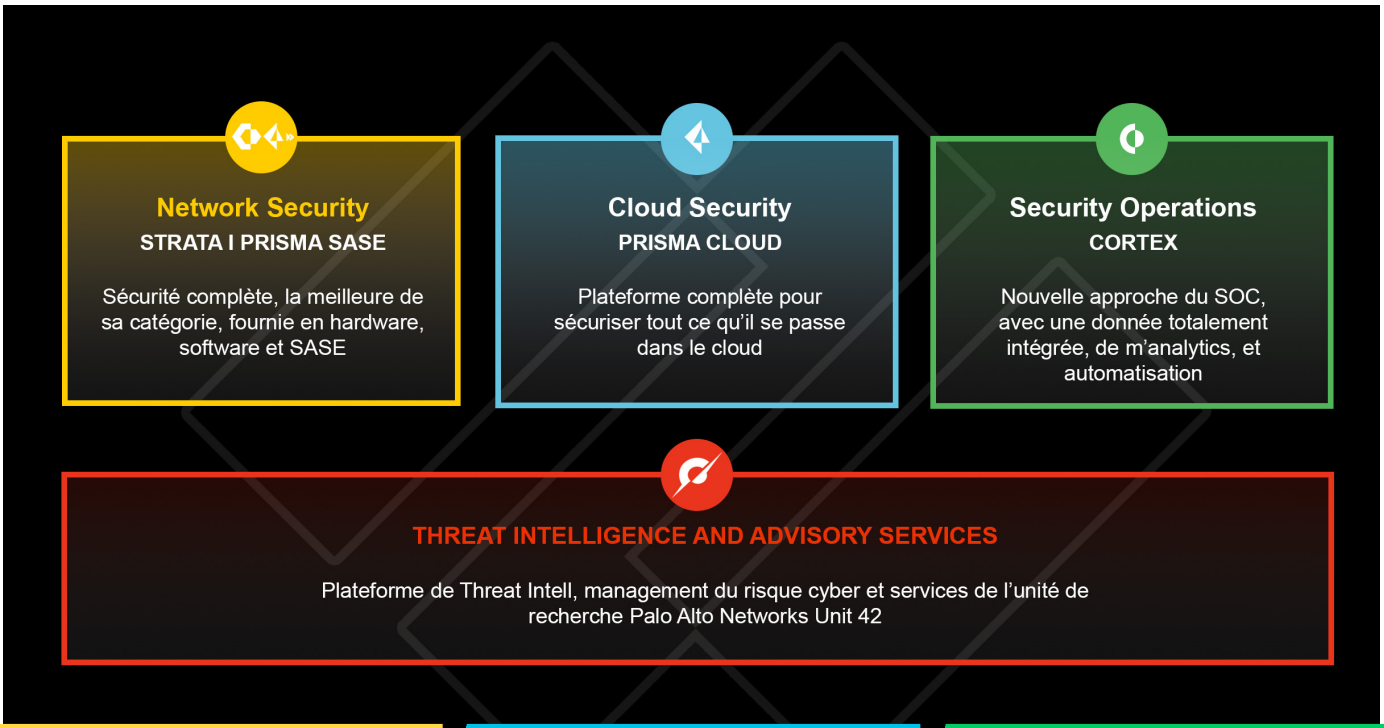
Palo Alto Networks

Le leader mondial de la cybersécurité

Les technologies de Palo Alto Networks permettent à 95 000 entreprises clientes de protéger des milliards de personnes dans le monde entier.
La plateforme de Palo Alto Networks simplifie la problématique de la sécurité, adresse le réseau, le endpoint et le cloud.
Elle met l'automatisation et l'innovation au cœur de son offre.

Une stratégie qui s'appuie sur 3 piliers



Network Security Platform

NGFW et SASE

- Intrusion detection
- URL Filtering
- Sandbox detection
- DNS Security
- IoT Security
- Data Loss Prevention
- Cloud Access Security broker
- Posture & health Management
- FWaaS
- SDWAN
- ZTNA
- Secure Web Gateway

Cloud Security Platform

Prisma Cloud

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection
- Identity & Access Management (IAM)
- Code Security
- Web Application / API Security

Modern SOC Platform

Cortex

- EPP + EDR
- XDR + Analytics
- NTA + NDR + UEBA
- XSOAR
- XSIAM

NETWORK SECURITY

FIREWALLS NOUVELLE GÉNÉRATION

Les firewalls nouvelle génération Palo Alto Networks donnent la priorité à la prévention et l'intégration d'innovations faciles à déployer. La plateforme de sécurité Palo Alto Networks vous protège contre les menaces connues et inconnues grâce à un contrôle granulaire des applications, des utilisateurs et des contenus, associé à une intelligence cloud partagée de détection des menaces.

Les 3 missions clés du Firewall Nouvelle Génération :

