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

Cognitive Sense and Decision-Making Expert System for Adaptive IT/OT Cyber Defense – Project Corbomite

tdi technologies

Single, intelligent, system-state analysis and end-to-end intrusion tool driven by human domain expert knowledge

This project team develops and demonstrates a solution that protects and secures access to operational technology assets, preventing both malicious and inadvertent operation. This work enables electric utilities and oil and natural gas recipients to leverage technologies – like ConsoleWorks and open-source projects like Elasticsearch, Logstash, and Kibana – to protect and secure access to operational technology assets, collect and validate configuration settings, and develop field device situational awareness to prevent incorrect operation. In addition, TDI is developing a cybersecurity solution that monitors running memory and firmware configurations of embedded devices used in energy delivery control systems to validate device integrity and ensure trusted operations. TDI will demonstrate the system in both a laboratory setting with real-time digital simulators and in a utility environment to validate the solution's capability to secure assets and operations.

KEY TAKEAWAYS

- Provides firmware integrity and situational awareness of cybersecurity posture for embedded devices used in the electric utilities and the oil and natural gas sectors
- Automates and streamlines human-driven monitoring, auditing, and analysis processes and monitors devices running memory and firmware configurations to provide insights into how devices change over time
- Prevents grid misoperation by protecting and securing human access to operational assets

OUTCOME

Corbomite incorporates human subject matter expert knowledge and experience into a single tool that provides end-to-end analysis of a cyber intrusion by automating tasks of domain security experts that have previously been reliant on manual or human cognitive analyses. Corbomite streamlines load balancing decisions using the same artificial intelligence that monitors cybersecurity for more efficient and secure system operations.

PARTICIPANTS	ROLE
tdi technologies	Leads research, development, and demonstration
RED TRIDENT INC	Provides assistance with lab infrastructure and building of scenarios
Pacific Northwest NATIONAL LABORATORY	Lab testing partner
Dominion Energy	Industry advisor
MITRE	ATT&CK technology and product development

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Bill Johnson
Principal Investigator
TDi Technologies
972-509-8511
bill.johnson@tditechnologies.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 – September 2021

Total Award Value: $1,865,615
DOE Share: $1,435,804
Cost Share: $429,811

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