U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Understanding the Special Case of Digital Forensics in EDS

Making Live Analysis work for Energy Delivery Systems

Background

In digital forensics forums, the idea of Live analysis is gaining momentum. Taking an image of an Information Technology (IT) system via a static analysis process has been the norm, but with more critical operational technology (OT) systems that control energy delivery, memory-only systems, and mobile devices, the concept of being able to take an image of a system while it is still functioning with a focus on its dynamic real-time memory is becoming more important. Static Analysis focuses primarily on creating an image of the internal hard drives while the system is at rest. Live Analysis looks at everything resident in memory at the time of imaging, and allows the system to remain up and operational.

Extending this capability to the dynamic systems that operate the electric grid is starting to generate interest but has not yet been fully explored.

Objectives

- Identify current Live Analysis capabilities for use in energy delivery systems (EDS).
- Test Live Analysis on operational EDS.
- Secure an industry partner to advise and to test the approach.

Project Description

Leveraging existing Live Analysis capabilities, this project is testing and identifying tools usable with EDS.

A scientifically robust approach is used for gathering requirements and identifying and testing tools. A panel of industry subject matter experts, with a focus on the electric sector, is advising the project team and reviewing work throughout the project.

Technical Approach

This project is evaluating existing Live Analysis monitoring and detection tools for EDS use. It is composed of three tasks.

Task 1: Identify an industry partner and advisory board

This area is maturing quickly as EDS sites are understanding the need for operational technology security. EDS operators can learn from and leverage the learning curve that IT navigated in developing these approaches and processes to establish sound forensic practices.

- Establish a panel of industry experts to serve on an industry advisory board (IAB).
- Identify a utility partner.
- Solicit IAB review and feedback on proposed approach.

Benefits

- Evidence of current or previous anomalous behavior can be discovered while the EDS is live.
- Data captured from monitoring the EDS and/or network can be evaluated and used to determine useful features of available tools.
- Industry involvement ensures technical applicability to industry needs.

Partners

- **Pacific Northwest National Laboratory** (lead)
- Avista
- Schweitzer Engineering Labs
- GE Digital Energy

Period of Performance

September 2014 – January 2017

Total Project Cost

$425,000

Content last updated: August 2016

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Lori Ross O'Neil
Principal Investigator
Pacific Northwest National Laboratory
509-375-6702
lro@pnnl.gov

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov

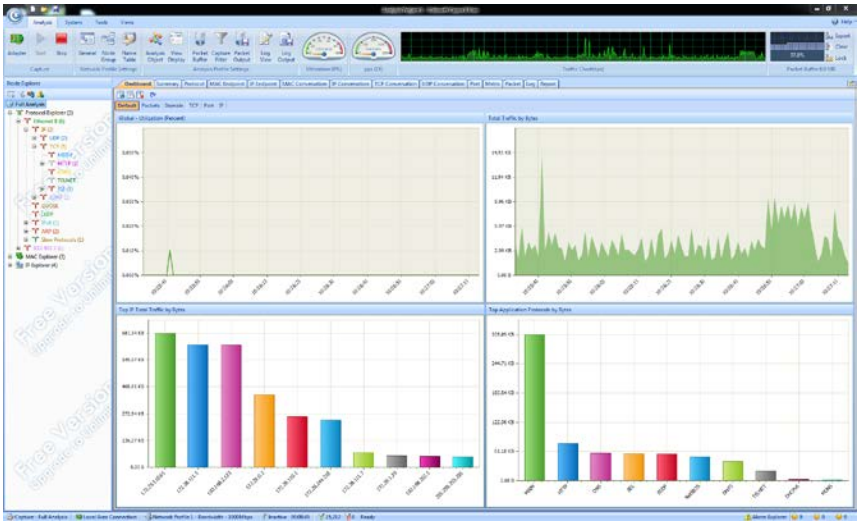

Figure 1: View of a live analysis window

Task 2: Evaluate EDS monitoring and Live Analysis capabilities

EDS event monitoring tools are maturing. Several versions of well-known IT monitoring and detection tools now come in a SCADA variant, which can be leveraged for EDS. Both commercial and open-source types are available and can be stood up as a basis for alerting to anomalous EDS system behavior, which would be the starting point to use EDS forensic live capture and analysis tools.

This task evaluates existing Live Analysis and event monitoring tools to determine existing capabilities and gaps.

Objectives of Task 2:

- Evaluate existing commercial and open source Live Analysis tools, using a review of the literature, and conduct basic testing of findings based on input from a project panel.
- Select and implement EDS Live Analysis tools on the Pacific Northwest National Laboratory Power Networking, Equipment, and Technology (powerNET) testbed, which allows experimentation on power system technology in a non-operational environment.

Task 3: Use Live Analysis for EDS active forensic capture and analysis

The focus of this task is to ensure that Live Analysis will not inadvertently impair the purpose or intended outcome of EDS systems or the delicate balance of the U.S. electric grid. This task is working closely with a utility to ensure our approach is real-world and takes into consideration the requirements of live EDS.

Objectives of Task 3:

- Generate malicious traffic to initiate and test forensic live capture.
- Test Live Analysis on powerNET with known malicious traffic.
- Develop and test identified capabilities, as identified by industry.
- Report on the test process and results of Live Analysis EDS tools testing.
- Update the cyber forensic plan based on results.
- Document results of the project and share with industry.

End Results

Project results will include the following:

- Evaluate and report on current Live Analysis and network monitoring tools for use with EDS using IAB defined requirements.
- Document our test network and quality assurance approach for future testing and to share with industry.
- Recommend a Live Analysis and digital forensic toolkit that can be used by industry.