Business Background

Copperbelt Energy Corporation Plc is an electricity generation, transmission, and distribution company with operations in Zambia and Nigeria. It operates in the Copperbelt province of Zambia, supplying power to national utility providers and to mines in the area. With a three person security team in a central Security Operations Center (SOC), the organization oversees 43 substations and a sprawling SCADA network consisting of remote terminal units and PLCs.

With our previous security stack, we only got to know about an incident once the damage was done. Now with Darktrace, it does all the analysis and remediation for us in real time, and we are able to receive notifications of certain events wherever we are.

Choolwe Nalubamba, Head of Telecommunications and Information Systems, Copperbelt Energy Corporation Plc

Challenge

As a leading player in the energy and utilities space, the main concern for the Copperbelt Energy Corporation Plc was safeguarding its complex OT infrastructure. Increasingly connected with general information networks, its operating machinery had become vulnerable to new vectors of attack. Whether indirectly compromised through disruption to the corporate network, or targeted by an ICS-specific attack, any disruption to the company's SCADA network would have resulted in significant financial and reputational loss.

Complicating this task was the overwhelming amount of digital information Copperbelt Energy Corporation Plc’s small team of security analysts were faced with on a daily basis. Scouring through hundreds of alerts was a time-consuming, laborious process. “We were very reactive to potential threats to the business, and that reactivity was extremely slow,” explained Choolwe Nalubamba, Head of Telecommunications and Information Systems.
“If an incident were to happen when we left the office, we would only find out about the attack once the damage had already been done.”

Prior to deploying Darktrace, Copperbelt Energy Corporation Plc’s existing security stack consisted primarily of log analysis tools, which could identify previously-encountered, ‘known’ threats, but had to be manually updated on a regular basis and failed to spot never-before-seen vulnerabilities and attacks.

Solution

After a 30-day Proof-of-Value, Copperbelt Energy Corporation Plc deployed both the Industrial Immune System and Darktrace Antigena to cover its OT and IT systems.

Like a human immune system, Darktrace’s core technology uses cyber AI to learn what’s normal for its environment, analyzing patterns in behavior for every user, device, and controller. From this baseline, it identifies abnormal activity indicative of a threat or vulnerability as it emerges.

Beyond simply raising an alert to the security team, Darktrace Antigena then takes action to respond autonomously, neutralizing malicious activity within seconds of the threat being identified. Notifications of Antigena’s actions are alerted via the Darktrace Threat Visualizer and the Darktrace Mobile App, with the security team now receiving alerts as soon as an incident takes place.

“Darktrace does all the analysis and remediation for us in real time, and we are able to receive notifications of certain events wherever we are”, commented Nalubamba.

Benefits

The value of the technology was instantly recognized for both its ability to identify novel threats and vulnerabilities as well as function as a force multiplier – augmenting the capabilities of the existing security professionals. The team has gone from being reactive to proactive, taking necessary action before an incident can escalate into a crisis.

“Darktrace is always alive, looking at traffic across the entire digital estate; something that you would otherwise need several analysts to do”, explained Nalubamba.

The security team has also benefited from increased visibility of its OT network, including complete oversight of the connections between its IT and OT systems. Darktrace shines a light into every corner of the network, displaying Copperbelt’s OT, IT, and IoT in a unified view.

Darktrace’s 3D Threat Visualizer is used extensively by the SOC team, displaying its findings in a unique and intuitive way. “We had connections between our IT and OT environments that we didn’t know existed. Darktrace gives us that crucial visibility of both the OT and IT on a single screen. And most importantly, we now get to see Darktrace Antigena blocking nefarious activity on the IT network that can have an impact on the OT”. The Threat Visualizer creates comprehensive and accessible forensic cyber analysis that is appropriate for security analysts as well as executive members of Copperbelt Energy Corporation PLC.

“After operating Darktrace for a couple of months, I had the confidence to take the Managing Director to the SOC to have a look at it,” commented Nalubamba. “He was totally impressed with the technology; it gave him assurance that something is watching over his entire infrastructure”.

“Whenever there is a brute-force attack, whenever someone is running a scan on the network, Darktrace immediately sees it and Antigena kicks in to block the anomalous traffic for a given amount of time.”

With Autonomous Response, the security team is now rest assured that its OT and IT systems are protected from attacks that can strike at any time of day. As Nalubamba explained, “I can definitely say I feel better now. There is no silver bullet to cyber security, and no way to stay 100% secure, but with Darktrace’s AI, I at least know I have a very watchful eye on the network at all times.”

Security Flaw Detected

Early in its deployment, Darktrace’s AI identified that the controller responsible for Copperbelt’s gas turbines was originally managed remotely from a single internet-connected laptop. This represented a significant security risk of which the SOC was previously unaware. The Industrial Immune System highlighted the vulnerability and Darktrace Antigena autonomously responded by isolating the laptop before any damage could be done.

Contact Us

North America: +1 415 229 9100
Latin America: +55 11 97242 2011
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
info@darktrace.com
darktrace.com