

Prévenir tout ce qui peut être prévenu

CORTEX XDR

Détecter et investiguer rapidement tout ce qui ne peut être prévenu

CORTEX XDR

Automatiser la réponse et progresser à chaque incident

CORTEX XSOAR

Cortex est LA PLATEFORME DE SECURITE OPERATIONNELLE.

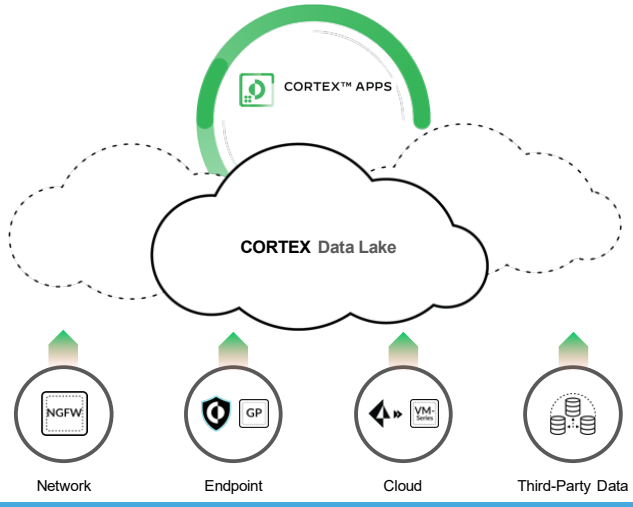
Elle est composée de 3 éléments clés :

- **Cortex XDR** pour la détection et la réponse qui étend la détection et la réponse au-delà du endpoint
- **Cortex XSOAR** pour l'orchestration, l'automatisation et la réponse de sécurité.
- **Cortex Data Lake** qui collecte, transforme et intègre les données des solutions Palo Alto Networks dans le réseau, le endpoint et le cloud.

CORTEX DATA LAKE

Les firewalls nouvelle génération, Prisma Access et les endpoints sont configurés pour envoyer des logs riches et corrélés vers Cortex Data Lake pour être exploitées par des services de machine learning et des applications de sécurité.

Cortex Data Lake est élastique, illimité et peut être configuré pour recevoir des données d'éditeurs tiers.

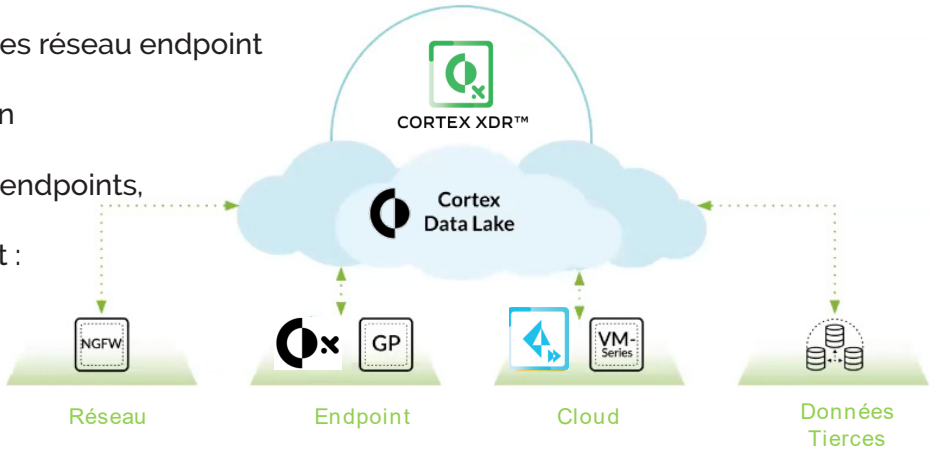


Distribué en France par MIEL

01 60 19 34 52 - www.miel.fr/palo-alto-networks/cortex

CORTEX XDR

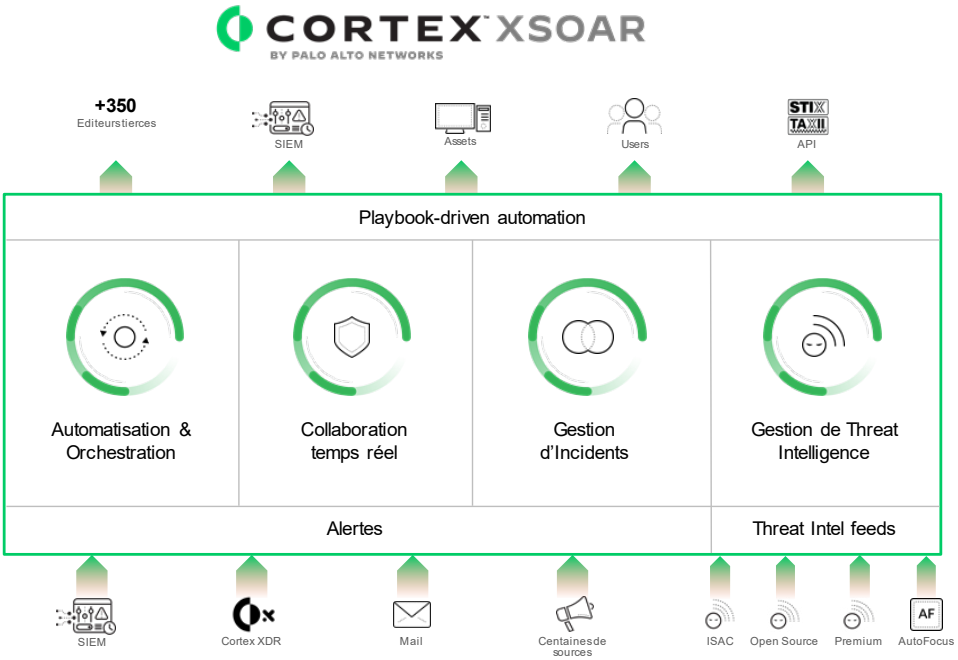
- Intégration de toutes les données réseau endpoint et cloud
- Découverte des menaces par un Machine Learning continu
- Réponse coordonnée entre les endpoints, le réseau et le cloud
- Protection avancée du endpoint : Prévention, détection et réponse
- Investigation 8x plus rapide
- Sécurisation des devices USB
- Management unifié du reporting, du triage et de la réponse en une seule console
- Nativement Intégré à Cortex XSOAR



Produit	Cortex XDR Prevent (Endpoint)	Cortex XDR Pro per Endpoint	Cortex XDR Pro Network per TB
Protection du Endpoint	X	X	-
Contrôle des devices	X	X	-
Gestion des incidents	Alertes Endpoint	Toutes les sources	Toutes les sources
Contrôle périphérique	X	X	-
Analytique	-	X	X
Threat Intelligence externe	Optionnelle	Optionnelle	X
Réponse Intégrée	Endpoint	Endpoint+Réseau	

CORTEX XSOAR

Cortex™ XSOAR est une plateforme d'orchestration, d'automatisation et de réponse de sécurité (SOAR) qui permet aux équipes de sécurité opérationnelles de piloter de manière unifiée la gestion d'incident, l'automatisation, la collaboration temps réel et la gestion des sources de Threat Intelligence tout au long du cycle de tout incident. La réponse est cordonnée avec + de 350 éditeurs différents de sécurité.



AUTOFOCUS

Est un portail qui offre un service de Threat Intelligence qui prend en compte les données de WildFire et les corrèle avec les informations de menaces de sources tierces. L'objectif est d'avoir une analyse contextuelle des menaces dont on est l'objet et de prioriser la réponse.