Industry Spotlight:
US Energy and Utilities

DARKTRACE

AT A GLANCE:

- **Unified Protection:** Self-Learning AI helps converge IT & OT professionals
- **Autonomous Response:** Customizable AI decision making to augment security teams
- **Asset Identification:** Passively identifies all assets based on device behavior
- **Learns On the Job:** Detects never-before-seen threats in real time by evolving with a business without the need for periodic baselining or updated rules.

The increasing convergence of IT and Operational Technology (OT) has expanded the attack surface and introduced new risks in both energy and utilities. Cyber-attacks that start in the corporate network are increasingly spilling over into Industrial Control Systems previously 'air gapped' from the Internet.

Carroll EMC

City of College Station
Home of Texas A&M University

TOMBIGBEE ELECTRIC COOPERATIVE

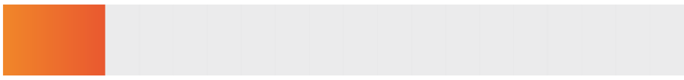
LEC Laurens Electric Cooperative, Inc.

Holston Electric Cooperative
A Touchstone Energy Cooperative

/ Industry Challenges

While the adoption of hybrid working patterns increase cloud and SaaS usage, the number of industrial IoT devices also continues to rise. The result is decrease in visibility for security teams and new entry points for attackers. Particularly for energy and utility organizations.

16% of all successful cyber-attacks
have been launched against energy companies.



90% of OT security teams
suffered at least one damaging cyber-attack in last two years

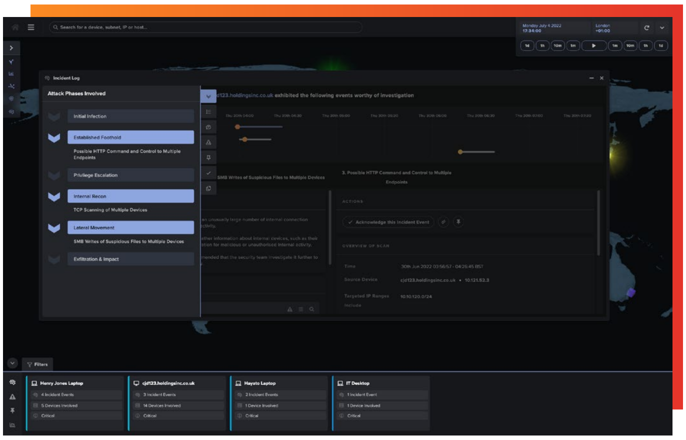
ASTORS
AMERICAN SECURITY TODAY
2022
PLATINUM AWARD WINNER
HOMELAND SECURITY AWARDS

WINNER OF:

BEST CYBER CRITICAL INFRASTRUCTURE SOLUTION

Larger energy utilities face a burden of an exorbitant number of IT, and OT devices, which require constant supervision. Further, their teams are tasked with monitoring all SaaS and email accounts. The sheer volume of information if not processed by AI can can lead to alert fatigue, or events being missed all together.

Smaller utilities or electric cooperatives tend to have one or two security employees overseeing IT, SCADA, SaaS, and email while simultaneously assisting other departments when called upon. Time is the biggest obstacle as one person cannot monitor the security around the clock while performing their other duties.


Search for a device, subnet, IP or host...
Monday July 4 2022
17:34:00
London
+01:00
1d
1h
10m
1m
1m
10m
1h
1d
Incident Log
Attack Phases Involved
Initial Infection
Established Foothold
Possible HTTP Command and Control to Multiple Endpoints
Privilege Escalation
Internal Recon
TCP Scanning of Multiple Devices
Lateral Movement
SMB Writes of Suspicious Files to Multiple Devices
Exfiltration & Impact
SMB Writes of Suspicious Files to Multiple Devices
3. Possible HTTP Command and Control to Multiple Endpoints
ACTIONS
Acknowledge this Incident Event
OVERVIEW OF SCAN
Filters

d123.holdingsinc.co.uk exhibited the following events worthy of investigation

an unusually large number of internal connection ctivity.

ther information about internal devices, such as their tion for malicious or unauthorised internal activity.

mended that the security team investigate it further to

Time 30th Jun 2022 03:56:57 - 04:26:45 BST

Source Device cjd123.holdingsinc.co.uk • 10.121.52.3

Targeted IP Ranges Include 10.10.120.0/24

Henry Jones Laptop: 4 Incident Events; 5 Devices Involved; Critical

cjd123.holdingsinc.co.uk: 3 Incident Events; 14 Devices Involved; Critical

Hayato Laptop: 2 Incident Events; 1 Device Involved; Critical

IT Desktop: 1 Incident Event; 1 Device Involved; Critical

Figure 1: Cyber AI Analyst attack phase

/ Unifying Teams

With its 'Unified View' of enterprise (IT) and industrial (OT) environments, Darktrace is uniquely positioned to deal with IT/OT convergence and IT/OT interdependence.

