# Comment huit entreprises ont transformé leurs opérations de sécurité avec Cortex®

INTRODUCTION

# Le SOC de demain, c'est maintenant

## À l'heure actuelle, la cybersécurité ne peut plus reposer uniquement sur l'humain.

Indépendamment de leur envergure et de l'expertise de leurs équipes, les centres opérationnels de sécurité (SOC) n'ont plus les moyens, à eux seuls, de stopper les cyberattaques.

Ce qu'il leur faut, c'est une intelligence artificielle combinant les bons modèles, les bonnes ressources et les bonnes données. Seule cette technologie leur permettra d'automatiser leur sécurité pour mieux faire face au volume et au niveau de sophistication des menaces qui planent sur les réseaux.

La nouvelle plateforme Cortex® a été conçue pour vous aider à détecter et à répondre aux incidents en quelques secondes seulement, contre plusieurs jours auparavant.

Dans cet e-Book, vous découvrirez de quelle manière des clients Cortex sont parvenus à optimiser l'efficacité de leurs équipes SOC en rendant leurs processus de sécurité plus visibles, complets et pérennes.

Nous remercions ces entreprises d'avoir bien voulu partager leurs expériences et d'avoir choisi Palo Alto Networks comme partenaire de confiance.

paloalto NETWORKS

ARRÊT SUR IMAGE N°1 : ÉTAT DU DAKOTA DU NORD

# Un organisme IT public mise sur un SOC tourné vers l'avenir

L'État du Dakota du Nord a pris l'engagement d'offrir à tous ses usagers un accès simplifié aux technologies. Pour l'accompagner dans cette mission, le North Dakota Information Technology (NDIT) est en charge de la sécurité de l'ensemble des entités publiques de cet État américain – dans les centres urbains comme dans les zones rurales. Un défi de taille pour un réseau dont l'envergure et la complexité n'ont rien à envier à celles des plus grands groupes internationaux.

NORTH Dakota
Be Legendary.

**Secteur d'activité**
Secteur public

**Pays**
États-Unis

**Site web**
www.ndit.nd.gov

| > 800 000 | > 1 600 | 183 |
|---|---|---|
| USAGERS | VILLES ET COMTÉS | ÉTABLISSEMENTS SCOLAIRES INDÉPENDANTS |

paloalto NETWORKS


# Le NDIT est devenu un modèle de sécurité opérationnelle (SecOps) pour le secteur public. Il offre aux usagers et aux organismes publics du Dakota du Nord une protection automatisée et proactive, sans incident majeur recensé à ce jour.

« Aujourd'hui, nous employons seulement la moitié des effectifs d'une entreprise de taille similaire au classement Fortune 30. Cette efficacité, nous la devons à l'automatisation et à l'utilisation du machine learning, rendue possible par la réécriture de nos playbooks. Résultat, notre équipe SOC peut se consacrer pleinement aux tâches prioritaires génératrices de valeur. »

**— Michael Gregg, Responsable de la sécurité des systèmes d'information, North Dakota Information Technology**

## Les problématiques

Pour prendre en charge des centaines de milliers d'utilisateurs, des milliers d'intégrations et d'applications et un nombre incalculable de terminaux, le NDIT devait planifier, concevoir et bâtir un SOC parfaitement opérationnel à l'échelle de différents systèmes.

+ Des attaques toujours plus sophistiquées ciblaient les données des usagers et les opérations des organismes publics.
+ Le NDIT avait besoin d'une solution intégrée pour gérer un volume de menaces détectées ayant doublé pour atteindre 4,5 milliards en 2021.
+ Le NDIT cherchait une solution tout-en-un évolutive et pérenne.

## La solution

Le NDIT s'est associé à Palo Alto Networks pour déployer son SOC sur une période de trois ans. L'intégration de tout le portefeuille de produits Cortex (comprenant notamment Cortex XDR, XSOAR et Xpanse) lui a permis de bâtir un socle complet, capable à la fois d'assurer la sécurité des terminaux, la découverte des ressources et l'automatisation des workflows.

