paloalto®

So haben acht Unternehmen ihre Security Operations mithilfe von Cortex® transformiert

VORWORT

Das SOC von morgen – schon heute im Einsatz

Wir leben in einer Zeit, in der man mit den Entwicklungen der Cybersicherheit kaum mehr mithalten kann.

Es spielt keine Rolle, wie groß das SOC-Team ist oder wie herausragend seine Mitglieder sind. Niemand kann schnell genug reagieren, um einen laufenden Angriff zu stoppen.

Wir brauchen KI – die richtigen Modelle, die richtigen Ressourcen und die richtigen Daten –, um die Cybersicherheit zu automatisieren. Nur so können wir die schiere Menge und die Komplexität der Bedrohungen bewältigen, die heute in unseren Netzwerken auftreten.

Aus diesem Grund haben wir Cortex® entwickelt – eine neue Vision für die Cybersicherheit. Damit lässt sich die Zeit, die verstreicht, bis eine Sicherheitsbedrohung erkannt wird und entsprechende Maßnahmen eingeleitet werden, von Tagen auf Sekunden reduzieren.

Wie Sie in diesem E-Book sehen werden, konnten Kunden, die Cortex verwenden, ihre SOC-Teams unterstützen, ihre Ergebnisse verbessern und gleichzeitig die Sicherheit transparenter, umfassender und zukunftssicherer gestalten.

Wir freuen uns, dass diese Unternehmen uns als Sicherheitsanbieter ausgewählt haben, und danken ihnen, dass wir hier über sie berichten dürfen.

paloalto® NETWORKS

SCHNAPPSCHUSS NR. 1: US-BUNDESSTAAT NORTH DAKOTA

Ein zukunftssicheres SOC für den öffentlichen Sektor

Der Bundesstaat North Dakota ist bestrebt, seinen Bürgern Technologie zugänglich zu machen. Entsprechend sorgt das Team der Abteilung North Dakota Information Technology (NDIT) für die Sicherheit aller Regierungsbehörden, von den städtischen Zentren bis zu den ländlichen Regionen. Umfang und Komplexität des betriebenen Netzwerks machen der eines Fortune-30-Unternehmens Konkurrenz, weshalb die Sicherheit gleichermaßen eine Herausforderung wie auch eine Priorität darstellt.

NORTH Dakota
Be Legendary.

Branche
Öffentlicher Sektor

Land
USA

Website
www.ndit.nd.gov

> 800.000	> 1.600	183
BÜRGER	STÄDTE UND GEMEINDEN	UNABHÄNGIGE SCHULBEZIRKE

paloalto NETWORKS

NDIT hat sich zu einem Musterbeispiel für erfolgreiche Sicherheitsmaßnahmen im öffentlichen Sektor entwickelt und bietet den Bürgern und Behörden des Bundesstaates automatisierten, proaktiven Schutz ohne größere Sicherheitsvorfälle.

> Wir arbeiten jetzt mit etwa der Hälfte der Ressourcen eines Fortune-30-Unternehmens ähnlicher Größe. Dies wurde durch die Automatisierung und die Überarbeitung von Playbooks zur Nutzung von maschinellem Lernen möglich. Dadurch kann sich das SOC-Team auf Aufgaben mit hoher Priorität konzentrieren, die einen Mehrwert für das Unternehmen schaffen.“
>
> **– Michael Gregg, Chief Information Security Officer, North Dakota Information Technology**

Die Herausforderungen

Mit Hunderttausenden von Benutzern, Tausenden von Integrationen und Anwendungen sowie unzähligen Endpunkten musste NDIT ein eigenes SOC planen, entwerfen und aufbauen, das systemübergreifend und mit beispielloser Effizienz arbeiten kann.

+ Immer raffiniertere Cyberangriffe bedrohten sowohl die Daten der Bürger als auch die Arbeit der Behörden.
+ Es wurde eine integrierte Lösung zur Verwaltung von Bedrohungsmeldungen benötigt, deren Anzahl sich 2021 auf 4,5 Milliarden verdoppelt hatte.
+ Die Lösung musste skalierbar, umfassend und zukunftssicher sein.

Die Lösung

NDIT ging eine Partnerschaft mit Palo Alto Networks ein und baute über einen Zeitraum von drei Jahren sein SOC auf. Durch die Integration des gesamten Cortex-Produktportfolios, einschließlich Cortex XDR, XSOAR und Xpanse, wurde eine umfassende Grundlage für Endpunktsicherheit, Aufgabenerkennung und Workflowautomatisierung geschaffen.

