# Advanced Grid Operational Technology Edge-Level Threat Detection

William Hupp,[1] Adarsh Hasandka,[1] Vivek Kumar Singh,[1] and Salam A. Baniahmed[2]

*1 National Renewable Energy Laboratory*
*2 Eaton Research Labs*

**NREL is a national laboratory of the U.S. Department of Energy**
**Office of Energy Efficiency & Renewable Energy**
**Operated by the Alliance for Sustainable Energy, LLC**

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

**Technical Report**
NREL/TP-5R00-83989
March 2023

# Advanced Grid Operational Technology Edge-Level Threat Detection

William Hupp,[1] Adarsh Hasandka,[1] Vivek Kumar Singh,[1] and Salam A. Baniahmed[2]

*1 National Renewable Energy Laboratory*

*2 Eaton Research Labs*

**Suggested Citation**

Hupp, William, Adarsh Hasandka, Vivek Kumar Singh, and Salam A. Baniahmed. 2023. *Advanced Grid Operational Technology Edge-Level Threat Detection*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-83989. https://www.nrel.gov/docs/fy23osti/83989.pdf.

**NREL is a national laboratory of the U.S. Department of Energy**
**Office of Energy Efficiency & Renewable Energy**
**Operated by the Alliance for Sustainable Energy, LLC**

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

**Technical Report**
NREL/TP-5R00-83989
March 2023

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

## NOTICE

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

# Acknowledgments

The authors thank the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER) for their support of this research through the Technology Commercialization Fund (TCF) supported by the Office of Technology Transitions (OTT). The authors express their gratitude to Walter Yamben, Jessica Perry, and Joseph Dygert of the U.S. Department of Energy for their valuable feedback, guidance, and support through monthly meetings. The authors are thankful to the Eaton Laboratories team for being an active key partner with their synergetic engagement in this project. We are grateful for their continuous technical support, for their participation in weekly meetings, for providing a device for developing the hardware-in-the-loop (HIL) test bed, and for facilitating the demonstration with their business team.

The authors are also thankful to the National Renewable Energy Laboratory's Cyber Range operations team, including Shane McFly, Simon Kim, and Michael Abbondanza, for their continuous technical support in operating the cyber range platform with a minimum contingency and for developing the HIL test bed. The authors are grateful to NREL's communications team, including Nika Durham, Katie Wensuc, Brittany Conrad, and Anthony Castellano, for proofreading this technical report, performing text and graphics editing, and coordinating with other team members. The authors are also grateful to Jean Schulte and Erin Beaumont for developing the nondisclosure agreement and for helping us to complete the technology transfer agreements with Eaton. Without their guidance and support, it would have been difficult to facilitate the commercialization-level discussion and develop the nondisclosure agreement with Eaton. The authors also appreciate Jared Macon and Dane Christensen for participating in regular principal investigator meetings to ensure that the project was on track and that each milestone was completed within the projected time frame.

# List of Acronyms

| | |
|---|---|
| ARIES | Advanced Research on Integrated Energy Systems |
| CIP | Critical Infrastructure Protection |
| CLI | Command Line Interface |
| DNP3 | Distributed Network Protocol 3 |
| DNS | Domain Name System |
| DoS | denial of service |
| FTP | File Transfer Protocol |
| HIDES | Hybrid Intrusion Detection for Energy Systems |
| HIL | hardware-in-the-loop |
| HTTP | Hypertext Transfer Protocol |
| IDS | intrusion detection system |
| IT | information technology |
| IViz-OT | Intrusion Detection Visualizer for the Operational Technology Network |
| MITM | man in the middle |
| NERC | North American Electric Reliability Corporation |
| NESCOR | National Electric Sector Cybersecurity Organization Resource |
| NREL | National Renewable Energy Laboratory |
| OT | operational technology |
| SCADA | supervisory control and data acquisition |
| SSH | Secure Shell Protocol |
| YAML | Yet Another Markup Language |

# Executive Summary

The current power grid is increasingly subjected to severe and sophisticated cybersecurity threats. There is a compelling urge to address and advance the legacy supervisory control and data acquisition (SCADA) system critical infrastructure readiness to tackle the cybersecurity and resilience concerns considering the newly deployed sensors, actuators, and data aggregators. From a utility perspective, cyberattacks might not be considered part of the required operator training. Recently published reports on attacks on U.S. and non-U.S. power grids show how the operator could have played a significant role in protecting the system from malicious controls and momentarily isolating the source of attack until the right response team could be dispatched. This project intends to improve the intrusion detection mechanism in a critical system where intelligence is involved to distinguish between a cyberattack and a regular electrical fault.

