EV Group

Die EV Group ist ein führender Anbieter von Equipment und Prozesslösungen für die Hochvolumenfertigung von Halbleitern, MEMS, Verbundhalbleitern, Leistungsbauteilen und Nanotechnologie-Produkten. Das Unternehmen unterstützt Kunden und Partner rund um den Globus und beschäftigt über 1100 Mitarbeiterinnen und Mitarbeiter weltweit.

Auf einen Blick

- Sicherheitsteam strebte Transparenz auf Paketebene und kürzere Reaktionszeit an
- Darktrace wurde neben anderen Technologien getestet und zeigte präzise Erkennung
- EVG war von den Entscheidungen der KI überzeugt und implementierte die Autonomous Response zur Bedrohungsabwehr rund um die Uhr

„Darktrace ist anderen Lösungen bestimmt um anderthalb Jahre voraus."

Josef Buttinger, Corporate IT & Security Manager, EV Group

Transparenz auf Paketebene und KI-gestützte Erkennung

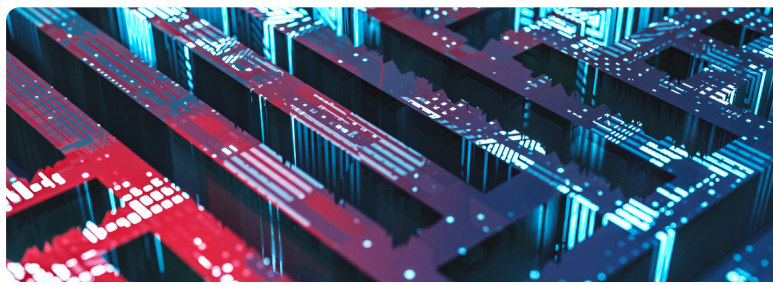
Die digitale Infrastruktur der EV Group war mit der Zeit immer komplexer geworden, daher wollte das Team seine Sicherheitsaufstellung verbessern. Die bisher von den vorhandenen Sicherheitstools genutzten protokollbasierten Analysen sollten durch eine neue Lösung ersetzt werden. Die protokollbasierte SIEM-Technologie gab einen guten Überblick des digitalen Bestands, aber aufgrund fehlender Transparenz auf Paketebene im Traffic-Layer des Netzwerks wurden Sicherheitsvorfälle nicht schnell genug erkannt und behoben.

„Es reicht einfach nicht aus, sich nur die Transaktionen anzuschauen. Vielmehr ist ein genaues Verständnis der Kommunikation zwischen den Geräten erforderlich", so Josef Buttinger, Corporate IT & Security Manager bei der EV Group. „Bei protokollbasierten Tools ist es in dem Moment, in dem wir einen gravierenden Sicherheitsvorfall entdecken, bereits zu spät."

In erster Linie wollte das Unternehmen die Zeit zwischen dem Eintritt eines Ereignisses und dessen Erkennung minimieren. „In einer idealen Welt würde diese Reaktionszeit weniger als 10 Minuten betragen", sagt Buttinger.

Das Team testete also Darktrace parallel zu anderen Tools und entschied sich letztendlich für die selbstlernende KI von Darktrace, hauptsächlich aufgrund der Genauigkeit der Erkennung. „Darktrace überhäuft uns nicht mit „falschen" Warnmeldungen, weil die Technologie genau weiß, was „normal" ist", so Buttinger über die Fähigkeit der KI, sich ein Bild von den normalen Verhaltensmustern, den „Patterns of Life", jedes Benutzers und Geräts im Unternehmen zu machen und subtile Abweichungen zu erkennen, die auf eine Bedrohung hindeuten. „Diese fortschrittliche und ausgereifte Technologie ist anderen Lösungen bestimmt um anderthalb Jahre voraus."

Darktrace hat Licht in die digitale Infrastruktur des Unternehmens gebracht und eine Reihe von Problemen aufgedeckt, von denen das Team nichts wusste. „Darktrace deckt alle Konfigurationsfehler auf, die eine Backdoor zu unserer digitalen Infrastruktur darstellen könnten. Und ich meine wirklich alle. Jedes Ereignis ist interessant, aber einige Ereignisse sind für uns besonders interessant, wenn es darum geht, etwaige Sicherheitslücken proaktiv zu identifizieren", sagt Buttinger. Die Technologie hat dem Sicherheitsteam geholfen, bei der Bereinigung der digitalen Infrastruktur strategischer vorzugehen und langfristig eine robustere Sicherheit zu gewährleisten.



