Guide pratique de l'adoption du Zero Trust dans le SOC

Développez votre stratégie Zero Trust autour d'une surveillance continue et d'une visibilité totale sur les ressources critiques

Sommaire

Introduction

À l'origine, le rayon d'action du centre opérationnel de sécurité (SOC) se limitait à la protection périmétrique, un concept désormais dépassé dans un monde où les infrastructures et systèmes de sécurité se projettent au-delà du périmètre du réseau traditionnel pour s'étendre au cloud public/privé et à tous les appareils ou terminaux connectés. Autant d'éléments sur lesquels les équipes de sécurité ont besoin d'un certain degré de visibilité et de contrôle, sans quoi elles seront incapables d'éviter des compromissions. Dans un contexte de foisonnement des systèmes embarqués, des objets connectés (IoT) et des connexions sans fil, notre surface d'attaque ne se restreint plus à un périmètre clairement délimité. D'où le besoin de remettre à plat les décisions d'octroi de la confiance pour protéger les écosystèmes d'entreprise d'aujourd'hui.

Pandémie oblige, les modes de travail distanciels et hybrides se sont généralisés. Si l'on ajoute à cela la migration des applications et données vers le cloud et la croissance exponentielle de l'IoT, on ne peut que constater l'élargissement considérable de notre surface d'attaque collective.

Le Zero Trust a été inventé il y a quelque temps déjà par John Kindervag, à l'époque où il était analyste chez Forrester Research. Ce concept avait alors pour but d'apporter une réponse aux menaces capables de contourner les modèles de sécurité conventionnels, en partant du principe qu'une infrastructure dite « de confiance » était en réalité compromise et potentiellement hostile. Ce postulat a révolutionné notre façon d'appréhender la sécurité informatique.

De manière générale, le Zero Trust repose sur une vérification et une validation rigoureuses et permanentes de chaque individu, appareil ou entité qui tente d'accéder aux ressources réseau. L'objectif principal : prévenir les attaques, les exploits, les compromissions et les corruptions de données, d'applications et de systèmes critiques.

Les principes du Zero Trust visent à réduire les expositions et les accès non autorisés à travers tout le champ des menaces. Ils ont été minutieusement pensés pour garantir la sécurité des applications critiques et des données sensibles dans toute une entreprise. Le mieux dans tout cela, c'est que vous pouvez aisément intégrer ces principes à votre stratégie de sécurité. Parmi eux :

- **Authentification multifacteur (MFA)** : Ce protocole impose aux utilisateurs de s'authentifier à l'aide de plusieurs procédures de sécurité obligatoires. Il s'agit généralement d'une combinaison d'éléments que l'utilisateur connaît (un mot de passe ou un code PIN, par exemple), qu'il possède (un jeton physique, un badge, etc.) et qui le constituent (des données biométriques comme la voix et les empreintes digitales).
- **Principe du moindre privilège** : L'idée est

LES UTILISATEURS TRAVAILLENT OÙ ILS VEULENT

Même après la pandémie,

76 % des salariés souhaitent rester sur un modèle de travail hybride.[1]

1. *Sécurité du travail hybride : état des lieux*, Palo Alto Networks, 25 août 2021.

d'octroyer aux utilisateurs uniquement les droits d'accès dont ils ont absolument besoin pour accomplir leur mission. Ainsi, vous réduisez les points d'entrée et les expositions aux malwares et aux attaquants, mais aussi les risques d'exfiltration de données.

- **Microsegmentation** : Pour isoler les utilisateurs, les appareils ou même les workloads individuels, vous pouvez découper votre réseau en plusieurs segments, ou « zones sécurisées », dans vos data centers ou environnements cloud, l'accès à ces zones étant soumis à la saisie d'identifiants différents. Cela limite également les déplacements latéraux (est-ouest) sur les réseaux internes en cas de compromission.

Qu'est-ce que le Zero Trust ? Cette stratégie de sécurité consiste à éliminer toute confiance implicite et à valider toutes les étapes d'une interaction numérique.

Le Zero Trust commence par la vérification et la validation des identités de vos utilisateurs.

- Chaque élément de votre architecture de sécurité doit pouvoir accorder ou bloquer l'accès d'un utilisateur après vérification.
- De même, vous devez être en capacité de vérifier l'identité des utilisateurs partout où votre architecture de sécurité octroie ou bloque l'accès.

L'approche du Zero Trust est sensiblement la même pour les applications.

