Researching the Next Generation of Automated Threat Response

CES-21 is a cybersecurity research and development program directed by the California Public Utilities Commission and the California Legislature. It is a collaborative effort between California-based investor-owned utilities (IOUs) and Lawrence Livermore National Laboratory.

The main objective of CES-21 is to explore the next generation of Industrial Control Systems (ICS) cybersecurity, in the form of machine-to-machine automated threat response (MMATR), to protect electric grid infrastructure from emerging cyberattacks. Program research, development, & demonstrations (RD&D) leverages automation methodologies, data integration, advanced modeling, simulation, and analytics, as well as virtual and physical test beds, to provide tools and approaches for enhanced grid security and flexibility.

Machine-to-Machine Automated Threat Response (MMATR)

What is MMATR's Research Objective? Why do we need it?

Due to the time criticality of cyberattacks on industrial control systems, an effective way to protect the power grid is through advanced detection and automated response capabilities. Automated response is a cybersecurity goal of growing importance as attack vectors—from a growing number of bad actors—are becoming more sophisticated and frequent. With the goal of improving reliability and operational efficiencies, MMATR is expected to:

- Enrich and streamline the gathering of threat intelligence
- Reduce the mean time to discovery and recovery
- Increase grid resiliency
- Lower risk posture
- Prevent attackers from reusing attacks

The research portfolio of CES-21 drives this strategy, by offering new channels for evaluation and prioritization of threats and remediation. The project will extend the research on advanced threat detection and automated response for application across all CES-21 California IOU participants, and, ideally, private sector vendors who could productize such research for the wider U.S. utility community.

Research and Primary Outcomes

Simulation Engine – The Modeling and Simulation (M&S) platform's purpose is to evaluate California's transmission system's resilience against cyber threats. The M&S platform is expected to provide the following key capabilities:

- Ability to test various MMATR technologies and concepts developed in this program at scale to evaluate performance, and to uncover any unintended, negative externalities introduced by automation.
- Modeling and simulation of grid and network devices to safely evaluate failures in a virtual environment to determine impact of cyber threats when applied at scale.
- Assisting in cybersecurity planning exercises to inform strategic investment and design decisions.
- Matching of anomalous ICS behavior with most probable cyber scenario cause and associated set of recommended remediation actions.

Substation Test Bed – A physical testbed environment, including substation equipment to test for vulnerabilities and potential mitigations. The reference control system architectures built here will also be used to test various research results offered by the CES-21 program.

ICS Cybersecurity Research Package – The goal of the research package is to provide new understanding of the logistical challenges and ICS priorities of automated threat response, in pursuit of accelerated commercialization by vendors. As such, the research package does not have the goal of developing production-level systems, but will provide the foundation for vendors and utilities to explore security automation more strategically.

Research Package Portfolio

- **Advanced Threat Detection** – The goal of advanced threat detection is to detect and identify sophisticated and previously unknown ICS cyberattacks. Advanced threat detection will explore various methodologies, using whitelisting and analytics, to evaluate possible solutions for identification of ICS threats.
- **Indicator and Remediation Language (IRL)** – IRL is a core component of a MMATR capability. IRL will be used to describe machine readable and actionable ICS indicators of compromise and remediation logic. The IRL of choice for this program is Structured Threat Information eXpression (STIX). CES-21 research findings will be submitted as extensions to the OASIS standards body. These extensions will improve the ability of STIX to describe ICS indicators of compromise and remediation.
- **SCADA Ecosystem Resiliency** – Investigation and testing on physical test beds unique to each IOU is crucial to an accurate assessment of MMATR technologies and concepts developed in the program and include the development of processes for threat and exploit prioritization and a tool to simplify Indicator and Remediation Language (IRL) generation. Machine-readable IRL will enable more resilient control system devices through early detection of illicit behavior and machine-speed remediation via preprogrammed responses to mitigate exploits before there is an impact.
- **Secure Systems Interfaces** – This effort includes investigation of next generation security protocols and quantum cryptography mechanisms to protect end-to-end communications between ICS devices. Technologies developed here include:
    - **Quantum Key Distribution** – Future-proof key distribution technology for immediate detection of interception of keys.
    - **Secure SCADA Protocol for the 21st Century (SSP-21)** – Cryptographic wrapper for existing legacy ICS protocols to ensure integrity of observation data and control signals.
- **ICS Data Aggregation** – Develop aggregation technologies, methodologies, and mechanisms to collect and process data from multiple, disparate sources, substation data, and threat intelligence. This effort will build test cases, test equipment, and test environments, as well as evaluate the effectiveness of data collection mechanisms.

Funding and Timeframe

$33 million over five years (2015-2019), enabled by California Senate Bill 96 and the CA Public Utilities Commission.

Participant Organizations

The Program utilizes teams of technical experts from the California IOUs, LLNL, and other partners who leverage and extend ongoing research in electric grid cyber security. Participating organizations include:

Lawrence Livermore National Laboratory

SOUTHERN CALIFORNIA EDISON
An EDISON INTERNATIONAL Company

SDGE San Diego Gas & Electric

PG&E Pacific Gas and Electric Company

Contact Info

CES21@pge.com