DARKTRACE INDUSTRIAL

BRANCHENFOKUS

Cyberabwehr für die Öl- und Gasindustrie

In den letzten Jahren ist die Digitalisierung der Prozesse in der Öl- und Gasindustrie in schnellem Tempo vorangeschritten. Diese Entwicklung bringt nicht nur immense Vorteile wie höhere Effizienz und Agilität mit sich, sondern hat auch das Sicherheitsparadigma grundlegend verändert. Öl- und Gasunternehmen müssen heute vernetzte Feldgeräte, Sensoren und Steuerungssysteme ebenso wie bestehende Altsysteme – häufig in anspruchsvollen entfernten Umgebungen mit niedriger Bandbreite – schützen.

> Da die operative Technologie (OT) und die Informationstechnologie (IT) immer mehr zusammenwachsen, muss sich die Branche nicht mehr nur mit traditionellen Cyberbedrohungen auseinandersetzen, sondern auch mit neuartigen Angriffen auf Industrieumgebungen.

Diese gemischten cyber-physischen Umgebungen stellen die ohnehin schon überlasteten Sicherheitsteams vor enorme Herausforderungen. Veraltete Lösungen für den Schutz von IT-Netzwerken sind hierfür nicht geeignet – sie schaffen es nicht, diese komplexen hybriden Umgebungen vor den sich ständig wandelnden Feinden zu schützen.

> Darktrace vermittelt Kunden umsetzbare Einblicke und Erkenntnisse, damit diese Bedrohungen schneller erkannt und kritische Anlagen vor schädlichen und kostspieligen Angriffen geschützt werden können.
>
> **Aymeric Sarrazin, Senior Vice-President Siemens**

Big West Oil LLC

DOLPHIN ENERGY دولفين للطاقة

Bedrohungen in Zahlen

68% der Öl- und Gasunternehmen wurden 2016-17 kompromittiert

Dem Ponemon Institute zufolge waren 68 % der Unternehmen aus dieser Branche mindestens einmal Ziel einer Cyber-Sicherheitskompromittierung. Zu den größten Sicherheitslücken gehören veraltete und nicht mehr zeitgemäße Steuerungssysteme für die einzelnen Phasen, von der Exploration und Förderung bis hin zu Raffinerie und Distribution. Diese Systeme wurden oft lange, bevor Cybersicherheit zur geschäftlichen Priorität erklärt wurde, implementiert und es ist sehr schwer, Patches zu installieren. So bleiben Sicherheitslücken in der Infrastruktur und Unternehmen sind böswilligen Angreifern ausgeliefert.

46% der Cyberangriffe in OT-Umgebungen bleiben unentdeckt

Das Ponemon Institute fand auch heraus, dass durchschnittlich 46 % aller Cyberangriffe in OT-Umgebungen unentdeckt bleiben. Der Öl- und Gasprozess setzt sich aus vielen verschiedenen Elementen zusammen und eine Vielzahl von Steuerungssystemen spielen zusammen, sodass Einblicke in die verteilte Infrastruktur und entlegene Standorte nur schwer möglich sind. Durch diese mangelnde Transparenz können sich Angreifer für längere Zeit in OT-Umgebungen einnisten und sich ein genaues Bild von dem Netzwerk machen, bevor sie dann zuschlagen.

29% der Öl- und Gasunternehmen haben keinen Echtzeiteinblick in Cyberbedrohungen

Um die Netzwerke von Öl- und Gasunternehmen richtig schützen zu können, ist eine Bedrohungserkennung in Echtzeit unerlässlich. Nur wenn Angriffe frühzeitig erkannt werden, können sie abgewehrt werden, bevor die operative Effizienz in OT-Umgebungen kompromittiert wird. Öl- und Gasunternehmen, die ihre OT-Netzwerke noch mit traditionellen Sicherheitssystemen schützen, brauchen innovative, selbstlernende Technologien, um sich in der sich ständig verändernden Bedrohungslandschaft behaupten zu können.

Darktrace Industrial

Einige der größten Öl- und Gasunternehmen weltweit vertrauen beim Schutz komplexer Industrieumgebungen vor Cyberbedrohungen auf Darktrace Industrial. Ganz gleich, ob Upstream, Midstream oder Downstream, Darktrace Industrial schützt in Industrieumgebungen in jeder Phase die Förderung und den Transport von Öl und Gas.