- Là aussi, il est essentiel de bien vérifier l'identité des utilisateurs qui cherchent à y accéder.
- Pour nous assurer que le contenu relatif aux applications n'est pas malveillant, nous devons également valider les accès entre celles-ci et les workloads ainsi que les transactions, peu importe le lieu d'hébergement des applications (cloud privé, cloud public, etc.).

Faites preuve de la même rigueur pour l'accès à l'infrastructure en validant l'identité des utilisateurs qui s'y connectent.

- Par son manque de sécurité intrinsèque, l'IoT présente un risque considérable. D'où l'importance de valider les identités sur tous les objets connectés.
- Pour ce faire, il est vital de découvrir et de surveiller en permanence toutes les ressources connectées à Internet, ainsi que les modifications qui y sont apportées, afin de préserver une visibilité totale sur les risques d'exposition.
- On appliquera les mêmes principes aux concepts d'« accès » et de « transactions ».
- Concrètement, segmentez les infrastructures natives et tierces de votre supply chain, soumettez-les au principe du moindre privilège et surveillez les transactions qui y sont exécutées.
- Analysez l'ensemble du contenu de l'infrastructure à la recherche d'activités malveillantes et de vol de données.

	Identité	Appareil/Workload	Accès	Transaction
Zero Trust pour les utilisateurs	Validation des utilisateurs par authentification forte	Vérification de l'intégrité de l'appareil utilisateur	Application du principe de moindre privilège pour l'accès des utilisateurs aux données et aux applications	Analyse de l'ensemble du contenu à la recherche d'activités malveillantes et de vol de données
Zero Trust pour les applications	Validation des développeurs, du DevOps et des administrateurs par authentification forte	Vérification de l'intégrité des workloads	Application du principe du moindre privilège pour les accès de workload à workload	Analyse de l'ensemble du contenu à la recherche d'activités malveillantes et de vol de données
Zero Trust pour l'infrastructure	Validation de tous les utilisateurs ayant accès à l'infrastructure	Identification de tous les appareils, objets connectés inclus	Segmentation des accès suivant le principe du moindre privilège pour l'infrastructure native et tierce	Analyse de l'ensemble du contenu de l'infrastructure à la recherche d'activités malveillantes et de vols de données

Figure 1 : Développer le Zero Trust requiert une approche complète couvrant les utilisateurs, les applications et l'infrastructure

LES APPLICATIONS N'ONT PLUS DE FRONTIÈRES

80 % des entreprises appliquent une stratégie cloud hybride[2] et chacune utilise en moyenne 110 applications SaaS.[3]

Approche holistique du Zero Trust : le rôle du SOC

Le Zero Trust est un processus continu qui doit être adapté et affiné en permanence, à mesure que les exigences métiers et les technologies opérationnelles de l'entreprise évoluent, en particulier dans le cadre de projets de transformation numérique. C'est pourquoi la surveillance permanente du champ des menaces doit constituer l'un des piliers du Zero Trust. Et pour un maximum de visibilité, cette surveillance doit dépasser les capacités d'un seul outil de sécurité. Le SOC a donc un rôle essentiel à jouer dans le contrôle et le maintien d'une posture de sécurité résolument Zero Trust.

Plus précisément, le SOC joue un rôle stratégique à plusieurs égards :

- Vérification continue des politiques Zero Trust
- Identification des failles dans votre stratégie Zero Trust
- Atténuation de l'impact des attaques par l'exécution automatique des politiques
- Automatisation de la collecte des données CTI pour accélérer les investigations
- Découverte en continu des ressources critiques

Exemple : une entreprise souhaite mettre en place la MFA pour identifier les utilisateurs et contrôler les accès aux applications. L'équipe SecOps pourra alors avoir recours au machine learning, à l'analyse comportementale et à l'expertise humaine pour passer à la loupe l'activité d'un utilisateur donné, détecter les menaces internes et désactiver le compte d'un utilisateur malveillant pour limiter les dégâts. Même avec une implémentation Zero Trust mature et couvrant les utilisateurs, applications et workloads, les entreprises ont toujours besoin du SOC pour assurer la détection des menaces, la réponse, l'automatisation et la gestion du risque.

Dans un premier temps, les entreprises doivent définir les besoins exacts de contrôles Zero Trust transverses aux utilisateurs, applications et infrastructures. Le SOC, lui, est le mieux placé pour ingérer une grande variété de données télémétriques de sécurité, effectuer une surveillance continue et valider les contrôles Zero Trust.