+ Ein einheitliches Framework verbessert die Erstlösungsrate (First Call Resolution, FCR) und reduziert die durchschnittliche Zeit bis zur Behebung (Mean Time To Respond, MTTR).
+ Die Arbeit von 2,17 VZÄ konnte auf Hintergrundsysteme verlagert werden, sodass sich die Teammitglieder nun auf Analysen mit hoher Priorität und die Beseitigung von Bedrohungen konzentrieren können.
+ Eine transparentere Organisationsstruktur, die sich an den Rahmenvorgaben des National Institute of Standards and Technology orientiert.

SCHNAPPSCHUSS NR. 2: HEALTHPARTNERS

Sicherheitsrevolution bei einem führenden Unternehmen im Gesundheitswesen

HealthPartners mit Sitz in Bloomington, Minnesota, bietet ein preisgekröntes integriertes Gesundheitssystem, das sowohl klinische Dienstleistungen als auch einen Gesundheitsplan bereitstellt. Das Unternehmen ist bestrebt, die Gesundheit und das Wohlbefinden der Mitglieder, Patienten und der Gemeinschaft insgesamt zu verbessern. HealthPartners ist mit 25.000 Mitarbeitern der größte von Verbrauchern geführte gemeinnützige Anbieter in den USA und versorgt 1,8 Millionen Mitglieder mit medizinischen und zahnmedizinischen Leistungen. Die klinischen Dienstleistungen umfassen eine multidisziplinäre Praxisgemeinschaft mit rund 1.800 Ärzten, die mehr als 1,2 Millionen Patienten versorgen.

HealthPartners®

Branche
Gesundheitswesen

Land
USA

Website
www.healthpartners.com

25.000
MITARBEITER

1,8 Mio.
MITGLIEDER

1.800
ÄRZTE

paloalto® NETWORKS

Cortex beschleunigt die digitalen Initiativen von HealthPartners, indem es das SOC befähigt, Schwachstellen proaktiv zu beseitigen und die Erkennung sowie Untersuchung zu automatisieren. So können die Mitarbeiter sich auf den kleinen Teil der Bedrohungen fokussieren, die ein manuelles Eingreifen erfordern.

> Aufgrund der Konsistenz und des hohen Prozentsatzes an True Positives, die wir von der Palo Alto Networks Plattform erhalten, sind wir nun in der Lage, die Bedrohungsabwehr zu automatisieren. Dazu hatten wir bisher noch nie die Möglichkeit.“
>
> **– Joel Pfeifer, Principal Security Analyst, HealthPartners**

Die Herausforderungen

Angesichts ständig drohender Cyberangriffe auf klinische Dienstleistungen und den Gesundheitsplan bezüglich privater Patientendaten musste HealthPartners seine Sicherheitslösung verbessern, ohne dabei erheblich in neue Hardware zu investieren.

+ Ältere Firewalls boten HealthPartners nicht länger die erforderliche Sicherheit.
+ Ein unzureichender Endpunktschutz führte zu Schwachstellen auf allen Geräten des Unternehmens.
+ Ungefilterte Alarme waren nicht detailliert genug, sodass eine manuelle Analyse im SOC erforderlich war.

Die Lösung

HealthPartners hat das Cortex-Portfolio von Palo Alto Networks implementiert, einschließlich Cortex XDR, XSOAR und Xpanse.

+ Cortex vereint mehrere Systeme in einer Plattform und kostet nur halb so viel wie vergleichbare Produkte.
+ Die integrierte Threat Intelligence hat im ersten Jahr Dutzende von Cyberangriffen abgewehrt.
+ Lückenlose Transparenz und detaillierte Einblicke in Cyberangriffe und deren Ursprung unterstützen das SOC.

SCHNAPPSCHUSS NR. 3: BETTER.COM

Optimierte Sicherheit für einen innovativen Finanzdienstleister

Als eine der am schnellsten wachsenden digitalen Plattformen für den Erwerb von Wohneigentum in den USA vereinfacht Better.com für seine Kunden das Aufnehmen von Hypotheken und den Abschluss von Versicherungen. Durch den Einsatz von Technologien werden diese Prozesse schneller, transparenter und zugänglicher gestaltet. Angesichts eines Finanzierungsvolumens von über $95 Milliarden sind der Schutz der Kundendaten und der dem Geschäft zugrunde liegenden Technologie von größter Bedeutung.

