CYREBRO

NetPlans®
CLOUD SOLUTIONS

CYREBRO
Partner Success Story:

NetPlans GmbH

Eigene Managed SOC Services erfolgreich aufbauen mit CYREBRO

Als Managed Services Provider mit Spezialisierung auf innovative Cloud-Lösungen betreut NetPlans europaweit Unternehmen mit den unterschiedlichsten IT-Anforderungen. Um Endkunden vor den wachsenden IT-Sicherheitsbedrohungen zukunftsfähig zu schützen, suchte NetPlans nach dem besten Weg, ein vollwertiges Security Operations Center (SOC) Serviceangebot aufzubauen. Auf Basis der interaktiven 24/7 Cloud Managed SOC Plattform von CYREBRO konnte dieses Vorhaben erfolgreich in die Realität umgesetzt werden.

Fakten zu NetPlans

Name: NetPlans GmbH

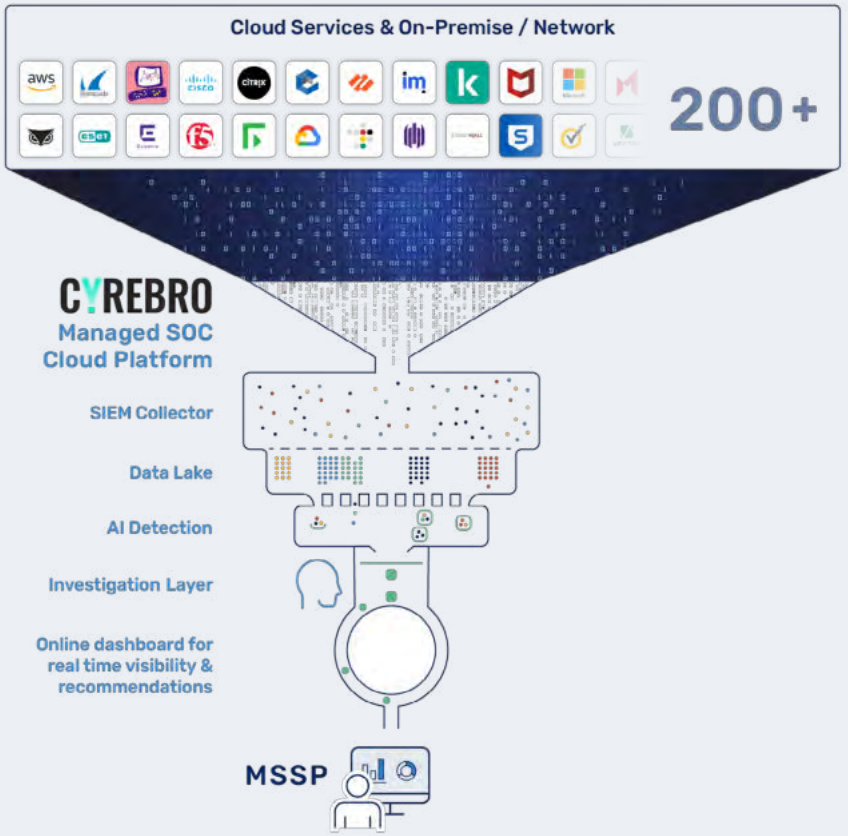
Unternehmensform: IT-Systemhaus

Gründung und Hauptsitz: 1998 in Ettlingen/Deutschland

Standorte: Bundesweite Niederlassungen in Deutschland sowie in der Schweiz

Unternehmensgröße: >300 Mitarbeiter

Spezialisierung: Führender Anbieter innovativer Cloud-Lösungen und Managed Services mit eigener Business Cloud sowie hauseigenem 24/7 Support



Die Anforderungen an die IT-Sicherheitsinfrastruktur von Organisationen nehmen weiter zu. Meldungen von erfolgreichen IT-Angriffen auf Unternehmen, die verheerende Schäden nach sich ziehen, reißen nicht ab. Untersuchungen von IT-Forensikern ergeben dabei immer wieder, dass Angreifer meist viele Monate unerkannt in einem Netzwerk unterwegs sind, bevor sie auffallen oder sich zu erkennen geben.

Doch es muss nicht mal ein erfolgreicher Cyberangriff sein – auch andere Akteure wie beispielsweise der Gesetzgeber oder Cyberversicherungen schreiben immer umfangreichere Überwachungs-, Absicherungs- und Reaktionsmaßnahmen für IT-Umgebungen verbindlich vor.

