U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Mitigation of Externally Exposed Energy Delivery Systems (MEEDS)

Pacific Northwest National Laboratory (PNNL)

Bev Johnson, PM / Michael Mylrea, PI

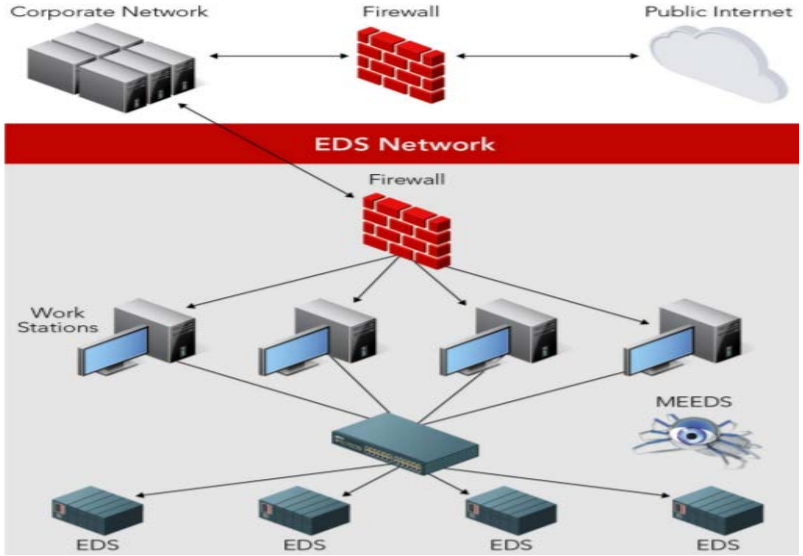
Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Mitigation of Externally Exposed Energy Delivery Systems (MEEDS)

Objective

- Develop and demonstrate a web-based application "MEEDS" to enable utilities to secure their networks by mitigating risks arising due to exposed and vulnerable energy delivery systems (EDS).



Schedule

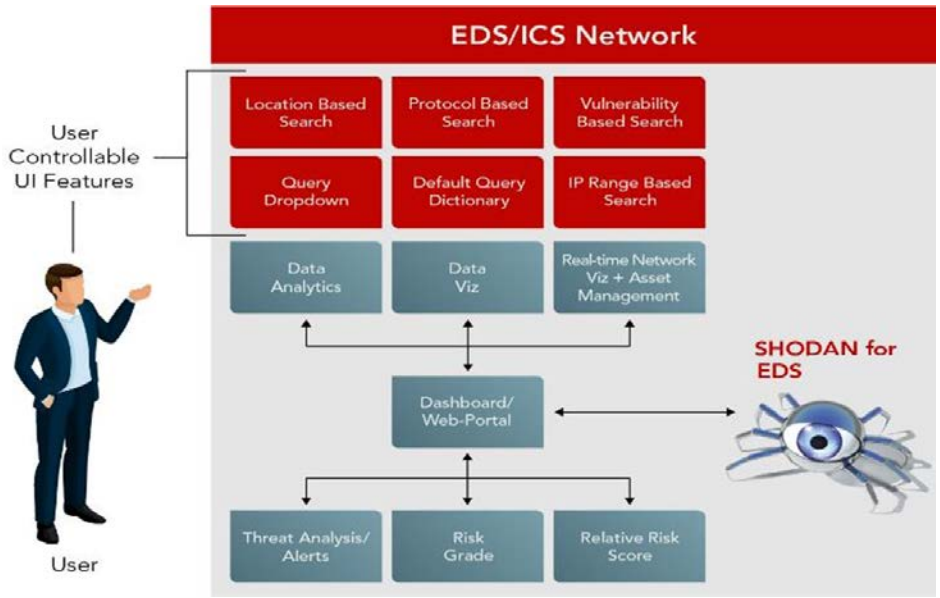
- October 2017 – September 2020
- Phase 1 – Design Application
- Phase 2 – Develop Prototype and Secure Infrastructure
- Phase 3 – Demonstrate Use of Prototype

