DARKTRACE INDUSTRIAL

Cyber Defense for Oil & Gas

In recent years, the oil and gas industry has seen accelerated digitization of its operations. As the sector reaps tremendous benefits such as greater efficiency and increased agility, this move has also fundamentally shifted the security paradigm. Oil and gas companies must now protect connected field devices, sensors and control systems, as well as legacy systems, often in low-bandwidth, remote, and challenging environments.

> As Operational Technology (OT) and Information Technology (IT) converge, the industry faces both traditional cyber-threats and novel attacks against industrial environments.

These mixed cyber-physical environments present a unique set of challenges for strained security teams. Legacy solutions for protecting IT networks are not fit for purpose: they fall short at defending these complex hybrid environments against an ever-changing adversary.

> Darktrace will give customers actionable insights and intelligence to be faster in identifying and neutralizing those threats, protecting critical assets from harmful and costly attacks.
>
> **Aymeric Sarrazin, Senior Vice-President**
> **Siemens**

Big West Oil LLC

DOLPHIN ENERGY دولفين للطاقة

Threats by Numbers

68% of oil and gas companies experienced a compromise in 2016-17

According to the Ponemon Institute, 68% of companies in this sector have experienced at least one cyber security compromise. One of the biggest vulnerabilities is outdated and aging control systems, which are relied on at every stage from exploration and production, to refining and distribution. Often created long before cyber security was considered a business priority, these systems are much more difficult to patch, leaving weaknesses in infrastructure security and companies exposed to malicious attackers.

46% of cyber-attacks in OT environments go undetected

The Ponemon Institute also reported that an average of 46% of all cyber-attacks in the OT environment go undetected. With so many different elements to the oil and gas process, and a whole host of control systems working in tandem, visibility across distributed infrastructure and remote sites is incredibly hard to achieve. Yet, this lack of visibility means that attackers can lie low in OT environments for long periods of time, building a thorough understanding of the network before striking.

29% of oil and gas companies have no real-time insight into cyber-threats

In order to adequately protect the networks that oil and gas companies rely on, real-time threat detection is paramount. Early detection is key to stopping threats in their tracks, defending OT environments before operational efficiency is compromised. Given the traditional security stack of OT networks, oil and gas companies need to deploy innovative, self-learning technologies to defend against a constantly-changing threat landscape.

Darktrace Industrial

Relied on by some of the largest oil and gas companies around the world, Darktrace Industrial defends complex industrial environments against cyber-threat. Whether upstream, midstream, or downstream, Darktrace Industrial can be deployed in industrial environments at every stage of operations, to protect oil and gas production and transportation.

Darktrace Industrial is the world's leading cyber AI technology that implements a real-time 'immune system' for both OT and IT environments, to defend networked devices across the entire spectrum of cyber-threat - from machine-speed ransomware to silent and stealthy cyber-campaigns that lie low in networks.

Powered by enterprise-grade artificial intelligence, Darktrace Industrial learns the 'pattern of life' for every controller and workstation on the control network, and every user and device on the corporate network, developing a rich understanding of 'self' for the entire environment. This evolving understanding of 'normal' enables Darktrace Industrial to detect the earliest indicators of an emerging threat, without relying on rules, signatures, or prior assumptions.

> Darktrace Industrial's unique, self-learning technology represents a step-change in defending industrial environments, allowing the protection of unique environments without distinguishing between OT, IT, or IoT devices.

Recognizing the diverse and difficult environments that oil and gas companies operate in, Darktrace Industrial can also support low-bandwidth and remote environments through the use of ruggedized industrial probes. Remote deployments on rigs can include local modeling and analysis, as well as central correlation for security monitoring of all assets.

Darktrace Industrial in Action

Suspicious downloads and Serpent ransomware infection

At an integrated oil refiner and supplier, Darktrace Industrial identified the first signs of a ransomware infection in the company's network. As well as writing its own ransom note files, a desktop device was found to be making a series of connections to rare external destinations, via an internal proxy server, and then downloading malicious files.

The device proceeded to make a number of SMB directory queries, amplifying the anomalous series of actions. Having identified ransomware before, Darktrace Industrial was able to recognize that this activity closely matched the pattern of behavior for the Serpent infection.

Darktrace Industrial alerted the security team to the incriminating pattern of behavior before the infection was able to spread into the OT environment.

Reconnaissance detected from blacklisted external device

Internal reconnaissance was detected at the heart of a US oil and gas production company. An external blacklisted device with an IP address in China was discovered connecting to several key elements of the network infrastructure, using a VPN. After briefly connecting to the domain controller, it then connected to an employee's computer and the mail server, attempting to gain access via three different entry points. The device even went so far as to test for the presence of a honeypot, which may have drawn attention to its presence.

Darktrace Industrial detected this malicious exploration attempt in its earliest stages, giving the security team the ability to reinforce its defenses and ensure no compromises occurred.

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100
Asia Pacific: +65 6804 5010
Latin America: +55 11 97 242 2011

info@darktrace.com
darktrace.com/industrial