Ontinue

CUSTOMER STORY

Mit Ontinue stellt die Vossloh AG ihre Weichen Richtung Sicherheit

Die Bahn kommt. In den meisten Fällen, in denen dieser ehemalige Slogan der Deutschen Bahn weltweit zur Realität wird, hat die Vossloh AG etwas damit zu tun. Der börsennotierte Bahntechnikkonzern aus Deutschland ist spezialisiert auf die Entwicklung, Produktion und Instandhaltung von Schienenbefestigungssystemen, Betonschwellen, Weichensystemen sowie innovative Dienstleistungen rund um den Lebenszyklus des Fahrwegs Schiene. Das 1888 im sauerländischen Werdohl gegründete Unternehmen beschäftigt heute mehr als 4.000 Mitarbeitende in rund 30 Ländern und erwirtschaftete zuletzt einen Umsatz von 1,2 Milliarden Euro. Die Produkte des Bahntechnikkonzerns sorgen für einen sicheren und zuverlässigen Bahnverkehr in mehr als 100 Staaten.

Über die Jahre haben sich drei übergeordnete Geschäftsbereiche herausgebildet: „Core Components“, in dem sich alles um Schienenbefestigungssysteme jeglicher Art dreht, „Customized Modules“, in dem die Vossloh AG individuell an die Kundenbedürfnisse anzupassende Produkte wie etwa Weichensysteme entwickelt und produziert, sowie „Lifecycle Solutions“, mit dem das Unternehmen Services rund um die Instandhaltung von Schienen und Weichen, Schweißdienstleistungen

vossloh
enabling green mobility

Motivation

- Aufbau eines voll funktionsfähigen Security Operations Center
- Konsolidierung der IT-Sicherheitsinfrastruktur
- 365/24/7-Monitoring nach dem Follow-the-Sun-Prinzip
- Schaffung einer holistischen Übersicht über die gesamte IT-Landschaft
- Nutzung von Synergieeffekten von Sicherheits-Tools aus der Hand eines Anbieters

Lösung

- Vollständige Umstellung der IT auf den Tech-Stack von Microsoft (ongoing)
- Implementierung von Microsoft Defender als EDR-Lösung für Clients und Server mit Hilfe von Ontinue
- Inbetriebnahme von Microsoft Sentinel als SIEM-Plattform mit Hilfe von Ontinue

Ergebnis

- Zentralisierte IT-Sicherheitsinfrastruktur
- Rund-um-die-Uhr-Überwachung der gesamten IT
- Holistisches SOC bestehend aus internen und externen Security-Experten
- Visibilität über die gesamte IT-Landschaft
- Deutliche Entlastung des unternehmensinternen IT-Teams
- Nur wenige der über 10.000.000 Alerts erreichen das Sicherheitsteam der Vossloh AG

Über die Vossloh AG

Vossloh ist ein weltweit tätiger, börsennotierter Bahntechnikkonzern und führender Anbieter für den Bau und für den Werterhalt der Bahninfrastruktur. Das Unternehmen bietet ein integriertes Angebot für den schienengebundenen Verkehr unter einem Dach an. Dies umfasst einzigartige, leistungsstarke Schlüsselprodukte und komplexe Systeme, darunter Schienenbefestigungssysteme, Betonschwellen, Weichensysteme und Kreuzungen, sowie innovative Dienstleistungen rund um den Lebenszyklus des Fahrwegs Schiene.

sowie Schienen- und Weichenlogistik anbietet. All diese Geschäftsbereiche waren bis vor etwa sechs Jahren noch sehr autark und die IT-Infrastruktur entsprechend dezentral organisiert. Durch die Initiative „One Vossloh“, durch die die Zentralisierung des Unternehmens notwendig wurde, wurde auch das Projekt „One IT“ und damit die Konsolidierung der IT-Infrastruktur in Angriff genommen. Frank Bäcker, Head of Shared Services and Platforms bei der Vossloh AG, und die Cybersecurity-Abteilung waren maßgeblich an dieser Entwicklung beteiligt und haben vor dem Hintergrund einer zunehmenden Bedrohungslage ein Sicherheitskonzept ausgearbeitet.

„Auf dem Weg zur Zentralisierung der IT setzen wir ganz klar auf Cloud-Services und Microsoft-Technologien wie Office 365 und Sharepoint für die Kollaboration, auch das Hosting findet vermehrt über Azure statt“, erklärt Bäcker. „In Sachen Cybersecurity haben wir natürlich erkannt, dass wir als globales Unternehmen ein Security Operations Center benötigen, das nach dem Follow-the-Sun-Prinzip organisiert und rund um die Uhr im Einsatz ist.“ Ein eigenes SOC aufzubauen, kam allerdings nicht in Frage, da die Ressourcen der Mitarbeitenden eine solch holistische Abdeckung aller damit verbundener Aufgaben nicht leisten können. Zudem machte der allgegenwärtige Fachkräftemangel allen entsprechenden Ambitionen einen Strich durch die Rechnung.