This report presents a deployable solution to improve the cybersecurity situational awareness of the legacy SCADA system infrastructure in power grids. The main goal of this project is to provide system owners and operators a highly trusted, intelligent alarm system and comprehensive situational awareness of ongoing or potential cybersecurity threats on the grid network. The key contributions of this project include: (1) the development of software, the Intrusion Detection Visualizer for the Operational Technology Network (IViz-OT), to visualize and locate intrusions on the grid network; (2) testing the signature-based Hybrid Intrusion Detection for Energy Systems (HIDES) (Singh et al. 2020) for different types of intrusions; (3) the integration of HIDES and IViz-OT into the visualization dashboard; and (4) real-time testing using a hardware-in-the-loop test bed.

The proposed IViz-OT was designed to manage alerts, generated from HIDES, and map them with tailored scenarios that could be easily comprehended by grid operators. This software visualizes the generated alerts in real time while providing information about the locations and types of attacks. The key features of IViz-OT include: (1) data storage and alert visualization, (2) user-based interaction with the application programming interface, (3) flexibility and compatibility with vendor devices and data models, and (4) user-based custom scenarios to prepare grid operators for the necessary corrective actions. This work used the signature HIDES to detect different types of information technology and SCADA-system specific cyberattacks based on the defined signature rules. The selected attack vectors and attack classes were also mapped with the defined National Electric Sector Cybersecurity Organization Resource (NESCOR) vulnerability classes (NESCOR 2014) and North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards (NERC 2022) while highlighting their potential impact on the distribution grid. These NESCOR vulnerability classes and NERC CIP standards showed the criticality of attacks that were considered in the experiment, and it is crucial for the proposed cybersecurity solutions to quickly detect and alert the grid operators. During the experimental analysis, both the HIDES and IViz-OT solutions were tested and validated in the laboratory environment and have been proven ready for field-testing and deployment in the utility environment.

# Table of Contents

# List of Figures



# List of Tables

# Introduction

The power grid is becoming an increasingly complex and interconnected cyber-physical system, with more dependencies on the communication infrastructure and the information technology (IT) network. With high penetrations of renewable energy resources, there has been a substantial expansion of the cyberattack surfaces because of the proliferation of cyber-physical systems in the physical, communication, and application layers of the grid network. Therefore, it is crucial to develop agile and innovative solutions that can address the cybersecurity threats and potentially be deployed in the utility environment. Further, a robust commercialization platform is required to support the technology transition from research to real-world deployment. To address these challenges and to support research-and-development-based cybersecurity development and technology commercialization, the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER) awarded funding to the National Renewable Energy Laboratory (NREL) and Eaton Research Labs to develop a deployable cybersecurity solution that can identify intrusions at the system and network layers with an intelligent alarming system to support cybersecurity situational awareness for system operators in real time.

The proposed solution, the Intrusion Detection Visualizer for the Operational Technology Network (IViz-OT), was designed to develop an intelligent alarming system integrated into the Hybrid Intrusion Detection for Energy Systems (HIDES) at the network layer. The combined IViz-OT and HIDES solution improves grid cybersecurity by continuously monitoring supervisory control and data acquisition (SCADA) system network traffic, detecting different types of anomalies, identifying their locations, and informing grid operators through a summary of different events and generated reports. A high-level overview is shown in Figure 1.

