Cybersecurity for the Operational Technology Environment (CyOTE™)

Capabilities to Identify Cyber Attack Techniques within Operational Technology (OT) Environments

DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) worked with energy sector partners and Idaho National Laboratory (INL) to develop a methodology and detection capabilities for asset owners and operators to independently identify adversarial tactics, techniques, and procedures (TTP) within their operational technology (OT) environments that could result in physical disruptions to energy flows or damage to equipment. CyOTE is based on the fundamental concepts of perception and comprehension, applied to a universe of knowns and unknowns that are increasingly disaggregated into observables, anomalies, and triggering events.

CESER embarked upon CyOTE due to: complexities in OT management and control of energy deliver; the interconnections with business operations systems; and these systems being a key target for highly sophisticated cyber attackers who "have conducted cyber espionage to collect intelligence and targeted our critical infrastructure to hold it at risk."[1] Energy companies have few tools to analyze these OT systems for malicious activity, in significant contrast to their information technology (IT) networks. Unlike the approach taken with commercial security solutions, CyOTE seeks to tie anomalies in operations to a cyberattack. By stringing together multiple techniques in the OT environment, AOOs can identify attack campaigns with ever-decreasing impacts.

For these reasons, CyOTE is a high-priority CESER investment to enhance energy sector threat detection of anomalous behavior potentially indicating malicious cyber activity in OT networks. Specifically, the CyOTE methodology and detection capabilities enable asset owners to better evaluate their production and transmission of energy and take mitigating measures when appropriate.

Alignment with the National Cyber Strategy

In addition to benefitting individual energy sector companies, as well as other industrial control system environments, CyOTE is also aligned with the National Cyber Strategy, Pillar 1, which states:

> *"The Federal Government will work with the private sector to manage risks to critical infrastructure at the greatest risk. The Administration will develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks."*

Goals and Objectives

CESER has been working with INL and the energy sector to develop and share OT security capabilities that will identify MITRE's ICS ATT&CK Framework TTPs used by adversaries. The CyOTE program has:

---

[1] Daniel R. Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community," Statement for the Record for the Senate Select Committee on Intelligence, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

- **Worked closely with energy sector partners** to create a methodology that uses orthogonal data to question and trace back anomalous OT events (outside the norm) to either attack indicators or explainable incidental causes (triggering events).
- **Identified high priority adversarial techniques** associated with energy infrastructure that could be involved with the event of interest.
- **Analyzed the events and associated data** related to those techniques.
- **Developed capabilities and mechanisms** to alert on indicators of attack on the affected infrastructure.
  - **Identified** the processes necessary to expose attack techniques and then developed detection capabilities that can be integrated into OT networks.
  - **Shared** CyOTE-developed detection capabilities (Recipes – a set of steps and methods for detecting techniques; Proof of Concept tools – representative implementation of a set of steps and methods for detecting techniques that are customized by AOOs to fit their specific environments) with energy sector asset owners and operators.
  - **Enabled** operators to discover techniques being used by adversaries in OT networks faster than current processes resulting in better defense for our industry partners.

Development Approach

- **Utilize Use Case approach** – CESER identified three Use Cases to focus the development efforts. The Use Cases were centered around identifying anomalies related to; Alarm Logs, Remote Logins, and Human Machine Interfaces (HMI) with the premise that identifying anomalies in these three areas would provide higher confidence that malicious activity was present. Using MITRE's ICS ATT&CK Framework, DOE worked with energy sector partners to identify triggering events and the associated data to enable effective evaluation of anomalous operational behavior. By tying triggering events to TTPs, CyOTE developed a methodology and capabilities that indicates attack pathways adversaries could use to compromise OT systems. For example, capabilities could monitor various data sources including logs, files, and network traffic where strategically placed sensors could best detect malicious activity.
- **Leverage commercial sensors** – Installed OT network sensors and monitoring capabilities may be used to identify and collect data appropriate to support asset owner-identified triggering events, which would translate the anomalous activities into identified potentially adversarial TTPs.
- **Correlate data from multiple sources** – The CyOTE methodology is promoting a holistic approach to identify malicious indictors including indicators from business, operational, and security sensors.
- **Refine data monitoring, sharing, and analysis** – Initial data analysis results were used to help energy sector partners to configure and refine data collection, analytics, and insights. These improved insights and capability development efforts provide timely alerts and actionable information for energy sector partners to take mitigating measures.
- **Develop and share Case Studies** – The CyOTE team has applied the CyOTE methodology to historical attack campaigns as well as pilot activities with sector partners to illustrate the identification of attack campaigns with ever-decreasing impacts.

Senior Technical Advisor	Edward Rhyne | | CyOTE.Program@hq.doe.gov | | 202-586-3557