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

Neighborhood Keeper

DRAGOS

An R&D initiative to analyze and share non-sensitive data supporting asset identification, threat detection, and intelligence for collective defense for operational technology/industrial control system networks to be completed by June 2022

The project team is researching, developing, and deploying an interconnected sensor network in the operational technology (OT) networks of participating utilities using the Dragos Platform to deploy threat analytics and to detect threats and malicious behaviors. Non-sensitive participant data is shared securely and pseudonymously across the Neighborhood Keeper (NK) community to create a broad and comprehensive picture of a combined threat landscape. NK is a zero-trust and non-privacy invasive cloud-based network that is accessible to municipalities and utility cooperatives. This generates threat intelligence insights for the NK community to better understand active risks.

KEY TAKEAWAYS

- Analyze the output of shared detections in real time, identify insights, and securely communicate pseudonymized data to the community of participants
- Operationalize an early-warning system of real threats in a participant's sector or geographic location, allowing them to focus investigations on related threat behaviors in their environment
- Identify and monitor supply chain risks and unauthorized/unallowed vendors and devices in participant environments and the energy sector

OUTCOME

When completed in June 2022, this initiative will source and combine non-attributable threat data from the NK community, providing a broader and common view of the industrial threat landscape. The threat insights gained will be immediately available for threat detection and response from the sector.

PARTICIPANTS	ROLE
DRAGOS	Program lead; directs research and development efforts to ensure the solution produces secure and rapid sharing of non-sensitive threat information from participant OT networks
Ameren	Utility participant; supports research and development by providing requirements, testing technology under real-world circumstances, reviewing use cases and detections
FirstEnergy	Utility participant; supports research and development by providing requirements, testing technology under real-world circumstances, reviewing use cases and detections
Southern Company	Utility participant; supports research and development by providing requirements, testing technology under real-world circumstances, reviewing use cases and detections
A DIVISION OF NERC E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER	Advisor; provides program review and input on development, detections, and overall outcome to ensure consistency with the needs of the electric sector
INL Idaho National Laboratory	Advisor; provides program review and input on development, detections, and overall outcome to address the national threat landscape

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Robert M. Lee
Principal Investigator
Dragos
210-540-3068
rlee@dragos.com

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 2018 – June 2022

Total Award Value: $4,335,459
DOE Share: $2,835,572
Cost Share: $1,499,887

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