INL/MIS-24-79011-Revision-0

Cybersecurity for the Operational Technology Environment (CyOTE)

July 2024

Alycia Brooke Honas

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed 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. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-24-79011-Revision-0

Cybersecurity for the Operational Technology Environment (CyOTE)

Alycia Brooke Honas

July 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Cybersecurity for the Operational Technology Environment (CyOTE™)

Overview

The Department of Energy's Cybersecurity, Energy Security, and Emergency Response Office (CESER) has partnered with Idaho National Laboratory (INL) and energy companies to develop CyOTE. This research initiative addresses cybersecurity threats against operational technology (OT) networks by sharing intelligence about adversarial tactics and techniques with the energy sector. CyOTE improves the sector's ability to detect anomalous behavior that indicates potential malicious cyber activity in OT networks.

Sponsorship

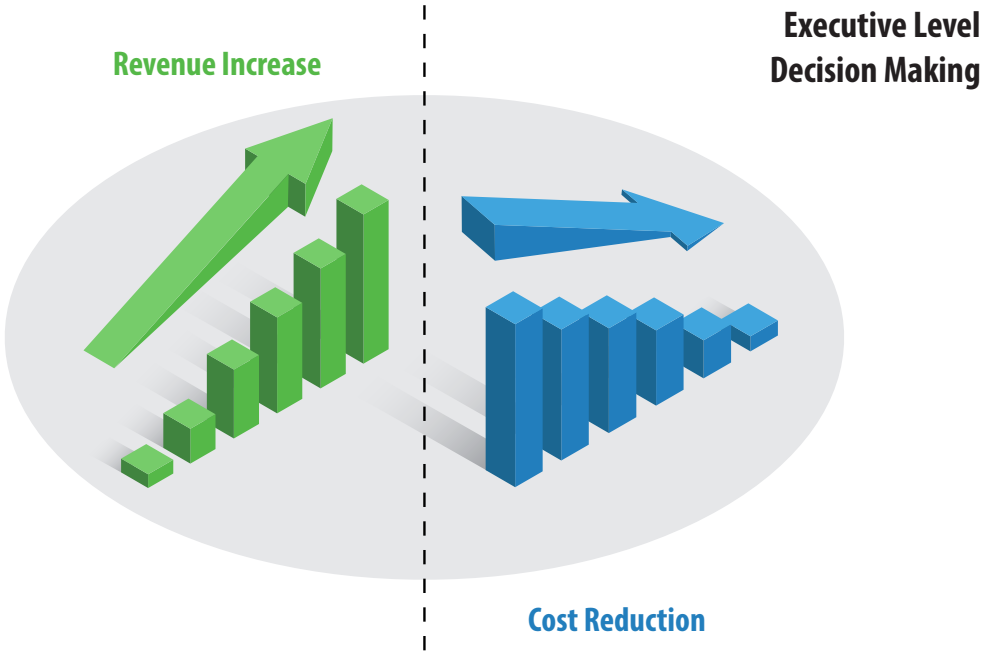
The CyOTE™ program is sponsored by the Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

Target Audience

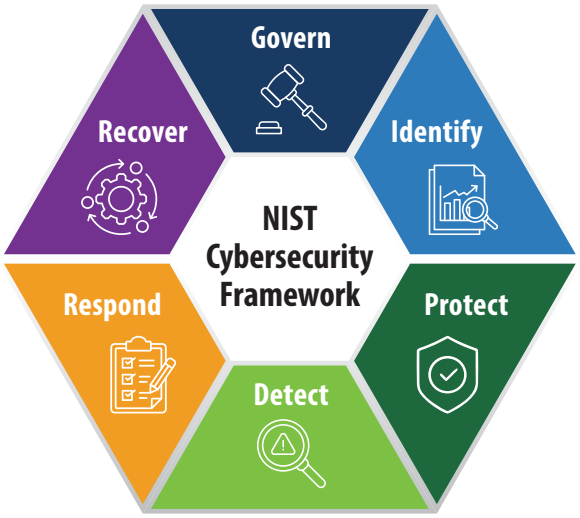
OT organizations seeking to maximize efficiency, reliability, and return on security investments. Primary functions and roles responsible for loss due to a cyberattack are Vice Presidents (VPs) of Engineering and Cybersecurity Information Security Officers (CISOs).