Die Herausforderung

Diese aktuellen Entwicklungen hat NetPlans zum Anlass genommen, um die Security-Angebote und -Services für seine Endkunden erneut auf den Prüfstand zu stellen. Zwei entscheidende Fragen standen im Fokus: Wie erkennt NetPlans als Managed Security Services Provider so früh wie möglich Anzeichen für einen Cyberangriff? Wie intervenieren sie als Kunde bei den ersten Warnsignalen am effektivsten? Das Ergebnis der anschließenden Recherche: Nur ein rund um die Uhr arbeitendes Analysten-Team mit professionellen Tools, in denen alle Events aus jedem Teil der betreuten Kundenumgebungen zusammenlaufen, kann diesen Anspruch erfüllen – ein klassisches Security Operations Center (SOC).

„Die Nachfrage unserer Kunden nach dieser Art von Services nimmt stetig zu. Die Kunden hören viele positive Meinungen über gemanagte Lösungen wie EDR, MDR, XDR und Managed SOC. Wir bekommen konkrete Anfragen, ob wir auch etwas in dieser Art anbieten“, so Thomas Frasch, NetPlans Security Systems Engineer.

Bei näherer Betrachtung der Alternativen für den Aufbau eines Managed SOC-Services, sind die Herausforderungen, auf die jeder IT-Dienstleister stößt, jedoch schnell deutlich geworden: Wer ein vom Start weg erstklassiges und skalierbares SOC mit eigenen Mitteln aufbauen und betreuen will, steht vor sehr hohen Investitionen. Zusätzlich gestaltet sich die Gewinnung des notwendigen Fachpersonals schwierig.

„Wir haben uns die Herausforderungen ganz deutlich vor Augen geführt und beschlossen: Es braucht eine zukunftssichere und erfolgreiche Kooperation mit einem Managed SOC-Spezialisten“, berichtet Thomas Frasch von NetPlans.

Eine Anforderung bei der Zusammenarbeit mit vielen Managed SOC-Lösungsanbietern sieht NetPlans in der transparenten Preiskalkulation. Basis einer solchen Lösung ist in der Regel ein SIEM – also ein Security Information und Event Management, das eine Echtzeitanalyse von Sicherheitsalarmen aus den Quellen-Anwendungen und Netzwerkkomponenten liefert. In diesem Bereich zählen die Events pro Sekunde (EPS), welche sich im Vorfeld für eine Angebotserstellung nur schwer abschätzen lassen. Hier war eine verlässliche und einfacher handzuhabende Berechnungsgrundlage gefragt.

Die Herstellerunabhängigkeit war eine zweite Anforderung seitens NetPlans. Die betreuten Endkunden haben die unterschiedlichsten IT-Systeme und Security-Lösungen im Einsatz – das Managed SOC sollte eine höchstmögliche Kompatibilität zu allen relevanten Lösungen am Markt mitbringen.

Die Lösung

Die CYREBRO Plattform bietet eine einfache Anbindung für eine Vielzahl von IT-Lösungen, die bei Endkunden im Einsatz sind. Das war ein sehr relevanter Pluspunkt für die Entscheidung von NetPlans. Neben der Vielzahl der bereits integrierten Log-Quellen werden bei Bedarf auch Anbindungen zu neuen Systemen entwickelt, um immer die maximale Transparenz über die Endkunden-Systeme zu erhalten.

Ein weiteres Argument für die Wahl von CYREBRO war die Kombination aus SOC-Expertenteam und interaktiver Cloud Plattform. Das Dashboard zeigt - pro Endkunde - alle relevanten Sicherheitsalarme und kritischen Events inklusive der dazugehörigen Handlungsempfehlungen, die durch die SOC-Analysten beim Hersteller bereitgestellt werden. Die Möglichkeit der Auslagerung ressourcenintensiver, SOC-bezogener Arbeiten von 24/7 Monitoring über Analyse bis hin zu konkreten Aktionsvorschlägen war der Schlüssel für NetPlans.

„Wir hatten eine genaue Vorstellung davon, wie die Integration und der Prozess aussehen sollen, damit ein Managed SOC Partner und unsere zuständigen Support- & Technik-Teams effektiv zusammenarbeiten können. CYREBRO konnte sich wunderbar auf unsere Arbeitsabläufe anpassen und wir mussten uns nicht verbiegen – das funktioniert einfach.“, führt Herr Frasch weiter aus. Das neu entwickelte übergeordnete Multimandanten-Dashboard der Lösung ermöglicht den Teams zusätzlich einen zentralen Überblick und bietet den schnellen Zugriff auf alle betreuten Endkunden-Umgebungen. Im Rahmen des ersten Endkunden-Projektes wurden zusammen mit dem Hersteller außerdem weitere Optimierungen und Verbesserungen identifiziert und umgesetzt.

