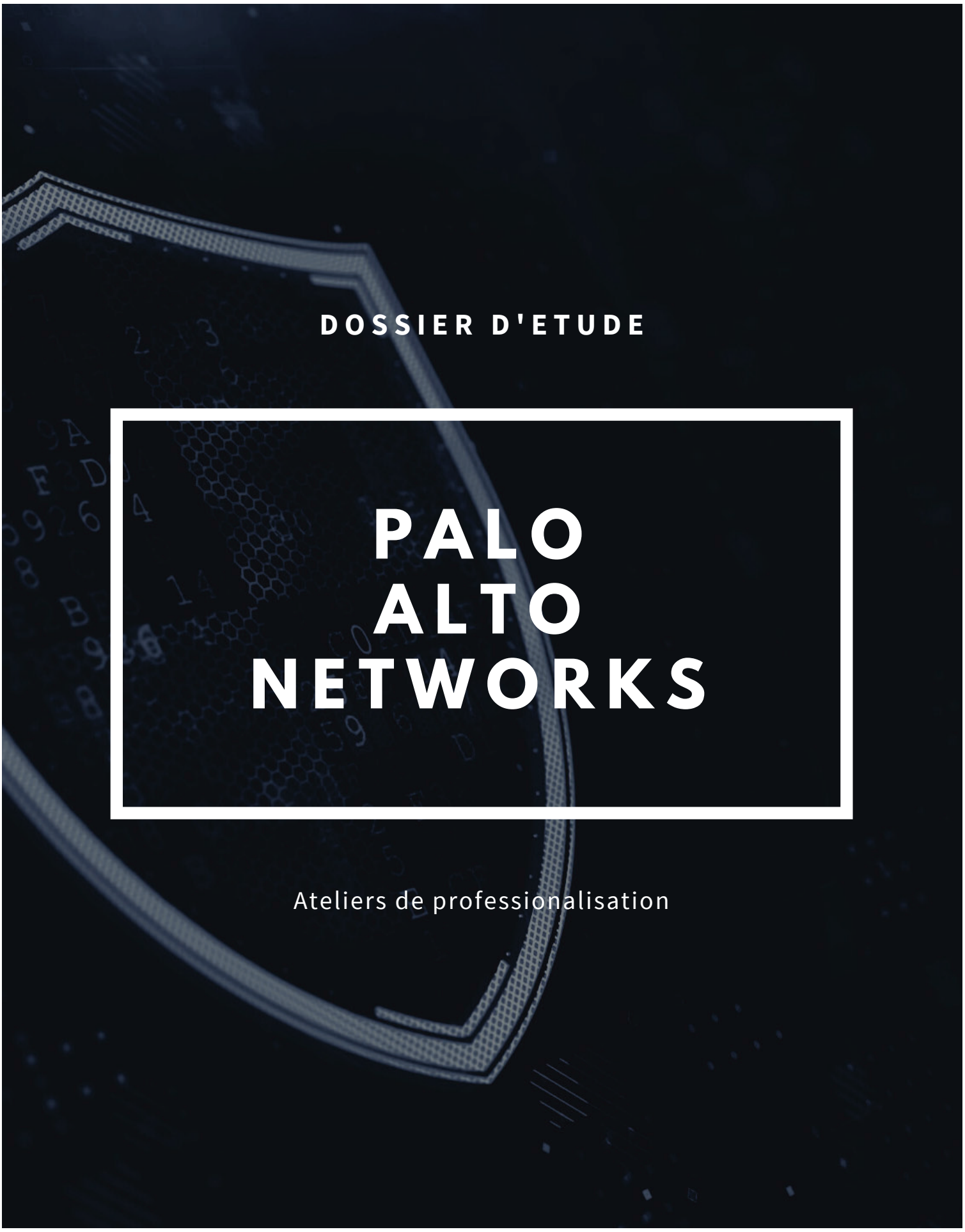

DOSSIER D'ETUDE

PALO ALTO NETWORKS

Ateliers de professionalisation

Travail réalisé par :

