DOE Award Number: DE-CR0000001

Sponsoring Program Office: U.S. Department of Energy-Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER)

Recipient: Southern Company Services, Inc.
600 North 18th Street
Birmingham, AL 35203

Project Title: Cybersecurity for the Operational Technology Environment (CyOTE)

Project Period: December 20, 2018 – December 19, 2023

Principal Investigator: Steve Sanders
Southern Company Services, Inc.

Contributors: Christopher Taylor, Alex Waitkus, Guy Palmer
Southern Company Services, Inc.

Acknowledgement:

This material is based upon work supported in part by the Department of Energy Award Number DE-CR0000001.

Disclaimer:

Contents

Executive Summary 4
CyOTE Pilot Goal[2] 4
CyOTE Pilot Challenges[3] 4
CyOTE Monitoring Approach 6
CyOTE Technology Selection 7
Primary Network Monitoring Tools 8
Supporting Infrastructure 8
Lessons Learned / Additional Considerations 9
Passive Network Ingest Feeds 9
Sensor Scoping and Placement 9
Business Partner Socialization 9
Importance of Automation 9
Sensor Maturity 10
Reference Architecture 10
Conclusion 10

Executive Summary

Electric grids have historically been susceptible to both physical attacks and environmental hazards but the implementation of smart grids, remote management, and self-healing networks, has now made the grid vulnerable to cyber attacks. To address risks introduced by routable connectivity, utilities must establish dynamic solutions to identify, protect, detect, respond to, and recover from cyber security threats and vulnerabilities.

In response to the evolving threat landscape U.S. Department of Energy-Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) initiated the Cybersecurity for the OT Environment (CyOTE) pilot program, a U.S. Department of Energy (DOE) effort designed to leverage U.S. intelligence capabilities to prevent, detect, or mitigate a cyber attack on utility operational technology (OT) networks. As part of the CyOTE pilot, The Southern Company (Southern Company or Southern)[1] researched, evaluated and deployed emerging Commercial off the Shelf (COTS) technologies and cyber security monitoring architectures to provide previously unrealized network visibility and situational awareness through deep packet inspection and data analytics.

This Final Scientific/Technical Report documents the objectives, methodology, lessons learned, and results of Southern Company's participation in the CyOTE pilot from December 2018 to September 2023.

CyOTE Pilot Goal[2]

Develop, test, and validate a reference architecture and process to identify high-risk OT attack scenarios and monitoring points, securely share OT network data, and leverage U.S. Intelligence Community capabilities to analyze data to detect sophisticated cyber threats. Evaluate feasibility to scale up the process and advance the capability industry-wide and recommend an approach for a national program using pilot findings.

To realize these objectives Southern Company developed a proposal to research, deploy, and evaluate commercially available OT sensors, data analytics tools, and monitoring architectures in a variety of Transmission and Distribution environments to evaluate potential detection and monitoring, data analytics, and information sharing solutions and provide findings and lessons learned to DOE.

CyOTE Pilot Challenges[3]

When the CyOTE pilot was initiated in 2017, there were limited capabilities available to utilities to monitor their OT environments and detect emerging cybersecurity threats. Early OT monitoring efforts at Southern Company had revealed that there were significant

[1] *Southern Company is a holding company that conducts its business through its subsidiaries; accordingly, unless the context otherwise requires, references in this report to Southern Company's operations refer to those operations conducted through its subsidiaries.*

challenges to adapting traditional information technology (IT) tools to work in OT environments and due to the significant differences in network design, functionality, and traffic, new approaches would have to be taken to monitor these environments. The following list of OT monitoring challenges was developed by DOE with support from Idaho National Labs (INL) and the CyOTE pilot participants:

- ***Visibility into OT environments is limited, and there are few commercial sensors targeting the OT space today.*** As a result, few utilities are widely using sensors in their OT networks to monitor traffic, with minimal detection and analysis capabilities for anomalous or malicious traffic in OT systems.