+ La mise en place d'un cadre référentiel unifié améliore la résolution au premier appel et réduit le temps moyen de réponse (MTTR).
+ L'administration des systèmes ne requiert que 2,17 équivalents temps plein (ETP), ce qui permet à un maximum de collaborateurs de se concentrer sur les analyses prioritaires et la résolution des menaces.
+ La structure organisationnelle, plus transparente, est conforme aux régimes réglementaires du National Institute of Standards and Technology.

ARRÊT SUR IMAGE N°2 : HEALTHPARTNERS

# Un leader de la santé réinvente sa sécurité

HealthPartners est un organisme de soins primé situé à Bloomington, dans le Minnesota. Sa mission est d'améliorer la santé et le bien-être de ses adhérents, de ses patients et des populations en général à travers des services médicaux et une couverture santé de qualité. Avec ses 25 000 salariés, HealthPartners est aujourd'hui la plus grande structure de santé américaine à but non lucratif, assurant des soins médicaux et dentaires à 1,8 million de personnes. Ses services cliniques s'articulent autour d'un pool de 1 800 médecins de toutes les spécialités qui soignent quelque 1,2 million de patients.

HealthPartners

**Secteur d'activité**
Santé

**Pays**
États-Unis

**Site web**
www.healthpartners.com

| 25 000 | 1,8 M | 1 800 |
|---|---|---|
| COLLABORATEURS | ADHÉRENTS | PRATICIENS |

paloalto NETWORKS

# Cortex a accéléré la transformation numérique de HealthPartners en permettant à son SOC d'éliminer en amont les vulnérabilités, d'automatiser la détection et l'investigation des incidents et d'augmenter le temps consacré aux menaces nécessitant réellement une intervention manuelle.

« Le pourcentage élevé et la régularité avec lesquels la plateforme Palo Alto Networks génère de vrais positifs nous permettent d'automatiser la neutralisation des menaces en toute sérénité. Et ça, nous étions incapables de le faire jusqu'à maintenant. »

**– Joel Pfeifer, Analyste de sécurité principal, HealthPartners**

## Les problématiques

Face aux tentatives permanentes de cyberattaques ciblant les données des patients de ses services médicaux et des adhérents de sa couverture santé, HealthPartners a décidé de renforcer sa sécurité globale – sans investir massivement dans de nouveaux équipements.

+ Les pare-feu existants n'offraient plus un niveau de sécurité à la hauteur des exigences de HealthPartners.
+ La protection aléatoire des terminaux rendait les appareils de l'organisme plus vulnérables.
+ Le manque de filtrage des alertes obligeait les équipes du SOC à analyser manuellement les menaces.

## La solution

HealthPartners a déployé le portefeuille de solutions Palo Alto Networks Cortex, avec notamment Cortex XDR, XSOAR et Xpanse.

+ Cortex consolide plusieurs systèmes sur une plateforme unifiée pour la moitié du coût affiché par ses concurrents.
+ La Threat Intelligence intégrée a permis de bloquer des dizaines de cyberattaques la première année.
+ Une visibilité de bout-en-bout et une analyse approfondie de l'origine des menaces et des activités malveillantes optimisent les performances du SOC.

ARRÊT SUR IMAGE N°3 : BETTER.COM

# Une FinTech rationalise sa sécurité

Better.com est l'une des plateformes de parcours d'accession à la propriété les plus dynamiques aux États-Unis. Cette FinTech facilite l'obtention de prêts hypothécaires et polices d'assurance en rendant les processus plus accessibles, plus rapides et plus transparents. La start-up américaine, qui a déjà contribué au financement de plus de 95 milliards de dollars de prêts immobiliers, fait de la protection des données de ses clients et technologies qui sous-tendent son modèle opérationnel ses deux priorités majeures.

Better

**Secteur d'activité**
Finance

**Pays**
États-Unis

**Site web**
www.better.com

| > 5 000 | > 10 000 | 95 Md $ |
|---|---|---|
| COLLABORATEURS | TERMINAUX | PRÊTS |


paloalto NETWORKS

# Cortex a permis d'accélérer et d'optimiser les procédures de sécurité de Better.com. Son équipe SOC adopte ainsi une approche plus proactive qui laisse à l'entreprise plus de temps pour se focaliser sur des initiatives visant à simplifier l'accession à la propriété des clients.

