Breitenfeld

Die Breitenfeld Edelstahl AG ist ein österreichischer Edelstahlhersteller. Das Unternehmen wurde 1942 gegründet und beschäftigt über 320 Mitarbeitende, die Kunden in Branchen wie der Erzeugung erneuerbarer Energie, Petrochemie (Öl und Gas), Werkzeugbau, Maschinenbau, Transportwesen/Rennsport, Luft- und Raumfahrt, Schiffsbau und Hochdrucktechnik unterstützen.

Auf einen Blick

- Erkannte, dass die zunehmende Digitalisierung der Infrastruktur neue Cybersicherheitsrisiken mit sich bringt
- Implementierte Darktrace in der gesamten digitalen Infrastruktur
- Vertraut auf Erkennung und Entscheidungen durch die KI; nimmt jetzt Upgrade auf Autonomous Response vor

„Vor Darktrace war der Netzwerk-Traffic praktisch ein schwarzes Loch. Jetzt ist alles komplett transparent und das SOC hat zusätzlich ein Auge darauf."

Simon Pucher, Head of IT, Breitenfeld

Neue Herausforderungen im Fertigungssektor

In den letzten Jahren hat Breitenfeld den Nutzen umfassender Digitalisierung erkannt, ebenso wie die erhöhten Cybersicherheitsrisiken, die unweigerlich mit diesem Wandel einhergehen. „Der Digitalisierungsbedarf in der Produktion nimmt immer mehr zu, genauso wie das Risiko von Produktionsausfällen durch Ransomware oder andere Angriffe", sagt Simon Pucher, Head of IT bei Breitenfeld.

Um die Integrität und Verfügbarkeit seiner Systeme zu bewahren, die Qualität sicherzustellen und die Produktivität aufrechtzuerhalten, musste das Unternehmen seine Produktionssysteme vor Cyberstörungen schützen. Die selbstlernende KI von Darktrace unterstützt das Unternehmen bei seinem Bemühen um mehr Transparenz und der Erkennung komplexester Bedrohungen. So wie das menschliche Immunsystem macht sich Darktrace nach und nach ein Bild von den normalen Verhaltensmustern, den „Patterns of Life", des gesamten Ökosystems und erkennt subtile Abweichungen, die auf eine Bedrohung hindeuten.

Schutz durch selbstlernende KI

Breitenfeld war eines der ersten Unternehmen, die auf KI-gestützte Cyberabwehr setzten, und testete 2017 das Darktrace Industrial Immune System. Nach dem Proof of Value (POV) entschied sich das Unternehmen sofort für Darktrace. „Die Einrichtung des POV ging extrem schnell und reibungslos vonstatten. Schon nach wenigen Stunden sahen wir erste Ergebnisse", so Pucher. Breitenfeld hat erkannt, dass man ultraschnellen Angriffen nur mit ultraschneller Abwehr begegnen kann. „KI kämpft gegen KI", so Pucher. „Schon heute sehen wir, dass die meisten Angriffe voll automatisiert sind, deshalb muss auch die Abwehr voll automatisiert sein."

Als 2020 die Vertragsverlängerung anstand, führte Breitenfeld eine umfassende Evaluierung seiner Sicherheitsprodukte durch und zog andere Systeme wie QRadar, Zeek, Corelight, Empow, Vector, Stealthwatch und ExtraHop in Betracht. Laut Pucher

gaben „die große Zufriedenheit mit Darktrace, der exzellente Kundensupport sowie der Benutzerkomfort“ den Ausschlag für die Vertragsverlängerung.

Die Technologie von Darktrace basiert auf selbstlernender KI und lernt im Einsatz. So kann das Unternehmen Bedrohungen frühzeitig erkennen, ohne auf Regeln, Signaturen oder Annahmen angewiesen zu sein. Dank der Warnmeldungen von Darktrace registriert Breitenfeld ungewöhnliche Aktivitäten, bevor diese zum Problem werden.

> „Schon heute sehen wir, dass die meisten Angriffe voll automatisiert sind, deshalb muss auch die Abwehr voll automatisiert sein.“
>
> **Simon Pucher, Head of IT, Breitenfeld**

Transparenz im gesamten Ökosystem

Darktrace hatte sich schon früher als sehr hilfreich erwiesen und Breitenfeld eine deutlich verbesserte Transparenz geliefert. Als etwa nach einem Antivirus-Update Probleme auftraten, erhielt Breitenfeld dank dem Darktrace Threat Visualizer Einblicke in die gesamte digitale Infrastruktur und den Kontext des Problems.

„Wir hatten das Antivirus-Update auf allen Clients aktiviert, was zur Folge hatte, dass die TLS-Protokolle teilweise deaktiviert wurden. Wir erkannten sofort eine Zunahme von TLS-Verbindungsproblemen in der Erweiterten Suche und konnten das Problem binnen Minuten lösen, bevor das Update auf alle Clients ausgerollt wurde. Das verhinderte zudem eine Sperrung des Netzwerks und damit Störungen bei unseren internen Kunden“, so Pucher.

Breitenfeld hat seine digitale Infrastruktur jetzt komplett im Blick! Darktrace brachte Licht in das gesamte digitale Ökosystem des Unternehmens und analysierte Daten sämtlicher Benutzer und Geräte sowie deren komplexe Beziehungen untereinander.

„Vor Darktrace war der Netzwerk-Traffic praktisch ein schwarzes Loch. Im Grunde wusste niemand, wer wann und wo Zugriff hatte. Jetzt ist alles komplett transparent und das SOC hat zusätzlich ein Auge darauf“, so Pucher. „Sicherheit lässt sich nur mit vollem Durchblick optimieren. Dafür brauchen wir Transparenz auf Paketebene. Dank der Darktrace KI ist bei uns alles transparent und es gibt kaum Warnmeldungen.“

Nachdem sich Breitenfeld von der Effizienz und Genauigkeit der selbstlernenden KI überzeugt hatte, entschied sich das Unternehmen für ein Upgrade auf Antigena. Die Autonomous-Response-Technologie von Darktrace neutralisiert schnelle und unberechenbare Angriffe binnen Sekunden, ohne den normalen Geschäftsbetrieb zu stören. Pucher erklärt: „Wir haben mit dem System gearbeitet und wissen jetzt, dass alles passt. Die Aktivierung von Antigena war der nächste logische Schritt.“

> „Das POV-Setup ging extrem schnell und reibungslos vonstatten. Schon nach wenigen Stunden sahen wir erste Ergebnisse.“
>
> **Simon Pucher, Head of IT, Breitenfeld**