- Erwan Cloux

Table des matières

1. Présentation de l'entreprise :

Fiche d'identité de Palo Alto Networks	
NOM DE L'ENTREPRISE :	PALO ALTO NETWORKS
TYPE D'ENTREPRISE :	ENTREPRISE PRIVEE
STATUT JURIDIQUE :	SOCIETE DE DROIT ETRANGER
METIER :	Entreprise fonctionnait majoritairement sur du B to B (Entreprise vers entreprise) et qui fournit des solutions logicielles et matérielles de cybersécurité. Ils sont spécialisés dans les pares-feux.
SECTEUR D'ACTIVITE :	Secteur tertiaire (fournir des solutions logicielles comme PAN-OS par exemple)
FINALITE :	ENVIRONNEMENTAL : Transition vers un neutre en carbone d'ici 2030. SOCIALE : Améliorer la valeur des employés en les payant au juste prix et en leur donnant des responsabilités.
CHAMP D'ACTION GEOGRAPHIQUE :	INTERNATIONAL : Fournit des produits à travers le monde entier (+ 150 pays)
RESSOURCES HUMAINES :	+ 10 000 salariés
RESSOURCES FINANCIERES :	3.4 milliards de dollars ($) de Chiffre d'Affaire en 2020 (Source : Palo Alto Network)
RESSOURCES MATERIELLES :	Siège social à Santa Clara (Californie), locaux à travers le monde (France, USA, etc.)
RESSOURCES IMMATERIELLES :	Savoir-faire, expertise dans leur domaine, PAN-OS et ensemble des logiciels développés par Palo Alto Networks
TAILLE :	Grande Entreprise (+ 10 000 salariés)

Palo Alto Networks est à l'heure actuelle le leader mondial des solutions de cybersécurité à destination des entreprises. Du fait de leur expertise dans les domaines matérielles et logicielles, ils ont su s'imposer sur le marché. Cependant, certains concurrents subsistent : nous pouvons d'abord parler de Cisco, entreprise mondialement connue pour son matériel et ses outils destinés aux entreprises et aux particuliers. Cisco propose des solutions logicielles et du matériel à destination des entreprises principalement dans un but de sécurisation et de protection de données. Un second concurrent pour Palo Alto Networks est Check Point. Palo Alto est installé dans le marché des solutions de cybersécurité depuis 2005, soit 12 ans après Check Point, mais cela n'a pas empêché à la firme de se démarquer et de faire de la concurrence à Check Point. Check Point se revendique comme un pionnier des pares-feux notamment avec son invention : FireWall-1 qui a été un des premiers pare feu en 1994.

2. Découverte d'un produit : le pare-feu

Dans le domaine de la cybersécurité, la présence d'un pare-feu est indispensable pour veiller à la sécurité des données. On définit un pare-feu (communément appelé firewall en anglais) comme un logiciel et/ou un matériel protégeant la totalité du trafic d'un réseau de toutes connexion malveillante. Il fonctionne sur un principe de « règles » qu'il va faire respecter. Par exemple, dans le cas d'un Windows Server si une règle du pare-feu stipule qu'au bout de 3 tentatives de connexion échoué au RDP l'IP doit être bloquée, alors le pare-feu va surveiller les connexions de chaque utilisateurs et bloqués ceux qui vont entrer des identifiants erroné 3 fois de suite. Il existe plusieurs types de Pare-feu comme les pares-feux par proxy, les pares-feux dynamiques ou encore ceux que l'on dit de nouvelle génération. Ceux-ci incorporent les interdictions à destination des utilisateurs et des applications, il filtre le trafic internet d'un réseau et émergent depuis plusieurs années.

Le pare-feu de Palo Alto Networks se décline en 2 formes : matériel et logiciel. Il s'inscrit dans les pares-feux de nouvelle génération du fait des fonctionnalités qu'il offre. Dans un premier temps l'utilisateur acquiert un Pare-feu physique (à l'heure actuelle, Palo Alto propose 10 modèles) ou alors il peut faire le choix d'en virtualiser un. Sinon, il peut aussi bénéficier de la protection offerte par ce Pare-feu grâce à la solution cloud proposée par Palo Alto : Prisma Access.

Dans un second temps, peu importe le choix de l'utilisateur, celui-ci aura accès à un « Dashboard » qui lui permettra de paramétrer son pare-feu et de retrouver des informations liées à celui-ci.