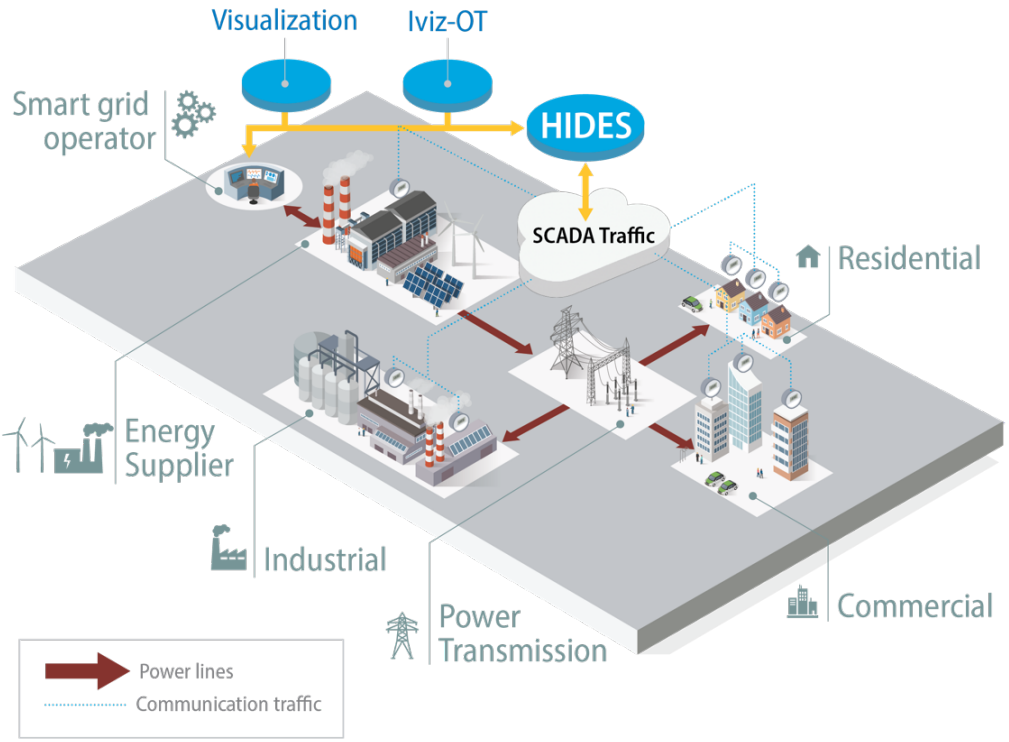



**Figure 1. A high-level overview of the integrated IViz-OT and HIDES environment**

## 1.1 Objective

The main goal of the project is to provide a highly trusted alarming system for grid operators that includes accurate detection with minimum false alarms for an ongoing or potential cyberattack while supporting network-based verification. That includes continuous IT asset logging and data traffic inspection. The early alarming system supports invoking incident management, speeds up system recovery, and ensures availability. The main project objectives are to:

1. Provide operators with a highly trusted alarming system for different types of intrusions into the grid network.
2. Demonstrate a proof of concept through the experimental case study and hardware-in-the-loop (HIL) test bed-based validation.
3. Discuss deployment opportunities in the operational technology (OT) environment for legacy SCADA systems to support technology commercialization.

## 1.2 Motivation

Existing cybersecurity solutions were mostly designed for IT applications and were not directly suitable for OT-based networks. Several manufacturers and systems engineers are updating their existing solutions to support security operations for critical industrial control system infrastructures. With the evolving cybersecurity threats, the IT-based solutions and "security by obscurity" approaches are not satisfactorily performing to the level at which critical asset owners and operators would be safe. It is imperative that OT-based solutions use grid information, along with network data, to ensure consistent and robust performance.

Also, the current market lacks the proposed technology, which can provide defense-in-depth solutions using analytical approaches. Consequently, because of the complexity and heterogenous nature of data in the OT environment, more effort should be given to commercialization by working closing with industry vendors and having regular discussions with utilities and stakeholders. Therefore, it is crucial for U.S. Department of Energy national laboratories to work closely with industry vendors and utilities to develop a deployable solution that can support technology commercialization and adoption by end users.

The development of the IViz-OT software is essential for grid operators because no tool exists that can help them analyze and correlate cyber and physical events in real time. This software assists grid operators in understanding the generated alert logs from the intrusion detector by mapping them with different scenarios. Here, *scenario* means an event that has occurred in the grid network and is defined in the simplest term such as attack classes, that will be easy to understand and interpret by the grid operators. This tool also correlates different events based on their timing and generates an outcome summary that is easy for grid operators to understand. Finally, a report will be generated for further forensic analysis and archiving of the occurred event. This project also leverages HIDES, which has signature and behavior-based rules to identify anomalies based on different SCADA-specific protocols for the grid network.

## 1.3 Key Contributions

The key project contributions are:

1. **Development of a visualization software (IViz-OT):** This project developed a software for visualizing intrusions in the grid network. It also provides information about different types of attacks and the nature of attacks with their locations in the grid network.
2. **Testing of HIDES in the OT network**: This project supported the testing of HIDES software by integrating it with the Eaton's SMP Gateway in the HIL platform for detecting intrusions using the applied signature-based rules.
3. **Integration of IViz-OT into HIDES for the visualization software**: This project supported the integration of IViz-OT into HIDES for detecting, visualizing, and comprehending anomalies to support cybersecurity situational awareness for grid operators.

