OTORIO

Automotive

OTORIO ermöglicht sicheres digitales Wachstum für einen globalen Automobilhersteller

Case Study

Der Kunde ist ein Fortune 1000-Hersteller (OEM) von Nutzfahrzeugen mit einem bekannten Markennamen. Die globale Präsenz des Kunden umfasst Fertigungsstätten auf vier Kontinenten und eine umfangreiche Lieferkette bestehend aus Tier-1- und Tier-2-Lieferanten..

Automatisierte, industrielle und kontextbezogene Transparenz über alle Anlagen und Systeme

Einführung einer kontinuierlichen Compliance-Überwachung

Weniger “Alert Fatigue” durch intelligente Priorisierung der Auswirkungen unterschiedlicher Risiken auf das Unternehmen

DIE HERAUSFORDERUNG

Die Automobilindustrie ist ein beliebtes Ziel für Cyber-Angreifer. Ein durchschnittliches Fahrzeug enthält bis zu 150 elektronische Steuergeräte und etwa 100 Millionen Zeilen Softwarecode. Diese Zahl wird bis 2030 voraussichtlich auf 300 Millionen Zeilen ansteigen.

Die zunehmende Digitalisierung von Fahrzeugen bringt viele Cybersecurity-Risiken mit sich. Autos und Lastwagen sind zu eigenständigen digitalen Plattformen geworden - mit Internetzugang, sich automatisch aktualisierenden Betriebssystemen und physischen Anlagen, die anfällig für Angriffe sind. Neue Vorschriften werden entwickelt, um die Sicherheit der Verbraucher zu gewährleisten - insbesondere die ISO/SAE 21434, die im Jahr 2024 in Kraft tritt.

Der Automobil-OEM hatte mit einer Reihe von Problemen zu kämpfen, darunter: unzureichende Sichtbarkeit des Anlageninventars sowie der dazugehörigen Schwachstellen und Risiken; fehlendes Verständnis der betrieblichen Auswirkungen von Risiken; nur wenige Anweisungen für den Schadensfall; und keine Sichtbarkeit der konvergierten OT-IT-Sicherheitslage.

Darüber hinaus wollte der OEM über den reaktiven, auf die Erkennung von Sicherheitsverletzungen ausgerichteten Ansatz hinausgehen, der von seinen bestehenden Cybersecurity-Tools angeboten wurde, da eine Reaktion nach einem Angriff kostspieliger und weniger effektiv ist als die Verhinderung von Angriffen. Darüber hinaus fanden es die operativen Teams des OEMs schwierig, die von ihrem bestehenden System vorgeschlagenen Abhilfemaßnahmen zu verstehen. Infolgedessen war das Unternehmen dem Risiko hochwirksamer Cyberangriffe ausgesetzt.

Das sagt unser Kunde:

> “OTORIO ermöglichte es uns zum ersten Mal, unsere Tausenden von Assets mit einer Business-Impact-Ansicht zu sehen. Als OEM, der die Compliance auf mehreren Kontinenten verfolgen muss, spart uns das Compliance-Tracking von OTORIO Zeit und Geld, da wir uns in einem ständigen Zyklus der Compliance-Vorbereitung befinden. Innerhalb weniger Wochen haben wir den Wandel von der Bedrohungserkennung zur Risikovermeidung vollzogen”

~~ CISO, Automobil OEM

ERSTE ERGEBNISSE

In enger Zusammenarbeit mit den Sicherheitsteams des OEMs konnten die Experten von OTORIO mehrere Lücken im organisatorischen Management von OT-Risiken aufzeigen, und zwar:

- Getrennte Systeme behandelten unterschiedliche Sicherheitsaspekte innerhalb der OT- und IT-Umgebung.
- Es gab nur ein teilweises Verständnis für die Priorisierung von Risiken oder die grundsätzliche Sicherheitslage.
- Sicherheitsrisiken wurden nicht im Zusammenhang mit ihren Auswirkungen auf die Produktionsprozesse bewertet.
- Die Risikoanalyse konzentrierte sich auf das Incident Management und den Input des CISO, während Entscheidungen über Sicherheitsmaßnahmen vom operativen Personal in der Produktion getroffen wurden.

DIE HERAUSFORDERUNG

OTORIO RAM² wurde im konvergenten OT-IT-Netzwerk des Automobilherstellers implementiert, um ein kontextbezogenes Asset-Inventar-Management, betriebliche Auswirkungen, Risikopriorisierung und -minderung sowie eine verbesserte Compliance Governance zu ermöglichen.