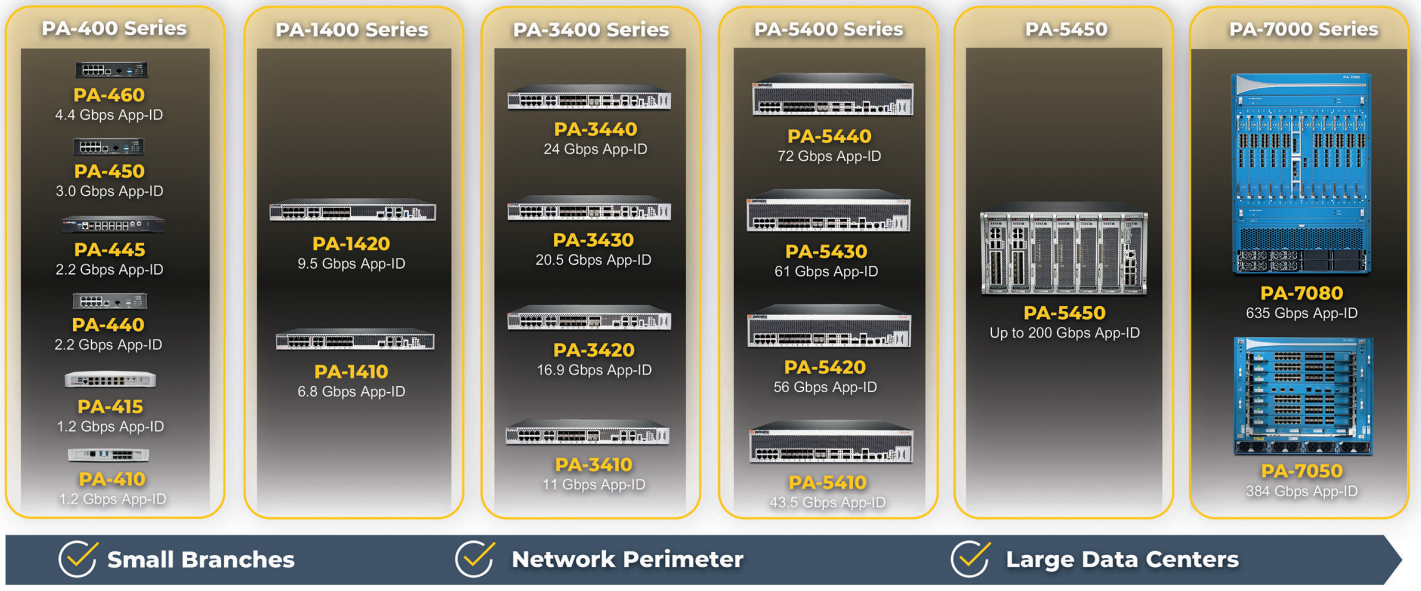
- Permettre à vos utilisateurs d'accéder aux données et aux applications selon les exigences de l'entreprise
- Vous prémunir des menaces connues et inconnues, y compris dans le trafic chiffré
- Vous protéger des attaques par vol d'identifiants

Les 3 technologies clés du Firewall Nouvelle Génération :

APP-ID	USER-ID	CONTENT-ID
Technologie de classification des applications	**Technologie de classification des utilisateurs**	**Technologie de classification des contenus**
App-ID ™ est une technologie de classification du trafic brevetée. Elle détermine l'identité d'une application indépendamment du port, du protocole, du cryptage SSH / SSL ou de toute autre tactique d'évasion que l'application peut utiliser	User-ID ™ permet d'identifier l'utilisateur par son identité, indépendamment de son adresse IP, grâce à plusieurs technologies combinant un mapping avec les annuaires ou le monitoring du trafic d'authentification	Content-ID ™ permet une analyse complète de tout le contenu du trafic autorisé comprenant les malwares, tous les types d'exploit, les catégories Web, et les fichiers par catégorie ou type de contenu. L'ensemble sera utilisé comme critère de contrôle

Gamme

NGFW alimenté par le ML - Cartes de chiffrement dédiées - Longue durée de vie - Puissance accrue



Les souscriptions

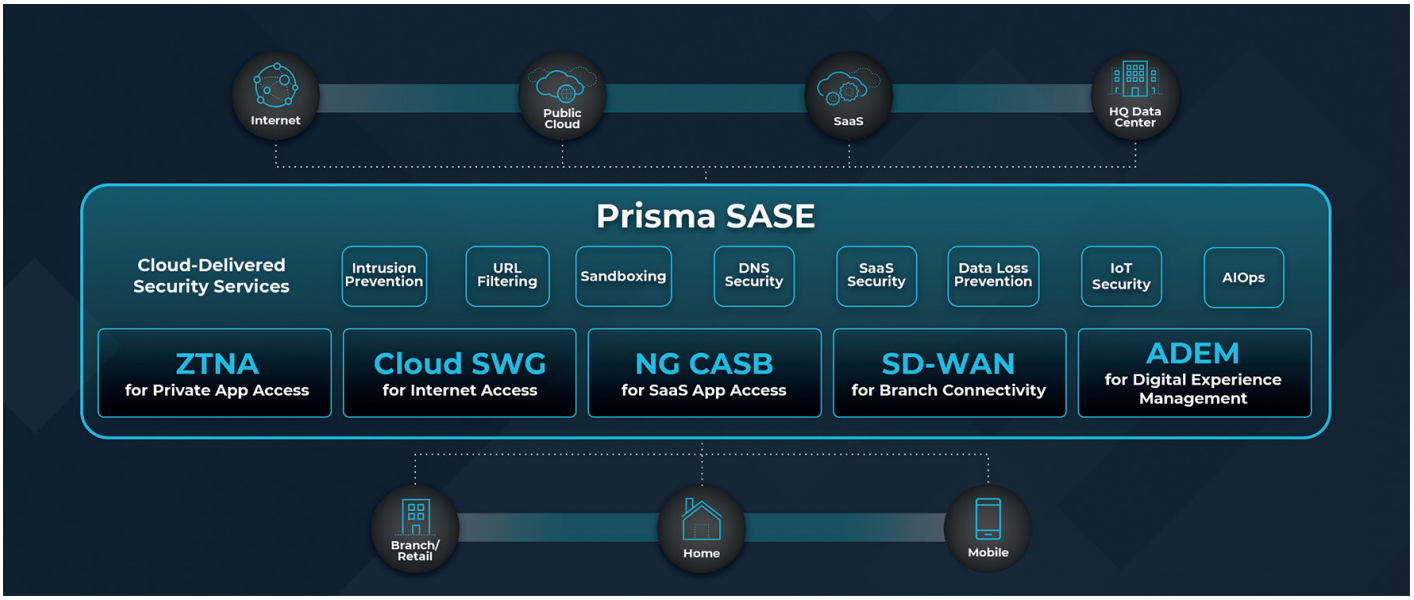
Les souscriptions de sécurité de l'offre Strata sont nativement Intégrées aux Firewalls Nouvelle Génération pour exploiter toutes les technologies d'identification et appliquer automatiquement une sécurité pilotée par l'analytique.