Total Value of Award:	**$ 3,260,000**
Funds Expended to Date:	**10%**
Performer:	**Pacific Northwest National Laboratory**
Partners:	**NRECA, Shodan, Tenable, Hawaiian Electric Company, FoxGuard - pending**

Advancing the State of the Art (SOA)

- MEEDS provides a cost effective, easy-to-use solution that empowers resource constrained utilities enabling them to rapidly identify and protect externally exposed energy delivery systems
- MEEDS also provides an associated CVE or risk score with the exposed EDS identified to help stakeholders prioritize their mitigation efforts
- MEEDS addresses unique challenges—identifying exposed devices, safely scanning/querying operational technology, and providing timely cyber risk identification— to resource-constrained utilities without requiring a deep learning curve or a big budget.
- Leveraging previous PNNL CEDS research to better understand how MEEDS outputs can be adapted and tailored to meet the needs of control-room operators, including technical and non-technical operators
- PNNL partners are advancing interoperability through development of plugins between Shodan and various open source security solutions

Advancing the State of the Art (SOA)



MEEDS Features:

- Executing specific queries of information to identify inadvertently exposed EDS using a wide range of OT filters
- Supporting EDS protocols commonly used across the U.S. grid
- Identifying brands and models of EDS devices
- Archiving searches and findings, and comparing results
- Providing security alerts on the dashboard upon discovering vulnerabilities
- Providing risk quantification measures and risk mitigation actions

Expected Operational Impact:

- Easy customization by utilities to perform testing with full knowledge of their systems and networks
- Integration of security information and event management to allow automatic collection of real-time event alerts, and therefore provide a holistic view of the system-wide risks
- The ability of each utility participant to securely maintain a private log of their searches and findings
- Information such as vulnerability risk grades and relative risk scores

Challenges to Success

Technical Challenges:

- Ensuring software design meet end-user needs, requirements and is compatible with operational context
- Designing test environment representative of typical utility network
- Developing and validating method for quantifying risk ratings and scores
- Ensuring software interactions/connections/integration with database/SIEM

Proposed Approaches to Addressing Technical Challenges:

- Sustaining close collaboration with project's partners, using their insight to inform software design and development, test environment setup, and software validation and verification
- Using modeling/simulation in initial risk assessment and validating the method based on partners' evaluation
- Partnering with utilities to design pertinent use cases and using feedback to feed into software improvement

Progress to Date

- ***Technical Accomplishments:***
  - Intellectual Property Management Plan (IPMP) completed on Jan 31, 2018
  - Technology Landscape Report completed on April 23, 2018
  - Utility information gathering (limited) response by 9/30/18 to begin aligning requirements with feedback
  - Information gathering feedback from NRECA, at least 50 utility respondents October 31, 2018
  - Software Requirements Specification Document completed on October 11, 2018
  - Assisted in the addition of Common Vulnerabilities and Exposures risk scores to MEEDS
  - Assisted in expanding OT protocols available in MEEDS platform
  - Developed limited MVP to get in front of users so we can prioritize feature development
- ***Programmatic Accomplishments:***
  - Established industry advisor roles with Hawaiian Electric Company
- ***Outreach and Presentations:***
  - Michael Mylrea presented MEEDS at Tenable Edge Cyber Conference (Los Angeles, CA) March 6–9, 2018
  - Partner Engagement Meeting at PNNL (Richland, WA) on April 10, 2018

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Technology transfer to vendor space specific to OT cybersecurity (portion or all of MEEDS solution).
- Transfer knowledge to end user of small utilities through NRECA
- Testing
  - Initial lab testing with limited physical EDS devices
  - Lab demonstration to NRECA and select utilities
  - Expand to additional physical EDS devices / module testing with select utilities
  - Expand module testing to prototype testing with select utilities

Next Steps for this Project

Phase 1:

- Complete Deliverable D1.2 – Results of Device Assessment (Nov 15, 2018)
- Complete Deliverable D1.3 – Technical Report Functional Requirements (Nov 15, 2018)
- Complete Go/No-Go – G1.1 – Function requirements passes peer and industry review (Dec 15, 2018)

Phase 2:

- Develop Prototype and Secure Infrastructure
- Develop draft Technology Transfer Plan