THE PROBLEM

Industrial organizations are battling adversaries in isolation.

Cyber threats targeting ICS/OT networks continue to increase in frequency and sophistication, but data collection and analysis is extremely limited for industrial defenders. Adversaries are allowed to move through ICS/OT networks undetected. This ultimately allows them to train and prepare for their next cyber attack.

THE SOLUTION

Dragos Neighborhood Keeper. Collective Defense for Industrial Cybersecurity

COMMUNITY CHALLENGES

Why we created Neighborhood Keeper

- **LIMITED VISIBILITY**
  Data collection, analysis, and understanding the hardware and software assets in an OT environment has been a struggle.

- **INCREASED CYBER ATTACKS**
  ICS-targeted attacks are increasing in frequency and sophistication.

- **INTEL SHARING STRUGGLES**
  Information sharing programs rarely share intelligence. Sensitive data could be shared without context.

IDaho NATIONAL LABORATORY

Neighborhood Keeper Program Review

“NEIGHBORHOOD KEEPER PROGRAM STAKEHOLDERS WILL SEE GREAT VALUE IN THIS WIDE AREA VIEW CAPABILITY AS PARTICIPANTS CAN IDENTIFY A COORDINATED ACTIVITY OR A BROAD CAMPAIGN TARGETING MULTIPLE CRITICAL INFRASTRUCTURE ENTITIES.”
HOW IT WORKS

1. Dragos Platform customers deploy passive sensor in ICS/OT environment, and opt-in to Neighborhood Keeper. When detections fire in the environment, all data stays on premises with the customer and only anonymized metadata is shared.

2. Neighborhood Keeper receives the anonymous alert and shares detections and insights across the community to inform them of what’s occurring elsewhere, the prevalence of certain adversary methods, vulnerabilities, and risks to amplify and inform their own security efforts.

3. Participants may also anonymously make an encrypted request for assistance from other members. Members who respond can identify themselves temporarily to the requestor. The requestor can then identify themselves to the team of their choice to help them and then coordinate response efforts.

NEIGHBORHOOD KEEPER
Participant Benefits

- MORE EFFICIENT & EFFECTIVE DEFENSE
- IDENTIFY SUPPLY CHAIN RISKS FASTER
- SHARED COMMUNITY INSIGHTS
- FASTER INCIDENT RESPONSE & CYBER MUTUAL ASSISTANCE

To learn more about Neighborhood Keeper and how to participate, visit https://dragos.com/neighborhood-keeper/

Acknowledgment: This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000898.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Last updated March, 2021