SOUSCRIPTIONS	DESCRIPTION
Advanced Threat Prevention	Protéger le trafic, bloquer les menaces, et attaques Command-And-Control en ligne
Advanced URL Filtering	Sécuriser la navigation Web, détecter des menaces URL, et nouveaux sites Web
Advanced Wildfire	Moteur d'analyse des menaces Zero-Day, Machine-Learning pour bloquer les attaques
DNS Security	Bloquer les menaces utilisant le DNS pour faire du Command-And-Control et du vol de données
SD-WAN	Optimiser de la bande passante entre les sites, et sécuriser l'interconnexion des sites
Global Protect	Améliorer les politiques VPN, contrôler l'intégrité des postes, et faire du VPN sans agent
IoT Security	Détecter, classifier, et stopper les menaces venant de l'IoT et machines inconnues sur le réseau
Enterprise Data Loss Prevention	Détecter et classifier la donnée sensible et limiter la fuite de donnée
SaaS Security	Protéger les utilisateurs sur les environnements SaaS connus et inconnus
AIOps	Améliorer la configuration des FWs en profondeur

Bundles de souscriptions – 5 Subs au prix de 2,7

PRISMA SASE

La suite de produits Prisma représente l'offre de sécurité et de conformité cloud la plus complète du marché. Elle sécurise l'accès vers le cloud, les ressources natives cloud ainsi que les environnements hybrides.



Prisma SASE = Prisma Access + Prisma SD-WAN

Prisma SASE Prisma SASE est l'offre de Palo Alto Networks qui converge les fonctionnalités de réseaux et de sécurité, en une seule et même plateforme délivrée depuis le Cloud.

Prisma Access est la plateforme de service cloud « Firewall-as-a-service » qui propose toutes les fonctions et toutes les souscriptions du firewall nouvelle génération Palo Alto Networks, gérées de manière centralisée et unifiée avec les firewalls physiques si l'entreprise en possède. La disponibilité et la montée en charge du service sont gérées et garanties par Palo Alto Networks.

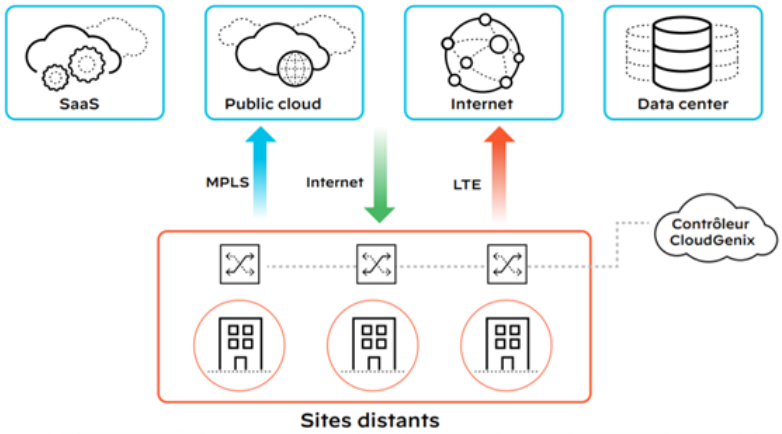
Prisma Access se décline en plusieurs offres en fonction des besoins de l'entreprise, pour assurer un retour sur investissement le plus rapide.

- Business – Sécurité des sites distants, incluant la Secure Web Gateway, Advanced URL Filtering, et DNS Security
- Business Premium – Sécurité avancée des sites distants, incluant la Secure Web Gateway, Advanced Threat Prevention, Advanced URL Filtering, WildFire, et DNS Security
- Zero Trust Network Access (ZTNA) Secure Internet Gateway (SIG) – Sécurité des utilisateurs nomades incluant toutes les fonctionnalités de sécurité
- Enterprise – Sécurité des utilisateurs nomades et sites distants, incluant toutes les fonctionnalités de sécurité

Prisma SD-WAN

La connexion des sites distants simple et sécurisée avec un ROI de 243%

Prisma SD-WAN (anciennement CloudGenix) est la première solution de SD-WAN nouvelle génération du marché capable d'assurer un retour sur investissement allant jusqu'à 243%, de simplifier les opérations réseau grâce au Machine Learning, éliminer 99% des tickets de support réseaux, et améliorer l'expérience des utilisateurs avec une bande passante WAN décuplée pour un coût inférieur à celui des architectures classiques.