RAM² löste das Inventarisierungsproblem durch die Orchestrierung von Daten aus verschiedenen Quellen im OT-Netzwerk des Automobilherstellers. Dies ermöglichte es dem Kunden, automatisch und in Echtzeit, Transparenz über alle Assets innerhalb seines Netzwerks (OT, IT und IIoT) zu erhalten. RAM² organisierte den Anlagenbestand des OEMs automatisch in einer hierarchischen Struktur, basierend auf dem physischen Standort und den operativen Einheiten (Werke, Werkstätten, Zellen). Darüber hinaus korrelierte RAM² die Assets mit Schwachstellen und operativen Prozessen. Schließlich berechnete RAM² die Risiken auf der Grundlage des Schweregrads jeder Schwachstelle und der betrieblichen Auswirkungen der zugehörigen Anlage - und lieferte vereinfachte, schrittweise Abhilfemaßnahmen.

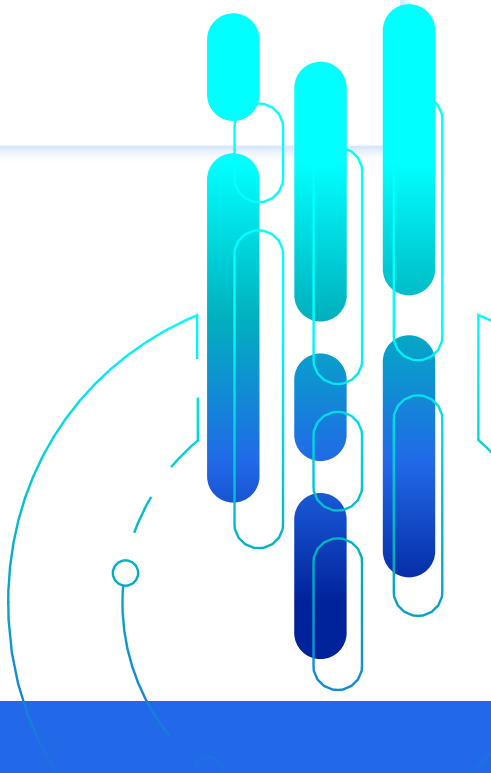
Durch den Einsatz von RAM² konnte der Automobilhersteller die Anzahl der Warnmeldungen deutlich reduzieren. Unterschiedliche Warnungen aus einer Vielzahl von Cybersecurity-Tools wurden nun zu klaren, kontextbezogenen Erkenntnissen zusammengefasst, die es den Sicherheitsteams ermöglichten, die Sicherheitsrisiken mit den größten Auswirkungen auf die Produktion als erstes zu identifizieren und zu entschärfen.

Dank der intuitiven Dashboards von RAM² konnte der OEM die Verwaltung des Anlagenbestands deutlich verbessern und wurde auf kleinere Änderungen in der Produktion aufmerksam.

Darüber hinaus ermöglichte die automatisierte Compliance Governance-Funktion von RAM² dem OEM eine genaue Messung der Einhaltung der relevanten Cybersicherheitsstandards der Branche. Nun wird das Produktionsteam laufend über den Stand der Compliance informiert. Wenn die Konformitätswerte unter den geforderten Schwellenwert fallen, stellt RAM² einfache Playbooks zur Verfügung, mit denen die operativen Teams des Automobilherstellers die Probleme schnell beheben können. Dadurch können sich die Teams auch auf die Einhaltung künftiger Cybersicherheitsstandards für die Automobilindustrie konzentrieren.

OTORIO wurde damit beauftragt:

- Sicherheitsrisiken zu identifizieren, die die Produktion beeinträchtigen könnten
- Die Sicherheitslage und Schwachstellen des Unternehmens zu bewerten und Maßnahmen zur Eindämmung und Verbesserung vorzuschlagen
- Daten von OT/IT/IOT-Anlagen aus verschiedenen Quellen innerhalb des industriellen Netzwerks des Kunden zu erkennen und zu korrelieren
- Änderungen an Anlagen und Konfigurationen in der Produktion in Echtzeit zu überwachen und nachzuverfolgen
- Die Komplexität zu reduzieren und die Effizienz der SecOp-Aktivitäten zu verbessern
- Sicherheitsanstrengungen über betriebliche Prozesse hinweg zu standardisieren
- Compliance-Lücken zu identifizieren und Lösungsschritte vorzuschlagen



