DARKTRACE

Drax

Overview

Industry

- Energy and utilities

Challenge

- Complex and sophisticated threat landscape
- Key target industry for advanced cyber attackers
- Large volumes of data but not enough insight
- Too many false positives
- Insider threat
- Too much reactive, not enough proactive measures

Results

- Self-learning approach
- Probabilistic assessment of risk
- Understanding of human behaviors
- Next-generation detection of emerging anomalies
- Complete network visibility and improved understanding of activity
- Addresses both external and insider threat

Business Background

Drax is a leading power infrastructure company, and provides around 7% of the UK's power. Having switched to the use of biomass generators, Drax is considered to be one of the most forward-looking organizations in the energy and utilities industry.

> " Darktrace's AI technology has proven instrumental in providing visibility of devices we didn't even know we had on our network. "
>
> **Martin Sloan**
> **Group Head of Security**

Challenge

The energy sector faces a rapidly-evolving threat landscape, in which increasingly sophisticated attackers have been successful in scaling network boundaries and infiltrating extremely sensitive operational systems. The stakes of cyber-threats in this eld are high, with major implications on the safety and integrity of national critical infrastructure.

Given the wide range of motivations that attackers have, and the looming risk of internal threat, it had become extremely difficult to pre-empt new attackers and anticipate their methodologies. Drax needed to be able to identify emerging threats, get ahead of up-and-coming attackers and intervene early in order to better protect its critical data and systems.

The threat to the energy sector is both more serious and more difficult to defend against as a result of the increasing integration of IT with operational technology (OT) – industrial control systems (ICS) and SCADA systems. This integration necessarily creates new attack surfaces for both, many IT systems are now able to act as a way into OT systems and vice versa.

Solution

Drax decided to implement an 'immune system' approach, because it needed to be able to respond to fresh threats that had not been previously identifed by other security tools. The company selected Darktrace, powered by Enterprise Immune System technology, in order to benefit from a self-learning system that does not require a priori knowledge in order to identify threats, but which instead forms an adaptive understanding of normality and abnormality within its data systems.

The ability to constantly adapt to a rapidly evolving information environment in real time was critical to Drax, as it needed to be able to intervene early in potentially dangerous situations.

After successfully implementing the Enterprise Immune System on its corporate network, Drax extended the coverage to defending its crucial industrial control system (ICS) from attack. With overall visibility of both IT and OT environments, Darktrace gives Drax the unique ability to analyze all parts of its enterprise and production networks, and to detect previously unidentified threats irrespective of their origin.

> " It helps us stay ahead of emerging threats and better defend our key systems. We are pleased to be working on cyber innovation with Darktrace's leading self-learning platform. "
>
> **Martin Sloan**
> **Group Head of Security**

Benefits

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 before they have the potential to cause signi cant damage.

On deploying Enteprise Immune System technology, the company was quickly alerted to potential intrusions within its systems that had already bypassed its other security tools. Following an easy implementation process, it now uses Darktrace to continuously analyze the overall health of its system and to spot irregular activities that have a high probability of being either malicious, dangerous or non-compliant.

Drax benefits from the most advanced cyber defense technology available today to protect itself against the most insidious attacks that jeopardize its critical infrastructure systems, whether those threats come from the inside or outside of its organization.