Mit der **Lizenzierung pro IT-Seat** ist auch die Anforderung an ein einfach zu berechnendes Lizenzmodells erfüllt. Die konkrete Definition und Kalkulierbarkeit dieses Wertes erlaubt NetPlans, das Business Modell für ihr neues Managed SOC-Serviceangebot aufzubauen. Dadurch hat das Vertriebsteam nun die Möglichkeit, interessierte Endkunden schon an einem frühen Punkt in den Gesprächen über die voraussichtlichen Kosten zu informieren. Für die Erstellung des Managed SOC- Services auf Basis von CYREBRO standen Leistungsbeschreibungen zur Verfügung, bereitgestellt von Infinigate. Diese haben wir gemeinsam an den NetPlans-Standard angepasst und für die ersten Kundenangebote vorbereitet.

NetPlans nutzt die interaktive Managed SOC-Plattform von CYREBRO als Basis für ihren neuen Managed Service namens NetPlans Managed SOC+. Damit wurde ein eigenes, vollwertiges Managed SOC-Angebot für Endkunden realisiert, das neben erstklassigem 24/7 Monitoring und einer Analyse aller sicherheitsrelevanten Events auch die schnelle Reaktion auf Cyberangriffe und IT-Vorfälle beinhaltet.

„Die CYREBRO Plattform bietet die Möglichkeit der direkten, interaktiven Zusammenarbeit zwischen dem Hersteller und NetPlans. Der Endkunde erhält im Ergebnis das Beste aus zwei Welten.“

Thomas Frasch, NetPlans

„Das Gesamtbild von CYREBRO hat
für uns einfach gepasst.
Die Vorstellung des SOCplus-Konzeptes
von Infinigate überzeugt.“

Thomas Frasch, NetPlans

Endkunden-Pilotprojekt

Produkt: NetPlans Managed SOC+ Services auf Basis von CYREBRO

Endkunde:

- Langjähriger Bestandskunde aus dem deutschen Mittelstand, tätig im produzierenden Gewerbe für Bau-Grundstoffe und Weltmarktführer in seinem Spezialgebiet
- IT-Sicherheit hat oberste Priorität, um das geistige Eigentum sowie die Entwicklungs- und Produktionsbereiche zu schützen

Serviceumfang NetPlans für den Endkunden: Komplette Betreuung von PC-Hardware bis zur IT-Absicherung

Ziel: Implementation eines vollwertigen SOC, betrieben durch NetPlans

- Lösungsübergreifendes 24/7 Monitoring der IT-Umgebung
- Analyse von Sicherheitsbedrohungen mittels KI und SOC-Analystenteam
- Umgehende Reaktion auf drohende bzw. laufende Cybersicherheitsvorfälle

Integration von CYREBRO in den NetPlans-Workflow

Im Falle eines kritischen Vorfalls geht eine Benachrichtigung von CYREBRO per Mail an ein zentrales NetPlans Support-Postfach. Der Betreff der Mail-Benachrichtigung beinhaltet unter anderem direkt den Endkunden-Namen, um eine schnelle Zuordnung des richtigen Teams zu ermöglichen. Die Teams haben den zentralen Zugriff auf das übergeordnete Multi-mandanten-Dashboard von CYREBRO. Diese Neuentwicklung des Herstellers erlaubt den zuständigen NetPlans-Mitarbeitern einen zentralen Überblick und Zugriff auf die Dashboards aller integrierten Endkunden.
Darüber hinaus wurden alle Support-Mitarbeiter entsprechend geschult: Was bedeuten bestimmte Ereignisse? Wie reagiere ich auf diese richtig? Wann und wie beziehe ich CYREBRO bzw. die internen Technik-Kollegen ein?

Anbindung der Endkundenumgebung an das Managed SOC

Nachdem die Rahmendaten der IT-Umgebung des Endkunden im Onboarding-Protokoll erfasst waren, folgte im zweiten Schritt die Installation des Event-Kollektors im Netzwerk. An diesen wurden Schritt für Schritt die Log-Quellen aller relevanten IT-Systeme angebunden, die der Kunde im Einsatz hat. Für zwei Lösungen wurden – mit Unterstützung von CYREBRO – neu erstellte Anbindungen bereitgestellt.

