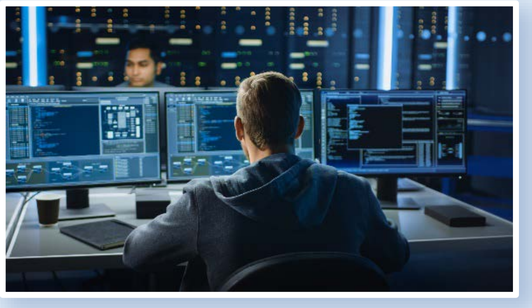
Supplemental Project Notice

CREATING EFFECTIVE ANALYTICS TO MONITOR OPERATION TECHNOLOGY (OT)



PROJECT HIGHLIGHTS

- Streamline the process of creating operational norms
- Leverage data to develop maintenance and engineering trends
- Validate trends against data sources such as work order system data
- Optimize TTP based alerting for defenders
- Prioritize alerting by emphasizng alerts that fall outside of operational norms
- Leverage operational insights to create validation processes for defenders

Background, Objectives, and New Learnings

David Bianco's Pyramid of Pain is a framework for understanding the types of indicators of compromise (IoCs) and how difficult they are for adversaries to change. At the top of the pyramid, representing the most difficult indicators for adversaries to change is TTPs. By building defenses around improving the capabilitiy to detect advsary TTPs, utilities can develop robust defenses that are not easily circumvented.

The objectives include:

- Streamlining The Process Of Creating Operational Cyber Security Norms For Operation Technology (OT) Activity
- Optimizing Cyber Security Alerts Based On Abnormal Deviations
- Developing Dashboard Visualizations For Faster Incident Response

This supplemental project opportunity “Creating Effective Analytics to Monitor Operation Technology (OT)” aims to address gaps in situational awareness of OT events, distinguish normal from abnormal behavior, and provide cyber defenders with improved visualizations.

The proposed project by EPRI aims to enhance the cybersecurity of electric utilities' Operational Technology (OT) by developing advanced analytic monitoring for OT events. Leveraging prior methodologies and insights, the project seeks to identify normal versus abnormal OT activity, enabling improved incident response and mitigation.

The desired outcomes include creating operational norms, optimizing alerting based on deviations from these norms, and developing dashboard visualizations to aid cyber defenders in better understanding and responding to potential threats. Utilities will gain a greater understanding into their own current capabilities to monitor and detect these attacks. Additionally, utilities will gain an understanding into how to better utilize the data they collect in their security organizations.

The public benefits of this project include providing guidance on the most effective and beneficial way to detect and discover cyber-attacks.

Project Approach and Summary

The project involves two main tasks:

- Task 1: Functional Architecture and Data Source Analysis. EPRI and its contractor will collaborate with funders to identify critical use cases, analyze substation functional architecture, and conduct tool and data source analysis to improve ICS cybersecurity. The goal is to identify gaps, recommend tooling changes, and propose additional data collection to enhance coverage.
- Task 2: Baselining and Dashboard Development that focuses on baselining normal operational activity, conducting trend analysis, and developing alerting dashboards to enhance cyber defenders' situational awareness and inform incident response actions.

Both tasks are expected to span a projected three (3)-month timeframe, contingent on timely utility support.

Deliverables

1. A Technical Report that presents findings and recommendations for the funders based on the analysis conducted, including both an individual behavioral trend analysis, and a trend analysis across all participating utilities.
2. A dashboard development methodology with reference implementation**.** This will include:
   - Requirements: data sources and SIEM capabilities for associated dashboards
   - Query pseudo-code
   - High-level dashboard structure
   - Playbooks

Price of Project

The price to join this project is $150,000 per utility. Funding qualifies for self-directed funding (SDF).

Project Status and Schedule

The project schedule is approximately 12 months depending on the availability of the participant's resources and facilities.

Who Should Join

Utilities that want to gain a greater understanding into their own current capabilities to monitor and detect cyber security attacks in OT.

Contact Information

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

Technical Contacts

Ben Sooter at 865.218.8108 (bsooter@epri.com)

Technical Advisor Contact Information

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

Northeast: Anne Haas at 704.608.6314 (ahaas@epri.com)

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

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

Product ID: 3002029440 **Project ID:** 1-119503 **March 2024**

EPRI

3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com