U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Neighborhood Keeper Dragos, Inc.

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- Provide a no-trust, low cost, interconnected sensor network to allow the rapid sharing of non-sensitive threat information from OT networks across participants to improve insight into the industrial threat landscape and reduce threat and risk exposure for a collective defense.

Schedule

- Start date: Oct 1, 2018/ End of Phase I: Feb 2021. End of Phase II TBD.
- Task 2.1 interviews complete and use cases gathered. Delivered report on lessons learned.

Total Value of Award:	**$ 4,323,309.00**
Funds Expended to Date:	**% 46**
Performer:	**Dragos, Inc.**
Partners:	**Ameren, FirstEnergy, Southern Co., INL, E-ISAC**

Project Overview

Schedule (cont)

- Neighborhood Keeper analytic framework developed, deployed, and operational for gathering and sharing analytical insights.
- Task 2.2 – COTS hardware/software (Dragos Platform) deployment to participant networks to then plug into Neighborhood Keeper analytic framework.
- Task 2.3 – Creating detections that track threats to electric sector. Deploying detections to customer environments and collecting output. Analyzing data to identify emerging patterns. Gathering input for deliverable report.

Advancing the State of the Art (SOA)

- Current OT threat information sharing is difficult, inefficient, costly, and often ineffective.
- To be able to share information, you must comb through your traffic, figure out what is important, package it up, and hope that you are not revealing anything about your environment.
- To consume it, you must take indicators of compromise, often without context, and operationalize them.
- Electric sector leaders recognize importance of improved threat awareness and synergistic value derived from sharing and receiving threat information but complexity of the process, fear of attribution or sharing sensitive data creates obstacles.

Advancing the State of the Art (SOA)

- Neighborhood Keeper approach removes these obstacles by:
  - Taking a behavioral based approach to threat detection instead of just indicators.
  - Based on the detections, collecting only non-sensitive data from inside OT networked environments.
  - Sharing them out in a way that is secure and removes identity of participant.
- This method frees up customers to participate in proactive information sharing thereby improving not only their own threat awareness but that of the other participants.
- Collective action for the win!

Advancing the State of the Art (SOA)

- Dragos, as the lead, partnered with electric sector utilities, to serve as participants allowing technology to be tested in real-world environments, and experienced advisors who represent national threat landscape and electric sector community to ensure program output was in line with current needs of the sector.
- Partner utilities serve as a guidepost to identify relevant use cases and ensure the detections are supplying the right level of insight for reduction of threats and improved risk awareness.
- The Neighborhood Keeper technology sits on top of Dragos COTS hardware/software solution (Dragos Platform) but uses separate security measures to protect data in-transit and data at-rest.
- Dragos took position that even if Neighborhood Keeper cloud environment was breached, attackers would only get non-sensitive data without association to a particular company. They would not learn anything which could discover what occurred or to whom.
- Machine-speed sharing of insights and intelligence on threats and assets without attribution or data risk

Advancing the State of the Art (SOA)

- Participant sharing results in broad insights supporting collective defense. Instead of each customer understanding just their own environments, they will also receive insights associated with threats to their sector and the community.
- Advanced insight improves resiliency through opportunity for reduction of risk and threat mitigation and prioritization.
- Each time the program adds another participant, the value of the insights available in the data set improves and the impact of data sharing magnifies.
- Evolving threat landscape is studied and tracked by experienced Dragos OT hunters and intelligence analysts. As new threats are identified, Dragos software engineers and experienced protocol experts codify knowledge into new detections.
- Also can identify risky equipment and vulnerabilities to inform participants and understand the environmental landscape.

Progress to Date

Major Accomplishments

- Completed Neighborhood Keeper technology (the cloud analytic framework).
- Already seeing demand for the solution. Expanded set of prospective customers from original three program participants to total of 20 utilities.
- Developed detections for and found network traffic associated with foreign vendors designated by the Department of Commerce as representing a threat to supply chain.
- Tested and proved out the ability to detect complex behaviors across environments to identify threats without access to the data or identity.

Challenges to Success

COVID-19 Impact

- Working with partners to overcome lack of availability through use of remote communications technology to mitigate as much as possible. There were delays associated with tasks which required physical access and availability of key personnel.
- Supply chain for hardware impacted by global pandemic pushing back deployments.

DCAA Audit Completion

- Working through logistics of completing DCAA audit.

Achieving critical mass of participants

- Adding participants outside of original program partners to improve quantity of data available to demonstrate value of research.

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

- Utilities of any size can benefit directly from this technology with sector wide visibility and insights; the program especially caters to small to medium sized utilities to give them a cost-effective mechanism and notification of critical events/attacks with the ability to reach out for help and support activating programs such as CMA.
- As part of the commercialization task, in preparation for execution in Phase II, Dragos will be preparing written material (white papers, data sheets) and planning events (webinars) to describe the program to potential customers and demonstrate how the technology works.
- Assuming travel is reasonable (e.g. diminished COVID-19), we plan to travel to industry events where we can present the technology and findings from the research and development phase.
- Once given the green light to begin Phase II, we will begin to execute on the commercialization plan by identifying and contacting interested customers to demonstrate the power of the solution on their OT cybersecurity and risk awareness programs.
- Customer acceptance is anticipated to grow throughout 2021 based on the value of the program and lack of available alternatives.

Next Steps for this Project

Approach for the next year or to the end of project

- Task 2.3 – Collect input from participants. Identify opportunities for improvement. Identify lessons learned. Complete report.
- Task 2.4 – Complete work with participants to evaluate use cases, identify new ones, and capture lessons learned. Gather findings. Compete report.
- Task 2.5 - Finish gathering input for industry benefits report. Complete report.
- Task 3.0 - Finalize commercialization plan. Socialize with partners. Develop written content and plan events to demonstrate the technology and lessons learned.
- Continue to attract additional program participants to prove out the value and acceptance. Sitting at 20 participants now.
- Prepare for Phase II and Task 4.0 by taking Task 3.0 commercialization plan and being ready to execute when approved.