2020 Industry Spotlight: Energy and Utilities

As organizations find themselves undergoing a difficult balancing act between defending themselves from attack while maintaining business continuity, organizations must rethink their approach to security.

Darktrace Industrial Immune System

- ✓ Protects more than 450 energy and utiltity organizations globally
- ✓ Self-learning AI which detects in-progress attacks
- ✓ Stops emerging cyber-threats in an average of 2 seconds
- ✓ Provides complete visibility of RTUs and remote Operational Technology

The challenges of securing a dynamic workforce

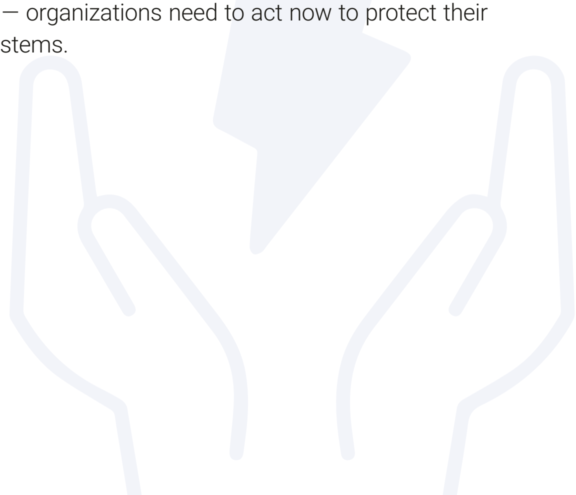
The energy and utilities sector faces unprecedented cyber challenges. As its strategic importance grows, the threat of nation-state attackers looms large. In May 2020, the US declared foreign cyber-attacks on this sector a national emergency, following the news that state sponsored hackers are exploiting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

Further, the hybrid working situation that has emerged as a result of global lockdowns has expanded the cyber-attack surface. Many OT security teams remain on site, while 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 from the traditional network to increased use of cloud and SaaS applications, industrial IoT adoption, and converging operational technology and IT, resulting in decreased visibility, and opening up potential new entry points for attackers.

The changes to workflow and security team structure have also exacerbated an existing cyber skills gap within the industry. Having to juggle securing 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 and 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, and have found themselves undergoing a difficult balancing act between keeping machinery on, and ensuring the security of the organization. In addition, many long-term projects such as NIS regulatory compliance testing have been relegated, leaving organizations more vulnerable.

The challenges facing this sector are vast and significant. Operational shutdown and sophisticated espionage have the potential to jeopardise 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 utilities 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 threats across the entire digital business – no matter how novel or esoteric. 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 for OT automatically 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. The AI Analyst bridges the cyber skills gap and ensures that when specialists are ill or on leave, the AI is able to support teams' remediation of all threat types – keeping the dynamic workforce protected. AI Analyst has been found to reduce time to meaning by 92%.

Darktrace's Cyber AI integrates seamlessly with organizations' existing security stacks and daily operations, acting as a second pair of eyes in order to augment security teams and remediate the most advanced threats at machine speed.

Threats by Numbers

56% of cyber-security professionals in the utility sector reported at least one shutdown or operational data loss in 2019.

25% of utility sector organizations in 2019 were hit by cyber-attacks likely developed by nation-state actors.

67% rise in ransomware attacks on Operational Technology in Q4 of 2019.

82% of power utility companies lack formal Industrial IoT cyber security programs.

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 detected the initial intrusion.

The attack began with an unusual use of credentials on several devices before attempting lateral movement in the form of PsExec, WinRM usage, and RDP brute forcing. At each stage, the Enterprise Immune System was able to detect the lateral movement and detonation of the payload, which was indicative of the malicious Shamoon virus activity. A junior analyst could have easily identified the threat, as high-severity alerts were consistently generated, and the infected devices were at the top of the suspicious devices list.

2 months after Darktrace detected the initial malicious activity, Shamoon's payload denoted, with 42 corporate devices scanning other machines before being wiped. The organization in question did not take action against the numerous alerts surfaced by Darktrace, and had yet to activate Antigena, Darktrace's autonomous response solution, which could have acted in the security team's stead.

Read more about this attack here.

For more information

Book a demo now

Email Threat Report

Hear from our customers

Follow us on Twitter

Follow us on LinkedIn

About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1,300 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.