# 2 Advanced Operational Technology Detector

## 2.1 Intrusion Detection System

Many in-line intrusion detection system (IDS) tools use real-time monitoring along with basic features such as packet inspection and analysis to enable real-time alerts and threat detection in IT networks. Various kinds of detection mechanisms can be used to generate alerts. Some of the more common are signature-based, anomaly-based, and state-based. Regardless, all mechanisms rely on the basic features of an IDS.

A signature-based IDS, such as Suricata, is a good example of an open-source IDS, which is used in many enterprise systems and might be used in a network security system for a site. There are various options for IDS tools to protect a site, both proprietary and open source. Some commonly used solutions with their top features are listed in Table 1.

**Table 1. Summary of Existing IDS Tools**

| IDS Tool | Open Source | Top Features | | |
|---|---|---|---|---|
| SolarWinds Security Event Manager | No | Collates IDS log | Generates risk assessment reports | Automated asset discovery |
| Kismet | Yes | Provides a basic feature set | Various plug-ins available | Data export functionality |
| Zeek | Yes | Tracks DNS, HTTP, and FTP activity[a] | Customizable policy scripts | Monitors various kinds of traffic |
| OpenDLP | Yes | Prevents data loss | Identifies at-rest data across multiple systems | Supports agents or agentless operation |
| Sagan | Yes | Multithreaded architecture | Compatible with rule management software | User-friendly Snort-like design |
| Suricata | Yes | Integrates with other databases | Supports standard input/output formats | Detects complex threats |
| Security Onion Solutions | Yes | Powerful suite of tools | Network and host-based IDS hybrid | Provides traffic pattern insights |

[a] DNS: Domain Name System; HTTP: Hypertext Transfer Protocol; FTP: File Transfer Protocol

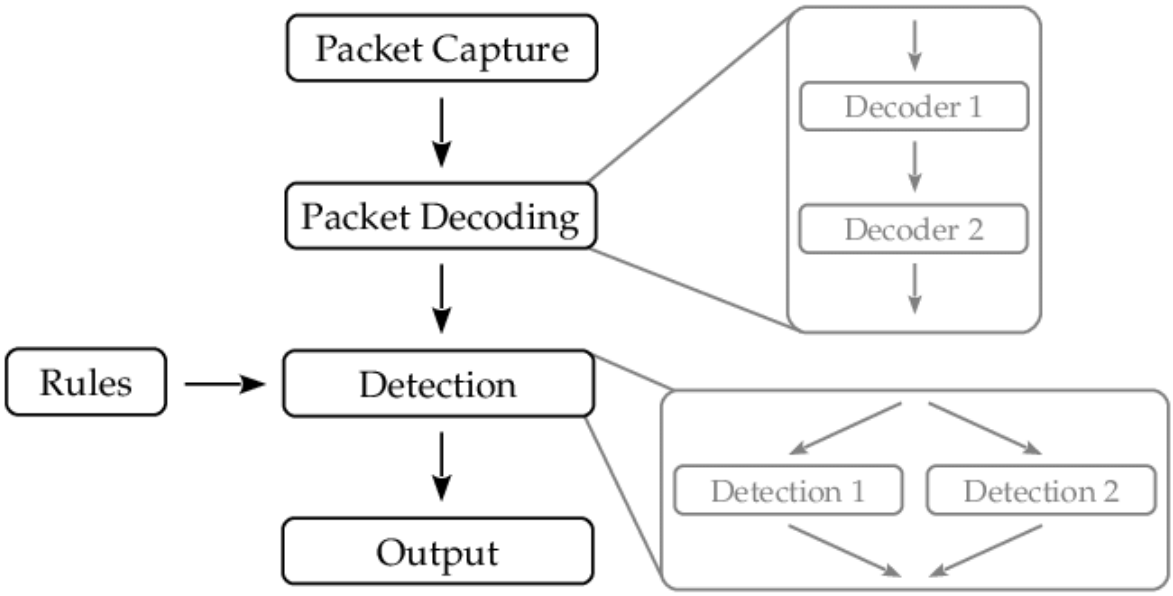



**Figure 2. The Suricata architecture**

Source: Ghafir et al. (2016)

## 2.2 ARIES Cyber Range

As part of the Advanced Research on Integrated Energy Systems (ARIES) platform, NREL's Cyber Range allows researchers and partners to study energy systems' interaction with and dependence on digital communication devices and networks. NREL's unique energy systems modeling, and co-simulation capabilities are the differentiating factors in realizing proven cybersecurity protocols for increasingly renewable and distributed energy systems. To match the complexity of modern, multilayer grids, the cyber range is designed to evaluate multi-owner power systems and visualize interdependencies with digital communication devices and networks.