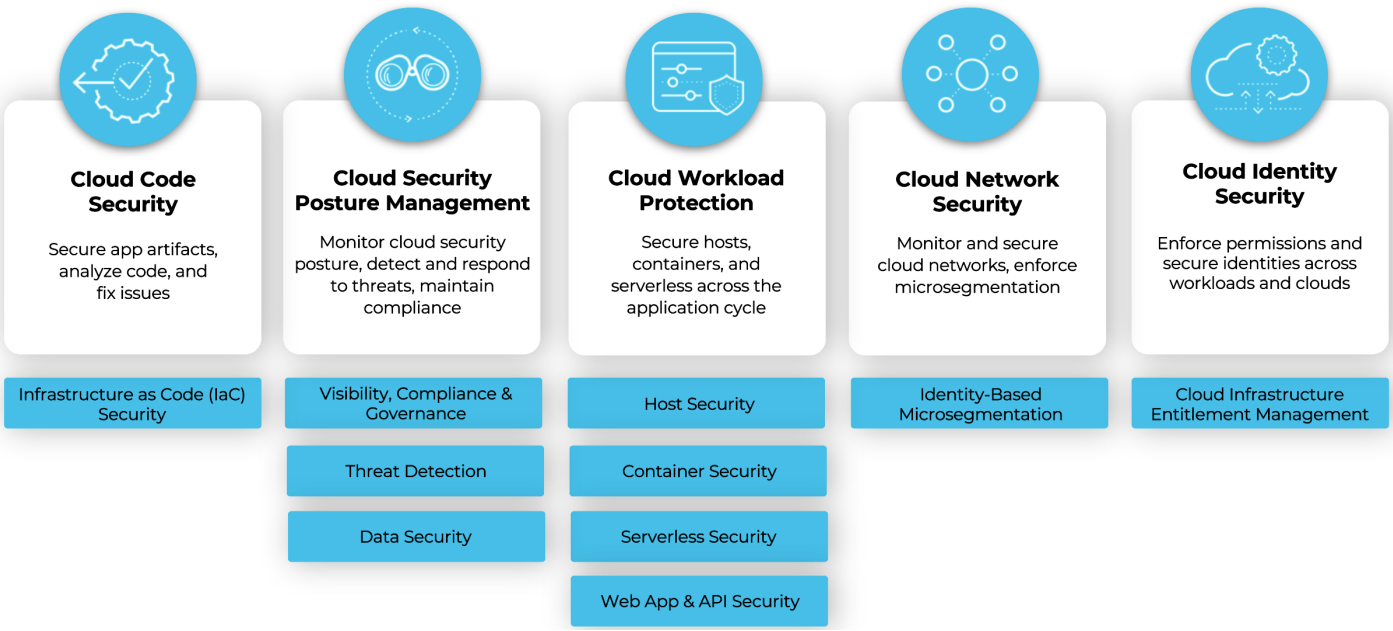


PRISMA™
BY PALO ALTO NETWORKS

Prisma Cloud, protection des applications cloud native

Prisma Cloud sécurise vos déploiements complexes multi cloud en assurant la visibilité et la sécurité de vos données et workloads sur les cloud publics GCP, AWS et Microsoft Azure. Prisma Cloud a une approche totalement intégrée aux outils de déploiement et de développement pour une sécurité « by-design ». Les licences Prisma Cloud sont basées sur le nombre de Workload à sécuriser.

- Protection des containers, Serverless et hosts
- Vue unifiée de la conformité et de la sécurité
- Encadrement complet des DevSecOps
- Gouvernance et conformité



CORTEX™
BY PALO ALTO NETWORKS

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.

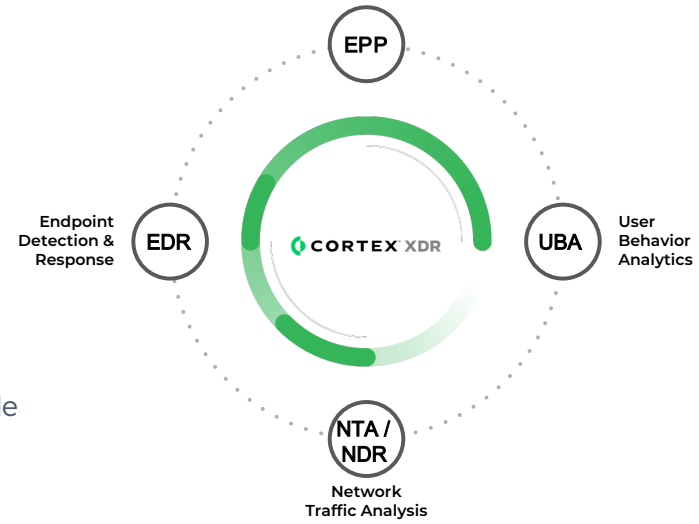
RÉINVENTER LA SECURITE OPÉRATIONNELLE

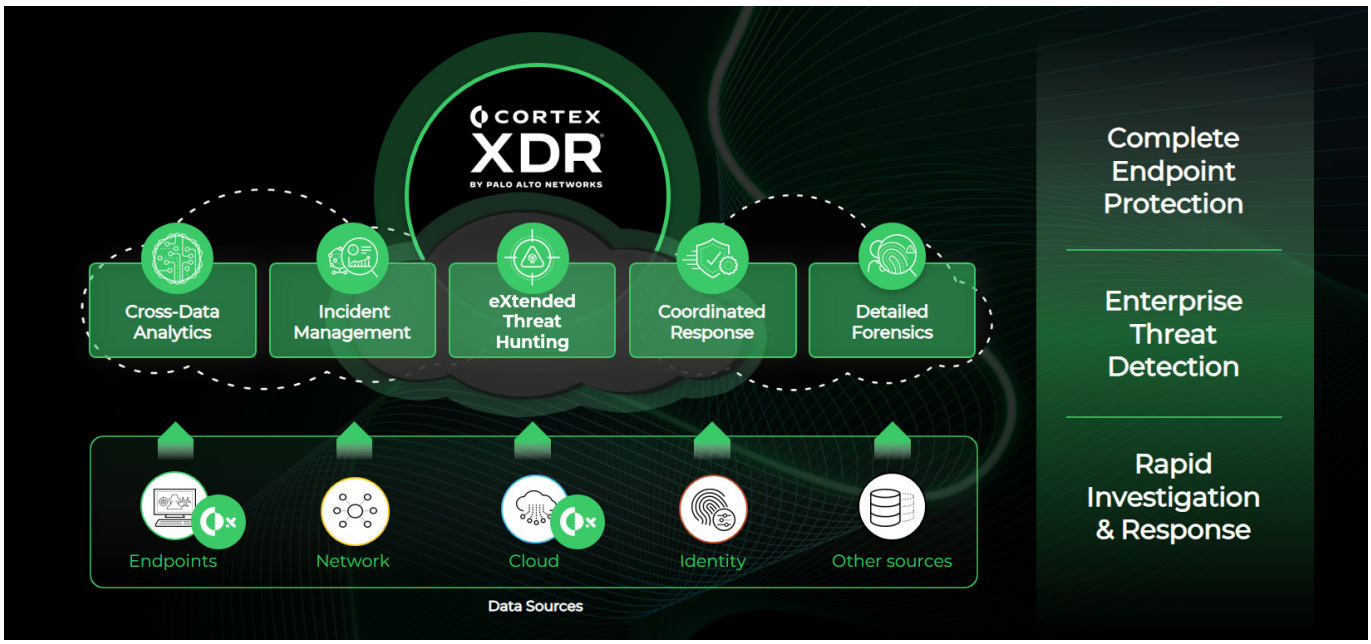
Elle est composée de 3 éléments clés :