Transformation du SOC : une étape critique pour une nouvelle approche du Zero Trust

Lorsqu'elles mettent en œuvre le Zero Trust, les équipes du SOC optent pour un réglage très sensible des paramètres de détection, ce qui se traduit par une avalanche d'alertes. Appliquez cette approche à la trentaine d'outils utilisés en

2. *2021 State of the Cloud Report*, Flexera, mars 2021.
3. « Average number of SaaS apps used by organizations worldwide 2015-2020 », Statista, 16 février 2022.

moyenne par les SOC, et les tableaux de bord des analystes deviennent vite saturés d'alertes peu fiables et de faible importance.

L'analyste doit alors les étudier une à une pour décider de l'action à engager : investigation plus poussée ou classement sans suite. Par conséquent, les analystes du SOC peuvent consacrer énormément de temps à analyser et à valider une *seule* alerte. En outre, ils doivent parfois avoir recours à plusieurs outils (bien souvent non intégrés) afin de rassembler suffisamment d'éléments pour pouvoir décider de faire remonter l'alerte ou non.

Faute de contexte, les analystes perdent encore plus de temps à recouper des données et à fouiller dans les journaux dans l'espoir de corréler des alertes sans lien apparent et d'établir un diagnostic du problème. Manque de consolidation des activités suspectes, prolifération des outils, pénurie de compétences dans les équipes de sécurité… les entreprises ont besoin d'une nouvelle approche pour renforcer la défense et la protection de leurs infrastructures critiques.

Aujourd'hui, les menaces de sécurité évoluent plus rapidement que les technologies destinées à les combattre. À l'heure où les groupes étatiques investissent sans compter dans de nouveaux outils comme le machine learning, l'automatisation et l'intelligence artificielle, les SOC qui s'appuient sur des solutions traditionnelles de gestion des

Figure 2 : Les méthodes de sécurité traditionnelles sont inefficaces

informations et des évènements de sécurité (SIEM) manquent de flexibilité et d'évolutivité pour suivre la cadence de la transformation numérique et des projets cloud, *sans parler* de leur impuissance face à des campagnes d'attaques avancées. Avalanche de faux positifs, volume et coût du stockage des évènements, lacunes des workflows d'investigation… tous ces problèmes entravent la capacité des analystes de sécurité à identifier, gérer et neutraliser les menaces les plus graves, dans un contexte d'adoption des architectures multicloud et hybrides et de prolifération des équipements et terminaux.

Les environnements SOC traditionnels présentent plusieurs problèmes :

- Manque de visibilité et de contexte
- Complexité accrue des investigations
- Accoutumance aux alertes et quantité de « déchets » dans les forts volumes d'alertes générés par les contrôles de sécurité
- Manque d'interopérabilité des systèmes
- Manque d'automatisation et d'orchestration
- Incapacité à collecter, traiter et contextualiser les données CTI

La voie à suivre : intégrer l'IA, l'automatisation et l'orchestration

Le parcours d'implémentation du Zero Trust doit commencer par la définition d'une politique de sécurité unifiée. Il s'agit généralement d'identifier les ressources critiques et de déployer une architecture Zero Trust imposant des règles d'accès strictes, basées sur le principe du moindre privilège et couvrant les utilisateurs, les applications et l'infrastructure.

Automatiser les workflows

Entre la configuration et l'exploitation des outils de sécurité, l'interprétation et le tri de résultats d'analyse et la conduite de tests, les responsables sécurité doivent s'interroger sur le rôle de l'humain dans le Zero Trust. Ils peuvent alors choisir d'automatiser des tâches de routine répétitives qui, associées au jugement humain, permettent d'accélérer les investigations d'incidents.

Si les progrès en machine learning et en intelligence artificielle s'avèrent prometteurs, il demeure impératif de conserver un élément humain pour assurer un transfert de connaissances réciproque, condition *sine qua non* à une transformation efficace du SOC. À mesure que les fonctionnalités d'automatisation gagnent en maturité, l'humain sera appelé à intervenir de moins en moins dans les workflows de sécurité.

Automatisation : prévisions sur un horizon à cinq ans

Les nouveaux SOC peuvent automatiser dès à présent, tandis que les organisations plus établies devront dresser un état des lieux de leurs outils et décider par où commencer. L'objectif pour ces dernières : automatiser 50 % du SOC sur trois ans. Au bout de la cinquième année, la plupart des équipes SOC auront automatisé environ 75 % de leurs activités, mais continueront d'en confier certaines comme le threat hunting à des ingénieurs.