The cyber range provides the ability to virtualize, emulate, and visualize energy systems subjected to energy disruption scenarios, with the fidelity needed to represent future energy and telecommunication systems—from individual devices to regional grids.

The cyber range enables powerful, interactive research, administration, and management front ends; adds a powerful visualization and demonstration capability; and provides a library of emulation tools, including component models, configuration scripts, and prebuilt prototype research environments. This world-class capability is designed to answer research questions at scale using virtual and physical assets by leveraging simulation, emulation, and power hardware-in-the-loop. Through the cyber range, NREL can emulate physical and communications-related aspects of distributed energy resources at scale to provide system-level security evaluation for bulk power renewables and distributed energy systems.

## 2.3 Software Definition and Requirements

To deploy this application for the test scenario, the following software are required:

- Suricata IDS
- Docker.

### *2.3.1 Suricata Intrusion Detection System*

As one of the more prominent open-source IDS tools in the market, Suricata was selected to implement within the site network for the virtual test bed in this experiment.

### *2.3.2 Docker*

Docker is a container virtualization platform that allows for easy development and deployment of containers. In this experiment, Docker is run on a Linux host; however, docker can be run on various kinds of operating systems, including Windows. The provided application container can be configured and run using Docker.

## 2.4 Hardware Requirements

To deploy this application for the test scenario, the following hardware are required:

- Eaton SC-2200 or other computing resource
- Eaton SMP 4/DP.

### *2.4.1 Eaton SC-2200*

In this scenario, the Eaton SC-2200 substation computer is used as a computing resource for the cyber range. This hardware resource also runs all the software components of the test bed and connects to the HIL resources under test. To run only the parser and detector containers that are necessary for the application, the hardware requirements are very low.

### *2.4.2 Eaton SMP 4/DP*

Eaton's SMP 4/DP device (Gateway automation platform) used in this scenario functions as a monitoring and control device for the virtualized power delivery "site" where the attack occurs. It is also part of the attack surface and could be a target for some specific attacks. The SMP device is an advanced substation automated solution that is configured to monitor the site devices and generate alarms when thresholds are crossed. These alarms are consumed via the SMP application programming interface by the parser element and in that manner are forwarded to the detector.

## 2.5 Technical Approach

Using the virtual resources of the cyber range, we deploy a test bed onto an Eaton SC-2200 to demonstrate the capability of the attack signature development and testing using the platform, and we subsequently leverage that capability to develop the IViz-OT visualization software. The team then aims to develop a packaged version of the detector that can run on any Eaton customer network or device. Containerization and Docker were used to achieve this in an easy-to-deploy fashion.

# 3 Attack Vectors

This section discusses the different types of intrusions that can be considered in the grid environment. The listed cyberattacks are classified into two categories: (1) IT-based attacks and (2) SCADA-based attacks, which are discussed in detail here.

## 3.1 IT-Based Attacks

IT-based attacks include traditional host- and network-specific attacks that are generally applied on the IT network and are not specific to the SCADA network. In this category, two attacks were considered: (1) unauthorized system access and (2) denial-of-service (DoS) attacks.

1. Unauthorized system access: This attack includes providing unauthorized access to the network or device using the existing communications, such as Secure Shell Protocol (SSH) or Telnet, using the default log-in credentials.
2. DoS: This attack involves sending a large number of packets to flood the network traffic or targeted hosts, which eventually disables the required service. There are different methods for performing DoS attacks, which include common attacks, such as Smurf and SYN floods.

## 3.2 SCADA-Based Attacks

SCADA-based attacks include those that depend on the SCADA-specific protocols, field devices, data aggregators, and several other digital access points that are deployed in the grid network. In this category, a man-in-the-middle (MITM) attack is considered.

- MITM: This attack includes hijacking an active network session from a legitimate source and injecting malicious measurements disguised as genuine measurements to provide incorrect situational awareness to the operator.