- 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 XDR

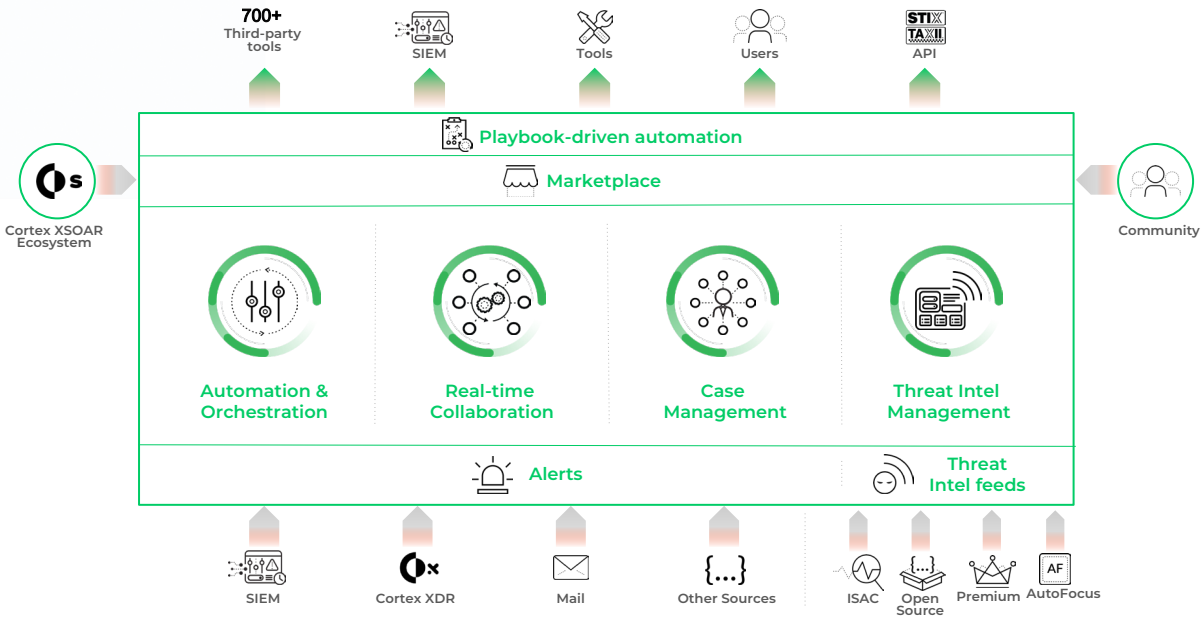
- Intégration de toutes les données réseau, endpoint et cloud
- Découverte des menaces par un Machine Learning continu
- Réponse coordonnée entre les endpoints, le réseau et le cloud
- Protection avancée du endpoint : Prévention, détection et réponse
- Investigation 8x plus rapide
- Sécurisation des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





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.

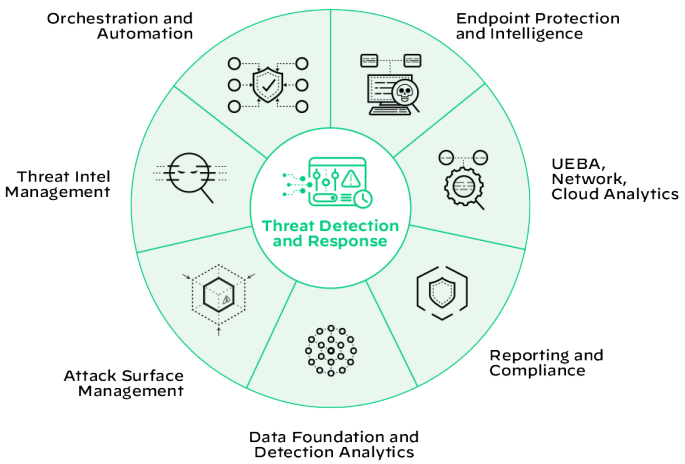


CORTEX XSIAM

Cortex XSIAM (eXtended Security Intelligence and Automation Management) est une solution qui rassemble la télémétrie de l'infrastructure, la Threat Intelligence et les données ASM au sein d'une base de données intelligente, garante d'une détection et d'une réponse plus efficace et entièrement automatisée.

Cortex XSIAM permet de ne plus perdre de temps sur les tâches répétitives et sur l'analyse de gros volumes de données. Les analystes gagnent ainsi en productivité tout en se consacrant à des besoins SecOps plus stratégiques.

CORTEX™
XSIAM
BY PALO ALTO NETWORKS



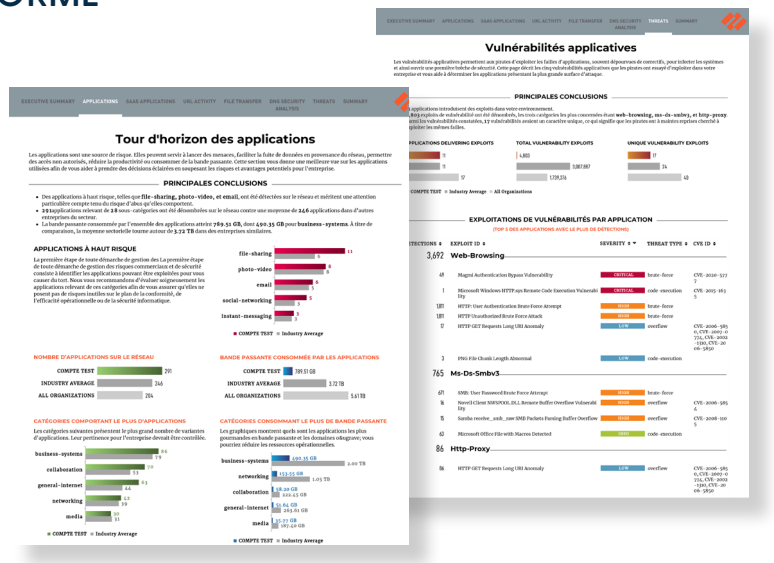
SLR :
SECURITY LIFECYCLE REVIEW

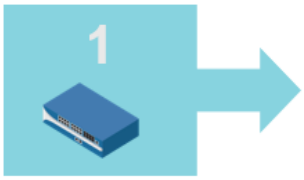
MONTREZ LA PUISSANCE DE LA PLATEFORME PALO ALTO NETWORKS

Le SLR (Security Lifecycle Review) est un outil destiné à offrir une visibilité sur les applications, les risques et les menaces, obtenue sous la forme d'un rapport généré sur la base d'informations recueillies par le firewall nouvelle génération grâce à une mise en place non intrusive.