OTORIO

Automotive

DIE VORTEILE

Durch die Implementierung von OTORIO RAM² profitierte der Automobilhersteller von unmittelbaren Vorteilen, darunter:

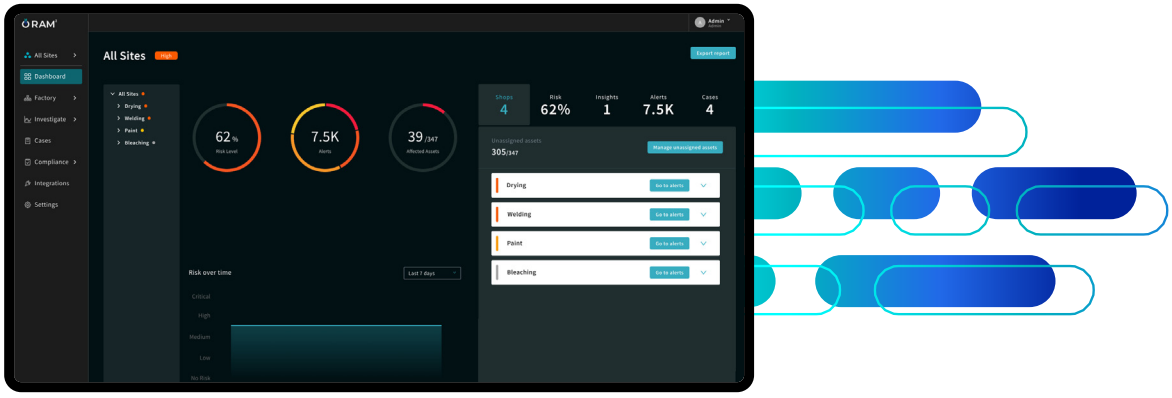
Risikoreduzierung – Durch die Erlangung von Asset-Transparenz und die Zuordnung von Assets zu Schwachstellen und Betriebsprozessen war der OEM in der Lage, seine organisatorische Risikolage schnell zu verstehen und Risiken proaktiv zu beseitigen, bevor sie zu Sicherheitsverletzungen werden konnten.

Beseitigung der Alarm-Müdigkeit – Durch die Orchestrierung von Daten aus verschiedenen Quellen und deren Korrelation zu aussagekräftigen Erkenntnissen, die mit dem Betriebsprozess kontextualisiert sind, hilft RAM² dem OEM, die Anzahl der Alarme zu reduzieren und sich nur auf die kritischsten Risiken zu konzentrieren.

Sichtbarkeit – OTORIOs unübertroffene Fähigkeit zur Inventarisierung von Anlagen passt die industrielle Umgebung des OEMs automatisch an - es wird eine hierarchische Ansicht der Anlagen in verschiedenen Werken, Shops und Zellen erstellt, mit einer Risikoberechnung und Dashboards für jede Geschäftsebene. Als Ergebnis konnte der OEM seine Sicherheitslage besser verstehen und Bereiche abbilden, die mehr Aufmerksamkeit erfordern.

Geschwindigkeit – Durch den Wegfall der manuellen Zuordnung neuer Schwachstellen zu den tausenden Anlagen im Werk und die Automatisierung der Triage und Korrelation zehntausender Warnmeldungen, machte RAM² eine gewaltige Aufgabe durchführbar. Darüber hinaus machte RAM² durch die Bereitstellung von einfach zu verwendenden Playbooks die Risikominderungsprozesse des OEMs schneller und effizienter.

Priorisierung – RAM² ermöglichte eine intelligentere Analyse von CVE-Informationen auf der Grundlage der OTORIO-Datenbank für industrielle Schwachstellen und löste nur Alarme für Elemente aus, die für die jeweiligen Anlagen, Modelle und Versionen relevant sind. RAM² berechnete außerdem das Risiko auf der Grundlage einer Kombination aus Schweregrad und Wahrscheinlichkeit der Cybersecurity-Bedrohung und den potenziellen Auswirkungen auf den Betrieb. So konnte der OEM die Risiken entsprechend seiner betrieblichen Auswirkungen priorisieren.



Über OTORIO

OTORIO liefert OT-Sicherheits- und digitale Risikomanagementlösungen der nächsten Generation, die eine zuverlässige, sichere und effiziente industrielle Digitalisierung gewährleisten. Das Unternehmen kombiniert die professionelle Erfahrung führender nationaler Experten für industrielle Cybersicherheit mit modernster Technologie für digitales Risikomanagement, um der Fertigungsindustrie ein Höchstmaß an Schutz zu bieten.

CN 300419G