The National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 defined cybersecurity failure scenarios (NESCOR et al. 2014) in different domains, including distributed energy resources. Table 1 presents the mapping of attack types and attack targets with the NESCOR vulnerabilities and North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. The NERC CIP standards are mandatory security standards for grid operators. They include 14 standards (CIP-001 to CIP-014) to cover the physical, cyber, and operational security of power grids. Further, the impacts of cyberattacks also depend on the nature and location of the attacks. For example, a failure in a control center application has more severe consequences than that of the monitoring application because of its control capabilities. Therefore, potential physical impacts are also discussed in Table 2 with attack types and attack targets.

**Table 2. Cyberattack Mapping With NESCOR Vulnerabilities and NERC CIP Standards**

| Attack Type | Attack Target | Potential Impacts | NESCOR Vulnerability Classes | NERC CIP Standards |
|---|---|---|---|---|
| DoS | Site meter | Loss of observability, communication failure | Inadequate network segregation, unnecessary network access, week credentials | CIP-0010: Configuration Change Management and Vulnerability Assessments, CIP-0011: Information Protection, CIP-0012: Physical Security |
| DoS | SMP manager | | | |
| Unauthorized system access (SSH) | SMP Gateway | System oscillation, transient instability | Unnecessary system access, inadequate patch management process | CIP-010, Configuration Change Management and Vulnerability Assessments |
| MITM | DNP3[a] | Communication failure, equipment damage, operational delay, market impacts, | Inadequate change and configuration management, lack of software patches | CIP-014: Physical Security |

[a] DNP: Distributed Network Protocol 3

# 4 Test Bed Architecture

The test bed is designed to mimic a small distribution power system environment. Specifically, this test bed allows a control device, such as the SMP, to connect to several virtual devices distributed across a simulated power system model (Cleveland et al. 2008).

## 4.1 Power System Model

In this project, the power system model under test is the IEEE standard 13-bus feeder model. This model consists of 13 buses that are interconnected by 10 lines, including both overhead and underground lines. It is a highly loaded, 4.16-kV, single-substation regulator model (Kersting 2001). It has one generation unit, one voltage regulator unit consisting of three single-phase units, as well as an in-line transformer. This model consists of the elements connected as shown in Figure 3.

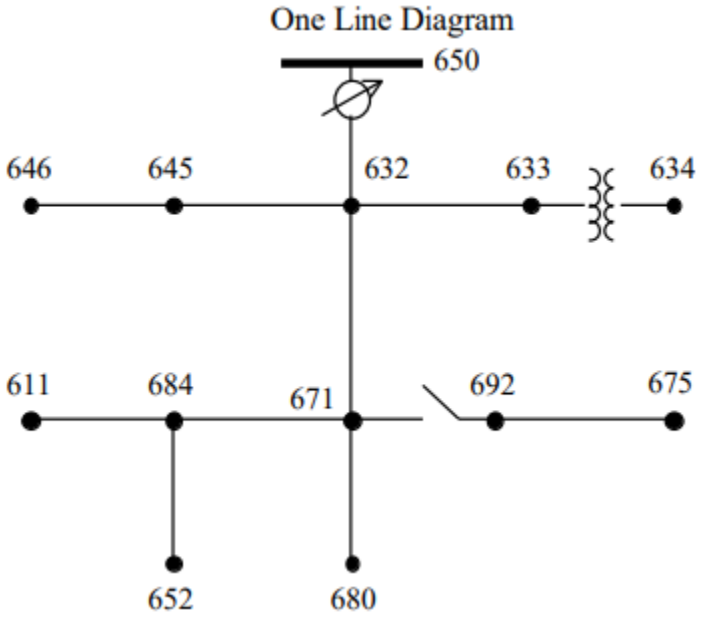



**Figure 3. An IEEE 13-node feeder diagram**

Source: Kersting (2001)

This model was selected for evaluation because it is a good generic distribution system feeder model for testing software. The aggregate load at node 634 was chosen to be represented by the virtual site elements. This leads to a model as depicted in the cyber range grid visualization screenshot in Figure 4.