Better

Branche
Finanzen

Land
USA

Website
www.better.com

> 5.000	> 10.000	$95 Mrd.
MITARBEITER	ENDPUNKTE	FINANZIERUNGSVOLUMEN

paloalto NETWORKS

Cortex hat die Sicherheit von Better.com schneller und effizienter gemacht, sodass das SOC-Team proaktiv statt reaktiv handeln kann. Zudem kann das Unternehmen sich auf Initiativen konzentrieren, die den Erwerb von Wohneigentum für seine Kunden vereinfachen.

> Dank der XSOAR-Untersuchungen und -Automatisierungen, die wir in Kombination mit XDR durchführen können, lassen sich Befehle innerhalb eines Arbeitsablaufs nahtlos ausführen, ein vollständiges Kill-Chain-Ereignis erstellen und Vorfälle sehr schnell beheben.“
>
> **– Jeff White, Director of Security, Better.com**

Die Herausforderungen

Better.com musste sein SOC befähigen, Schwachstellen schneller zu bewerten und Bedrohungen in einem großen und schnell wachsenden Netzwerk zu beseitigen.

+ Die bestehende EDR-Lösung erzeugte unzuverlässige Alarme mit unzureichender Granularität.
+ Das SOC war aufgrund von manuellen Arbeitsabläufen und Behebungsschritten überfordert.
+ Das Unternehmen benötigte einen lückenlosen Überblick über sämtliche Daten.

Die Lösung

Better.com entschied sich für ein umfassendes Paket an Sicherheitslösungen von Palo Alto Networks, einschließlich Cortex XDR, XSOAR, NGFWs, Panorama und Prisma Access, um die Sicherheit einfacher und proaktiver zu gestalten.

+ Eine zentrale Konsole bietet Überblick über Daten, Benutzer, Anwendungen, Infrastruktur und Endpunkte.
+ Die Automatisierung von EDR und die Orchestrierung der Reaktion verbessern die Arbeitsabläufe und sorgen für eine breitere Abdeckung.
+ Die Lösung verhindert alle Angriffe und bietet vollständigen Überblick über die Angriffsversuche, im gesamten Netzwerk und bei Penetrationstests.

SCHNAPPSCHUSS NR. 4: KHIPU NETWORKS

Sorgenfreiheit für Sicherheitskunden

KHIPU Networks ist ein preisgekröntes internationales Cybersicherheitsunternehmen, das weltweit hochsichere Netzwerke für Kunden aus den verschiedensten Branchen bereitstellt. Für Kunden mit der Sorge, dass ein Cyberangriff ihre Daten zerstören, ihre digitalen Strategien beeinträchtigen oder ihren Ruf schädigen könnte, hat KHIPU Networks 2019 den ersten eXtended Managed Detection and Response(XMDR)-Service im Vereinigten Königreich eingeführt.

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

KHIPU CYBER SECURITY

Branche
Cybersicherheit

Land
Vereinigtes Königreich

Website
www.khipu-networks.com

1.
XMDR-ANBIETER IM VEREINIGTEN KÖNIGREICH

> 19
JAHRE ERFAHRUNG IM CYBERSICHERHEITSBEREICH

> 500
KUNDEN

paloalto NETWORKS

Mithilfe von Cortex kann KHIPU Networks die Sicherheitsinformationen seiner vielfältigen, über die ganze Welt verteilten Kundenbasis zuverlässig erfassen und dabei die Erkennung und Reaktion verbessern sowie fortlaufend Threat Intelligence aufbauen.

> Das Portfolio von Palo Alto Networks hebt sich durch seine Einfachheit, Automatisierung und Genauigkeit von anderen Security-Operations-Lösungen ab. Unsere Kunden können sich nun von einer zentralen Datenquelle aus einen vollständigen Überblick verschaffen und umgebungsweit als Managed Service reagieren.“
>
> **– Guy Jermany, Chief Information Officer, KHIPU Networks**

Die Herausforderungen

Um erfolgreich zu sein, musste KHIPU Networks die Vorteile eines internen SOC als Managed Service für Kunden der verschiedensten Branchen mit unterschiedlichen und komplexen Anforderungen bereitstellen.