Le SLR est une évaluation sur mesure des risques comprenant l'exposition réelle aux menaces, le comportement utilisateur, l'utilisation des applications, pour comprendre les risques "cyber" de l'entreprise.

Le SLR est généré par l'intermédiaire d'un partenaire en récupérant un fichier de logs.





Un boîtier est installé sur le réseau

Le traffic est monitoré passivement pendant 1 semaine

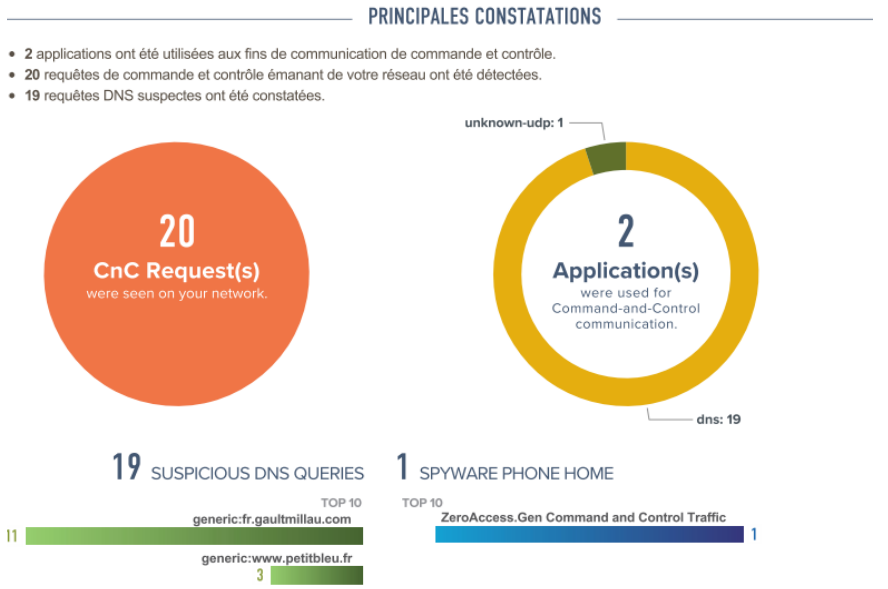
Le rapport expliquant les résultats est fourni

QUE FAIT LE SLR ?

- Identification et usage des applications
- Identification et usage des applications SaaS
- Comportement des utilisateurs
- Rapport sur les risques et les menaces

SLR : DANS QUEL CAS ?

- Construire un cas d'usage Palo Alto Networks pour les architectes, les managers et les décisionnaires.
- Montrer comment restaurer la visibilité et le contrôle sur les applications, les utilisateurs et le contenu
- Prouver la nécessité d'une telle solution dans le réseau
- Gérer le cycle d'évaluation et mettre un cadre autour de l'évaluation/POC



AIOps :
ARTIFICIAL INTELLIGENCE FOR IT OPERATIONS

Renforcer la posture de sécurité grâce à des recommandations sur les meilleures pratiques et éliminer les risques

Suivre le cycle de vie de l'adoption des fonctions et services de sécurité configurés

Maximiser le retour sur investissement des NGFW en utilisant toutes les fonctionnalités disponibles et proposer des recommandations sur les meilleures pratiques

Remédier aux mauvaises configurations

L'analyse en direct des politiques détecte et suggère des remèdes aux anomalies qui dégradent la posture de sécurité

Améliorer de manière proactive la posture de sécurité

Corriger les mauvaises configurations, et mettre en place les meilleures pratiques avant les Commit

Résoudre les perturbations du pare-feu pour maintenir une santé et des performances optimales

Éviter de manière proactive les perturbations du pare-feu

Détecte les problèmes de santé et de performance du pare-feu jusqu'à 7 jours à l'avance avec des recommandations pour y remédier.

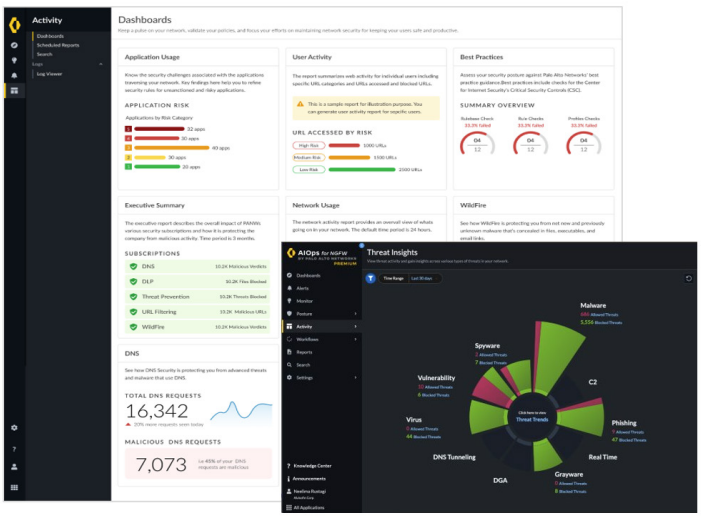
Relever les principaux défis opérationnels des FW

Résoudre les problèmes liés à l'utilisation des ressources, aux matériels, logiciels, à l'épuisement de la mémoire, aux logs, au trafic, à la surcharge, à la détection des vulnérabilités spécifiques aux fonctionnalités, etc.

Planifier les mises à jour et minimiser les temps d'arrêt

Conseils sur les versions logicielles les mieux adaptées à votre environnement en fonction des fonctionnalités activées, des modèles NGFW et des vulnérabilités connues.

