Industrie: Manufacturing

Use Case: Maschinenbauer

Ein europäisches Maschinenbauunternehmen mit etwa 10.000 Mitarbeitern und mehreren Produktionsstandorten in Europa und Asien steht vor der Herausforderung, die nationalen und EU-Compliance-Anforderungen gemäss **NIS2** und Maschinenverordnung zu erfüllen und sich einer veränderten Cyber-Bedrohungslandschaft und -exposition zu stellen. Insbesondere **mit der Integration von Operational Technology (OT)** und Industrial Internet of Things (IIoT) steigt für die Branche die Anfälligkeit für Cyber-Bedrohungen signifikant.

Effektive Minimierung von Produktionsausfällen und Einhaltung der Richtlinien

Als Teil der nun kritischen Infrastruktur des Landes ist das Unternehmen verpflichtet, seine Cybersicherheit und Resilienz gegenüber IT-Risiken weiter zu verbessern. Die besonders beachteten Punkte aus NIS2 umfassen, die Identifizierung und Minimierung von IT- und Cybersicherheitsrisiken, die Implementierung eines effizienten Incident Management Systems und die Möglichkeit, Sicherheitsvorfälle prägnant an die zuständigen Behörden zu melden. Das Unternehmen will geeignete Massnahmen schnell und effektiv umsetzen, um auch bei zunehmender Bedrohungslage, Schäden durch Produktionsausfälle, Daten- oder Wissensabfluss, Reputationsschäden und Bussgelder an nationale Behörden zu vermeiden.

Auch die ab 2027 verbindliche “EU-Maschinenverordnung” zielt auf die Erhöhung der Cybersicherheit im Maschinenbau ab und verlangt von Maschinenherstellern, dass alle Maschinenprodukte “über eine robuste Sicherheitsarchitektur verfügen, die gegen Cyberangriffe geschützt ist”.

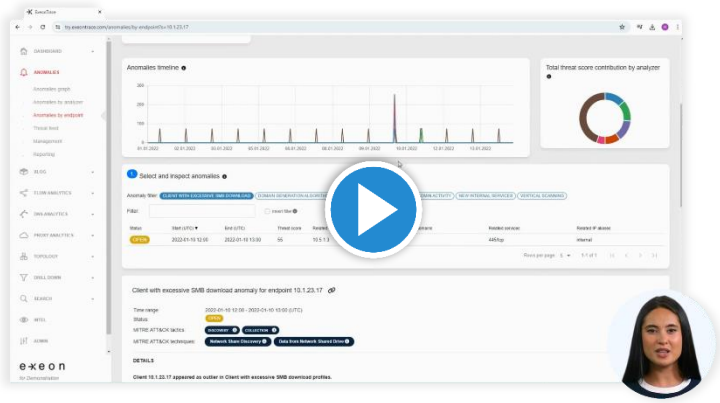
Dies gilt insbesondere für vernetzte Maschinen und Produktionsanlagen, die regelmässig mit externen Netzwerken kommunizieren. Die Maschinenbauer müssen ausserdem sicherstellen, dass alle neuen Maschinen bereits in der Entwicklungsphase die Anforderungen an die Cybersicherheit erfüllen und so konstruiert sind, dass sie unbefugten Zugriffen standhalten.

Weltweite Geschäfte, weltweite Produktion, weltweites Risiko

Durch die zunehmende Vernetzung der Produktionsstandorte und die Digitalisierung von Maschinen und Prozessen ist das Unternehmen bereits heute mit einem signifikanten Anstieg der Cyber-Risiken konfrontiert. Angriffe auf industrielle Kontrollsysteme (ICS) über IT, IIOT- und OT-Systeme können die Produktion unterbrechen und sensible Konstruktions- Kunden- oder Patentdaten gefährden. Ende 2022 wurde das Unternehmen schon einmal Ziel eines Ransomware-Angriffs: Nach einem langen unentdeckten Eintritt durch eine Phishing-E-Mail konnten Produktionsdaten verschlüsselt und die Steuerung der Produktionsmaschinen lahmgelegt werden.