Die Software von Darktrace ist die weltweit führende Cyber-KI-Technologie, die in Echtzeit ein „Immunsystem" für OT- und IT-Umgebungen aufbaut, um vernetzte Geräte vor dem gesamten Spektrum an Cyberbedrohungen zu schützen – von ultraschneller Ransomware bis hin zu verborgenen Cyberkampagnen, die ungesehen in Netzwerken lauern.

Darktrace nutzt künstliche Intelligenz, um die Verhaltensmuster jedes Controllers und jeder Workstation im Steuerungsnetzwerk sowie jedes Benutzers und Geräts im Unternehmensnetzwerk zu lernen und sich nach und nach ein Bild von der normalen Funktionsweise der gesamten Umgebung zu machen. So ist Darktrace Industrial in der Lage, die ersten Anzeichen einer sich entwickelnden Bedrohung zu erkennen – und das ganz ohne Regeln, Signaturen oder Annahmen.

> Die bahnbrechende selbst lernende Technologie von Darktrace Industrial verändert grundlegend die Art und Weise, wie Industrieumgebungen geschützt werden, ohne Unterscheidung zwischen OT, IT oder IoT.

Darktrace Industrial ist mit den vielfältigen und schwierigen Umgebungen vertraut, in denen Öl- und Gasunternehmen tätig sind, und kommt durch den Einsatz besonders robuster industrieller Analysegeräte auch mit entfernten Umgebungen mit niedriger Bandbreite zurecht. Remote-Installationen an Bohranlagen können die lokale Modellierung und Analyse sowie die zentrale Erfassung der Zusammenhänge für die sicherheitsrelevante Überwachung sämtlicher Anlagen beinhalten.

Darktrace Industrial in Aktion

Verdächtige Downloads und Serpent Ransomware-Infektion

Bei einer integrierten Ölraffinerie, die gleichzeitig Lieferant ist, erkannte Darktrace Industrial erste Hinweise auf eine Ransomware-Infektion im Netzwerk des Unternehmens. Ein Desktop-Gerät schrieb nicht nur seine eigenen Dateien mit Lösegeldforderungen, sondern baute zudem über einen internen Proxyserver Verbindungen zu ungewöhnlichen externen Zielen auf und lud dann schädliche Dateien herunter.

Das Gerät nahm eine Reihe von SMB-Verzeichnisabfragen vor, wodurch das Spektrum der anormalen Verhaltensweisen noch größer wurde. Da Darktrace Industrial die Ransomware bereits identifiziert hatte, konnte die Technologie diese Aktivität sofort mit der Serpent-Infektion in Verbindung bringen.

Darktrace Industrial informierte das Sicherheitsteam über das eindeutig zuzuordnende Verhaltensmuster, bevor die Infektion auf die OT-Umgebung übergreifen konnte.

Erkannte Auskundschaftung durch ein auf der Blacklist stehendes externes Gerät

Bei einem US-amerikanischen Öl- und Gasförderunternehmen wurde interne Auskundschaftung aufgespürt. Ein externes Gerät, das auf der Blacklist stand und eine IP-Adresse in China hatte, baute VPN-Verbindungen zu verschiedenen kritischen Elementen in der Netzwerkinfrastruktur auf. Das Gerät baute kurzzeitig eine Verbindung zum Domain-Controller auf und verband sich dann mit dem Computer eines Mitarbeiters und dem E-Mail-Server, um sich Zugang über drei verschiedene Eintrittspforten zu verschaffen. Das Gerät prüfte sogar, ob ein Honeypot vorhanden ist, und nahm dafür in Kauf, entdeckt zu werden.

Darktrace Industrial erkannte diesen schädlichen Auskundschaftungsversuch frühzeitig und gab dem Sicherheitsteam so die Möglichkeit, geeignete Schutzmaßnahmen zu ergreifen, damit das Unternehmen nicht kompromittiert wurde.

Kontakt

Nordamerika: +1 415 229 9100
Europa: +44 (0) 1223 394 100
Asien/Pazifik: +65 6804 5010
Lateinamerika: +55 11 97 242 2011

info@darktraceindustrial.com
darktrace.com/industrial