Obtenir une vue unifiée de l'efficacité de la sécurité



Connaître l'efficacité de votre sécurité

Voir les menaces les plus dangereuses et les plus récentes du réseau, celles qui ont été empêchées et celles qui requièrent une attention particulière

Comprendre l'évolution d'une menace

Exploiter le réseau partagé et les renseignements sur les menaces pour obtenir une visibilité sur les menaces avancées potentielles avec des mesures correctives actionnables pour arrêter les risques de sécurité émergents

Vue unifiée des artefacts de sécurité

Vue centralisée de l'activité à travers les applications, les menaces, les réseaux, les utilisateurs et les souscriptions de sécurité

EXPEDITION

MIGREZ INTELLIGEMMENT ET RAPIDEMENT VERS UNE CONFIGURATION PALO ALTO NETWORKS

Expedition est un outil open-source qui va permettre d'accélérer la migration de configuration de firewalls traditionnels vers les technologies de firewall nouvelle génération Palo Alto Networks, donnant ainsi accès aux meilleurs processus et aux meilleures pratiques de protections contre les menaces.

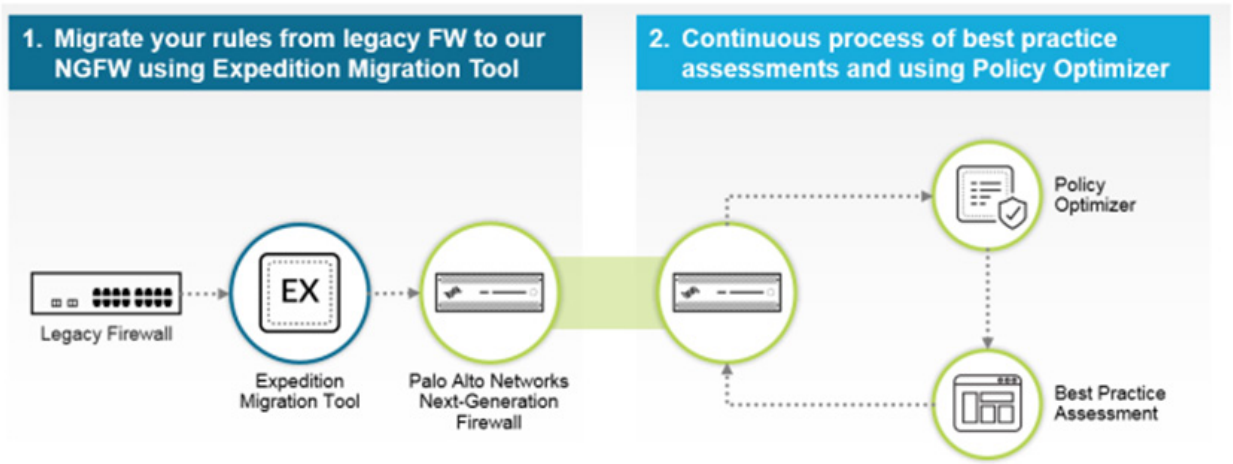
Expedition transpose facilement les règles de sécurité à la couche 3/4 des firewalls tiers vers des règles à la couche 7, améliorant ainsi la protection. Expedition aide à l'implémentation de ces règles à travers les technologies App-ID™, User-ID™ et Content-ID™ de Palo Alto Networks.

Expedition permet d'importer automatiquement les configurations des firewalls

- Cisco
- Fortinet
- Check Point
- Forcepoint
- Juniper
- IBM XG.

Les configurations d'autres types de firewalls peuvent être migrés par l'intermédiaire d'Expedition avec l'aide de scripts.

Expedition va automatiquement mettre à jour vos règles existantes. Il va également utiliser l'analytique pour générer et implémenter de nouvelles règles et des recommandations de configuration. L'objectif sera d'améliorer les contrôles de sécurité tout en optimisant les processus.



UTD : ULTIMATE TEST DRIVE

METTEZ VOUS AUX COMMANDES DE LA PLATEFORME PALO ALTO NETWORKS

Les UTD (Ultimate Test Drive) sont des sessions sous forme d'ateliers techniques qui vous permettent de prendre en main la plateforme Palo Alto Networks à travers des cas d'usage scénarisés avec pour objectif de démontrer toute la valeur de la plateforme de sécurité Palo Alto Networks.

Les ateliers peuvent se faire en ligne ou sous forme de workshop sur site et donnent accès dans tous les cas à des labs virtuels.

LES DIFFÉRENTS UTD

SECURE ACCESS SERVICE EDGE (SASE) AVEC PRISMA ACCESS

- Protéger les sites distants et les users mobiles où qu'ils soient.
- Assurer la connectivité et la sécurité pour toutes les applications grâce au Firewall as-a-service (FWaaS).
- S'adapter aux changements d'environnement grâce à une infrastructure cloud qui converge les fonctions de réseau et de sécurité.

CYBERSECURITY PORTFOLIO

- Protéger les users des Ransomware avec les VM-Series et Cortex XDR.
- Prévenir les malwares inconnus avec WildFire et AutoFocus
- Sécuriser les app SaaS critiques avec Prisma™ SaaS.
- Automatiser les détections et les investigations avec Cortex XDR and Cortex Data Lake

NEXT-GENERATION FIREWALL

- Etablir des règles pour sécuriser l'utilisation d'appli et en bloquer d'autres
- Activer l'analyse sandbox des malwares inconnus avec WildFire®
- Configurez des règles de déchiffrement et d'inspection du flux SSL
- Sécuriser les devices mobiles avec GlobalProtect

NETWORK SECURITY MANAGEMENT (PANORAMA)

- Centraliser des déploiements de règles globales et locales
- Utiliser des templates Pour faciliter la configuration réseau et device
- Gestion de la hiérarchie logique de groupes pour une meilleure gestion
- Importer facilement des configurations existantes dans Panorama

VIRTUALIZED DATA CENTER

- Avoir une visibilité complète des applications dans le DC
- Contrôler le trafic entre les VM par applications pour limiter l'exposition
- Prévenir la propagation des attaques connues et inconnues dans le DC
- Adapter dynamiquement les règles aux changements dans le DC

CLOUD DELIVERED SECURITY SERVICES

- Etablir des règles pour prévenir les menaces connues
- Activer l'analyse sandbox WildFire pour contrôler les malwares inconnus
- Configurer le déchiffrement et le filtrage URL
- Activer les règles contre les attaques inconnues et les exploits zero-day avec Cortex XDR

