KTR Systems

Seit über fünfzig Jahren ist KTR Systems führender Hersteller von hochwertigen Antriebsbauteilen für den Maschinen- und Anlagenbau.

Auf einen Blick

- Wurde Ziel raffinierter E-Mail- Impersonation- und Spear- Phishing-Angriffe
- Begrenzte menschliche IT-Ressourcen, die rund um die Uhr Cyberangriffe abwehren müssen
- Begrenzter Einblick in globale Aktivität der Belegschaft

„Nach zwei CEO Frauds stand außer Frage, dass wir in puncto E-Mail-Sicherheit etwas unternehmen mussten."

Head of IT and Organization, KTR Systems

Gravierende Bedrohungen umgehen herkömmliche Schutzmaßnahmen

Als globales Unternehmen mit über 1.200 Mitarbeitern und 24 Niederlassungen muss KTR Systems eine vielfältige und komplexe digitale Infrastruktur schützen. Aufgrund immer mehr subtiler und raffinierter Cyberangriffe auf sämtliche Bereiche des digitalen Ökosystems brauchte das IT-Team eine neue Lösung für die Erkennung und eigenständige Abwehr dieser Bedrohungen. „Mit traditionellen Tools, die anhand historischer Daten nach Hinweisen auf eine Bedrohung suchen, hinkt man immer einen Schritt hinterher", sagt Olaf Korbanek, Head of IT and Organization bei KTR Systems. „Diese signaturbasierten Sicherheitstools können gegen neuartige Angriffe nichts ausrichten."

2019 gab es zwei Fälle von CEO Fraud in dem Unternehmen. Damit bewahrheitete sich, was man schon lange befürchtet hatte: Die traditionellen Sicherheitstools mit ihren statischen Regeln und Signaturen waren nicht in der Lage, komplexe moderne Bedrohungen zu erkennen. Nachdem er die Angriffe den Behörden gemeldet hatte, geriet sogar Korbanek selbst zu Unrecht als Hauptverdächtiger ins Visier der Justiz, denn man ging zunächst von einer Insiderbedrohung aus.

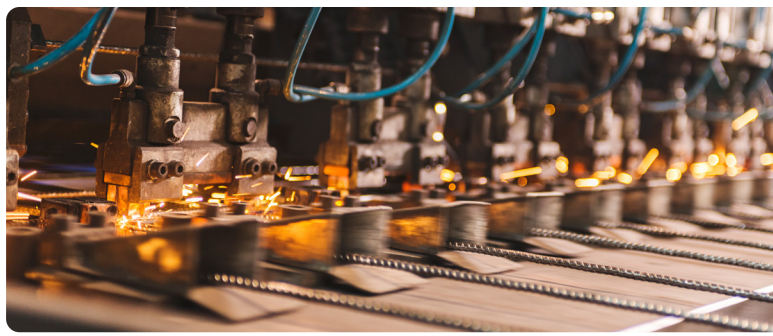
Während das Unternehmen noch mit den Folgen des CEO- Betrugs zu tun hatte, folgte schon zwei Monate später ein Ransomware-Angriffsversuch, der mit einer Phishing-E-Mail seinen Anfang nahm. Das Sicherheitsteam erkannte die Bedrohung, bevor sie Schaden anrichten konnte. Doch spätestens jetzt war klar, dass es eine robuste Lösung brauchte, um rund um die Uhr auf E-Mail-Angriffe reagieren zu können.

Eine eigenständig agierende Sicherheitslösung

KTR Systems entschied sich für das Darktrace Immune System, um sein umfangreiches digitales Ökosystem zu schützen. Mithilfe selbstlernender Cyber-KI begann Darktrace sofort, die normalen Verhaltensmuster, die sogenannten „Patterns of Life", aller Benutzer und Geräte im Unternehmen zu lernen. Die KI passt dieses Wissen kontinuierlich an sich verändernde Verhaltensweisen an und erkennt so anormale Aktivitäten, die auf eine Bedrohung hindeuten. So erkennt sie beispielsweise auch neue Malware-Stämme und subtile Insider, die mit statischen Regeln und signaturbasierten Tools unbemerkt bleiben.

„Wir brauchten eine intelligente Lösung, mit der wir unsere Prozesse automatisieren konnten."

Head of IT and Organization, KTR Systems



Die Darktrace Cyber-KI hat sich als extrem hilfreich erwiesen, weil sie dem überlasteten Sicherheitsteam des Unternehmens unter die Arme greift. Die Mitarbeiter haben jetzt mehr Zeit, sich auf strategische Aufgaben zu konzentrieren. Die offene Architektur des Darktrace Immune System ermöglicht die nahtlose Integration in separate Sicherheitstools, sodass das IT-Sicherheitsteam immer sofort gewarnt wird und mehrere Silos überblickt. „Das KI-Konzept von Darktrace würde ich jedem Unternehmen empfehlen“, so Korbanek.

> „Traditionelle Sicherheitslösungen sind für Cyberkriminelle berechenbar. Künstliche Intelligenz hilft, sich an neue Verhaltensweisen der Benutzer anzupassen.“
>
> Head of IT and Organization, KTR Systems

Abwehr eines Zero-Day-Angriffs mit KI

Wie wertvoll die Selbstlernfähigkeiten von Darktrace sind, wurde deutlich, als KTR Systems Ziel eines Zero-Day- Angriffs wurde. Kurz nachdem der Schutz durch die Cyber-KI mit Antigena Email auf die E-Mail-Umgebung ausgeweitet worden war, wurde KTR Systems Ziel eines Cyberangriffs mit extrem schneller Ausbreitung. Mithilfe der Autonomous Response-Technologie erkannte und stoppte Antigena Email die Bedrohung sofort durch gezielte Maßnahmen.

„Auch in dieser Situation hat sich Darktrace bewährt – alle verdächtigen Aktivitäten wurden gestoppt und Schlimmeres wurde verhindert.“ Antigena Email versteht den Menschen an der Tastatur und analysiert E-Mails im Kontext. Die Technologie macht sich ein nuanciertes Bild der Kommunikation im Unternehmen und passt dieses fortwährend an. Sie erkennt subtile Abweichungen, die auf eine Cyberbedrohung hindeuten und von traditionellen Tools übersehen werden. Antigena Email ergreift eigenständig und in Echtzeit Maßnahmen, ohne den Geschäftsbetrieb zu stören.

Auf die Darktrace Cyber-KI kann sich KTR Systems verlassen: Sie gewährleistet rund um die Uhr durchgängige Transparenz und eigenständigen Schutz für das umfangreiche digitale Ökosystem des Unternehmens.

> „Das KI-Konzept von Darktrace würde ich jedem Unternehmen empfehlen.“
>
> Head of IT and Organization, KTR Systems

Die Benutzeroberfläche von Darktrace, der Threat Visualizer, liefert Echtzeit- Einblicke in das gesamte digitale Ökosystem

Weitere Informationen

- Kostenlos testen
- Lesen Sie das Whitepaper zum Darktrace Immune System
- KTR Video Fallstudie ansehen