« La plateforme XSOAR permet de mener des investigations et des automatisations en conjonction avec l'application XDR, ce qui simplifie grandement l'exécution de commandes dans un workflow, la reconstitution d'une chaîne d'attaque complète et la résolution très, très rapide d'éventuels problèmes. »

**— Jeff White, Directeur de la sécurité, Better.com**

## Les problématiques

Better.com voulait donner à son SOC les moyens d'accélérer l'évaluation des vulnérabilités et la neutralisation des menaces à travers un réseau de plus en plus étendu.

+ La solution EDR existante générait des alertes peu fiables, avec un niveau de granularité insuffisant.
+ Le SOC croulait sous les workflows et les étapes de remédiation manuels.
+ L'entreprise avait besoin d'une visibilité complète sur toutes les données.

## La solution

Better.com a opté pour un éventail de solutions de sécurité de Palo Alto Networks comprenant notamment Cortex XDR, XSOAR, des pare-feu nouvelle génération (NGFW), Panorama et Prisma Access pour déployer des procédures de sécurité plus simples et plus proactives.

+ Une console unique fournit une vue complète sur les données, les utilisateurs, les applications, l'infrastructure et les terminaux.
+ L'automatisation des outils EDR et l'orchestration des réponses améliorent les workflows et élargissent la couverture.
+ La solution bloque toutes les attaques et offre une visibilité complète sur les tentatives de compromission, à travers le réseau et lors de tests d'intrusion.

ARRÊT SUR IMAGE Nº4 : KHIPU NETWORKS

# Une tranquillité d'esprit absolue pour les clients de solutions de sécurité

KHIPU Networks, une société de cybersécurité internationale primée, déploie des réseaux sécurisés de très haute qualité dans différents pays et secteurs d'activité. Pour aider ses clients à lutter contre les cyberattaques susceptibles de compromettre leurs données, de perturber leurs stratégies digitales et de porter atteinte à leur réputation, KHIPU Networks a lancé le premier service managé de détection et réponse étendues aux incidents (XMDR) du Royaume-Uni en 2019.

By Appointment to
Her Majesty the Queen
Network Security Provider
KHIPU Networks Limited
Hampshire

KHIPU CYBER SECURITY

**Secteur d'activité**
Cybersécurité

**Pays**
Royaume-Uni

**Site web**
www.khipu-networks.com

**1er**
FOURNISSEUR XMDR AU ROYAUME-UNI

**> 19**
ANNÉES DANS LA CYBERSÉCURITÉ

**> 500**
CLIENTS

paloalto NETWORKS

# L'entreprise s'est appuyée sur Cortex pour agréger les informations de sécurité de sa base de clients mondiale, ce qui lui a permis d'améliorer la détection et la réponse aux incidents tout en mettant en place une Threat Intelligence continue.

« Les solutions de sécurité opérationnelle Palo Alto Networks se distinguent de la concurrence par leur simplicité, leur niveau d'automatisation et leur degré de précision. Nos clients bénéficient d'une visibilité complète depuis une source de données unique et disposent d'une solution de réponse managée couvrant tout leur environnement. »

**— Guy Jermany, Directeur des systèmes d'information, KHIPU Networks**

## Les problématiques

KHIPU Networks devait pouvoir offrir les avantages d'un SOC maison, sous forme de service managé, pour répondre aux besoins aussi complexes que variés de ses clients évoluant dans une grande diversité de secteurs.

+ Les clients étaient confrontés à des défis de sécurité de plus en plus nombreux liés, entre autres, à la complexité IT croissante, à l'essor du télétravail et au déploiement d'infrastructures cloud et hybrides.
+ La solution devait être suffisamment flexible pour répondre aux exigences de tous les clients, environnements, priorités et budgets.
+ Les clients avaient le plus grand mal à recruter et fidéliser des experts en cybersécurité, surtout pour assurer des interventions et investigations 24h/7j.
+ KHIPU Networks devait pouvoir détecter et neutraliser des attaques de ransomware en pleine prolifération.