VM-SERIES SUR AMAZON WEB SERVICES (AWS)

- Implémenter des règles pour sécuriser les applications dans le VPC Amazon®
- Comprendre les différentes VM-Series pour les cas d'usage AWS
- Protéger le déploiement AWS en bloquant une attaque brute-force proactivement

VM-SERIES SUR MICROSOFT AZURE

- Déployer des VM Series dans Azure
- Autoriser les applications et prévenir les menaces dans Azure
- Publier des métriques PanOS grâce à l'intégration des VM-series dans Azure
- Rediriger le trafic des VM pour la tolérance de panne

VM-SERIES SUR GOOGLE CLOUD PLATFORM

- Déployer des VM-Series dans GCP
- Améliorer la sécurité native de GCP par une protection contre les attaques avancées
- Utiliser Policy Optimizer pour passer des règles basées port vers des règles applicatives
- Adapter dynamiquement les règles de sécurité dans GCP grâce aux VM-Series et aux DAG (Dynamic Address Groups)

MIEL ACADEMY :
FORMATIONS PALO ALTO NETWORKS

Miel est un centre de formation ATP pour Palo Alto Networks depuis près de 10 ans.
Nos formateurs ont tous une très solide expérience avant-vente et après-vente afin de délivrer la formation la plus pertinente possible.

Nos sessions inter-entreprises se déroulent à Paris, à Bièvres (91) et ponctuellement en région. Nous proposons aussi des sessions sur-mesure en « intra » pour un minimum de 3 participants.

Il est également possible de suivre des formations virtuelles avec formateurs, en ligne, pour toutes les dates sur Paris et Bièvres.

Les formations disponibles sont les suivantes :

PAN-EDU-210
Firewalls : Essentials - Configuation et Management
5 jours - PCNSA / PCNSE

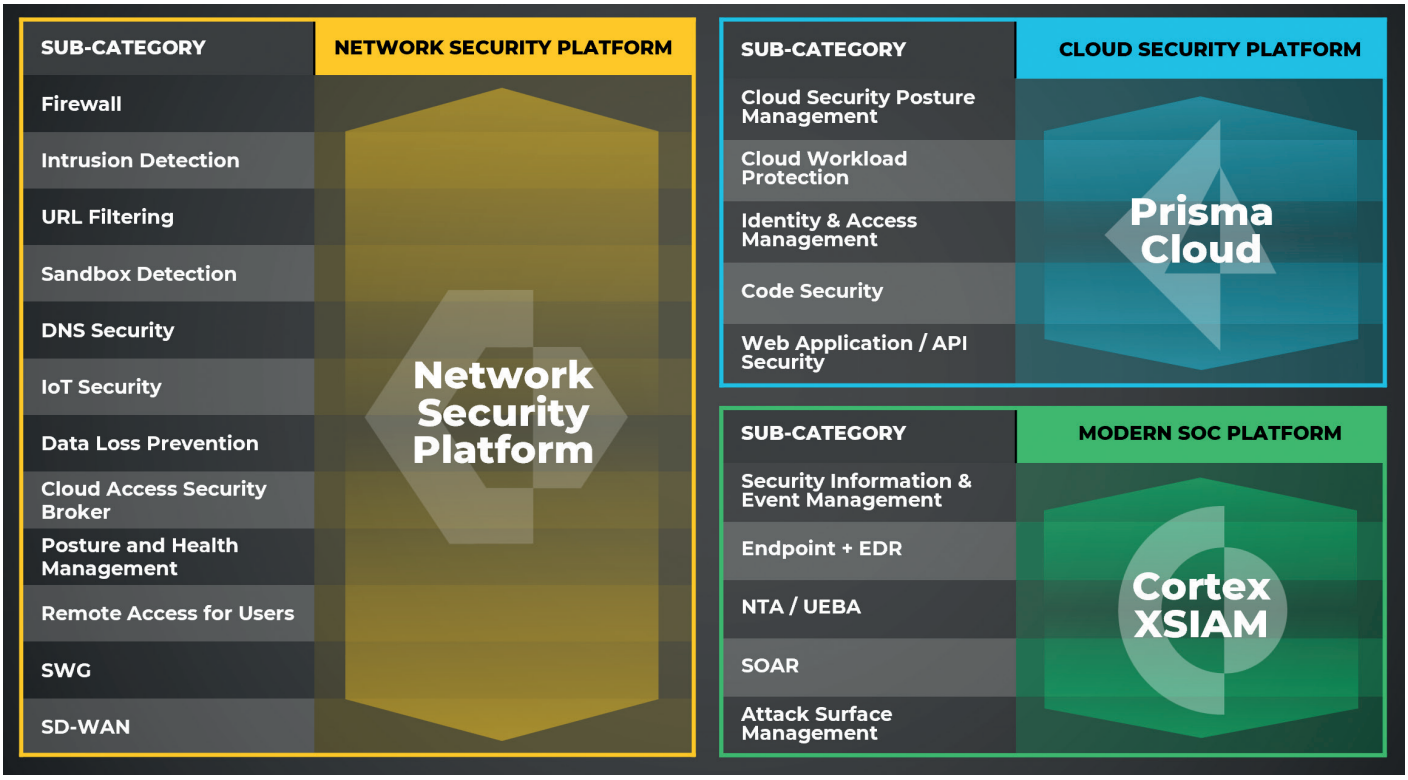
PAN-EDU-260
Cortex XDR : Prevention and Deployment
3 jours - PCDRA

PAN-EDU-262
Cortex XDR : Investigation and response
3 jours - PCDRA

PAN-EDU-330
Firewalls : Troubleshooting avancé des firewalls.
3 jours - PCNSE

PAN-EDU-220
Panorama : Administration
2 jours - PCNSE

PAN-EDU-318
Prisma Access SASE Security Design and Operation - 4 jours



Distribué en France par MIEL
www.miel.fr/palo-alto-networks-next-gen-firewall