INL/MIS-24-79492-Revision-0

Collection and Analysis of Telemetry for CyOTE Heuristics (CATCH)

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

INL/MIS-24-79492-Revision-0

Collection and Analysis of Telemetry for CyOTE Heuristics (CATCH)

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

Collection and Analysis of Telemetry for CyOTE Heuristics (CATCH)

Overview

The Collection and Analysis of Telemetry for CyOTE Heuristics (CATCH) provides a framework for augmenting an organization's existing security controls with CyOTE developed analyses. CATCH collects, stores, analyzes, and creates STIX reports on anomalous data. CATCH connects the CyOTE analysis framework together with the MITRE ICS ATT&CK® patterns and highlights areas of improvement and further research. This tool is designed to enhance an organization's security controls by providing a structured approach to collecting, storing, analyzing, and reporting anomalous data.

Sponsorship

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

The CATCH tool was developed by the Idaho National Laboratory (INL) CyOTE program 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.

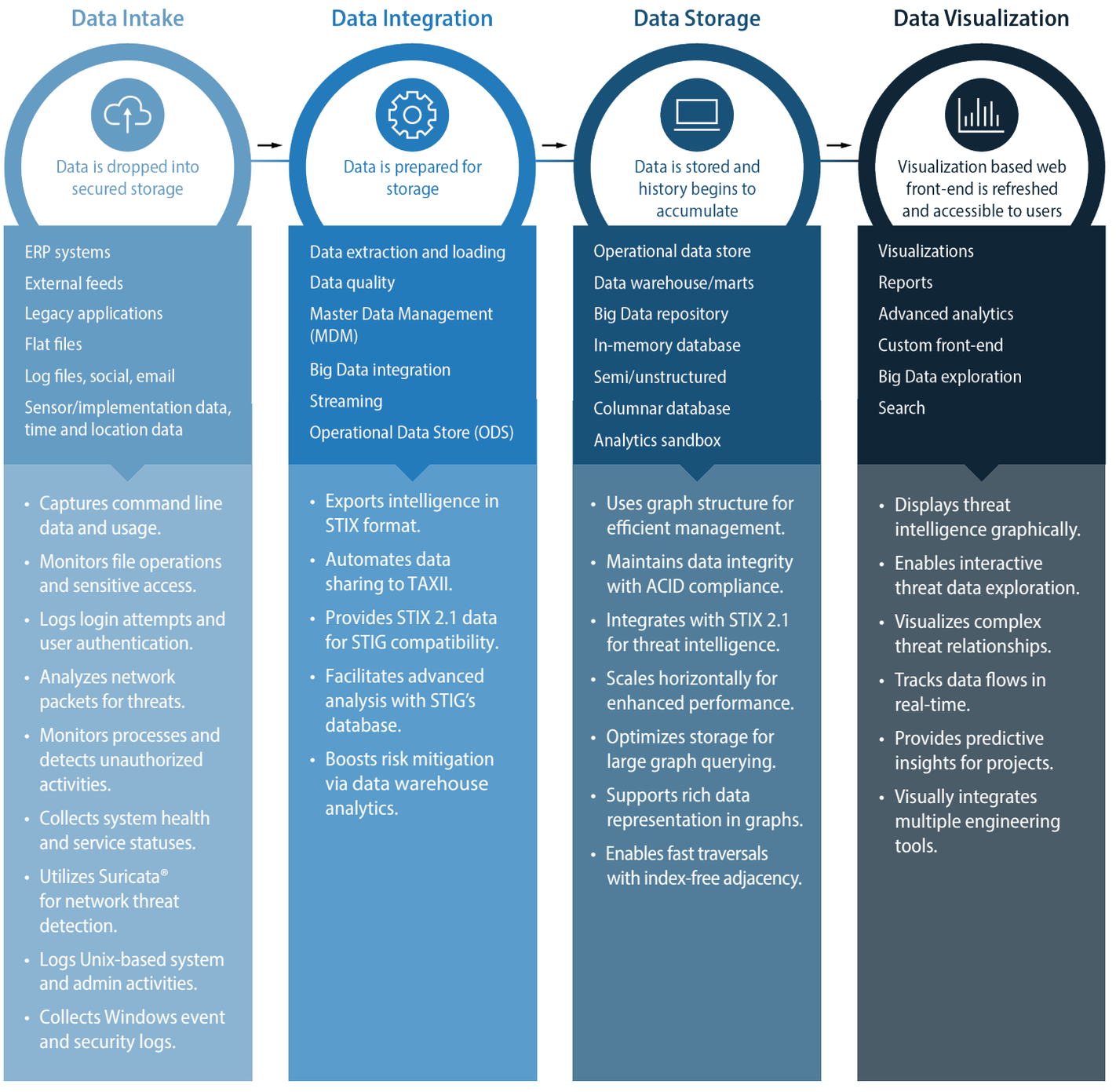
Use Cases

- Real-Time Threat Detection:
  - » Monitors network traffic and command line activities for immediate threat alerts.
- Incident Response and Forensics:
  - » Correlates data across systems for quick response; utilizes STIX 2.1 for tracking threats.
- Cyber Threat Intelligence Sharing:
  - » Automates threat data sharing in STIX format via TAXII; utilizes Security Technical Implementation Guide (STIG) standards for collaborative analysis.

Key Benefits

- Provides nine detection engines for flexible and varied threat collection capabilities, allowing for a comprehensive approach to identifying cybersecurity threats.
- Allows creation of profiles for data collection and analysis across network systems, optimizing resource use and enhancing the timeliness of threat detection.
- Uses a Neo4j database for storing telemetry data, enabling complex analyses to identify cyber threats through sophisticated query capabilities.
- Includes error handling and logging for system reliability and troubleshooting support, ensuring data integrity and system performance.
- Generates and transfers STIX 2.1 reports for streamlined sharing of threat intelligence through an integrated TAXII client, facilitating enhanced collaboration and communication among cybersecurity communities.
- Offers analysis against 25 MITRE ICS techniques for broad coverage of industrial control system vulnerabilities, providing a deep understanding of potential threats.
- Features automatic tool selection for effective use based on the threat landscape, ensuring that the most relevant tools are employed for threat analysis.
- Connects the CyOTE analysis framework with MITRE ICS ATT&CK patterns for cybersecurity defense improvement insights, aiding in the identification of areas for enhancement.
- Helps organizations augment their security controls with advanced analyses, enhancing cybersecurity defenses and overall security posture.

CATCH Workflow



Upcoming Integrations

- Integrate with the CyOTE developed Bayesian Attack Model (BAM) to inform the current phase of attack detection, for more precise response activities. **(Integration planned for FY25)**
- Integrate with CyOTE Operational Process for Trigger Identification and Comprehension (OPTIC) to increase users perceivably and comprehension of cyber events with STIX reports and data visualization using STIG. **(Integration planned for FY25)**

email: CyOTE.Program@hq.doe.gov

Revision 0, JUNE 2024

21-50125_05