+ Kunden hatten Sicherheitssorgen aufgrund der zunehmenden IT-Komplexität, der pandemiebedingt etablierten Remotearbeit, der hybriden On-Premises- und Cloud-Infrastruktur und anderer Herausforderungen.
+ Die Lösung musste flexibel sein, um den Anforderungen, Umgebungen, Prioritäten und Budgets der einzelnen Kunden gerecht zu werden.
+ Kunden hatten Schwierigkeiten, kompetente Fachkräfte für Cybersicherheit zu finden und zu halten, insbesondere wenn eine Verfügbarkeit rund um die Uhr für die Abwehr und Untersuchung entscheidend war.
+ KHIPU Networks musste in einem Umfeld zunehmender Cyberangriffe Ransomware abwehren und eindämmen.

Die Lösung

KHIPU Networks baute seinen XMDR-Service auf Cortex XDR und XSOAR von Palo Alto Networks auf. Dies ermöglicht eine proaktive Erkennung und Reaktion sowie die Analysen, Arbeitsabläufe und Aufgabenverwaltung, die zur Unterstützung des SOC erforderlich sind.

+ Dank der verbesserten Integration mit mehreren Einzellösungen ist KHIPU Networks in der Lage, sofort auf Bedrohungen zu reagieren, sie einzudämmen und zu untersuchen.
+ Automatisierte KI- und ML-Prozesse verhindern, erkennen und beseitigen Bedrohungen und ermöglichen es KHIPU Networks, für zahlreiche Unternehmen als SOC zu fungieren.
+ Durch die Aufdeckung sämtlicher Schritte eines Angriffs wird die Untersuchungszeit verkürzt und die Wertschöpfung der Analysten von KHIPU Networks maximiert.
+ Dank erschwinglicher, flexibler und skalierbarer Cybersicherheitsservices können Unternehmen aller Größen in jedem vertikalen Markt in den XMDR-Service von KHIPU Networks investieren, ohne sich um die Sicherheit zu sorgen.

SCHNAPPSCHUSS NR. 5: ASCEND MONEY

Automatisierung des SOC bei einem Fintech-Unicorn

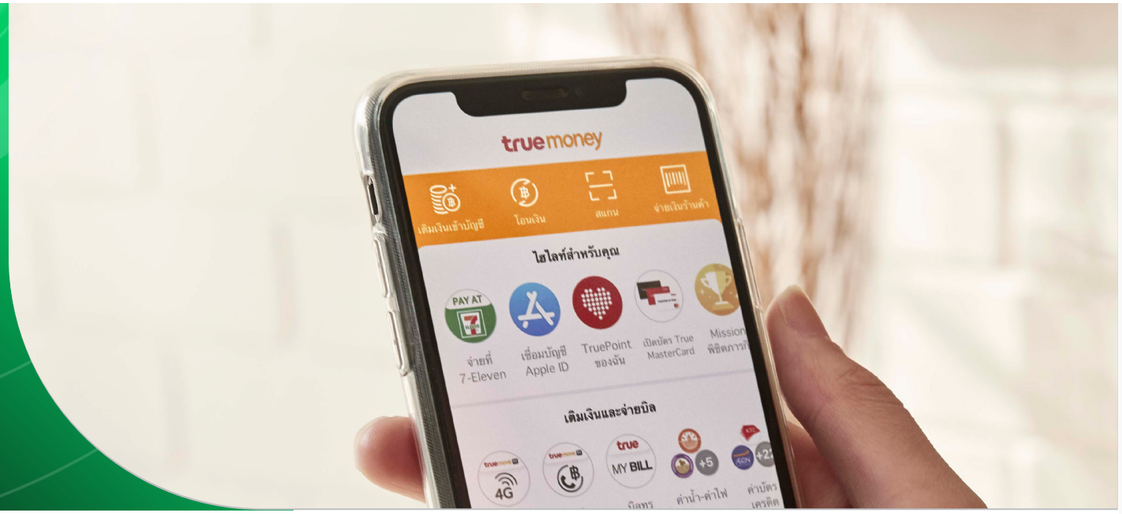
Ascend Money wurde 2013 mit dem Ziel gegründet, modernste Finanztechnologie für die unterversorgten Bevölkerungsgruppen in Südostasien bereitzustellen, und ist derzeit das am schnellsten wachsende Startup in Thailand. Heute wird TrueMoney Wallet, die digitale elektronische Geldbörse des Unternehmens, von mehr als 50 Millionen Menschen in Thailand, Indonesien, Vietnam, Myanmar, Kambodscha und auf den Philippinen genutzt.