Darktrace im alltäglichen Einsatz

Darktrace ist für das Sicherheitsteam der EV Group die wichtigste Technologie. Das Team lässt sich nur die Ereignisse der letzten 24 Stunden anzeigen und überprüft jede Anomalie, um am Ende des Tages auf ein sauberes Darktrace Dashboard zu blicken.

„Wenn Darktrace der Meinung ist, dass ein Ereignis genauer analysiert werden sollte, müssen wir es untersuchen. Wir vertrauen der KI-Technologie und ihrer Einschätzung“, so Buttinger. Die Warnmeldungen von Darktrace sind klar und präzise und die KI priorisiert die Sicherheitsvorfälle eigenständig nach Dringlichkeit. So bleibt das Sicherheitsteam proaktiv und motiviert. „Wenn man jeden Tag das Gleiche sieht, verliert man im digitalen Getümmel den Blick für das Wesentliche.“

> „Autonomous Response ist das Nonplusultra in der Informationssicherheit. Die Technologie kann unterschiedlichste und genau auf die Art der Bedrohung zugeschnittene Maßnahmen auslösen.“
>
> **Josef Buttinger, Corporate IT & Security Manager, EV Group**

Ausweitung auf Autonomous Response

Das erklärte Ziel der EV Group lautet operative Sicherheit rund um die Uhr. Im Moment besteht das Sicherheitsteam aber nur aus fünf Personen, sodass eine permanente Kontrolle nicht möglich ist. Da Bedrohungsakteure häufig nachts oder am Wochenende zuschlagen, musste der Sicherheitsstack mit Autonomous Response aufgerüstet werden, damit jederzeit gezielte und verhältnismäßige Maßnahmen gegen Bedrohungen ergriffen werden können.

Die Darktrace Autonomous Response basiert auf selbstlernender KI, die sich ein Bild von der digitalen Infrastruktur – jedem Benutzer und jedem Gerät – macht, dabei Hunderte Signale analysiert und mithilfe fortschrittlicher KI nur diejenigen Anomalien meldet, die einen bestimmten Schwellenwert überschreiten.

„Autonomous Response ist das Nonplusultra in der Informationssicherheit“, sagt Buttinger. „Die Technologie kann unterschiedlichste und genau auf die Art der Bedrohung zugeschnittene Maßnahmen auslösen. So schützt sie die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme. Wir haben höchstes Vertrauen in die Technologie: Eine Abweichung von den Antigena-Modellen deutet mit Sicherheit auf eine schwerwiegende Bedrohung hin.

Antigena ist an das Alarmsystem gekoppelt, das die Mitglieder des Sicherheitsteams im Ernstfall per Text-to-Speech-Benachrichtigung warnt – auch mitten in der Nacht. So kann das Team jederzeit schnell auf sich entwickelnde Cyberbedrohungen reagieren.

Die EV Group nutzt das Potenzial der Darktrace Technologie, um mit künstlicher Intelligenz im praktischen Einsatz echte alltägliche Herausforderungen zu bewältigen. Buttinger dazu: „Der Begriff KI wird inflationär verwendet, aber für mich ist Darktrace echte KI. Das System lernt wirklich eigenständig, ich habe mit den Modellen nichts zu tun. Dabei ist es unfassbar genau.“

Das Unternehmen testet gerade Autonomous Response in seiner E-Mail-Umgebung, um seine Mitarbeitenden vor raffinierten Phishing-Angriffen zu schützen.

> „Darktrace ist echte KI. Das System lernt wirklich eigenständig, ich habe mit den Modellen nichts zu tun. Dabei ist es unfassbar genau.“
>
> **Josef Buttinger, Corporate IT & Security Manager, EV Group**

Weitere Informationen

- Kostenlos testen
- Blog lesen
- Besuchen Sie unseren YouTube-Kanal