Orange
Cyberdefense

Kundenreferenz

EDAG setzt nach Ransomware-Attacke auf Vectra -

KI-basierte Cybersicherheit sichert Neustart und Betrieb des Netzwerks

Auf einen Blick

Kunde:
EDAG Engineering GmbH

Branche:
Mobilitätsindustrie

Firmensitz:
Wiesbaden, Deutschland

Leistungen:
Incident Reponse

Das Unternehmen

Die EDAG Group ist der weltweit größte unabhängige Entwicklungsdienstleister der Mobilitätsindustrie. Das Leistungsportfolio umfasst das 360 Grad Engineering von Fahrzeugen, Produktionsanlagen sowie im Bereich EE und Software & Digitalisierung.

Ausgangssituation

Die EDAG wurde Opfer eines Verschlüsselungstrojaners, der schnell eine Vielzahl businesskritischer Systeme unbenutzbar machte. Um den Aggressor aus dem Netzwerk zu entfernen und einen sicheren Geschäftsbetrieb wiederherzustellen, setzte die EDAG auf die Unterstützung von externen Experten. Außerdem sollte diese Zeit genutzt werden zu verhindern, dass die momentane Schwäche von subversiven Elementen genutzt werden kann, um weitere Schäden oder Schwachstellen, wie eine reverse backdoor, im Netzwerk zu etablieren.

Lösung

Aufgrund der bereits positiven bestehenden Beziehungen seitens der EDAG zur Orange Cyberdefense und dem Hersteller Vectra war der Lösungsweg recht schnell vorgezeichnet.

Der bereits erfolgreich abgeschlossene POC der Vectra Technologie ermöglichte ein besonders schnelles Handeln an dieser Stelle.

Durch die schnelle Reaktion von Orange Cyberdefense konnte in Zusammenarbeit mit EDAG in kürzester Zeit ein praktikabler Vertrauensanker geschaffen werden, der sich perfekt in die Incident Response Strategie des Kunden integriert hat. Vectra sorgte mit seiner Cognito-Technologie dafür, dass die EDAG die Visibilität in seinem Corporate Network deutlich verbessern konnte und so Fortschritte bei der Bereinigung vor Rückfällen durch den Threat Actor abgesichert wurden. Orange Cyberdefense hat dies direkt mit Knowhow, Best-Practices und Empfehlungen unterstützt und die Koordination mit Vectra übernommen, um das bestmögliche Endergebnis für den Kunden zu erzielen.

Erbrachte Dienstleistung

- Incident Response
- Consulting
- MTD [network]

Eingesetzte Hardware

- Vectra Brain
- Vectra Sensor

Eingesetzte Software

- Vectra Cognito Detect for Network
- Vectra Cognito Detect for O365 and Azure
- Vectra Recall

Vorteile

Die EDAG hat nun eine umfassende Sicht über potenzielle Bedrohungen in ihrem Netzwerk; und das ohne invasive Eingriffe oder auszurollende Agents. Die EDAG profitiert außerdem von der umfangreichen Erfahrung eines auf diese Lösung spezialisierten SOC Teams sowie einer speziellen Threat Intelligence, welche die Ergebnisse der Vectra Instanz noch weiter verbessert und für eine noch vollständigere Sicht sorgt.

Kundenstatement

„Wir haben mit Vectra und der Plattform Cognito einen Vertrauensanker in unserem IT-Netzwerk gewonnen und die Visibilität erheblich erhöht. Uns war klar, dass wir nach dem Angriff nur dann wieder sinnvoll und sicher starten können, wenn wir in der Lage sind gefährliches Verhalten im Netzwerk schnell und präzise zu erkennen. Die automatisierte Plattform von Vectra ermöglicht uns genau das– und zwar rund um die Uhr. Unsere IT-Sicherheitsexperten können somit nun viel effizienter arbeiten“, erklärt Maria Fladung, IT Security Officer bei EDAG.

Über Orange Cyberdefense

Orange Cyberdefense ist eine Geschäftseinheit der Orange Group, welche sich der Cybersecurity widmet. Als Europas führender Anbieter für Cybersecurity ist unser Bestreben eine sichere digitale Gesellschaft aufzubauen. Wir bieten unseren Kunden Consulting, Solutions und Managed Security Services. Speziell mit unseren Managed Detection & Response und Threat Intelligence Services helfen wir unseren Kunden Bedrohungen zu erkennen, Risiken zu identifizieren und auf Vorfälle angemessen zu reagieren. Mit über 2.100 Mitarbeitern in weltweit 19 Ländern sind wir stets dort, wo unsere Kunden uns brauchen. Erfahren Sie mehr auf unserer Website.

Mehr Infos finden Sie auf
www.orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00