VECTRA
SECURITY THAT THINKS®

SOLUTION BRIEF

How the Cognito platform protects the oil and gas sector from cyberthreats

Energy companies are increasingly vulnerable to cyberthreats. This industry holds a wide variety of proprietary information, such as exploration and production technologies, trade strategies, financial holdings, as well as a trove of consumer and business data. This makes them attractive targets to cyberthreat actors.

Oil and gas companies are also quickly digitalizing. Industrial-internet-of-things (IIoT) systems, critical operational technology, and industrial control systems (ICS) – such as control valves, pressure monitors and other equipment – are all connected. These systems typically connect to wireless networks and are vital to daily operations.

Digitalization simplifies management, but it can also increase security risk. Connected systems expand the attack surface and provide opportunities for lateral movement after the initial compromise. In fact, according to the 2019 Cyber Threatscape Report from Accenture, two-thirds of oil and gas IT managers say digitalization has made them more vulnerable to security compromises.

Facing constant threats

In 2018, a cyberattack on a shared data network forced four U.S. natural-gas pipeline operators to temporarily shut down communications with customers. The attack came shortly after the U.S. Department of Homeland Security reported that Russian hackers had gained access to control rooms of U.S. electric utilities. This gave the attackers direct access to U.S. critical infrastructure.

Two-thirds of oil and gas IT managers say digitalization has made them more vulnerable to security compromises.

2019 Cyber Threatscape Report
Accenture

KEY HIGHLIGHTS

- With a large number of entry points along the value chain, the rise of IIoT – and the high security and financial impact a cyber incident could inflict – the oil and gas industry continues to attract hackers of all kinds.
- Vectra and its flagship Cognito® platform provide continuous, automated threat surveillance to proactively expose hidden cyberattacks inside the network.
- Cognito integrates with leading firewall, endpoint detection and response, SIEM, NAC, virtualization platform, traffic optimization, and security orchestration solutions.
- Cognito platform from Vectra enables security teams to respond with unprecedented speed, accuracy and efficiency to detect and mitigate threats before they cause damage.

These attacks are not isolated to the United States. In 2017, the Industroyer (CrashOverride) malware and NotPetya ransomware attacks compromised electric power grids in Ukraine.

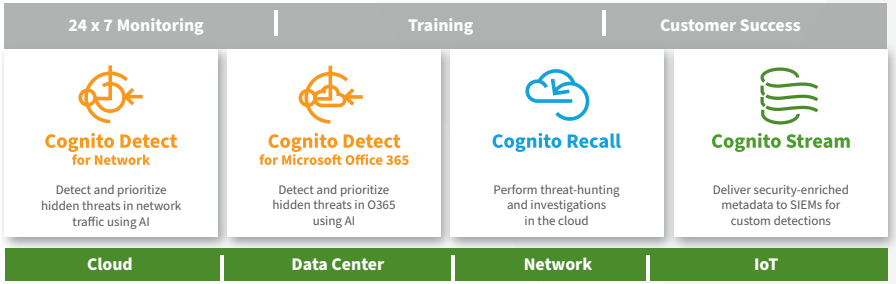
Nation-state threat groups like the Russian BLACK GHOST KNIFEFISH group (aka Dragonfly) regularly target oil, natural gas and energy production firms. The goals of these attacks range from reconnaissance and testing security response to disrupting operations.

