U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Validation and Measuring Automated Response (VMAR)

Idaho National Laboratory

Securing energy infrastructure by providing a response comparison capability as technology changes

Automated response techniques used to combat a cyberattack rely on in-line tools and traditionally require continuous system monitoring. These techniques are not compatible with control systems in an energy delivery environment, because of the impact on latency requirements for safety. Using the common structured threat framework, detection and response can move to just-in-time with no impact on performance. VMAR instruments and analyzes latency performance metrics on four unique asset owner provided testbeds (distribution, transmission substation automation, and energy management system) with six unique automated response systems proving feasibility of using automated response in the operational technology environments. VMAR leverages the testbeds in the California Energy System for the 21st Century (CES-21) project funded by the California Public Utility Commission. Idaho National Lab has created three products for CES-21 in structured threat to support automated response: Structured Threat Intelligence Graph (STIG) – a visual threat analysis and programing application; Exploit, Malware, and Vulnerability (EMV) Scoring application for asset owners to prioritize and track cyber issues to their configurations; and Structured Threat Observable Tools Set (STOTS) – a just-in-time detection utility. All three products are available on https://github.com/idaholab/. The VMAR product measures, collects, and analyzes performance metrics proving these structured threat concepts have little to no impact on operations. VMAR has also created a response utility to enable others to investigate and adopt automated response – Structured Threat Automated Response (STAR) available on https://github.com/idaholab/STAR.

KEY TAKEAWAYS

- Delivers structured threat detection and response tools to provide automated response without impact to the operational environments
- Demonstrates no latency concerns on instrumented testbeds that enable measuring, collecting, and analyzing performance metrics
- Operationalizes a novel automated response proof of concept – Structured Threat Automated Response (STAR)

OUTCOME

VMAR proves that the use of automated cyber detection and response has little to no operational impact on the most sensitive equipment. Using structured threat concepts in the STAR utility enables system operators to share actionable and implementable threat intelligence for detection and response providing the ability to operate through cyberattacks.

PARTICIPANTS	ROLE
INL Idaho National Laboratory	Leads the lab for instrumenting CES-21 test beds, analyzing performance metrics during automated detection/response testing, and creating novel automated response utility
SDGE A Sempra Energy utility®	Provides asset owner testbed and serves as a project advisor
CES-21 Partners	Advisors
BYU BRIGHAM YOUNG UNIVERSITY	Intern support for instrumentation and STAR creation

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Rita Foster
Principal Investigator
Idaho National Laboratory
208-526-3179
Rita.Foster@inl.gov

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: May 2016 – February 2020

Total Award Value: $994,893
DOE Share: $994,893
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: May 2021