Aujourd'hui, les opérations de sécurité et la réponse aux incidents (IR) reposent sur un trop grand nombre de processus manuels, notamment pour la surveillance d'innombrables flux CTI. En investissant dans des fonctionnalités d'automatisation comme celles des solutions SOAR, vous pouvez faciliter une orchestration transverse à toute la stack de produits pour une IR plus rapide et plus évolutive.

Renforcer l'efficacité des équipes à l'aide d'une CTI pilotée par ML

Pour redéfinir l'architecture du SOC dans une configuration Zero Trust, les équipes de sécurité doivent exploiter tout le potentiel du machine learning en appui et en renfort de leurs moyens humains. L'IA et les outils d'analyse avancée peuvent considérablement accélérer le traitement d'énormes volumes de données dans l'entreprise, avec à la clé des éclairages inestimables sur les évènements de sécurité. En automatisant la détection de signaux faibles à travers de multiples sources de données et en ajoutant systématiquement du contexte aux alertes, le machine learning tient aujourd'hui ses promesses d'accélération des investigations et d'élimination des angles morts dans l'entreprise.

À condition cependant d'entraîner les modèles de machine learning à détecter des patterns spécifiques dans les schémas de données, puis de tester et d'optimiser les processus.
Les techniques de machine learning permettent de collecter, d'intégrer, d'analyser et d'interroger les données, réduisant considérablement le temps et les connaissances nécessaires à l'humain pour exécuter ces tâches. Le ML facilite également la vie des équipes SOC en les libérant de la recherche de preuves et d'informations contextuelles dans les données générées par de multiples couches de sécurité.

Globalement, les techniques de machine learning couvrent trois grands volets :

- **Intégration** : permettre aux données d'informer sur les évènements.

« Nous traitons tous les cas d'usage de la même façon, c'est-à-dire de la façon la plus extrême possible. Nous n'accordons aucun passe-droit à quiconque du simple fait que nous savons qui ils sont, où ils se trouvent, ce qu'ils essaient de faire, etc. Cette approche simplifie grandement l'infrastructure : nous n'avons plus à acheter des équipements ou des solutions différentes selon les personnes, les situations ou les applications.

Comme nous exécutons les mêmes contrôles de sécurité pour les utilisateurs, les applications, etc., nous pouvons utiliser une seule architecture, une seule solution, une seule technologie pour protéger tous nos collaborateurs, à tout moment, partout où ils se trouvent et quelle que soit leur intention. ***Voilà la philosophie de l'entreprise Zero Trust.*** »

— Nir Zuk, Cofondateur et CTO, Palo Alto Networks

- **Analyse** : extraire des éclairages sur un sujet donné et établir des prévisions.
- **Automatisation** : accélérer le processus décisionnel humain, enrichir les données d'incident et automatiser les actions, les workflows et la prise de décision au niveau du système.

Cap sur un Zero Trust intégral avec la suite de produits Cortex

Pour entamer ou accélérer la transformation de votre SOC, vous pouvez déployer la suite de produits Cortex selon vos besoins. Cortex XDR, Cortex XSOAR et Cortex Xpanse fonctionnent en synergie pour démultiplier l'efficacité de vos opérations de sécurité.

L'union fait la force ! Les équipes SOC profitent d'avantages aussi immédiats que convaincants :

Cortex XDR : Assure la sécurité de votre entreprise en offrant une protection des terminaux, une détection des menaces et une capacité de réponse couvrant tout le réseau, le cloud, les terminaux et pratiquement n'importe quelle source de données. Basée sur le machine learning et les analyses comportementales, cette technologie brevetée identifie avec précision les menaces furtives et fournit toutes les informations nécessaires pour agir avant toute compromission.

Cortex XSOAR : Plateforme unifiée qui permet aux équipes SOC de gérer tous leurs flux CTI et de données sur les incidents. XSOAR compte plus de 800 intégrations préconfigurées pour les outils de sécurité utilisés dans le SOC, ainsi que des milliers de playbooks et de scripts d'automatisation des workflows. La solution permet ainsi aux équipes SOC de définir leurs paramètres d'alertes aux niveaux de sensibilité requis pour le Zero Trust, sans s'inquiéter de submerger les analystes de faux positifs. En automatisant les processus opérationnels de son SOC avec XSOAR, un fournisseur d'électricité basé aux États-Unis a réduit le nombre de tickets d'incidents de 30 % dès le premier mois d'utilisation.