„Heimvorteil“ für Ontinue

Der Evaluierungsprozess begann mit der Überlegung, wie die zu-künftige IT-Sicherheitsinfrastruktur aussehen müsste, um den ma-ximalen Synergieeffekt zu bewirken. Daher fasste die Vossloh AG schnell den Entschluss, auch bei der Cybersicherheit auf Microsoft-Technologien zu setzen. „Alles aus einem Guss zu haben, sorgt für weniger Reibung“, so Frank Bäcker. Für die Endpoint Detection and Response (EDR) lobte das Unternehmen Microsoft Defender aus und als SIEM (Security Information and Event Management)-Plattform stand Microsoft Sentinel ganz oben auf der Liste der ge-wünschten Security-Tools. Nun galt es, den passenden MXDR (Ma-naged Extended Detection and Response)-Serviceanbieter zu fin-den, der mit diesen Technologien vertraut ist und den Weg der Im-plementierung mit der Vossloh AG gemeinsam gehen konnte.

> „ Mit Ontinue ION haben wir nicht nur eine konsolidierte und zentralisierte Sicherheitsstrategie auf die Schiene gebracht. Gemeinsam mit unserem Partner haben wir das Fundament für weitere Maßnahmen im Kampf gegen Cyberattacken gelegt.“

Frank Bäcker
Head of Shared Services and Platforms
Vossloh Ag

Abgesehen von der Versiertheit im Umgang mit dem Tool-Stack von Microsoft musste der MXDR-Anbieter natürlich die interne IT-Abteilung der Vossloh AG zu einem voll funktionsfähigen SOC ausbauen. Dazu gehört auch die Option, die IT-Infrastruktur an 365 Tagen im Jahr rund um die Uhr überwachen zu können. „Unsere Wahl fiel relativ leicht und schnell auf Ontinue. Wir haben uns selbstver-ständlich viele Service-Provider angesehen und miteinander vergli-chen, jedoch hat uns das Leistungsportfolio von Ontinue überzeugt. Am Ende des Tages hatten sie auch einen leichten Heimvorteil, da wir bereits sehr erfolgreich mit Open Systems im Bereich Netzwerksicherheit zusammenarbeiten, also dem Unternehmen, aus dem Ontinue hervorgegangen ist“, so der Head of Shared Services and Platforms. Nachdem die Entscheidung getroffen war, wurden der Defender und Sentinel gemeinsam implementiert, sodass die Daten aus der Network Detection and Response (NDR) und der Endpoint Detection and Response (EDR) nun in der SIEM-Plattfrom zusammenlaufen. Für die Cyber Defender und Cyber Advisor von Ontinue sowie Frank Bäcker und sein Team ergibt sich somit zu jeder Zeit ein holistisches Bild über die Sicherheitslage im Unterneh-men.

Alles aus einem Guss

Die Kommunikation innerhalb des aus internen wie externen IT-Sicherheitsexperten bestehenden Security Operations Center findet über Microsoft Teams statt. Dort laufen Warnmeldungen über Events und Incident-Reports in einem entsprechenden Kanal zusammen, in dem auch die Kollaboration stattfindet. Gleichzeitig bietet der MXDR-Service Ontinue ION ein umfangreiches Dashboard, in dem alle Informationen aus Sentinel übersichtlich zusammengefasst bereitgestellt werden. Die Cyber Defender und Cyber Advisor entlasten das Security-Team der Vossloh AG maßgeblich, indem sie viele Automatisierungsprozesse in der First-Level-Response implementieren und bis zu einem gewissen Grad autark auf Sicherheitsvorfälle reagieren dürfen.

„Die Unterstützung durch Ontinue ist wirklich spürbar“, so Bäcker. „Von über zehn Millionen Security Events, die Sentinel erkennt, landen nur drei auf unserem Schreibtisch. Vor unserer Zusammenarbeit konnten wir uns kaum einen Überblick verschaffen, geschweige denn sinnvolle Verteidigungs- und Response-Strategien entwickeln. Es fehlte eine konsolidierte Sicherheitsinfrastruktur und entsprechende Sicherheitstools.“ Für die Zukunft steht bei der Vossloh AG der Abschluss der Zentralisierungsarbeiten auf der Agenda. Zudem ist seit der Pandemie immer wieder der Zugriff von außerhalb durch Angestellte im Homeoffice oder externe Lieferanten auf das Unternehmensnetzwerk im Fokus. Dort möchten Frank Bäcker und sein Team womöglich zukünftig einen Zero-Trust-Ansatz etablieren, der die bisherige Client-VPN-Strategie ersetzt und die IT-Sicherheit insgesamt steigert.

Der Head of Shared Services and Platforms zeigt sich mit der aktuellen Entwicklung sehr zufrieden: „Mit Ontinue ION haben wir nicht nur eine konsolidierte und zentralisierte Sicherheitsstrategie auf die Schiene gebracht. Gemeinsam mit unserem Partner haben wir das Fundament für weitere Maßnahmen im Kampf gegen Cyberattacken gelegt.“

Ontinue

Über Ontinue

Ontinue, der Experte für KI-gestützte Managed Extended Detection and Response (MXDR), ist ein rund um die Uhr verfügbarer Sicherheitspartner mit Hauptsitz in Zürich. Um die IT-Umgebungen seiner Kunden durchgehend zu schützen, ihren Sicherheitsstatus zu bewerten und kontinuierlich zu verbessern, kombiniert Ontinue KI-gesteuerte Automatisierung und menschliches Fachwissen mit dem Microsoft-Sicherheits-Produktportfolio. Durch die intelligente, Cloud-basierte Nonstop SecOps-Plattform reicht Ontinues Schutz vor Cyberattacken weit über die grundlegenden Detection- und Response-Services hinaus.

Weitere Informationen gibt es unter www.ontinue.com