- ***Classic tools and analytics for IT monitoring and detection don't readily transfer.*** OT systems have significantly different traffic, using Industrial Control Systems (ICS) or vendor-specific protocols. Commercial sensors often offer limited or no support for the special protocols used, and custom parsers are not readily available.

- ***There are no one-size solutions for OT environments.*** Single sensor solutions and placement are unlikely to work in all OT environments given the diversity of equipment, protocols, and monitoring locations. Analysis of this data requires tools that can accept these disparate sources of information and leverage any new technologies developed.

- ***Sophisticated attacks and advanced persistent threats***—those that CyOTE is focused on defending against—are the most difficult to detect, as attackers may use low-level reconnaissance to map networks, steal credentials, and, ultimately, impersonate valid system actions to cause disruption or damage. Detecting malicious actors that lurk on OT networks and play the rules is the key challenge CyOTE must solve.

- ***Identifying malicious anomalies in OT network data often depends on understanding complex system behaviors instead of leveraging generic indicators.*** IT network monitoring commonly looks for attack signatures in varied and unpredictable traffic. In contrast, OT network traffic is repetitive and well-defined, making it possible to detect anomalies from an expected baseline that can be unique to each site. Defining this baseline of "normal" operations for pilot participants will be a large undertaking. Developing analytics that can then detect an abnormal event—and distinguish if it is malicious or benign—requires a great deal of additional context about the system components and devices involved, expected behaviors, and potential impacts on operational control schemes. This analysis is more time- and resource-intensive to implement, but can unlock powerful new detection capabilities to specifically protect critical power grid functions, rather than simple networking anomalies that are present in all computer networks.

- ***Government intelligence reporting for OT systems may be limited in its ability to deliver OT-specific insights or actionable information that utilities can use to prevent, detect, or delay an attack.*** The pilot will identify the type and amount of information needed from different network levels to support intelligence informed attack detection and correlation. The pilot will also provide critical data and context to inform and expand Intelligence capabilities.

- ***OT network information may be highly sensitive, requiring significant trust and a framework of legal agreements for utilities to voluntarily share data with government partners***. Sensor placement must also consider and respect North American Electric Reliability Corporation (NERC) Critical Information Protection (CIP) requirements.

CyOTE Monitoring Approach

One of the first things the team needed to determine where the pertinent data was within Southern's OT networks and where network monitoring should occur. To determine this, Southern partnered with INL to design plausible attack scenarios and map the cyber kill chain and the steps a potential attacker might use to impact operations. Using these scenarios, the team was able to identify monitoring locations opportunities and determine the potential value of the data collected at those sources.

The output of this analysis led to the identification of 4 categories or tap-points of network areas that were of interest for monitoring:

- **Point A:** Tap both corporate and OT sides of the firewall
- **Point B:** Aggregate data at hub sites (network choke points) for all substations within a geographic region to capture Distribution Supervisory Control and Data Acquisition (SCADA) and other OT network traffic
- **Point C:** Capture localized OT network traffic and communications of intelligent electronic devices (IED)/RTU class devices
- **Point Z:** Security event aggregation that aggregates and analyzes multiple data streams from both IT and OT environments

Adaption of the tap-point analysis led to DOE and the CyOTE team developing an OT Tap-Point Monitoring Framework.

