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

# REACT

NRECA America's Electric Cooperatives

## *Rapid detection and mitigation of cyberattacks*

The project team is developing a system for the rapid detection of cyberattacks and compromised systems and supports users in rapid remediation. This project combines National Rural Electric Cooperative Association's (NRECA) Essence rapid cyberattack detection technology with N-Dimension's N-Sentinel, which is a commercial cybersecurity monitoring and anomaly detection system. Together, in REACT, they detect attacks by sensing anomalies. REACT also examines packet information and deep content in all major utility protocols. This project tests the technology through field demonstrations at six electric utilities and releases it as a self-administered tool or as a remotely managed service. Underlying this technology, is the application of software-defined networking (SDN), which is revolutionizing management of operational networks within electric utility environments.

### KEY TAKEAWAYS

- Incorporates National Rural Electric Cooperative Association's ESSENCE technical prototype with a commercial monitoring and anomaly detection system
- Reduces time to detect a breach to less than one hour
- Provides a commercially viable technology as a managed service, hosted services, or open source

## OUTCOME

The application of SDN on an electric utility's operational network bridges the gap between security policy and implementation, detects and prevents potentially malicious traffic flows, and enables an electric utility to use fewer information technology staff members.

| PARTICIPANTS | ROLE |
|---|---|
| NRECA America's Electric Cooperatives | Conceived the project and provides overall leadership; high-level architecture; functional and non-functional system requirements; manages testing at cooperative utilities. |
| nrtc | Conceived the project and provides overall leadership; high-level architecture; functional and non-functional system requirements; manages testing at cooperative utilities. |
| n-dimension | Integrates React technology into their product offering; contributed to functional requirements during the development phase of the project. |
| MILSOFT Utility Solutions | Advises on the design of utility supervisory control and data acquisition (SCADA) systems and telemetry, and the detection of anomaly in SCADA data. |
| BLACKBYTE Cyber Security, LLC | Leads software developer with particular emphasis on data capture and parsing of engineering protocols. |

## CONTACT INFORMATION


**Initial Leads:**

Carol Hawk
Program Manager

Doug Lambert
Principal Investigator
National Rural Electric Cooperative Association
571-389-0446
doug.lambert@nreca.coop

**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:** October 2016 – September 2019

**Total Award Value: $2,049,710**
DOE Share: $1,473,582
Cost Share: $576,128


**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: June 2021