## La solution

KHIPU Networks a développé son service XMDR autour de Palo Alto Networks Cortex XDR et XSOAR. L'objectif : offrir une détection et une neutralisation proactives des incidents, ainsi qu'une analyse, des workflows et une gestion des tâches à la hauteur des besoins du SOC.

+ Une intégration améliorée avec de multiples produits spécialisés permet à KHIPU Networks de répondre, d'endiguer et d'investiguer les menaces en temps réel.
+ L'automatisation des processus IA/ML permet de détecter, neutraliser et éliminer les menaces. KHIPU Networks peut ainsi faire office de SOC pour de nombreuses entreprises.
+ L'identification des différentes étapes d'une attaque contribue à accélérer l'investigation et à optimiser la productivité des analystes de KHIPU Networks.
+ Grâce à ses services de cybersécurité abordables, flexibles et évolutifs, KHIPU Networks se positionne comme le partenaire de sécurité idéal pour les entreprises de toute taille, dans tous les secteurs.

ARRÊT SUR IMAGE N°5 : ASCEND MONEY

# Une licorne de la FinTech automatise son SOC

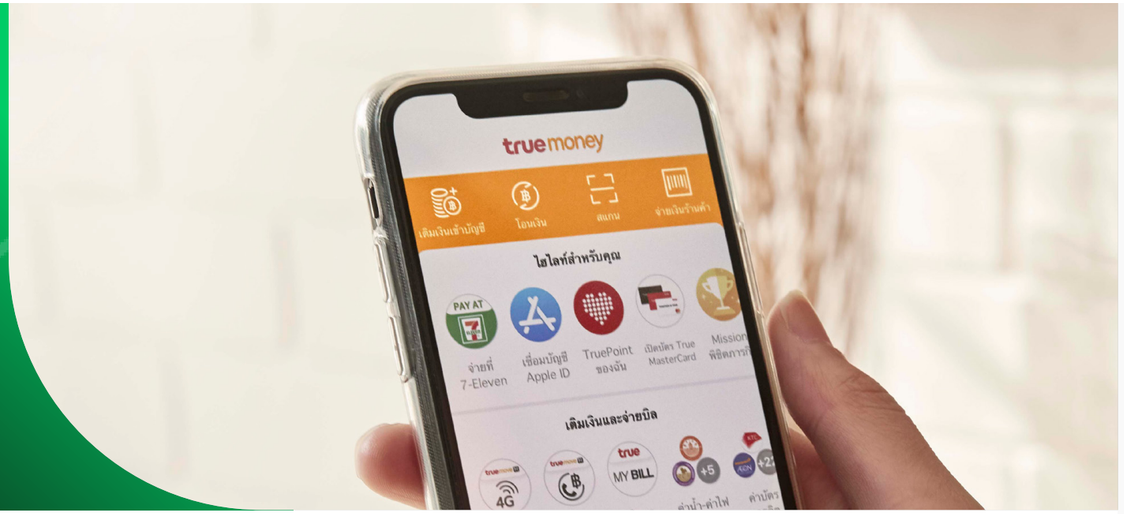
Fondée en 2013, la FinTech Ascend Money propose ses services aux consommateurs sous-bancarisés d'Asie du Sud-Est, avec un succès qui lui vaut d'être aujourd'hui la start-up à plus forte croissance de Thaïlande. Son application de paiement en ligne TrueMoney est utilisée par plus de 50 millions de personnes en Thaïlande, en Indonésie, au Vietnam, au Myanmar, au Cambodge et aux Philippines.