Branche
Finanzen

Land
Thailand

Website
www.ascendmoneygroup.com

2.000	50 Mio.	6
MITARBEITER	KUNDEN	LÄNDER



Als die Bedrohungen während der jüngsten globalen Krisen sprunghaft anstiegen, sorgten Cortex XDR und XSOAR für die Sicherheit von Ascend Money und gaben dem Unternehmen die Gewissheit, dass die Daten seiner Partner und Kunden geschützt blieben.

> Cortex XDR von Palo Alto Networks bot uns eine vereinfachte Integration und Sicherheitsautomatisierung, wodurch sich die Einsatzzeit erheblich verkürzte.“
>
> **– Kanokwan Aimsumang, Head of IT Security and Governance, Ascend Money**

Die Herausforderungen

Angesichts der konstanten Angriffe auf Fintech-Unternehmen benötigte Ascend Money eine Lösung, um seine eigenen Vermögenswerte und die Finanzdaten seines schnell wachsenden Kundenstamms zu schützen.

+ Das wachsende Netzwerk ließ Bedenken hinsichtlich möglicher Lücken bei der Endgerätesicherheit aufkommen.
+ Das SOC hatte mit einem hohen Aufkommen an ungefilterten Alarmen zu kämpfen.
+ Es galt sicherzustellen, dass der Geschäftsbetrieb im Falle eines Cyberangriffs nicht unterbrochen wird.
+ Bei der Umrüstung der Technologie für die Nutzung von KI und ML wurde Unterstützung benötigt.

Die Lösung

Ascend Money nutzte Cortex XDR zur Automatisierung der Bedrohungserkennung und -abwehr am Endpunkt in Kombination mit Cortex XSOAR, bereitgestellt vom Sicherheitspartner True Digital Cyber Security.

+ Der erweiterte Endpunktschutz von XDR bietet eine größere Abdeckung, um potenzielle Lücken zu schließen.
+ Dank KI- und ML-gesteuerter Sicherheitsautomatisierung kann sich das SOC auf Aufgaben mit höherem Mehrwert konzentrieren.
+ Durch die Skalierbarkeit von XDR und XSOAR kann die Sicherheit mit kontinuierlichem Wachstum Schritt halten.
+ Vereinfachte Integration und Sicherheitsautomatisierung verkürzten die Einsatzzeit erheblich.