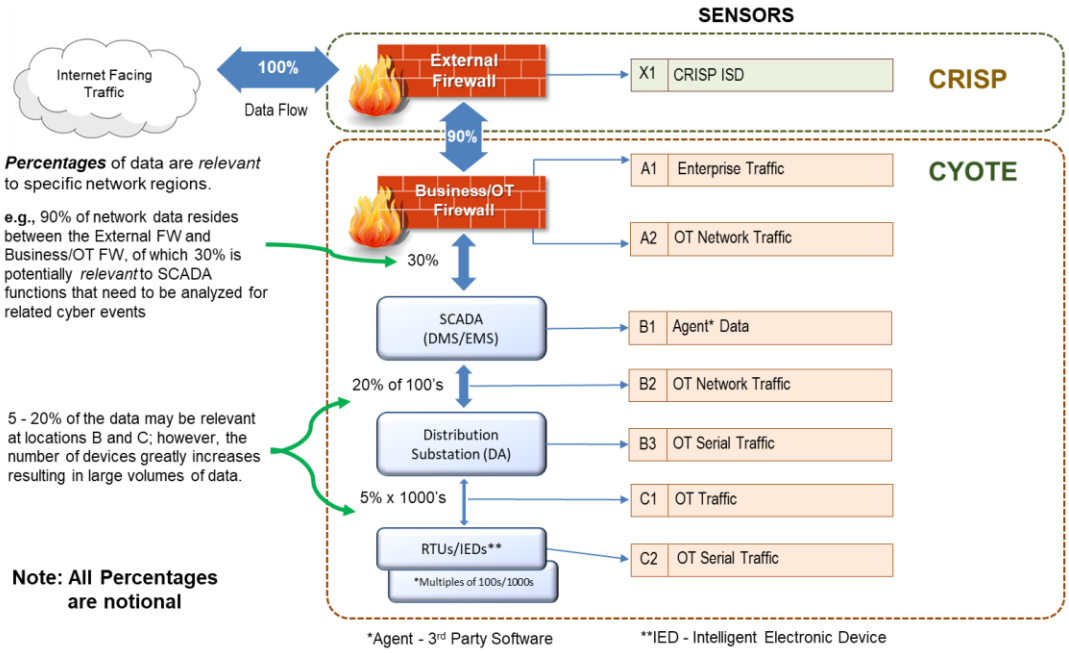

Figure 1

Analysis of the framework shows that an organization attempts to monitor deeper in the OT environment (progressing from tap points A to C), the number of devices and the amount of data to process increases exponentially and the scalability of monitoring these environments becomes challenging. However, despite the challenges, over the course of the CyOTE pilot it was determined that numerous attack scenarios would not be discoverable without visibility into these environments.

While the "Z Tap Point" concept was not incorporated into the DOE Framework, event aggregation and data analytics remained an integral part of Southern Company's CyOTE pilot solution.

CyOTE Technology Selection

Once Southern Company determined where they needed to monitor to achieve CyOTE goals, COTS technologies needed to be selected to implement the pilot. A wide-net was cast and 69 vendors with OT security capabilities were evaluated as potential solutions. Ultimately, Southern Company evaluated selected solutions based on their potential ability to perform:

- Network asset detection and mapping
- Deep packet inspection and analysis of ICS protocols
- Enhanced visibility & real-time situational awareness
- Early indicators and detection of anomalous activity
- Increased troubleshooting and IR capability
- Validation of network changes and maintenance operation

Figure 1: The OT Tap-Point Monitoring Framework was never published but was presented by DOE and Southern Company at the CyOTE Demonstration & Deployment Working Group Call on July 20, 2021

- Advanced threat detection and integration with Security Operations Center
- Information sharing with Government and partner utilities

The next section highlights the types of security tools were selected for the CyOTE pilot monitoring.

Primary Network Monitoring Tools

OT-centric Intrusion Detection Sensors

Southern Company selected 2 sensors that would take input from raw network taps, as well as many Security tools and OT applications, analyzes the data in the sensors to generate analytics and alerts.

Artificial Intelligence (AI) /Machine Learning (ML)

Many traditional Security Operations Centers (SOCs) lack the expertise and context of OT Networks to effectively respond to OT alerts. The project team wanted to evaluate the concept of advanced learning software system that follows the decision-making process and judgement of a SOC analyst. While this type of technology was nascent, there were several successes and as the AI/ML technology matures should be considered to supplement OT cyber security tools

Supporting Infrastructure

In addition to tools selected to monitor OT environments, it was determined that additional supporting infrastructure was necessary to gather the data needed for monitoring and to ensure that monitoring the OT environment didn't introduce new attack vectors into the environment. The following tools were selected as support tools for CyOTE pilot monitoring:

Rugged Firewall

A ruggedized firewall was deployed to the CyOTE substations to segment those systems in a substation to ensure systems that perform similar functions or have similar requirements are protected, allowing access to and from expected local and remote systems. The firewalls were deployed using a zoning model to ensure that there is only one entry/exit point for a network security zone and all traffic entering and leaving the zone should be subject to inspection and prioritization by the firewall. The chosen products for this deployment were:

Software-Defined Networking (SDN)

SDN switches were implemented to streamline and standardize deployment of a physically-segmented substation audit zone. The SDN switches enable management of the CyOTE

sensors and spray a mirrored stream of OT traffic to both sensors within the local substation environment.

