DARKTRACE

INDUSTRY SPOTLIGHT

Cyber Defense for Energy & Utilities

Cyber security has been a high priority for the energy and utilities sector for years. Complex industrial control systems and geographically distributed internal networks are crucial to modern energy generation and distribution, but the exposure of such systems often introduces significant risks.

Nation-state attacks remain a key concern for the energy and utilities sector. The threat landscape has also ramified in unexpected ways, meaning that a whole range of possible attackers must be considered – from industrialized crime units, to ideologically driven hacktivists hoping to force costly downtime periods or expose their targets to public scrutiny.

In today's sophisticated threat landscape, attackers are taking aim at power grids, attempting to dismantle critical infrastructure, and conducting extensive sabotage campaigns. When targeting energy and utilities companies, they have a number of unique vulnerabilities to exploit, which can, in some cases, cause catastrophic damage to physical infrastructure and have significant unexpected consequences downstream of the attack.

Additionally, devices from third-party suppliers are often internet-facing or accidentally connected to the corporate network. As the Industrial Internet of Things (IIoT) becomes increasingly pervasive, it will be a constant challenge to keep track of every device on the network and make sure they are appropriately secured.

Using cutting-edge machine learning and AI algorithms, Darktrace learns the 'pattern of life' for both OT and IT environments, creating a comprehensive and seamless picture of the entire enterprise in all of its unique complexity. With the threat landscape evolving rapidly, many of the world's leading energy and utilities companies rely on Darktrace to keep pace with emerging anomalies and incidents as they arise within their systems.

> "Darktrace makes everything simple. It is invaluable to us to know exactly what is happening on our network, as it happens."
>
> **Patrick Conreaux, CISO, Apave**

Threats By Numbers

Critical infrastructure cyber-attacks increased **20%**

According to the Department of Homeland Security, cyber incidents against critical infrastructure rose 20% from 2014 to 2015. This trend is expected to continue as governments pour more resources into cyber warfare and criminals re-purpose malware devised by state-sponsored hacking cells.

75% of companies in oil, gas, and electricity reported a cyber-attack in 2016

Intruders were able to bypass firewalls, antivirus programs, or other forms of protection. 80% of those companies also said that they expect an attack will harm physical infrastructure in 2017.

DARKTRACE

CASE STUDY

Drax

Background

Drax is a leading power infrastructure company, providing around 7% of the UK's electricity. It is in the process of switching to the use of biomass generators and is considered one of the most forward-looking organizations in the energy and utilities industry.

Challenge

The energy sector faces a rapidly evolving threat landscape, in which increasingly sophisticated attackers have been successful in undermining network boundaries and infiltrating extremely sensitive operational systems. The stakes in this field could not be higher, with major implications for the safety and integrity of national critical infrastructure. As a vital part of the UK's power network, Drax needed to be able to identify emerging threats and intervene early in order to protect its data and systems.

> Darktrace has identified threats with the potential to disrupt our networks.
>
> **Martin Sloan, Group Head of Security, Drax**

Solution

Drax decided to implement an 'immune system' approach, because it needed to be able to respond to novel threats that had not been previously identified by other security tools. The company selected Darktrace's advanced cyber AI platform in order to benefit from a self-learning system that forms an adaptive understanding of normality and abnormality within its data systems.

After successfully implementing the Enterprise Immune System on its corporate network, Drax extended the coverage to defending its critical Industrial Control System from attack. By deploying the Industrial Immune System alongside the Enterprise Immune System, Drax gained overall visibility of both IT and OT environments in a single pane of glass.

Darktrace has quickly become a fundamental part of Drax's cyber security strategy, due to its unique probabilistic approach and ability to detect emerging threats. "Darktrace's technology adds another level of sophistication to our defense systems, and has already identified threats with the potential to disrupt our networks," commented Martin Sloan, Group Head of Security at Drax. "It helps us stay ahead of emerging threats and better defend our key system", Sloan added.