SCHNAPPSCHUSS NR. 6: FORVIA FAURECIA

Sicherheit für die digitale Transformation des Herstellers

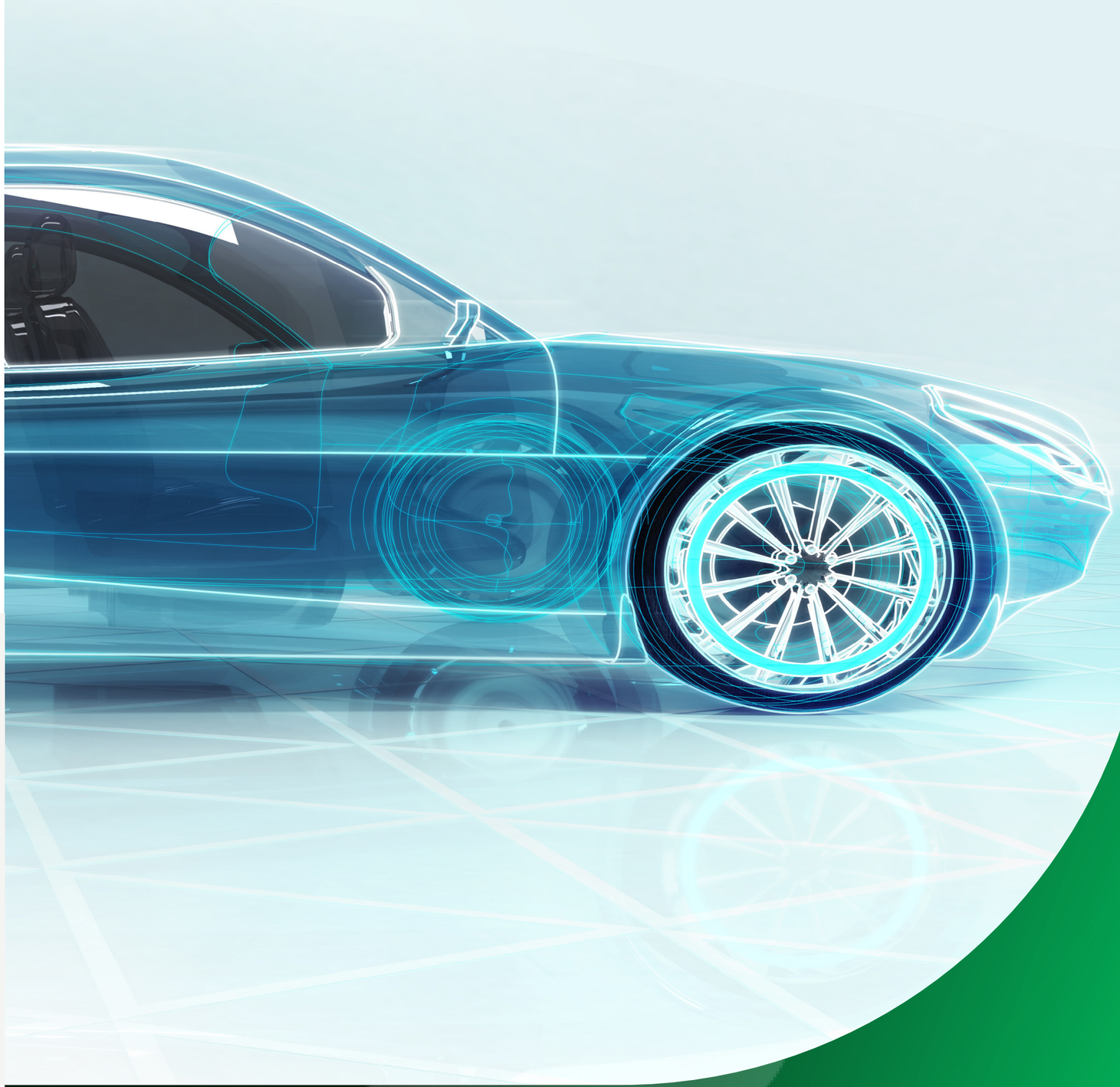
Forvia Faurecia, einer der weltweit führenden Hersteller von Automobilkomponenten, führt in hohem Tempo Technologien der nächsten Generation ein, um mit dem Wandel in der Branche in Richtung autonomes Fahren, Elektrifizierung, Konnektivität und anderen Trends Schritt zu halten. Das global agierende Unternehmen benötigt eine moderne, widerstandsfähige Cybersicherheitsstrategie, um die digitale Transformation zu steuern, die Betriebsbereitschaft zu sichern und Risiken zu verringern.

Branche
Fertigung

Land
Frankreich

Website
www.faurecia.com

> 100.000	> 30	> 250
MITARBEITER	LÄNDER	INDUSTRIESTANDORTE



Cortex XSOAR ermöglichte dem SOC-Team die intelligentere, effizientere und einheitlichere Abwehr, was zu einer Produktivitätssteigerung von 70 % geführt hat.

> Vor Kurzem wurden bei der Einführung einer neuen internen Lösung fast 20.000 Alarme generiert, davon wurden aber weniger als 200 manuell bearbeitet. Der Rest wurde automatisch erledigt. Dies entspricht einer Reduzierung des manuellen Arbeitsaufwands um 99 % und führte zu einer sofortigen Amortisierung unserer XSOAR-Investition.“
>
> **– Matthieu Favris, Incident Response Manager, Forvia Faurecia**

Die Herausforderungen

Angesichts der ungefilterten Alarme, die von EDR- und SIEM-Systemen, Multi-Cloud-Umgebungen und Endbenutzern eingingen, war die Arbeitslast für das SOC-Team kaum zu bewältigen.

+ Das SOC-Team konnte nicht zwischen Alarmen mit niedriger Priorität und echten Notfällen unterscheiden.
+ Es fehlte eine zentrale Plattform für die Erfassung und Bearbeitung von Alarmen.
+ Wenn nicht auf alle Alarme reagiert wird, ist das Unternehmen gefährdet.

Die Lösung

Forvia Faurecia implementierte Cortex XSOAR zur Integration von Alarmen und zur Unterstützung der Aufgabenverwaltung für sein SOC.

