



CrowdStrike Kundenreferenz



Internationaler Technologiekonzern schützt IT-Infrastruktur mit Cloud-basierter Sicherheit von CrowdStrike

Die Schunk Group ist ein internationaler Technologiekonzern mit 60 Gesellschaften und mehr als 9.000 Beschäftigten in 29 Ländern. Schunk ist ein führender Anbieter von Produkten aus Hightech-Werkstoffen, wie Kohlenstoff, technischer Keramik und Sintermetall, sowie von Maschinen und Anlagen – von der Umweltsimulation über die Klimatechnik und Ultraschallschweißen bis hin zu Optikmaschinen.

Bei einer derart diversen Firma stellen sich der IT-Abteilung verschiedenste IT-Security Herausforderungen, wie Christian Maxeiner, Head of IT Technology bei Schunk, berichtet: „Unsere Security-Herausforderungen sind heutzutage vielfältiger denn je. Wir stellen beispielsweise zunehmend fest, dass die Trennung von IT und OT immer mehr aufweicht, wodurch Industrieanlagen mit Zugang zum Internet als potenzieller Angriffsvektor berücksichtigt werden müssen. Auch die sichere Abkopplung von Altsystemen, die nicht mehr gepatcht werden können, gehören zu unserem Aufgabenspektrum. Natürlich spielt für uns auch das Thema Industriespionage und der Schutz unseres geistigen Eigentums eine wichtige Rolle. Hinzu kommen, bedingt durch unsere global verteilten Gesellschaften, unterschiedliche Bedrohungslagen in den verschiedenen Ländern, denen wir wirkungsvoll entgegentreten müssen.“

Um diese mannigfaltigen Herausforderungen erfolgreich zu meistern, machte sich Schunk auf die Suche nach einer neuen Security-Lösung, nachdem die Lizenz für das alte, signaturbasierte Produkt abgelaufen war. Für das international agierende Unternehmen kam nur eine Cloud-basierte Next Generation Antivirus-Lösung in Betracht. Nach ausgiebiger Recherche erstellten die Inhouse-Experten eine Shortlist mit fünf Anbietern, von denen drei in die finale Auswahl kamen. Nach einer fachlichen und kaufmännischen Evaluation entschied sich Schunk für die Cloud-native Next Generation-Lösung von CrowdStrike.

Schon früh machte sich der Wechsel zu CrowdStrike bezahlt. Dank der stark gestiegenen Sichtbarkeit in Schunks Systeminfrastruktur konnte das Team um Christian Maxeiner Dinge im Netzwerk erkennen, die dem vorherigen Produkt verborgen geblieben waren. Diese Entdeckungen verursachten zwar Mehrarbeit für das Team, allerdings konnte die potenzielle Angriffsfläche durch die behobenen Schwachstellen signifikant verringert werden.

BRANCHE:

Hightech-Werkstoffe, Maschinen und Anlagen

STANDORT/ KONZERNZENTRALE:

Heuchelheim, Deutschland

HERAUSFORDERUNG:

Absicherung der Unternehmens-IT, Schutz von geistigem Eigentum

LÖSUNG:

Die CrowdStrike Falcon® Plattform und das CrowdStrike® Falcon OverWatch™ Managed Threat Hunting-Team bieten Schunk eine umfassende IT-Sicherheitslösung, die nicht nur mehr Sichtbarkeit und Transparenz bedeutet, sondern auch zuverlässigen Schutz vor modernen Bedrohungen bietet und das geistige Eigentum des Unternehmens schützt.

„CrowdStrike ermöglicht uns einen sehr tiefen Einblick, den wir so vorher nicht hatten. Das sieht auch mein Chef, der CIO, so. Er ist froh, dass wir jetzt diese Lösung haben. Wir können jetzt auch viele Dinge im Bereich Risikomanagement adressieren.“

Christian Maxeiner

Head of IT Technology
Schunk Group



CrowdStrike Kundenreferenz



Schunk setzt zum Schutz seiner Netzwerke auf Sicherheit aus der Cloud

Der Rollout der CrowdStrike-Lösung verlief dabei denkbar unkompliziert. Zunächst liefen CrowdStrike und das alte Sicherheitsprodukt noch im Parallelbetrieb, bis CrowdStrike am Stichtag dann durch Deinstallation des alten Produkts als primäre Sicherheitslösung in Betrieb ging. Dabei kam es weder im Parallelbetrieb noch während der Umstellung auf CrowdStrike zu irgendwelchen Fehlern oder anderen technischen Komplikationen. Dank der Cloud-nativen Technologie von CrowdStrike konnten 9.400 Endpunkte innerhalb von zwei Monaten auf die neue Sicherheitslösung umgestellt werden.

