Branchenfokus 2021: Produktion

Da Bedrohungen für OT-Umgebungen immer komplexer werden und Lieferketten zunehmend unter Druck stehen, ist ein ganzheitlicher Sicherheitsansatz für IT- und OT-Umgebungen wichtiger denn je.

Auf einen Blick

- ✔ Protokoll- und technologieunabhängig, keine festen Regeln
- ✔ Ganzheitlicher Schutz für IT-, OT- und IoT-Umgebungen
- ✔ Erkennt neuartige Bedrohungen in Echtzeit, sobald sie auftauchen
- ✔ Versteht die gesamte Kommunikation innerhalb einer Umgebung, von ständigem PLC-Datenverkehr bis hin zu verteilten IIoT-Sensor-Grids

Eine neue Ära von OT-Angriffen

Im Juni 2020 griff der neuartige Ransomware-Stamm EKANS mehrere Produktionsstätten von Honda weltweit an. Dieser Angriff löste einen Herstellungsstopp in mehreren Ländern aus, der dramatische Verluste aufgrund ausgefallener Produktionsstunden und Personalkosten verursachte – ganz zu schweigen von den Kosten für die Wiederherstellung der Systeme, ohne den Lösegeldforderungen nachzugeben.

Das Besondere an diesem Angriff: EKANS zielt direkt auf ICS-Schwachstellen, anstatt ungepatchte IT-Software als Einfallstor zu nutzen. EKANS greift mit seiner Kill Chain 64 spezifische ICS-Mechanismen an und erfordert neue Verteidigungsstrategien bei der Bekämpfung von OT-Cyberangriffen.

Darüber hinaus stehen Hersteller mehr denn je unter Druck, die globale Nachfrage zu erfüllen und die weltweiten Lieferketten aufrechtzuerhalten – die Sicherheit von OT-Technologie wird zu einer wichtigen Priorität. Im Frühling 2020 mussten viele Hersteller von einem Tag auf den anderen ihre Produktion umstellen und Güter herstellen, die sie nie zuvor produziert hatten. Sie mussten ihre Fertigungslinien überholen und neue Technologien implementieren – und viele dieser einschneidenden Veränderungen bleiben langfristig bestehen.

> „Vor zehn Jahren war Cybersicherheit nur eine Firewall. In der heutigen Welt mit 5G und Remote-Arbeit sind Unternehmen viel angreifbarer. Hier kommt Darktrace ins Spiel."
>
> Frédéric Carricaburu, CIO, Saniflo

> „Der Cyber AI Analyst von Darktrace setzt neue Standards in der Cyberabwehr, weil die Teams nicht mehr auf einen Monitor starren müssen, sondern sich ihren eigentlichen Aufgaben widmen können. Außerdem verkürzt sich die Zeit für die Auswertung von Vorfällen."
>
> Laura Tibodeau, CIO, AmSty

Ein Immunsystem für die Fertigungsindustrie

Das Industrial Immune System von Darktrace nutzt KI-basierte Technologie, um die geschäftskritischen und komplexen cyber-physischen Umgebungen hunderter Hersteller weltweit zu schützen. Die Immune System-Technologie von Darktrace deckt alle verteilten vernetzten Maschinen, Konfigurationen und Umgebungen ab. Dank nicht überwachtem und überwachtem maschinellem Lernen ist die Darktrace KI nicht auf ein bestimmtes digitales Format beschränkt, sondern lernt selbstständig, schnell und umfassend.

Das Industrial Immune System von Darktrace ist an das menschliche Immunsystem angelehnt und lernt das Verhalten vernetzter cyber-physischer Geräte und operativer Technologie sowie der Nutzer und IT-Systeme in einer breiten cyber-physischen digitalen Infrastruktur.

Die Darktrace KI entwickelt ein Verhaltensmuster, das „Pattern of Life“, indem sie digitale Informationen „bei der Arbeit“ erfasst – ohne zusätzliches Anlernen oder Hinzufügen von Datenbeständen. Aus diesem Grund kann Darktrace bedrohliche Aktivitäten sofort in Echtzeit erkennen, ganz gleich, wo sie stattfinden – sei es in der Fabrikhalle oder im Posteingang eines Mitarbeiters.

Geistiges Eigentum im Visier hochentwickelter Malware – Hersteller von Medizintechnik

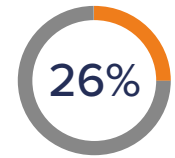
Bei einem europäischen Hersteller von Medizintechnik erhielt eine Sachbearbeiterin eine gezielte Phishing-E-Mail, die eine Zahlung betraf. An die Nachricht war eine Rechnung angehängt. Sie glaubte, der Anhang sei legitim, klickte ihn an und lud unwissentlich schnell agierende Malware herunter, die alle anderen Sicherheitsmechanismen umgangen hatte.

Angriffsziel der heimtückischen Malware war das geistige Eigentum des Unternehmens, zu dem auch streng vertrauliche medizinische Zusammensetzungen gehörten. Wären diese Unternehmenswerte kompromittiert worden, wären die Wettbewerbsfähigkeit und der Ruf des Unternehmens in Gefahr gewesen.

Nachdem die Malware heruntergeladen wurde, begann das Gerät blitzschnell, sich mit einem ungewöhnlichen externen Ziel zu verbinden, und versuchte, auch in andere Umgebungen einzudringen. Innerhalb von nur zwei Sekunden hatte die Darktrace KI den Eindringling erkannt.

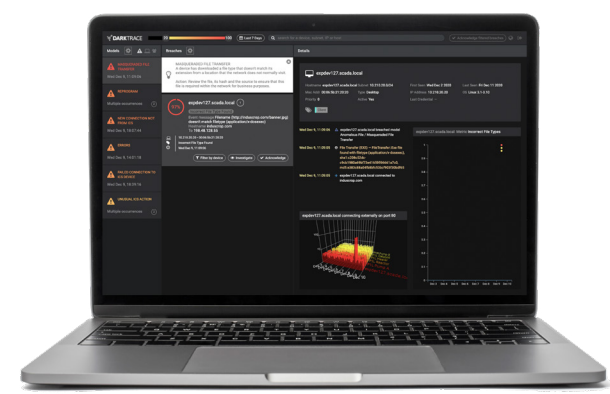
> „Maschinelles Lernen erkennt Dinge, die wir selbst nicht vorhersagen und definieren können. Das ist wie die Suche nach der Nadel im Heuhaufen.“
>
> Stuart Berman, Information Security Architect, Steelcase

Produktionssicherheit in Zahlen



der Unternehmen haben keine Abteilung, die die Sicherheit von Fabrikmanagementsystemen überwacht.

Darktrace erkannte im Sommer 2020 über 6.500 verdächtige Vorfälle bei der ICS-Protokollnutzung in 1.000 Umgebungen in IT-Netzwerken seiner Kunden.



Das OT Engineer Dashboard von Darktrace zeigt nur die betriebsrelevantesten Alarme an