Cortex Xpanse : Dresse un inventaire exhaustif, précis et à jour des erreurs de configuration et des ressources cloud d'entreprise connectées à Internet à l'échelle mondiale. Sa mission ? Cerner, évaluer et diminuer continuellement les risques au niveau de votre surface d'attaque externe, évaluer les risques liés aux fournisseurs, ou encore déterminer le niveau de sécurité d'une cible de rachat.

Si chaque produit propose des fonctionnalités et avantages uniques, ils offrent à eux trois des résultats bien supérieurs à la somme de leurs parties. La suite complète de ces trois produits destinés aux SecOps intègre des fonctionnalités leaders de détection, d'investigation, d'automatisation et de réponse pour réduire le risque et l'impact des compromissions.

L'interopérabilité et l'intégration natives de bout en bout créent des synergies permanentes à travers l'écosystème Cortex pour permettre aux équipes SOC de neutraliser plus facilement les menaces.

Ensemble, ces trois produits surveillent tout le champ des menaces et offrent des fonctionnalités de détection, de réponse et d'investigation de pointe :

- Cortex XDR et Cortex Xpanse fournissent des outils de détection et une visibilité optimale sur la surface d'attaque Internet, les terminaux, le cloud et le réseau, y compris pour les collaborateurs en distanciel.
- Cortex XDR s'appuie sur les capacités de Cortex XSOAR pour automatiser l'investigation et la réponse aux malwares.
- Ensemble, Cortex Xpanse et Cortex XSOAR enrichissent automatiquement les données d'incident, grâce aux informations fournies par Xpanse, et automatisent la remédiation des dernières ressources découvertes.
- Cortex XSOAR utilise Cortex XDR et Cortex Xpanse pour assurer une détection haute fidélité des menaces et automatiser les workflows de réponse aux incidents.

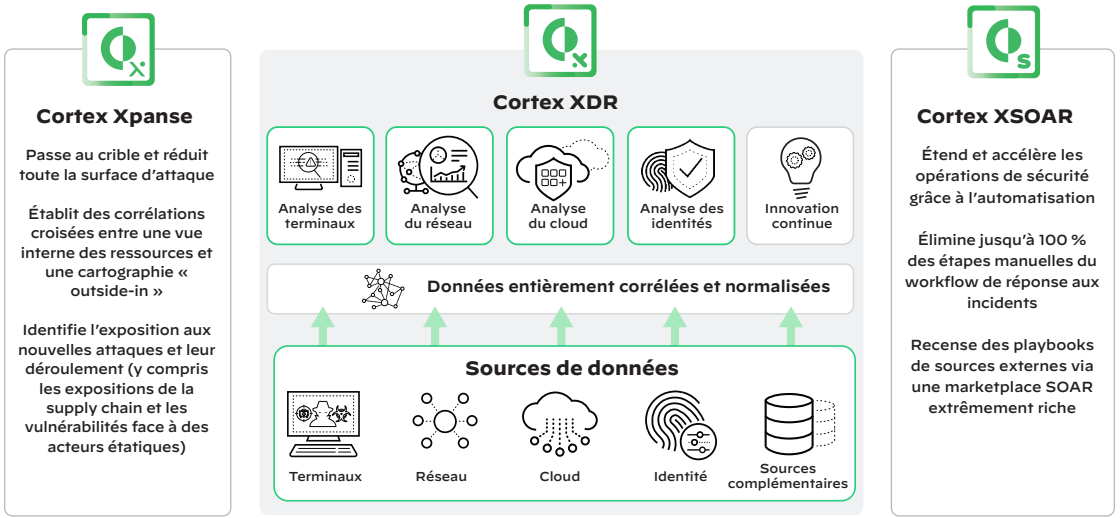

Figure 3 : La suite de produits Cortex

Et demain ? Embarquez pour le futur avec XSIAM

Même si les produits Cortex répondent aux exigences du SOC en termes de visibilité, de protection et d'automatisation, les équipes SecOps de la plupart des entreprises dépendent encore des systèmes SIEM. Or, les produits SIEM n'ont pas tenu leurs promesses de centralisation des fonctions de détection et de réponse aux menaces, si bien que les analystes restent aux prises avec des processus manuels et un flot ininterrompu de données. Les équipes de sécurité ont besoin d'une plateforme unifiée centralisant et automatisant les fonctions de sécurité fondamentales, tout en offrant une visibilité sur les données de toute l'entreprise.