+ XSOAR berücksichtigt in vollem Umfang die von SIEM, EDR und anderen Quellen gesammelten Alarme.
+ Durch die Definition von Verfahren für die Vorfallsanalyse und Incident Response mithilfe digitaler Arbeitsabläufe kann sich das SOC auf strategisch wertvollere Aufgaben konzentrieren.
+ Threat Intelligence und Automatisierung reduzieren den Workload des SOC erheblich.

SCHNAPPSCHUSS NR. 7: BANCO DE GALICIA Y BUENOS AIRES

Stärkung des SOC bei einer führenden Bank

Mit über 350 Geschäftsstellen, die umfassende Bankdienstleistungen für Unternehmen und Privatpersonen in ganz Argentinien anbieten, ist die Banco de Galicia y Buenos Aires eine der größten Privatbanken des Landes. Über drei Millionen Kunden vertrauen ihr die Verwaltung ihrer finanziellen Angelegenheiten an. Die Bank bietet die Flexibilität und die digitalen Möglichkeiten, die moderne Kunden erwarten. Im Rahmen der Digitalisierung möchte sie ihren Kunden Bankdienstleistungen örtlich flexibel bereitstellen – in den Filialen, online und über ihre Galicia-App.

Branche
Finanzen

Land
Argentinien

Website
www.bancogalicia.com

350	> 5.000	3 Mio.
STANDORTE	MITARBEITER	KUNDEN

Die Einführung von XSOAR spart Zeit im SOC, sodass sich das Team auf ernsthafte Bedrohungen konzentrieren und sie schnell beseitigen kann. Das bedeutet weniger Unterbrechungen für die Bankmitarbeiter und eine höhere Produktivität im gesamten Unternehmen.

> Mit der Implementierung von Cortex XSOAR sind wir in der Lage, [gängige Alarme] fast vollautomatisch zu verwalten. Was früher mehrere Minuten dauerte, ist jetzt innerhalb von Sekunden erledigt.“
>
> **– Ezequiel Invernon, SoC & IR Manager, Banco de Galicia y Buenos Aires**

Die Herausforderungen

Die ständige Bedrohung durch Phishing, Datenausschleusung, Ransomware und andere Angriffe erschwerte die Bemühungen der Bank, die Digitalisierung und Automatisierung im gesamten Unternehmen voranzutreiben.

+ Alarme von zahlreichen, isolierten Sicherheitsprodukten machten es unmöglich, die schwerwiegendsten Bedrohungen zu identifizieren.
+ Die manuelle Behebung von Alarmen niedriger Priorität belastete die Ressourcen des SOC-Teams erheblich.
+ Das Team lief Gefahr, schwerwiegende Bedrohungen zu übersehen und damit die Sicherheit der Bank zu gefährden.

Die Lösung

Die Banco de Galicia y Buenos Aires entschied sich für Cortex XSOAR, um das Alarmmanagement für ihre Sicherheitslösungen und Content Services zu konsolidieren.

+ XSOAR integriert nahtlos Alarme aus allen Sicherheitsprodukten und Technologien der Bank und bietet eine zentrale konsolidierte Ansicht.
+ Playbooks für IoCs, Phishingvorfälle, DLP und Ausweitung von Zugriffsrechten sorgen für eine Automatisierung und Orchestrierung der SOC-Arbeitsabläufe.
+ Dank automatisierter Incident Response kann das Team sich auf Alarme mit hoher Priorität konzentrieren.

SCHNAPPSCHUSS NR. 8: AVRASYA TÜNELI

Automatisierte Sicherheit für eine interkontinentale Verbindung

Der Avrasya Tüneli (Eurasien-Tunnel), der unter dem Bosporus zwischen Istanbul und Göztepe in der Türkei verläuft, verbindet die Kontinente Europa und Asien. Eine hochentwickelte technologische Infrastruktur regelt Mautgebühren, Kameras, Belüftung, Störungsbeseitigung und eine Vielzahl weiterer Funktionen, um die Sicherheit der Strecke für mehr als 65.000 Reisende pro Tag zu gewährleisten. Die Infrastruktur muss vor Cyberbedrohungen geschützt werden. Murat Çalışırişçi, Director of Information Technology, benötigte daher eine Sicherheitslösung, die so modern ist wie der Tunnel selbst.

