OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Cybersecurity for the Operational Technology Environment (CyOTE™)

Developing Tools to Detect Indicators of Cyber Attacks within Operational Technology (OT) Environments

DOE's Office of Cybersecurity, Energy Security and Emergency Response (CESER) is working with energy sector partners to develop a threat detection capability for energy sector asset owners and operators to detect sophisticated cyber threats. CESER, through the CyOTE Program, is leading a research partnership with Idaho National Laboratory (INL) and the energy sector to develop tools and capabilities for monitoring and detecting indicators of attack within operational technology (OT) networks.

CESER has embarked upon CyOTE due to the fact that complex operational technology managing and controlling energy delivery – and the interconnections of those systems with business operations systems – are now 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 currently have few tools to analyze these OT systems for malicious activity, in significant contrast to their IT networks.

For these reasons, the CyOTE program is a high-priority CESER investment to enhance energy sector threat detection of anomalous behavior potentially indicating malicious cyber activity in OT networks. Specifically, CyOTE tools will enable the asset owners to take mitigating measures by providing timely alerts and actionable information.

Alignment with the National Cyber Strategy

In addition to benefitting individual energy sector companies, the CyOTE Program 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."*

CyOTE Program Goals

- **Engage with energy sector companies** to identify triggering events and use cases which indicate anomalous activity on energy infrastructure and collect the associated data.
  - For example, a power outage caused by a squirrel or an errant command has the same result. However, the outage caused by a squirrel may be easily explained, whereas an outage caused by malicious intent may appear anomalous. Analyzing anomalous data, such as network traffic, configuration files, firmware and software, alarm logs and operations files may identify indicators of attack.
- **Develop tools and capabilities** that will monitor and analyze asset owner and operator data for indicators of attack.

[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.

- **Demonstrate tools** and their effectiveness in operational and simulated OT environments. These tools will alert on conditions that indicate an attack may be progressing.
- **Make tools available** for the energy sector companies to implement and enhance their on-site threat detection capability.

Objectives

CESER is working with INL and the energy sector to develop and share OT security tools that will identify tactics, techniques, and procedures used by adversaries. In order to develop these tools, the CyOTE program will:

- **Work closely with each partner utility** to share data associated with their triggering event of interest.
- **Identify high priority adversarial techniques** associated with energy infrastructure that could be involved with the event of interest.
- **Analyze the events and associated data** related to those techniques.
  - The CyOTE team will identify the processes necessary to expose attack techniques and then develop detection tools that can be integrated into utility OT networks.
- **Develop tools and mechanisms** to alert on indicators of attack on the affected infrastructure.
- **Share** CyOTE-developed tools with the energy sector asset owners and operators.
  - **Enable** 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

- **Design targeted monitoring approaches** – Using MITRE's ICS ATT&CK framework, DOE is working with energy sector partners to develop processes and tools that will monitor and detect the attack pathways adversaries could use to compromise their OT systems. For example, these tools 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 tools may be used to identify and collect data appropriate for asset owner-identified use cases, which would be needed for analysis by the CyOTE researchers to develop tools to translate the use case data into identified potentially adversarial tactics, techniques, and procedures.
- **Refine data monitoring, sharing, and analysis** – Initial data analysis results will be used to help energy sector partners to configure and refine data collection and analytics. This will improve insights and tool development efforts for energy sector partner environments. These tools, when deployed, will provide timely alerts and actionable information for energy sector partners to be able to take mitigating measures.
- **Enrich tool development with U.S. government tools and insights** – DOE and INL are working with the intelligence community to better understand the threat to the energy sector and prioritize the development of CyOTE tools and capabilities to better support the energy sector.

DOE Program Manager	Edward Rhyne | | Edward.Rhyne@hq.doe.gov | | 202-586-3557