Organizational Challenge

With the increasing complexity of OT systems, VPs of Engineering and CISO's face growing cybersecurity threats that can disrupt operations and compromise safety. The consequences of an insecure OT environment can be catastrophic – cascading failure, lost revenue, a tarnished reputation, legal repercussions, and potentially life-threatening incidents.



Why Does This Matter? (2000-22 CyOTE Data)



Govern | Identify | Protect

Average Number of Precursor Events Prior to Disruption: 13 Unique Adversarial Behaviors associated with 150 observable events over 185 days

Detect | Respond | Recover

Average Time to Detect, Investigate, and Remediate: 254 days

Detect | Respond | Recover

Average Disruption Time Publicly Reported Cyber Attack: 69 days

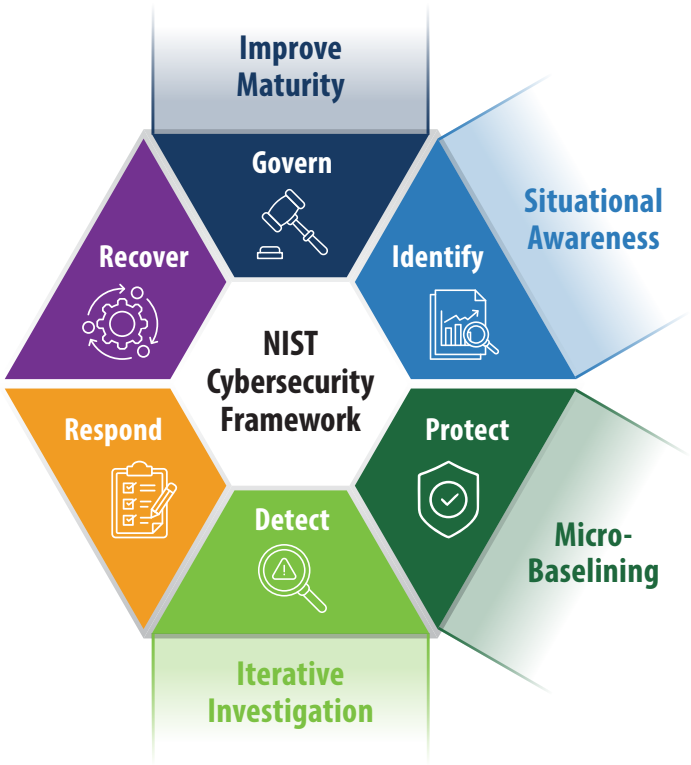
Govern | Identify | Protect
Detect | Respond | Recover

Average Financial Loss per Publicly Reported Cyber Attack: $614,128,203.00

CyOTE Solutions and Benefits

CyOTE offers a suite of tools designed to fortify your OT systems and empower your organization. These resources are the result of a trusted team from CESER and National Lab cybersecurity experts with years of research experience securing OT environments.

- **Situational Awareness:** *Identify* gaps in knowledge about adversarial behavior leveraging MITRE ATT&CK® for Industrial Control Systems (ICS).
- **Improve Maturity:** *Govern* your business goals with cybersecurity maturity goals aligned with Cybersecurity Capability Maturity Model (C2M2).
- **Micro-Baselining:** *Prioritize* understanding normal conditions on critical systems and implement countermeasures aligned with National Institute of Standards and Technology (NIST) Cybersecurity Framework to limit damage and resume operations quickly in case of an attack.
- **Iterative Investigation:** *Detect* through continuous monitoring and assessment of OT infrastructure activity to identify threats before loss of ICS control or disruption of business operations.
- **Tools & Training:** *Engage* in our purpose built tooling to parse through 13,000 + observable items and over 3,000 pages of data rich material to systematically inform and evolve OT Cybersecurity, coupled with training products that evolve diversified teams to identify anomalous behavior within a control process.



Implementing CyOTE

A key outcome is to increase operational resilience, deny adversaries the ability to create unplanned outages, and prevent unsafe working conditions.

Become a partner: Speak with one of our experts to see how you can participate and benefit from our partnership network and applied research.

email: CyOTE.Program@hq.doe.gov
url: https://cyote.inl.gov/

Revision 1, October 2023
21-50125_02