**Secteur d'activité**
Finance

**Pays**
Thaïlande

**Site web**
www.ascendmoneygroup.com

| 2 000 | 50 M | 6 |
|---|---|---|
| COLLABORATEURS | CLIENTS | PAYS |




**Dans un contexte international marqué par une augmentation exponentielle des menaces, Ascend Money s'est appuyé sur Cortex XDR et XSOAR pour assurer sa protection et garantir la sécurité des données de ses partenaires et clients.**

> Avec Cortex XDR de Palo Alto Networks, nous avons pu simplifier l'intégration et automatiser la sécurité, avec à la clé une réduction considérable de la durée de nos opérations ! »
>
> **— Kanokwan Aimsumang, Responsable de la sécurité IT et de la gouvernance, Ascend Money**

### Les problématiques

Dans un secteur soumis à un barrage d'attaques incessant, Ascend Money cherchait une solution capable de protéger ses ressources, mais aussi les informations financières de sa base de clients en pleine expansion.

+ La croissance de son réseau risquait d'entraîner des failles dans la sécurité des terminaux.
+ Le SOC était confronté à un niveau très élevé d'alertes non filtrées.
+ Ascend Money voulait éviter toute interruption de ses activités en cas de cyberattaque.
+ L'entreprise voulait moderniser sa technologie pour introduire l'IA et le ML.

### La solution

Ascend Money a choisi Cortex XDR pour automatiser la détection et l'intervention sur les terminaux (EDR), tout en déployant la plateforme Cortex XSOAR par le biais de notre partenaire True Digital Cyber Security.

+ XDR offre une protection étendue des terminaux, ce qui permet de combler d'éventuels écarts dans la posture de sécurité.
+ Grâce à l'automatisation de la sécurité pilotée par IA/ML, le SOC peut se focaliser sur les tâches à forte valeur ajoutée.
+ L'évolutivité de XDR et XSOAR permet à l'entreprise de développer sa sécurité au rythme de sa croissance.
+ La simplification de l'intégration et l'automatisation de la sécurité ont fortement réduit la durée des opérations.

ARRÊT SUR IMAGE N°6 : FORVIA FAURECIA

# Un industriel place sa transformation numérique sous le signe de la sécurité

Le grand équipementier automobile Forvia Faurecia déploie des technologies de nouvelle génération pour maintenir sa compétitivité sur un marché en pleine transition vers la conduite autonome, l'électrification du parc automobile et la connectivité des véhicules. Pour cette entreprise française présente aux quatre coins de la planète, la transformation numérique, la haute disponibilité des systèmes et la réduction du risque passaient par une stratégie de cybersécurité moderne et résiliente.

**Secteur d'activité**
Industrie

**Pays**
France

**Site web**
www.faurecia.com

| > 100 000 | > 30 | > 250 |
|---|---|---|
| COLLABORATEURS | PAYS | SITES INDUSTRIELS |

# Grâce à Cortex XSOAR, les réponses de l'équipe du SOC ont gagné en intelligence, en efficacité et en homogénéité, générant une hausse de 70 % de sa productivité.

« Le déploiement d'une nouvelle solution interne a généré presque 20 000 alertes, dont moins de 200 ont dû être traitées manuellement. Le reste a été totalement automatisé. Cela équivaut à une réduction de 99 % des opérations manuelles, pour un retour sur investissement immédiat. »

**— Matthieu Favris, Responsable de la réponse aux incidents (IR), Forvia Faurecia**

## Les problématiques

Avec la multiplication des alertes non filtrées provenant des systèmes EDR et SIEM, des environnements multicloud et des utilisateurs, l'équipe du SOC croulait sous la charge de travail.

+ Les collaborateurs du SOC avaient du mal à distinguer les alertes de faible priorité des urgences réelles.
+ Ils ne disposaient d'aucune plateforme unique pour ingérer et traiter les alertes.
+ L'impossibilité de répondre à toutes les alertes mettait leurs activités en danger.

## La solution

L'intégration de Cortex XSOAR a permis à Forvia Faurecia d'intégrer les alertes et d'aider le SOC à mieux gérer les tâches.

+ XSOAR intègre toutes les alertes générées par le SIEM, l'EDR et les autres sources.
+ L'utilisation d'un workflow numérique pour définir des procédures d'analyse et de réponse aux incidents permet au SOC de se concentrer sur les tâches stratégiques.
+ La Threat Intelligence et l'automatisation ont fortement réduit la charge de travail du SOC.