Cortex XSIAM (EXtended Security Intelligence and Automation Management) a été spécifiquement conçue dans cette optique. Elle exploite toute la puissance de l'automatisation pilotée par l'IA pour renforcer la sécurité tout en réduisant considérablement les tâches SecOps manuelles. XSIAM crée une base de données intelligente et automatise les fonctions SOC unifiées pour accélérer la réponse aux incidents, neutraliser les menaces et simplifier considérablement le travail des analystes.

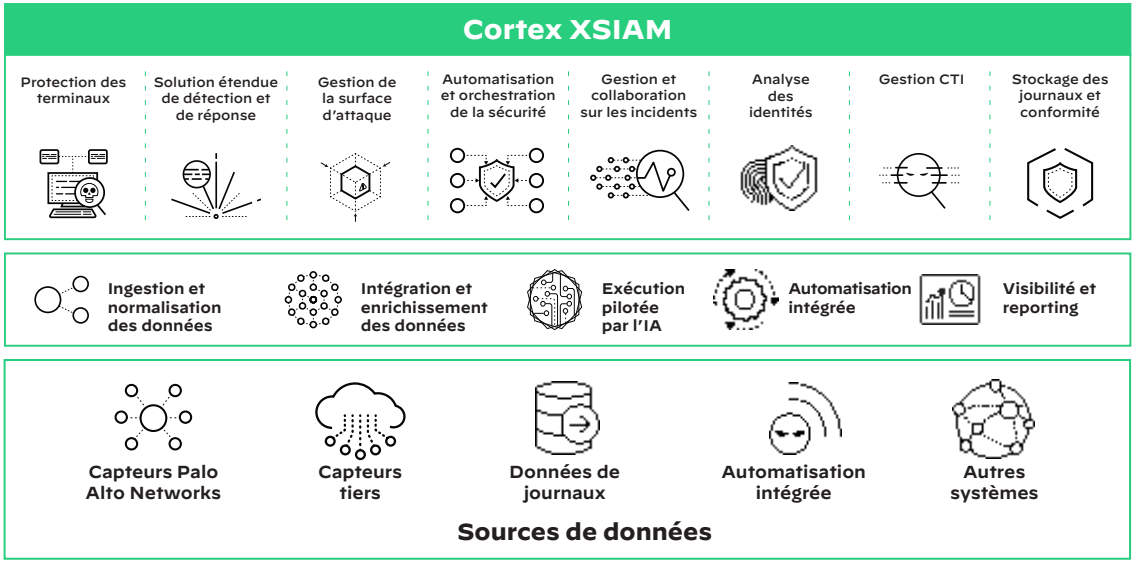

Figure 4 : XSIAM est une plateforme pilotée par l'IA conçue pour le SOC moderne

Bref, en unifiant toutes les fonctionnalités au sein d'une solution holistique et automatisée, XSIAM est appelée à supplanter les outils SIEM et autres produits spécialisés pour devenir le centre névralgique des activités du SOC. Si le modèle opérationnel de XSIAM représente un tel changement de paradigme, c'est parce qu'il utilise l'automatisation pour se départir des processus manuels qu'imposent les produits de sécurité actuels. XSIAM améliore la protection et rationalise les SecOps en consolidant les données et les outils de sécurité des entreprises, en automatisant leurs activités et en comblant les failles de sécurité.

Puissance et protection avec Cortex

Palo Alto Networks s'engage à offrir les solutions de sécurité les plus avancées et les mieux intégrées du marché. N'attendez pas pour les découvrir et n'hésitez pas à nous contacter pour échanger. Nous serons ravis de vous accompagner sur la voie de la transformation de votre SOC.

Pour en savoir plus, lisez nos pages produits :

Cortex Xpanse

Cortex XSOAR

Cortex XDR

Cortex XSIAM

Rendez-vous sur la page du portefeuille Cortex.

Autres ressources Zero Trust

Entre montée en puissance des modes de travail hybrides et migration des applications et données vers le cloud, la transformation numérique va en s'accélérant. Pour les équipes SSI, le moment est idéal pour adopter une approche Zero Trust qui répond à ce tournant fondamental.

Consultez ces ressources complémentaires pour approfondir la question :

Lisez notre blog : « L'entreprise Zero Trust : le rôle du SOC »

Téléchargez notre livre blanc : « Zero Trust : comment créer votre architecture ».

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam, Pays-Bas

+31 20 888 1883

www.paloaltonetworks.fr

cortex_ebook_practical-guide-to-adopting-zero-trust_092022-fr