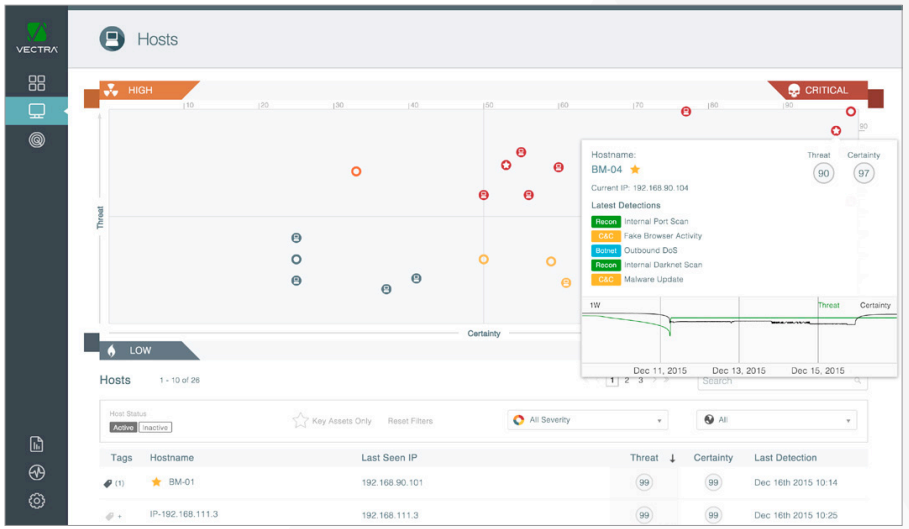
Along with nation-state adversaries, the oil and gas sector also attracts hacktivists seeking to promote a political, religious or ideological agenda. With a large number of entry points along the value chain, the rise of IIoT – and the high security and financial impact a cyber incident could inflict – the oil and gas industry continues to attract hackers of all kinds.

Protecting OT begins with IT

The oil and gas industry has been at the forefront of converging operational technology and information technology. In fact, it has been working towards a unified network for quite some time.

And although an IT worker may not repair oil drills, the entire organization uses much of the underlying technologies, such as sensors and analytics. This means using predictive analytics to protect the corporate network from cyberthreats also protects the production network.





Cognito automatically correlates threats with host devices under attack. It presents security operations teams with a real-time view of the highest risk threats and a trail of forensic evidence to launch conclusive incident investigations.

AI-driven network protection for the IT environment

Security teams need a network detection and response (NDR) solution that streamlines operations. An ideal solution condenses vast amounts of security-related data down to simple, actionable information.

Instead of creating extra work, this reduces the security operations center workload and allows security teams to focus on stopping attacks in progress. By surfacing all devices involved in an attack, NDR empowers security teams to respond rapidly to threats before damage is done.

This requires an NDR solution that is comprehensive, easy to deploy and automates real-time threat detection and reporting. And it should add value from day one.

Vectra® is the world leader in applying artificial intelligence to detect and respond to cyberattacks in real time. Vectra and its flagship Cognito® platform provide continuous, automated threat surveillance to proactively expose hidden cyberattacks inside the network. Cognito monitors and analyzes all network traffic – from cloud and data center workloads to user and IIoT devices.

Leveraging artificial intelligence that uniquely combines data science, advanced machine learning and behavioral analysis, Cognito detects all phases of an attack. This includes command-and-control communication, internal reconnaissance, lateral movement, data exfiltration, and botnet monetization.

As a critical part of a well-coordinated security ecosystem, Cognito integrates with leading firewall, endpoint detection and response, SIEM, NAC, virtualization platform, traffic optimization, and security orchestration solutions.

For more information please contact a service representative at info@vectra.ai.

Cognito Sidekick service

Vectra also offers the Cognito Sidekick service, a subscription program that gives organizations access to a dedicated team of Vectra security analysts. This specialized team delivers custom, prioritized recommendations to enhance overall security posture.

Security that thinks®

Oil and gas organizations will continue to be a top target of cyberattacks. Fortunately, the Cognito platform from Vectra enables security teams to respond with unprecedented speed, accuracy and efficiency to detect and mitigate threats before they cause damage.

With automated, real-time cyberattack detection and AI-assisted threat hunting, the Cognito platform allows security teams to conduct conclusive incident investigations. The combination of people and AI can find and stop threats faster, protecting energy companies from security threats and business disruption.

Vectra and its flagship Cognito® platform provide continuous, automated threat surveillance to proactively expose hidden cyberattacks inside the network.

Email info@vectra.ai vectra.ai

© 2020 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.
Version **110520**