Erkennung von fortgeschrittenen Bedrohungen in der OT

Zum Demo-Video



exeon
Smart Cyber Security.

Da das IT-Team zu diesem Zeitpunkt, wegen fehlender Visibilität nur verzögert reagieren und die betroffenen Systeme erst spät isolieren und die Ausbreitung der Malware stoppen konnte, dauerte es fast 5 Arbeitstage, bis die Produktionsdaten wiederhergestellt waren und der Betrieb wieder aufgenommen werden konnte. Der Betrieb kam zum Stillstand, was zu Lieferschwierigkeiten und in der Folge zu Umsatzeinbussen führte.

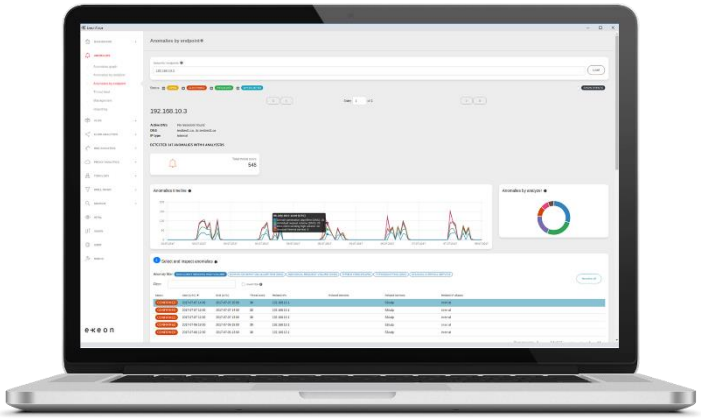
Herausforderungen: ICS, APTs, NIS2,...

Mit der neuen ExeonTrace-Lösung im—intern betriebenen—SOC will der Maschinenbauer die Anforderungen der NIS2-Richtlinie nach kontinuierlicher Netzwerküberwachung, schnellerer Reaktion auf Vorfälle sowie besserer Transparenz und Berichterstattung «im Fall der Fälle» erfüllen und für zukünftige Bedrohungen besser gerüstet sein. Darüber hinaus soll das Sicherheitsteam des Unternehmens von Routineaufgaben wie der Nachverfolgung von Fehlalarmen (False Positives) entlastet werden.

Schutz vor Bedrohungen der Lieferkette und Zero-Day-Exploits

Die eingesetzte Sicherheitstechnologie soll präventive und reaktive Ansätze kombinieren, um Cyber-Angriffe zu erkennen und zu stoppen, ohne den laufenden Betrieb zu stören. Durch eine umfassende Netzwerktransparenz sollen Ransomware, Advanced Persistent Threats (APTs) und Insider-Angriffe frühzeitig erkannt und eingedämmt werden. Darüber hinaus sollen Bedrohungen für das Unternehmen aus der Hard- und Software Supply Chain oder durch Zero-Day Exploits, also auch bisher unbekannte Gefahren ausserhalb des Perimeters, abgewehrt werden.

