INL/MIS-24-79013-Revision-0

Operational Process for Trigger Identification and Comprehension (OPTIC)

July 2024

Changing the World's Energy Future

Alycia Brooke Honas

Idaho National Laboratory

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-24-79013-Revision-0

Operational Process for Trigger Identification and Comprehension (OPTIC)

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

Operational Process for Trigger Identification and Comprehension (OPTIC)

Overview

The Operational Process for Trigger Identification and Comprehension (OPTIC) is a standalone, downloadable application designed to enhance the CyOTE (Cybersecurity for the Operational Technology Environment) methodology and will be made available for free download to industry. OPTIC brings key CyOTE functionalities into focus.

OPTIC aids OT professionals in analyzing and determining whether an observed anomaly may indicate possible malicious activity or merely a maintenance related irregularity.

OPTIC guides users through an easy-to-follow workflow, referencing several industry-recognized best practices and standards, as well as the MITRE ATT&CK® framework for Operational Technology (OT) environments. In addition to empowering users to make informed decisions earlier in the process of a potential cyberattack, OPTIC functions as a cyber-awareness training tool, as well as a forensic research mechanism designed to strengthen cyber defense.

Sponsorship

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

The OPTIC application was developed by the Idaho National Laboratory (INL) as part of the DOE's Office of Cybersecurity, Energy Security, and Emergency Response research, development, and demonstration (RD&D) mission to improve and strengthen energy security.

Use Cases

The OPTIC application has three main use cases.

OPTIC is:

A job aid to assist users in documenting observed anomalies. OPTIC creates a timeline of events and assists in informed decision making. An OPTIC investigation may be initiated via a company's networked computer or on an approved mobile device.

A cyber forensics tool used to aid in post-event perception and comprehension. The OPTIC application may be used to investigate the details of a cyberattack, documenting anomalous events and their timelines. The OPTIC application will assist in identifying system vulnerabilities, including those vulnerabilities exploited by an adversary. System Admins can then use this analysis to harden exploited systems and pathways.

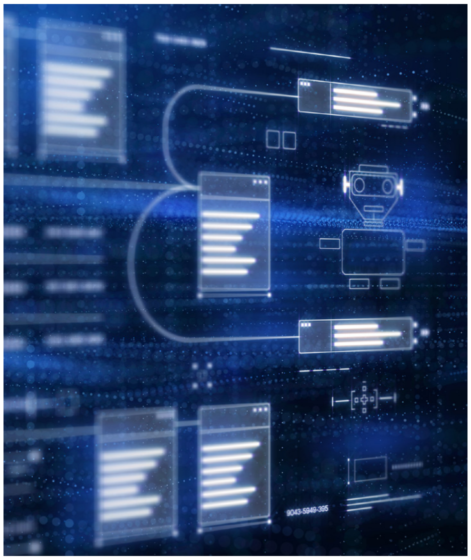
A training tool to help OT professionals expedite the identification of cyber anomalies. The main objective of OPTIC training is to foster the adoption of Heightened Awareness, with the goal of enabling accurate identification of the tell-tale-signs of a cybersecurity event.

Workflow

OT system operators know their systems and operational environments. The OPTIC application was designed with this in mind. Many OT professionals say they can often "sense" when something goes sideways. The OPTIC application empowers these "human sensors" to identify such sideways events and document their associated timelines.

A typical OPTIC investigation is initiated by an OT professional who observes something out of order, and then records that anomaly using the OPTIC application as a job aid — thereby empowering users to make informed decisions earlier during a potential cyber-attack.

After completing an investigation, the user will receive information to make an informed decision on how to proceed (i.e., escalate to investigate as a cyber event, or pursue additional avenues of investigation). If a documented anomaly is raised to the level of a potential cyber event, the OPTIC workflow will provide specific steps for mitigation and controls to strengthen cyber security posture. Additionally, the user may evaluate their organizational cybersecurity maturity based on the C2M2 (Cybersecurity Capability Maturity Model).



Key Benefits

- Provides an easy-to-follow workflow to assist decision making regarding potential cyber events based on the CyOTE™ methodology.
- Provides functionality to document an anomaly, either using a networked computer or an approved mobile device.
- Provides a systematic and repeatable analytical process based upon MITRE ATT&CK, NIST SP 800-53 Ver 5, and C2M2 Rev 2.1.
- Empowers users to make informed decisions earlier during a cyberattack.
- Provides the ability to analyze a company's cybersecurity maturity for vulnerabilities based on the C2M2 maturity framework.
- Provides avenues for mitigation during cyber events.
- Saves time by eliminating the need to research government and industry standards as they apply to a company's cybersecurity posture.

Capabilities Under Development

A tool to establish a baseline depicting "normal" operation, using the OPTIC mobile photographic functionality to document assets.

Implementation of an AI-based object recognition functionality to help establish a "normal" baseline.

The ability to map to NIST SP 800-82 Rev. 3.

Integration of cyber countermeasures to allow more effective and efficient execution of defensive response.

email: CyOTE.Program@hq.doe.gov

Access the CESER funded C2M2 website:
https://c2m2.doe.gov/