Lessons Learned / Additional Considerations

Through the CyOTE pilot there were numerous lessons learned on how to successfully monitor OT network environments. The following provides an overview of the CyOTE pilot's lessons learned:

Passive Network Ingest Feeds

- Packet Aggregation is key for successful passive tapping
    - Provides ingest of multiple feeds into a single sensor
    - Provides "spraying" of feeds to multiple sensors
- Solution had to meet NERC CIP standards
    - While the CyOTE pilot exclude NERC CIP environments, early engagement with Compliance team was key to ensure solutions are scalable for potential future NERC CIP inclusion
- SDN provides flow capabilities for passive monitoring in C Tap point environments where a hardened device is needed for operations
    - Acted as a hardened packet aggregator by providing "spray" capability with "flows"

Sensor Scoping and Placement

- Technology selected at the start of CyOTE had limited ingest rates which required additional filtering and/or hardware to support monitoring
- Some sensors struggle to understand same traffic passing through multiple tap points (leads to duplicate findings)
- Packet aggregators and SDNs enable flexible deployment options of multiple sensors/feeds
- Successfully piloted serial taps at C2 tap points for added substation visibility (relays and other IEDs) to support serial traffic attack scenarios
- Hardened firewalls were key to properly segment substations and create audit/monitoring zone

Business Partner Socialization

- Early engagement with Business Partners (OT personnel) needed for buy-in
- Identify additional CyOTE tool value beyond pilot assists in buy-in. Many of these tools provide operational business intelligence beyond their cyber security capabilities

Importance of Automation

- Scalability and timeliness remains a concern
    - Full deployment to C Tap Points may be unrealistic and a risk based approach may be the more desirable approach to tap point selection

- Traditional IT Security personnel may lack context and specialized skillset to analyze OT networks and protocols and automation and context opportunities should continue to be developed

Sensor Maturity

- Specialized OT IDS capability was an emerging field at the onset of CyOTE and still is a rapidly maturing field
- Vendors differ on implementation of ICS protocols which can lead to inconsistent findings
- CyOTE sensors struggled in IT-like environments like Distribution SCADA due to high network traffic (10 GB) but significant strides have been made in the last 5 years to address these challenges
- Advancements in Containerization/Virtualization in OT environments may address scalability issues in C Tap Point environments

Reference Architecture

- Successfully monitoring requires as OT Security reference architecture to define monitoring and information sharing necessities
    - DOE's tap point framework was key to achieving this objective
- A "do-no-harm" mentality is required to monitor OT environments. Reliability is the OT priority
    - Quality of Service (QoS) was integral to address network bandwidth constraints to ensure monitoring tools didn't impact SCADA traffic
    - Zoning using hardened next generation firewalls was necessary to ensure new risk wasn't introduced through monitoring solutions

Conclusion

The implementation of the CyOTE pilot provided two major accomplishments for DOE, Southern Company and the Energy Sector. First, it identified the challenges utilities face in monitoring their OT environments and developed a monitoring framework to provide utilities with a starting point to develop a cyber security monitoring solution. Secondly, Southern Company demonstrated the feasibility of using commercial-off-the-shelf OT cybersecurity monitoring technologies to gain deep visibility within their OT environments.

While solutions selected at the beginning of this project were nascent and had limited capability, these technologies and other have matured tremendously over the last five years to address detection and scalability concerns. Implementation of these and similar technologies that are evaluated against an organization's cyber security requirements along can effectively be used to provide visibility deep within an organization's OT environment and reduce cyber risk.