2021 Industry Spotlight: Energy and Utilities

As organizations undergo a difficult balancing act between defending themselves from attack while maintaining business continuity, a unified approach to cyber defense across both IT and OT environments has never been more important.

At a Glance

- ✔ Protects more than 450 energy and utiltity organizations globally
- ✔ Self-learning AI which detects in-progress attacks
- ✔ Autonomously investigates, triages, and reports on all security incidents
- ✔ Provides complete visibility of RTUs and remote Operational Technology

The Challenges of Securing a Dynamic Workforce

The energy and utilities industry faces unprecedented cyber challenges. As its strategic importance grows, the threat of nation-state attackers looms large. In May 2020, the US declared foreign cyber-attacks on this sector a national emergency, following the news that state-sponsored hackers were exploiting latent vulnerabilities in countries' critical infrastructure. The reality is that such attacks not only have the potential to cause significant operational outages, but even the potential to jeopardize economic and national security.

Meanwhile, the hybrid working situation that has emerged as a result of global lockdowns has expanded the attack surface. Many OT security teams remain on site while their IT counterparts have gone remote, creating a fragmented digital infrastructure where collaboration has become increasingly difficult. This transition is happening against the backdrop of an ongoing shift towards increased cloud and SaaS usage, industrial IoT adoption, and converging operational technology and IT systems. The result is decreased visibility and new entry points for attackers.

These changes to workflow and security team structure have exacerbated an existing cyber skills gap within the industry. Having to juggle protecting employees working remotely on VPNs and internal systems, as well as safeguarding cyber-physical environments, has meant that security teams have found their workload dramatically increasing and their responsibilities changing. Already a rare resource, the expertise gap between IT and OT specialists is widening, becoming one that is more difficult to fill and more dangerous to be lacking.

Crucially, these changes are happening at a time when employers have had to make difficult trade-offs to ensure operational continuity while maintaining security practices. In addition, many long-term projects such as NIST regulatory compliance testing have been relegated, leaving organizations more vulnerable.

The challenges facing the energy and utilities sector are vast. Operational shutdown and sophisticated espionage risk not only profitability but also the capacity to provide energy to citizens who need it most; organizations need to act now to protect their data and digital systems.

How AI Safeguards Energy and Utility Organizations Across the Globe

Relied on by some of the world's largest energy and utility companies, Darktrace's Industrial Immune System defends organizations from cyber-threats across their IT and OT environments. The self-learning AI technology detects in-progress attacks, instantly alerting security teams to nascent threats.

Inspired by the human immune system, Darktrace's Cyber AI works by passively learning what 'normal' looks like across OT, IT, and industrial IoT. This understanding of an organization's digital DNA allows the AI to detect even the most subtle signals of emerging threat across the entire business – no matter how novel or sophisticated. Protocol and technology agnostic, the AI is operative across substations and all physical devices through the insertion of probes, meaning that even air gaps and restricted connections are protected.

Once an incident is flagged to security teams, Darktrace's Cyber AI Analyst autonomously triages, interprets, and reports on the in-progress attack. It produces a natural language summary of the event which takes an average of three minutes to read and is able to be reviewed even by a non-technical responder. Cyber AI Analyst bridges the cyber skills gap and ensures that when specialists are ill or on leave, AI is able to support teams' remediation of all threat types – keeping the dynamic workforce protected. Darktrace Cyber AI Analyst has been found to reduce time to meaning by up to 92%.

Autonomously Detecting Shamoon 3.0

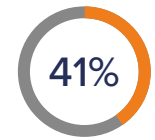
At a global energy company, Darktrace's Industrial Immune System detected Shamoon, a highly destructive malware, in its earliest stages – flagging the threat to the security team as soon as it identified the initial intrusion.

The attack began with an unusual use of credentials on several devices before lateral movement occurred in the form of PsExec, WinRM usage, and RDP brute-forcing. At each stage, the Industrial Immune System detected the threat and detonation of the payload, which was indicative of the malicious Shamoon virus. High-severity alerts were consistently generated, and the infected devices were at the top of the suspicious devices list, making it simple for even a junior analyst to identify the threat and where it was coming from.

> "Darktrace adds another level of sophistication to our defence systems and has already identified threats with the potential to disrupt our networks."

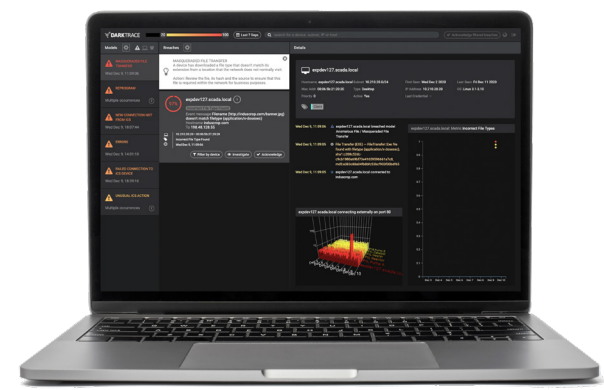
Martin Sloan, Group Head of Security, Drax

Threats by Numbers



of organizations in the energy industry experienced a cyber-attack in the last 12 months.

$6.4 million is the average cost of a data breach in the energy industry.



Darktrace's OT Engineer Dashboard surfaces only the most operationally relevant alerts