Darktrace unified view allows the AI technology to:

- Follow threats as they pivot from IT to OT
- Stop them in IT before they spread to OT
- Illuminate unknown points of IT/OT convergence.

Also, in an anonymized study, Darktrace detected over 6,500 suspected instances of ICS protocol use across 1,000 environments.

Darktrace scales to the size of any business or organization.

For smaller teams with just one or two dedicated employees, Cyber AI Analyst and Enhanced Monitoring features allow end users to provide the team with only the most critical incidents. AI Analyst brings all the information into centralized UI for smaller teams.

For larger teams, Darktrace alerts can be forwarded to 3rd party platforms such as a SIEM, where security team decision making is augmented. Additionally, executive reports and autonomous response reduce the alert fatigue generally associated with legacy tools.

Most importantly, Darktrace's unique understanding of normal allows security teams to find zero-days and signatureless attacks regardless of the size of the organization and how alerts are consumed.

/ Case Study: Supply Chain Risk

To demonstrate Darktrace's capabilities, Proof of Value or free trials are offered to our energy clients.

During one such trial with an electric cooperative, during which Darktrace's autonomous response system was turned off, Cyber AI Analyst identified a device connecting to suspicious endpoints that had never made connections to any device on the network before. Because these devices had never made a connection to the network before, an AI investigation was launched and a report was created that found these devices had originated in Russia, China, Bulgaria, and 15 other countries.

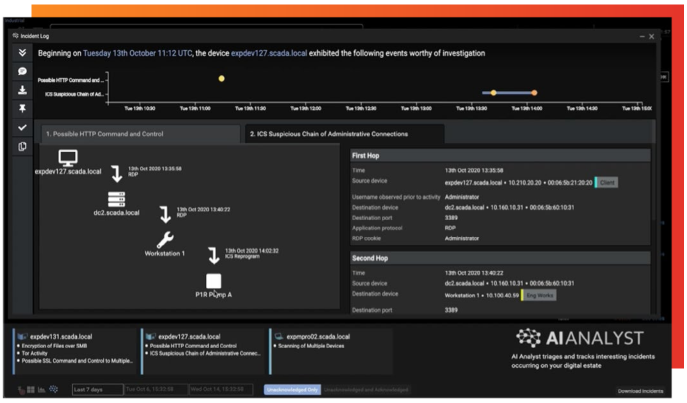
The incident reports it generated enabled the security team to quickly identify the device as a contractor's personal device which was improperly brought into their environment. The full visibility offered by Darktrace confirmed the malware infected host had not yet spread to other parts of the network, and the team could remove the device and alert the third-party supplier.

/ Cyber AI Analyst Designed to Save Time

Unlike traditional tools, Darktrace does not rely on rules, signatures, or historical attack data. Instead, it understands everything in your organization from the ground up and detects subtle deviations indicative of a cyber-threat. Darktrace DETECT identifies anomalous behavior in real time and alerts are autonomously investigated with Cyber AI Analyst. AI Analyst generates reports using executive-level summaries explaining what has happened, how the event was detected, and recommendations for next steps

Darktrace can read inside protocols and can look at contextual factors like metadata and other forms of information to identify unusual activity, without having to read into the content of the machine-to-machine communications itself. Cyber AI Analyst conducts autonomous investigations across IT and OT, that automatically triage all unusual behavior, connecting the dots among disparate events to form fleshed out incident reports, which are 'human readable' with timelines spelled out in attack phase terminology. Darktrace's analysis has shown that this reduces time to triage by an average of 92%.

Darktrace also provides both passive and active asset identification. By default, Darktrace passively identifies all assets based on device behavior, which eliminates the risk of any operational disruption that may stem from the process of asset identification. Over time, end-users develop a trust in the system and spend only a few minutes in the day looking at their UI or triaging alerts through the mobile phone app.



Incident Log

Beginning on Tuesday 13th October 11:12 UTC, the device expdev127.scada.local exhibited the following events worthy of investigation

1. Possible HTTP Command and Control

2. ICS Suspicious Chain of Administrative Connections

First Hop

Time: 13th Oct 2020 13:35:58
Source device: expdev127.scada.local • 10.210.20.20 • 00:06:5b:21:20:20 Client
Username observed prior to activity: Administrator
Destination device: dc2.scada.local • 10.160.10.31 • 00:06:5b:60:10:31
Destination port: 3389
Application protocol: RDP
RDP cookie: Administrator

Second Hop

Time: 13th Oct 2020 13:40:22
Source device: dc2.scada.local • 10.160.10.31 • 00:06:5b:60:10:31
Destination device: Workstation 1 • 10.100.40.59 Eng Works
Destination port: 3389

expdev131.scada.local
- Encryption of Files over SMB
- Tor Activity
- Possible SSL Command and Control to Multiple...

expdev127.scada.local
- Possible HTTP Command and Control
- ICS Suspicious Chain of Administrative Connec...

expmpro02.scada.local
- Scanning of Multiple Devices

AI ANALYST

AI Analyst triages and tracks interesting incidents occurring on your digital estate

Figure 2: Darktrace's Cyber AI Analyst incident report