ARRÊT SUR IMAGE N°7 : BANCO DE GALICIA Y BUENOS AIRES S.A.

# Un grand établissement financier optimise son SOC

Avec plus de 350 bureaux répartis dans tout le pays, le groupe propose un très large éventail de services bancaires aux entreprises comme aux particuliers. Plus de 3 millions de clients ont confié la gestion de leurs intérêts financiers à Banco de Galicia y Buenos Aires, qui leur offre par ailleurs des services d'e-banking très flexibles et performants. Cette digitalisation avancée lui permet de proposer à ses clients des services bancaires sur le canal de leur choix – en agence, sur Internet ou via l'application mobile Galicia.

**Secteur d'activité**
Finance

**Pays**
Argentine

**Site web**
www.bancogalicia.com

| 350 | > 5 000 | 3 M |
|---|---|---|
| BUREAUX | SALARIÉS | CLIENTS |

## L'adoption de XSOAR a permis à l'équipe SOC de se focaliser sur les menaces sérieuses et de les neutraliser plus rapidement. Cette plus grande réactivité réduit les perturbations pour tous les employés de la banque et augmente la productivité de l'entreprise.

« Depuis que nous avons implémenté Cortex XSOAR, nous pouvons gérer automatiquement la quasi-totalité des [alertes courantes]. Ce qui nous prenait de longues minutes auparavant est devenu l'affaire de quelques secondes ! »

**— Ezequiel Invernon, Responsable SoC & IR, Banco de Galicia y Buenos Aires S.A.**

### Les problématiques

Phishing, exfiltration de données, ransomware… les menaces en tous genres représentaient un frein à la transformation numérique et à l'automatisation des activités de la banque.

+ Des alertes générées par de multiples produits de sécurité silotés ne permettaient pas d'identifier les menaces les plus sérieuses.
+ La remédiation manuelle des alertes à faible risque était aussi chronophage que frustrante pour l'équipe du SOC.
+ L'équipe courait le risque de passer à côté de menaces sérieuses, susceptibles de compromettre la sécurité de la banque.

### La solution

Banco de Galicia y Buenos Aires s'est tourné vers Cortex XSOAR pour consolider la gestion des alertes pour l'ensemble de ses solutions de sécurité et services de contenus.

+ XSOAR intègre en toute transparence les alertes déclenchées par les produits de sécurité et autres technologies de la banque, avec à la clé une vue générale et unifiée.
+ IoC, attaques de phishing, pertes de données, escalades de privilèges… des playbooks couvrent tous les types de scénarios pour automatiser et orchestrer les workflows du SOC.
+ L'automatisation des réponses aux incidents permet à l'équipe SOC de concentrer toute son énergie sur les alertes prioritaires.

ARRÊT SUR IMAGE N°8 : AVRASYA TÜNELI

# Un tunnel routier intercontinental automatise sa sécurité

Le tunnel Eurasia (Avrasya Tüneli) traverse le détroit du Bosphore entre Istanbul et Göztepe, en Turquie, pour relier l'Europe à l'Asie. Une infrastructure technologique sophistiquée gère les péages, les caméras, la ventilation, les interventions d'urgence et de nombreuses autres fonctions pour assurer la sécurité des plus de 65 000 voyageurs quotidiens. Pour protéger cette infrastructure des cybermenaces, Murat Çalışırişçi, Directeur des services informatiques, voulait une solution de sécurité aussi moderne que le tunnel lui-même.

**Secteur d'activité**
Transports

**Pays**
Turquie

**Site web**
www.avrasyatuneli.com

| 150 | > 200 | > 2 000 |
|---|---|---|
| COLLABORATEURS | TERMINAUX | APPAREILS IoT |


# Pour Avrasya Tüneli, le moindre incident de sécurité peut avoir un impact sur la sécurité des plus de 65 000 automobilistes qui empruntent le tunnel chaque jour. Cortex XDR lui permet de garantir un niveau de sécurité maximal, sans aucun recrutement.