Erfahrungen im Einsatz von CYREBRO

Während des bisherigen Einsatzzeitraums von CYREBRO als Basis des NetPlans Managed SOC+ Services gab es keinen größeren externen Angriff auf die Umgebung des Endkunden. Es wurden kleinere Alarme aus der Endpoint Security-Lösung analysiert, die beim Endkunden im Einsatz sind. NetPlans setzte die konkreten Handlungsempfehlungen von den Analysten bei CYREBRO, die diese Events untersuchten, umgehend um. Hierbei geht es beispielsweise darum eine bestimmte Domain auf die Blacklist zu setzen, die durch verdächtige Anfragen aufgefallen ist. Weiterhin gab es einen konkreten Fall, bei dem der Login eines Benutzers zu einer ungewöhnlichen Zeit registriert wurde. Dieser Benutzer erweiterte seine Rechte auf ungewöhnliche Weise. Dieser Vorfall wurde entdeckt, analysiert und es wurden sofort Gegenmaßnahmen eingeleitet.

Ein erster richtiger Stresstest für die CYREBRO Plattform war der von einem externen Partner durchgeführte Penetrationstest der Endkundenumgebung.
Aufgrund des umfangreichen und detaillierten Reportings von CYREBRO konnten außerdem viele wichtige Erkenntnisse gewonnen werden: Beispielsweise über besondere Verhaltensweisen verschiedener IT-Lösungen und deren Benutzer. Hieraus wurde eine Reihe von Optimierungen abgeleitet, welche neue Konfigurationen und Prozessabläufe nach sich zogen.

Herzstück des Infinigate SOCplus Konzeptes ist die Managed SOC Lösung von CYREBRO.
Weitere Infos unter infinigate.de/Portfolio/Fokusthemen/SOCPlus-Security-Operations-Center

Über CYREBRO

CYREBRO ist der Pionier des ersten online verwalteten Security Operations Center (SOC) in Unternehmensqualität, das die Cybersicherheit für KMUs demokratisiert und schnelle und effiziente Reaktionen auf Cyber-Bedrohungen und deren Abwehr gewährleistet. Die Plattform bündelt alle Sicherheitsinformationen in einem leicht verständlichen Dashboard, das durch seine proprietären Erkennungsalgorithmen vollständige Klarheit, Einblicke und Echtzeit-Cyberempfehlungen an einem Ort bietet. CYREBRO ist technologieunabhängig und kann 750 Systeme in jede Sicherheitstechnologie, -plattform und -lösung integrieren, um eine Netzwerkabdeckung aller Endpunkte, Cloud- und Netzwerkgeräte zu gewährleisten.

Über Infinigate

Der einzige Fokus der Infinigate Gruppe liegt auf dem Vertrieb nachhaltiger IT-Sicherheitslösungen zum Schutz und zur Verteidigung der IT-Infrastruktur sowie der Cloud. Als echter Value Added Distributor unterstützt die Infinigate Gruppe innovative, erstklassige Sicherheitslösungen, die ein hohes Maß an Fachwissen erfordern. Die Infinigate Gruppe bietet ihren Partnern, MSSPs und Anbietern einen kompletten Service, um ihr Produktportfolio mit speziellen technischen Marketing-, Vertriebs- und professionellen Dienstleistungen zu ergänzen. Nach einer Reihe erfolgreicher Markteintritte und Akquisitionen will die Infinigate Gruppe ihre Strategie der geografischen Expansion in ganz Europa weiter vorantreiben. Heute hat die Infinigate-Gruppe etwa 500 Mitarbeiter und Niederlassungen in 11 europäischen Ländern, darunter Großbritannien, Frankreich, Deutschland, Schweiz, Österreich, Niederlande, Belgien, Schweden, Norwegen, Dänemark und Finnland. Mit dieser starken Aufstellung deckt Infinigate fast 85 % des westeuropäischen IT-Sicherheitsmarktpotenzials ab und etabliert sich als führender europäischer Value Added Distributor für IT-Sicherheit, Cloud und MSP: www.infinigate.com.

Über NetPlans

Die NetPlans ist ein global agierender Managed Service Provider, der sich auf innovative Cloud Lösungen mit einer eigenen Business Cloud in Deutschland spezialisiert hat. Die angebotenen Managed Services basieren auf den Erfahrungen seit der Gründung 1998 und der Tätigkeit als klassisches IT Systemhaus, das stetig in neue Technologien investiert.

Mittlerweile hat die NetPlans ein bundesweites Niederlassungsnetz sowie einen Standort in der Schweiz und betreibt mit mehr als 300 Mitarbeitern eine hauseigene Supportabteilung. Durch diese Firmenstruktur gewährt die NetPlans Systemhausgruppe Präsenz und Kundennähe, deren langfristige Zufriedenheit und Erfolge ihr Leistungsantrieb ist.

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

Infinigate SOCplus-Team
+49 89 89048 399
mssp@infinigate.de

SOC plus INFINIGATE