Dans la vidéo « Next Generation Firewall Demo », on nous présente un Pare-feu virtualisé, on peut l'observer au titre du Dashboard : PA-VM mais aussi aux différentes indications liées à la machine virtuelle sur le Dashboard : VM Mode = VMware ESXi notamment. L'interlocuteur nous présente les différentes fonctionnalités : les widgets qui permettent d'avoir une vue d'ensemble en un coup d'œil sur la page d'accueil, mais aussi les différents outils plus poussés qui permettent de mesurer l'activité du réseau, les activités bloqués, l'usage des machines, etc. L'outil ne s'arrête pas seulement à la simple surveillance, on peut bloquer en temps réel l'accès à certains sites, ou encore créer des règles 100% personnalisées pour des postes particuliers ou des groupes de postes. Le pare-feu s'accompagne d'une solution d'antivirus déployable sur les postes et entièrement paramétrable.

Cette présentation nous permet de découvrir un outil relativement complet se basant sur le Machine Learning qui permet d'avoir une vue rapide mais aussi précise du trafic de données d'un réseau, en fonction du site et de la machine mais aussi d'assurer une prévention inégalée. Cet outil semble être une solution extrêmement complète pour tout les administrateurs réseaux afin de sécuriser et surveiller au mieux leur réseau. De plus, le fais que cette solution ne s'accompagne ici d'aucun matériel mais seulement d'un pare-feu virtualisé sur une machine montre d'autant plus la puissance des outils de Palo Alto. La virtualisation offrirait beaucoup plus de possibilités aux administrateurs réseaux de bénéficier de ces solutions de sécurisations. Enfin, Palo Alto, à dévoiler une réelle innovation technologique puisque son pare-feu est le premier au monde à fonctionner sur le principe du Machine Learning. Bien loin d'être gadget, l'usage du Machine Learning permet de prévoir de manière plus intelligentes les dangers dans un but de sécurisation toujours plus poussée.

3. Présentation de Cortex

Cortex se repose énormément sur un principe d'IA pour automatiser les tâches de sécurisation ce qui réduit les alertes car il agit de manière autonome. Cortex serait la révolution des SOCs. Un SOC est une plateforme qui permet la supervision et l'administration de la sécurité d'un poste informatique.

On retrouve la technologie Cortex dans l'antivirus Cortex XDR. Cortex XDR est considéré comme l'antivirus du futur. Il permettrait de lutter plus efficacement contre les attaques grâce à la technologie de l'intelligence artificielle. Palo Alto est parti du principe qu'une entreprise ne peut bloquer à 100% les attaques, c'est dans cette idée que la suite Cortex XDR a été développée, afin de faciliter l'identification des attaques et leur blocage.

En adéquation avec Cortex XDR, Cortex a développé Cortex XSOAR qui est un outil permettant d'automatiser des processus et d'avoir une gestion plus autonome des postes.

Enfin, la solution Cortex intègre Crypsis qui est une assistance humaine disponible 24h/24h qui permet de résoudre des crises (ransomwares sur tous les postes d'un réseau par exemple).

Le but de Cortex est au final d'identifier et bloquer plus facilement les attaques, mais aussi d'optimiser une panoplie de processus. Cependant, plusieurs questions sont soulevables lorsque l'on intègre une IA au cœur d'une solution de sécurisation.

4. Nos questions

Nos questions relatives au parcours professionnel de Mr Jordan TREHOUT :

- Avez-vous appris de nouvelles choses au sein de Palo Alto que vous ne connaissiez pas en sortant d'études ?
- Selon vous l'accès à Palo Alto est-il difficile par rapport à une entreprise traditionnelle ?
- Qu'avez-vous fait comme étude et quel conseil donneriez-vous au vous d'avant ?

Nos questions relatives aux aspects techniques du Pare-feu pour Mr Jordan TREHOUT :

- Comment est venu l'idée d'intégrer le Machine Learning au sein d'un Pare-feu ?
- Ne pourrait-il pas y avoir des problèmes d'estimations des risques par le Pare-feu ?
- A termes, est ce que l'idée serait d'avoir un Pare-feu qui se pilote seul ?

Nos questions relatives à Cortex pour Mr Jordan TREHOUT :

- Ne serait-ce pas créer du risque que l'administrateur soit moins prévenu des risques éventuels sur son réseau ?
- Y'a-t-il un réel gain de temps grâce à Cortex pour les entreprises ?
- Sur le site, il est indiqué 95% d'automatisation de la réponse. Comment fonctionne l'automatisation de la réponse aux attaques ? Elle bloque elle-même l'attaque ou fais appel à l'administrateur ?