Technologie wird durch CrowdStrike Falcon OverWatch ergänzt

Um auch wirklich effektiv vor bekannten und unbekanntem Bedrohungen geschützt zu sein, verlässt sich Schunk nicht allein auf Technologie. Um diese sinnvoll zu ergänzen, hat man sich dazu entschieden, Falcon OverWatch Managed Threat Hunting zur vorhandenen CrowdStrike Implementation hinzuzufügen. Die Expertise des Falcon OverWatch Teams steht Schunk rund um die Uhr zur Verfügung und sorgt dafür, dass das Unternehmen auch in Zukunft gut gegen potenzielle Angriffe jeder Art gerüstet ist.

Neben Falcon OverWatch Threat Hunting setzt Schunk auf CrowdStrike Falcon®, CrowdStrike Falcon® Insight XDR, Endgeräte Erkennung und Reaktion (EDR) und CrowdStrike Falcon® Device Control. Darüber hinaus hat sich das Unternehmen nach der erfolgreichen Implementierung dieser Module und einer zusätzlichen Evaluierungsphase dazu entschieden, sein Sicherheitsportfolio noch um die Schwachstellen-Management-Lösung CrowdStrike Falcon® Spotlight und die IT-Hygiene-Lösung CrowdStrike Falcon® Discover zu erweitern. „Jetzt haben wir dank der gut abgestimmten Module endlich den zentralisierten Gesamtüberblick, den ich mir für unser Unternehmen immer gewünscht habe. Dadurch fühlt man sich natürlich auch sicherer. Das sieht auch mein Chef, unser CIO, so“, ergänzt Maxeiner.

„Auch wenn wir jetzt Schwachstellen entdecken, die man vorher nicht gesehen hat, fühle ich mich trotzdem sicher, weil ich sie jetzt kenne. Und zu wissen, dass es das Falcon OverWatch-Team gibt, das bestimmte Dinge zusätzlich detektiert, spielt in diese Sicherheit zusätzlich hinein.“

ÜBER CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), ein global führendes Unternehmen im Bereich der Cybersicherheit, definiert mit der weltweit fortschrittlichsten Cloud-nativen Plattform zum Schutz von Workloads, Endgeräten, Identitäten und Daten moderne Sicherheit. Dank der CrowdStrike Security Cloud und erstklassiger künstlicher Intelligenz verarbeitet die CrowdStrike Falcon®-Plattform in Echtzeit Angriffsindikatoren, Bedrohungsdaten, sich ständig weiterentwickelnde Methoden der Gegner sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen und ermöglicht hochpräzise Erkennungen, automatisierte Schutz- und Abhilfemaßnahmen, hervorragendes Threat Hunting und eine nach Prioritäten geordnete Beobachtung von Schwachstellen. Die funktionsorientierte Single-Agent Cloud Architektur der Falcon Plattform bietet eine schnelle und skalierbare Anwendung, ausgezeichnete Sicherheit und Leistung, weniger Komplexität und sofortige Wertschöpfung.

CrowdStrike: **We stop breaches.**

ERGEBNISSE:



Übergeordneter Einblick in alle Systemes



Höhere Transparenz ermöglicht Überblick über Systeme und Software und zeigt bisher unbekannt Schwachstellen auf



Erhöhte Sicherheit dank Falcon OverWatch

ENDPUNKTE



CROWDSTRIKE-PRODUKTE:

- Falcon Prevent - Antivirus der nächsten Generation
- Falcon Intelligence
- Falcon Insight - Endgerätebasierte Erkennung und Reaktion
- Falcon OverWatch - Threat Hunting
- Falcon Device Control - Endgerätekontrolle
- Falcon Spotlight - Vulnerability Management
- Falcon Discover - IT-Hygiene