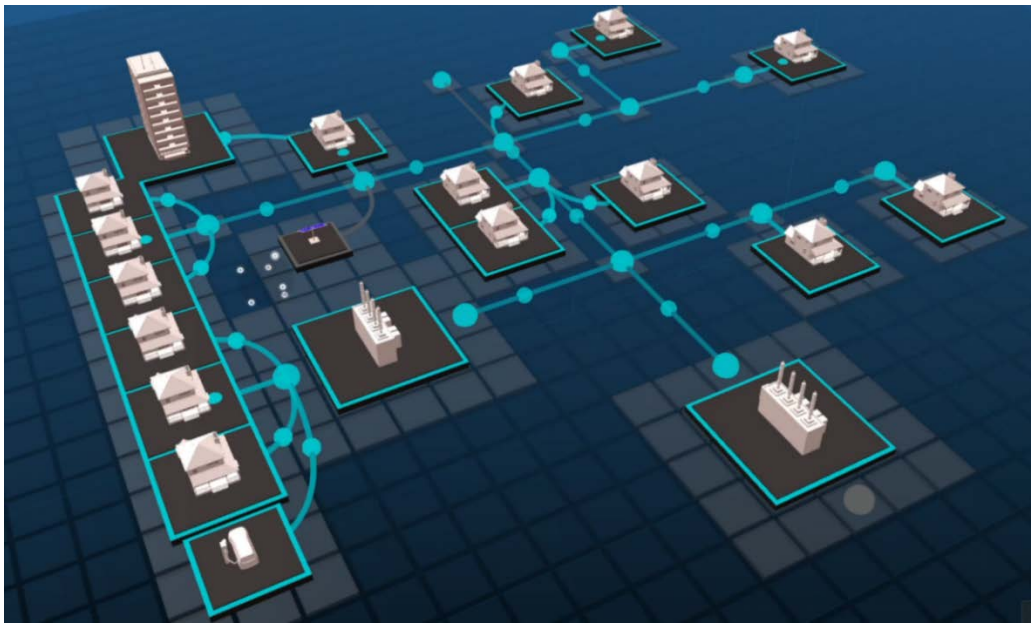


**Figure 4. A 3D visualization of the power system model**

As shown in Figure 4, the total load at that node is represented with an electric vehicle supply equipment load element, as well as a residential load element. These network elements are connected to the corresponding power system elements in the OpenDSS simulation software that they relate to using the internal co-simulation framework of the platform (Hasandka et al. 2020). OpenDSS is an open-source, steady-state power solver, developed by the Electric Power Research Institute, which is used to produce near-real-time solutions for the underlying power system model. The time step used for these solutions can be reduced to improve the resolution of the elements. In this scenario, a 1-second time step is used for the solutions. The OpenDSS model used looks like the screenshot shown in Figure 5.

```
Clear
Set DefaultBaseFrequency=60

!
! This script is based on a script developed by Tennessee Tech Univ students
! Tyler Patton, Jon Wood, and David Woods, April 2009
!

new circuit.IEEE13Nodeckt
~ basekv=115 pu=1.0001 phases=3 bus1=SourceBus
~ Angle=30                                          ! advance angle 30 deg so result agree with published angle
~ MVAsc3=20000 MVASC1=21000    ! stiffen the source to approximate inf source



!SUB TRANSFORMER DEFINITION
! Although this data was given, it does not appear to be used in the test case results
! The published test case starts at 1.0 per unit at Bus 650. To make this happen, we will change the impedance
! on the transformer to something tiny by dividing by 1000 using the DSS in-line RPN math
New Transformer.Sub Phases=3 Windings=2   XHL=(8 1000 /)
~ wdg=1 bus=SourceBus   conn=delta  kv=115  kva=5000   %r=(.5 1000 /)
~ wdg=2 bus=650            conn=wye    kv=4.16  kva=5000   %r=(.5 1000 /)

! FEEDER 1-PHASE VOLTAGE REGULATORS
! Define low-impedance 2-wdg transformer

New Transformer.Reg1 phases=1 bank=reg1 XHL=0.01 kVAs=[1666 1666]
~ Buses=[650.1 RG60.1] kVs=[2.4  2.4] %LoadLoss=0.01
new regcontrol.Reg1  transformer=Reg1 winding=2  vreg=122  band=2  ptratio=20 ctprim=700  R=3   X=9

New Transformer.Reg2 phases=1 bank=reg1 XHL=0.01 kVAs=[1666 1666]
~ Buses=[650.2 RG60.2] kVs=[2.4  2.4] %LoadLoss=0.01
new regcontrol.Reg2  transformer=Reg2 winding=2  vreg=122  band=2  ptratio=20 ctprim=700  R=3   X=9

New Transformer.Reg3 phases=1 bank=reg1 XHL=0.01 kVAs=[1666 1666]
~ Buses=[650.3 RG60.3] kVs=[2.4  2.4] %LoadLoss=0.01
new regcontrol.Reg3  transformer=Reg3 winding=2  vreg=122  band=2  ptratio=20 ctprim=700  R=3   X=9