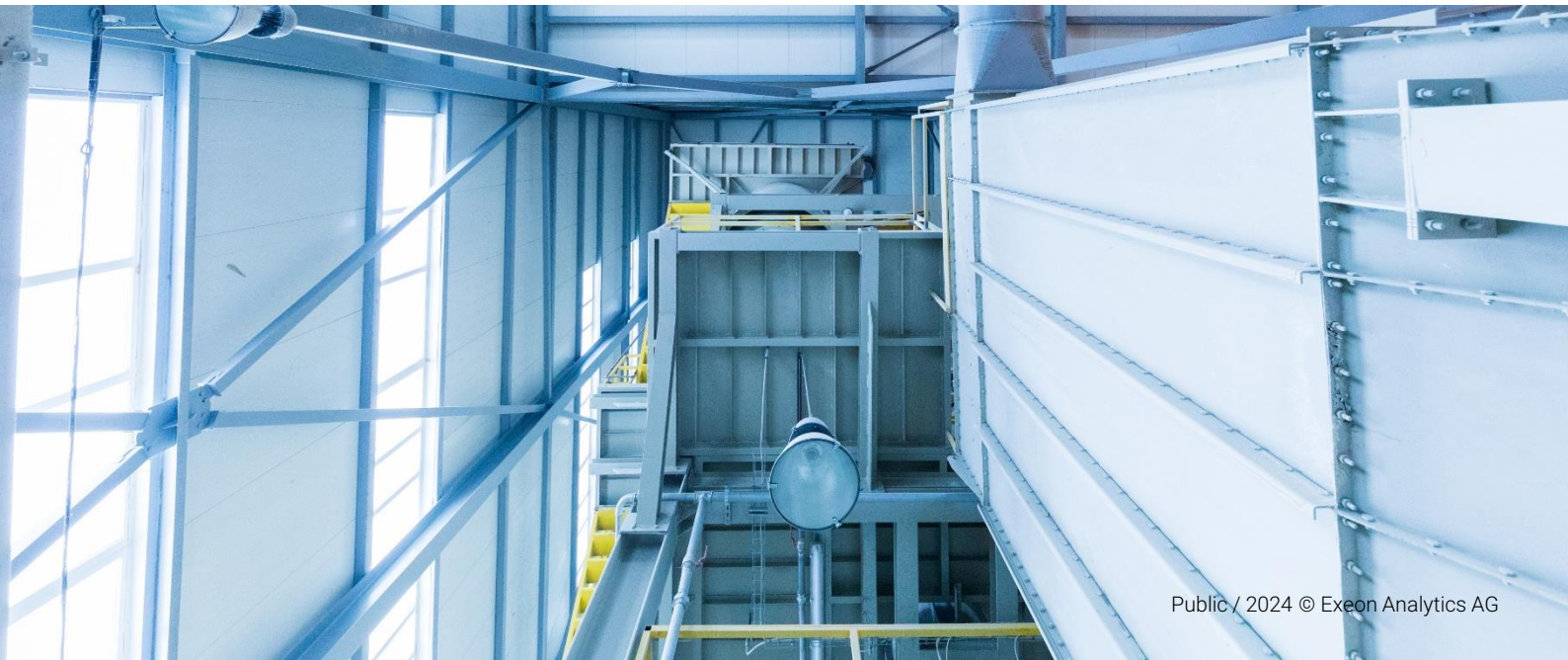
Die Implementierung soll so erfolgen, dass die Datenschutzbestimmungen nach DSGVO einge-halten werden, weshalb das Unternehmen die On-Premise-Variante der Lösung in Betracht gezogen hat.



Implementierung von ExeonTrace

Die komplexe Infrastruktur des Maschinenbauers, bestehend aus IT- und OT-Systemen, erforderte eine gründliche Analyse der Netzwerkarchitektur, um eine nahtlose Integration zu gewährleisten. Ausserdem wurde der bestehende Security-Stack mit EDR, SIEM und Firewalls integriert. ExeonTrace monitort über die Kommunikationsprotokolle alle Assets, aller Netzwerksegmente, darunter interne IT-Netzwerke, industrielle Kontrollsysteme (ICS), Produktionsumgebungen und externe Verbindungen zu Drittanbietern. Dies gewährleistet eine vollständige Abdeckung und einheitliche Überwachung aller kritischen Systeme.

ExeonTrace überwacht seit dem Rollout kontinuierlich und in Echtzeit alle Netzwerksegmente, einschliesslich interner, externer und Produktionsnetzwerke, anhand von Metadaten wie IP-Adressen, Ports, Kommunikationsprotokollen und Übertragungsraten. Die Metadaten werden mit KI-basierten Algorithmen analysiert, um ungewöhnliche Kommunikationsmuster und potenzielle (auch neuartige) Bedrohungen der CC-Kanäle schnell zu erkennen und die False-Positive- und False-Negative-Rate von Ereignissen zu reduzieren. ExeonTrace verwendet fortschrittliche Verhaltensanalyse und Machine Learning, um eine Baseline des normalen Netzwerkverkehrs zu erstellen.