« Avec Palo Alto Networks, nous disposons d'une solution intégrée, automatisée et simple à utiliser. Leur plateforme offre une protection complète en consolidant toutes les données de sécurité essentielles sur une console unique. Tous les composants de la plateforme sont les meilleurs de leur catégorie. Quant à la feuille de route produit, elle montre à quel point Palo Alto Networks est un partenaire visionnaire. »

**— Emrah Dündar, Responsable senior des systèmes d'information, Avrasya Tüneli**

## Les problématiques

Avrasya Tüneli devait protéger l'infrastructure technologique sous-tendant les opérations du tunnel avec une équipe de seulement trois professionnels de la sécurité.

+ L'équipe de sécurité avait besoin d'une interface unique qui lui fournisse une visibilité de bout-en-bout.
+ Plus de 200 terminaux et plus de 2 000 appareils IoT devaient faire l'objet d'une surveillance 24h/7j/365j.
+ Les temps de réponse jouaient un rôle crucial dans la sécurité du tunnel.

## La solution

Avrasya Tüneli a implémenté Cortex XDR pour développer ses capacités de détection et de réponse étendues en parallèle d'une suite intégrée de produits de sécurité Palo Alto Networks.

+ XDR a bloqué la totalité des menaces pendant les tests effectués en laboratoire.
+ L'automatisation réduit les opérations manuelles, maximisant ainsi la productivité des collaborateurs.
+ Les technologies ML d'analyse du trafic réseau, de détection sur les terminaux et d'analyse du comportement des utilisateurs permettent de simplifier la surveillance de tout l'environnement, notamment du parc IoT.

# Passez à l'étape suivante

Détection et prévention des menaces, gestion de la surface d'attaque, automatisation de la sécurité… les solutions Cortex offrent des fonctionnalités leaders sur une seule et même plateforme intégrée. À la clé : un centre des opérations de sécurité (SOC) efficace, adaptatif et réactif, conçu pour un champ des menaces en constante mutation.

Comme nous l'avons vu dans ces quelques exemples, Cortex aide des entreprises de toutes tailles et de tous horizons à simplifier, automatiser et accélérer les opérations de cybersécurité et les réponses aux incidents.

**Découvrez comment Cortex peut optimiser les performances de votre SOC.**

**Cliquez ici** ⟶



**Le portefeuille Cortex aide les entreprises à poursuivre leurs projets de transformation numérique tout en apportant aux équipes SOC la garantie d'une sécurité absolue. Une vraie révolution dans le monde de la sécurité.**

**Cortex® XSIAM**

**Misez sur une plateforme de sécurité autonome, pilier du SOC moderne**

**Cortex XDR®**

**Prévenez, détectez et investiguez les attaques dans toute l'entreprise**

**Cortex® XSOAR™**

**Automatisez la réponse et renforcez votre sécurité à chaque incident**

**Cortex® Xpanse™**

**Découvrez et protégez la totalité de votre surface d'attaque Internet**

+ **Cortex XDR®** est la première plateforme XDR du marché à intégrer nativement les données issues des terminaux, des réseaux, du cloud et de sources tierces pour bloquer les attaques sophistiquées.
+ **Cortex® XSOAR™**, la plateforme d'orchestration de la sécurité la plus complète du marché, optimise vos SecOps en automatisant les workflows pour n'importe quel cas d'usage de la sécurité.
+ **Cortex® Xpanse™** identifie les risques inconnus sur une surface d'attaque en mutation permanente, améliorant ainsi le ROI de tous vos investissements de sécurité.
+ **Cortex® XSIAM™** est une plateforme SOC autonome qui exploite toute la puissance de l'automatisation pilotée par IA pour renforcer la sécurité et transformer radicalement les SecOps.
+ **Unit 42™ MDR –** Capitalisez sur nos années d'expérience pour surveiller votre environnement et repérer toute activité anormale. Nos analystes travaillent H24 pour décortiquer les données Cortex XDR® et dresser un tableau complet de votre sécurité.