Branche
Transport

Land
Türkei

Website
www.avrasyatuneli.com

150	> 200	> 2.000
MITARBEITER	ENDPUNKTE	IoT-GERÄTE

Ein Sicherheitsvorfall bei Avrasya Tüneli könnte die Sicherheit von mehr als 65.000 Tunnelbenutzern täglich beeinträchtigen. Mit Cortex XDR wird das Sicherheitsniveau des Tunnels aufrechterhalten, ohne dass zusätzliches Personal eingestellt werden muss.

> Die Lösung ist integriert, automatisiert und einfach. Die integrierte Plattform [von Palo Alto Networks] bietet umfassenden Schutz, indem sie alle wichtigen Sicherheitsdaten über eine zentrale Konsole verbindet. Jede Komponente der Plattform ist erstklassig, und an den geplanten Produkten lässt sich ablesen, dass wir es mit einem visionären Partner zu tun haben.“
>
> **– Emrah Dündar, Senior Manager, Information Technologies, Avrasya Tüneli**

Die Herausforderungen

Avrasya Tüneli musste die Technologie-Infrastruktur des Tunnels schützen, ohne die Belastung für die lediglich drei Sicherheitsfachkräfte zu erhöhen.

+ Das Sicherheitsteam benötigte einen lückenlosen Überblick mittels einer zentralen Oberfläche.
+ Mehr als 200 Endpunkte und über 2.000 IoT-Geräte erforderten eine Überwachung rund um die Uhr, 365 Tage im Jahr.
+ Entscheidend für die Tunnelsicherheit waren die Reaktionszeiten.

Die Lösung

Avrasya Tüneli implementierte Cortex XDR für erweiterte Erkennung und Abwehr von Bedrohungen, kombiniert mit einer integrierten Suite von Palo Alto Sicherheitsprodukten.

+ Bei Lösungstests in einer kundenspezifischen Laborumgebung blockierte XDR jede Bedrohung.
+ Die Automatisierung reduziert den manuellen Arbeitsaufwand und maximiert die Produktivität der Mitarbeiter.
+ Die integrierte ML-basierte Analyse des Netzwerkverkehrs, die Erkennung von Endpunkten und die Analyse des Benutzerverhaltens vereinfachen die Überwachung, auch von IoT-Geräten.

Wagen Sie den nächsten Schritt

Cortex führt branchenführende Lösungen für die Bedrohungsprävention und -erkennung, das Management der Angriffsfläche und die Sicherheitsautomatisierung auf einer integrierten Plattform zusammen. Damit schaffen Sie ein ideales Fundament für den Aufbau eines effizienten, anpassungsfähigen und reaktionsschnellen Security Operations Center, das optimal für immer neue Bedrohungen gewappnet ist.

Wie die Kundenbeispiele zeigen, unterstützt Cortex Unternehmen aller Größen dabei, ihre Security Operations und Incident Response zu vereinfachen, zu automatisieren und zu beschleunigen.

Erfahren Sie mehr darüber, wie Cortex Ihr SOC unterstützen kann.

Hier klicken ⟶

Das Cortex-Portfolio transformiert die Sicherheitslandschaft: Unternehmen können nun ihre Digitalisierungsstrategien verfolgen, während die SOC-Teams, die für ihre Sicherheit sorgen, beruhigt arbeiten können.

+ **Cortex XDR®** integriert als branchenweit erste XDR-Plattform Endpunkt-, Netzwerk-, Cloud- und Drittanbieterdaten, um raffinierte Angriffe zu stoppen.
+ **Cortex® XSOAR™**, die branchenweit umfassendste Plattform zur Sicherheitsorchestrierung, unterstützt Ihre Security Operations mit automatisierten Arbeitsabläufen für alle sicherheitsrelevanten Anwendungsbereiche.
+ **Cortex® Xpanse™** bildet das Unbekannte in der sich ständig weiterentwickelnden Internetangriffsfläche ab. So wird das Unsichtbare sichtbar gemacht und der ROI aller Sicherheitsinvestitionen verbessert.
+ **Cortex® XSIAM™** ist eine autonome SOC-Plattform. Die Lösung nutzt die Vorteile der KI-gestützten Automatisierung, um die Effizienz von Sicherheitsmaßnahmen radikal zu verbessern und Ihre Security Operations zu transformieren.
+ **Unit 42™ MDR** nutzt unsere jahrelange Erfahrung für die Überwachung Ihrer Umgebung und die Erfassung verdächtiger Aktivitäten. Unsere Analysten arbeiten rund um die Uhr und durchforsten die Cortex XDR®-Daten, um ein vollständiges Bild zu erstellen.