Abweichungen, wie plötzliche Datentransfers zu externen IPs oder ungewöhnliche Login-Versuche, werden als Anomalien markiert und sofort gemeldet. Wird ein Vorfall erkannt, können sofort Massnahmen eingeleitet werden, wie z.B. die Isolation betroffener Systeme, die dynamische Anpassung von Netzwerkregeln oder das Blockieren verdächtiger IP-Adressen.

Die Möglichkeit des Whitelistings und der Identifizierung besonders risikoreicher Subnetze durch das Riskbased Alerting in ExeonTrace ermöglicht eine noch gezieltere Alarmierung und erleichtert die Arbeit im Soc weiter. Alle sicherheitsrelevanten Informationen und Netzwerkaktivitäten werden in einem zentralen Dashboard visualisiert. Dies ermöglicht dem Sicherheitsteam, Bedrohungen in Echtzeit zu überwachen, den gesamten Netzwerkstatus auf einen Blick zu sehen und sofort Massnahmen zu ergreifen. Aktivitäten können frühzeitig erkannt werden, das Sicherheitsteam kann betroffene Geräte schnell isolieren und Produktionsprozesse vor möglichen Angriffen schützen.

ExeonTrace wird bei dem Unternehmen vollständig On-Premises betrieben, wodurch alle Daten innerhalb der sicheren Infrastruktur des Unternehmens verbleiben. Dies erfüllt sowohl die Anforderungen der DSGVO als auch der NIS2-Richtlinie und sorgt für maximale Kontrolle über sensible Produktions- und Unternehmensdaten.

Impact von NDR

Diese umfassende Sicherheitslösung schützt den Produktionsprozess des Maschinenbauers, ohne ihn zu beeinträchtigen, und ermöglicht eine proaktive Abwehr von Cyberangriffen, wodurch die betriebliche Belastbarkeit und das Vertrauen in die Sicherheitsmassnahmen gestärkt werden. ExeonTrace erkennt frühzeitig ungewöhnliche Netzwerkaktivitäten wie unerwartete Datenübertragungen an externe IP-Adressen und verdächtige Anmeldeversuche auf Produktionssystemen. Dank der schnellen Reaktionsmöglichkeiten kann das Sicherheitsteam potenziell schwerwiegende Vorfälle rechtzeitig eindämmen, infizierte Systeme schneller isolieren, die Ausbreitung von Malware stoppen und verschlüsselte Daten aus Backups wiederherstellen, sodass die Produktion nicht unterbrochen werden muss. Die unter anderem von NIS2 geforderte Incident-Response-Zeit kann somit drastisch reduziert werden.

Durch den Einsatz verbesserter KI-Algorithmen konnte die Anzahl der Fehlalarme um 50% reduziert werden, was die Effizienz des Sicherheitsteams weiter erhöht.

Darüber hinaus können nun alle potenziellen Sicherheitsvorfälle vollständig dokumentiert und in Berichten an die zuständigen Behörden übermittelt werden, wodurch die Compliance-Anforderungen der NIS2-Richtlinie innerhalb von 12 Stunden erfüllt werden. ExeonTrace ermöglichte auch die vollständige Rückverfolgbarkeit aller böswilligen Aktivitäten, wodurch Infektionswege und Bedrohungsursprünge zu 100% nachvollzogen werden konnten. ExeonTrace reduziert das SIEM-Datenvolumen des Unternehmens, indem es irrelevante Informationen herausfiltert, Ereignisse korreliert und ähnliche Vorfälle aggregiert und komprimiert, bevor sie weitergeleitet werden. Dadurch werden nur sicherheitsrelevante und optimierte Daten im SIEM verarbeitet, was die Gesamtbelastung deutlich reduziert. Da ExeonTrace Daten in einem optimierten Format an das SIEM transferiert wird die Datenmenge weiter reduziert.

Andere Maschinenbauer, die ExeonTrace vertrauen:

WIN GD

trafag sensors controls

Allianz für Cyber-Sicherheit

CYBERSECURITY MADE IN EUROPE

ATTESTA ISO 27001 CERTIFIED

Exeon Analytics AG
contact@exeon.com
exeon.com

Grubenstrasse 12
8045 Zürich
Schweiz

LinkedIn

YouTube