EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security Operational Technology Equipment Familiarization Course

Objective

Utility operational technology (OT) cyber security analysts must objectively be familiar with the systems they are tasked to protect, which can often be quite different than enterprise information technology (IT) environments. This includes not only the network communications protocols used in OT environments, but also general familiarity with various protection device functionality and their operations.

This supplemental project provides utility cyber security engineers, analysts, and managers with hands-on exercises and supporting discussions for a variety of components commonly used to monitor and protect both the power delivery networks and the network infrastructures that support grid operations.

Benefits

By having basic knowledge of the types of equipment used in OT environments, which can range from protective relays to intrusion detection systems, cyber security resources will improve their proficiencies and productivity in the OT environments they are tasked to monitor and protect.

- Familiarize OT cyber security employees with different types of equipment commonly used in substations.
- Learn about different types of communications protocols and network monitoring tools to identify potentially malicious traffic.
- Obtain hands-on access with real equipment in a sandboxed laboratory environment, such as relays and automation controllers.
- Develop confidence in cyber security processes and technologies.
- Enhance knowledge to monitor and protect equipment from cyber-attacks.

Learning about different equipment in a sandboxed laboratory environment allows utility cyber engineers an opportunity to solve unique challenges as a cohesive team and forces them to explore and experiment with various solutions without the risk of damaging production devices.

Approach

EPRI's OT cyber security engineers and subject matter experts developed this course with hands-on interaction as a primary goal. The modules created cover a wide breadth of topics that are applicable to transmission and/or distribution utilities of any size.

Leveraging EPRI's Cyber Security Research Lab in Knoxville, TN, attendees can have safe and interactive access with physical devices in a lab environment.

The current curriculum consists of the following topics:

- Substation architectures and communications protocols
- Intrusion Detection and Protection Systems (IDS/IPS)
- SEL Real-Time Automation Controller (RTAC) and AcSELerator QuickSet

- NovaTech OrionLX Substation Automation Controller
- Simulation and test harnesses (Triangle MicroWorks)
- Security Orchestration, Automation and Response (SOAR) solutions

Courses are held for individual utility teams and can accommodate up to eight participants. The course size is limited to promote interaction from all participants and to ensure that every participant has an opportunity to actively engage with equipment during hands-on activities.

Should a utility be interested in making slight modifications to the course curriculum, EPRI may be able to develop an additional module at no cost to make the course more relevant to the interested utility. Module development time may impact course scheduling.

Deliverables

Each participating utility will receive:

- Approximately 32 hours of interactive, hands-on, instructor-led training on a variety of topics to familiarize attendees with OT equipment and environments.
- Remote access to EPRI's Cyber Security Research Lab to interact and explore a variety of OT equipment in a safe, sandboxed environment. This access will expire approximately one month after the completion of the course.
- Electronic copies of all training materials used during the course, along with audio/video recordings of the course lectures, discussions, and exercises (with consent).

Price of Project

The cost of this supplemental project is $30,000. Certain members of GridEd may qualify for discounts up to 50%. This supplemental project qualifies for Tailored Collaboration (TC) and Self-Directed Funding (SDF).

Project Status and Schedule

The project schedule is based on the availability of both the utility employees who will be attending this course and the EPRI cyber security engineers. A schedule will be proposed and mutually agreed upon by the utility and EPRI in the project SOW.

Who Should Join

Utilities with OT cyber security engineers or OT protection and control engineers whose roles require cyber security knowledge should join this project.

Technical Contact

William Webb at 865.218.8132 (wwebb@epri.com).

Technical Advisor Contact Information

Central: Chuck Wentzel at 618.320.0011 (cwentzel@epri.com).

Northeast: Tim Anderson at 704.595.2054 (tanderson@epri.com).

Southeast: Barry Batson at 704.595.2879 (bbatson@epri.com).

West: Brian Dupin at 650.906.2936 (bdupin@epri.com).

Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com