```

**Figure 5. An OpenDSS model file for the IEEE 13-bus feeder**

## 4.2 Test Bed Network Architecture

The test bed is enabled by using the available virtualization resources to deploy it virtually. In this case, the SC-2200 was chosen as a small computing resource that could demonstrate the capability of this tool. Choosing more expensive hardware computing resources might allow for a larger number of emulated devices in the test bed. Three network devices were virtualized for the resources available in the selected system. A meter was connected to the electric vehicle supply equipment load, an additional meter was connected to the site head, and the third device was connected as an inverter controller. These virtual devices hosted on the SC-2200 were connected to the SMP 4/DP device, as shown in the network architecture diagram in Figure 6.

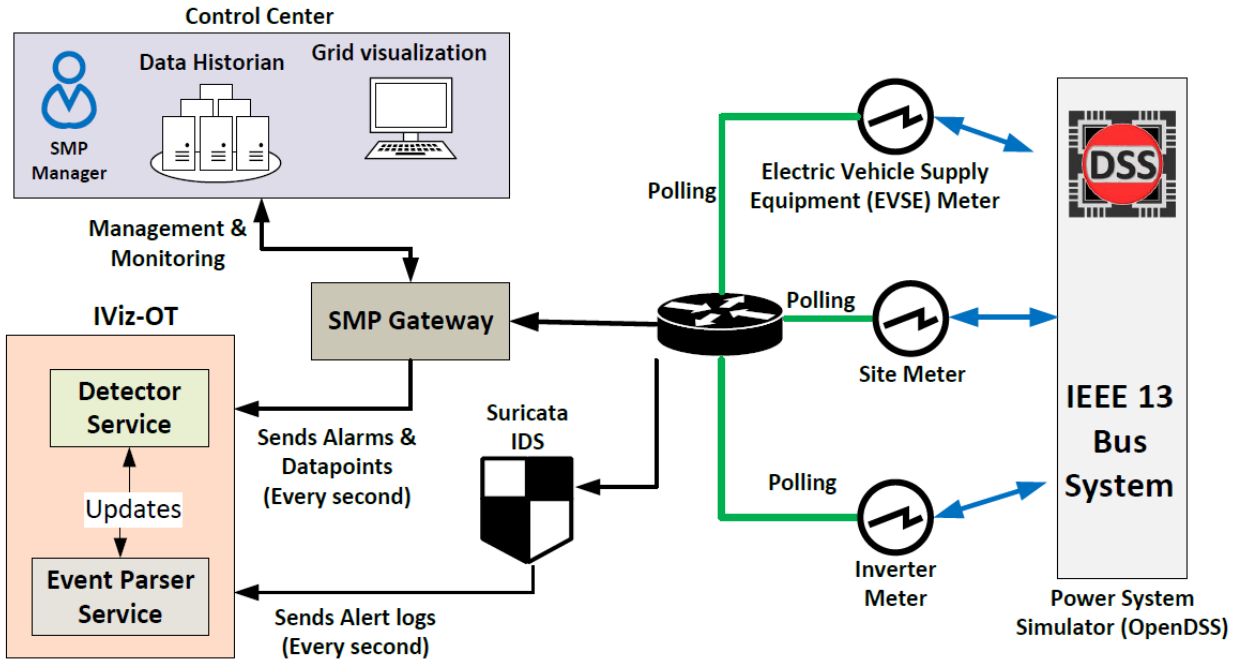



**Figure 6. An HIL experimental setup for attack detection**

These devices were physically hosted in NREL's data center in adjacent racks. Although multiple SMP 4/DP devices as well as an SG2460 are connected to the computing resource, only one SMP 4/DP device is selected to participate in the developed scenario. This was only because of the limitations of the computing resource in terms of the size of the test bed that can be tested, not because of any limitations on the number of HIL devices that might be connected. For a test bed with more computing capability, all the devices could be deployed to evaluate a more complex scenario.

The network visualization is shown in the 3D representation in Figure 7. A sphere is located near the visualization of the 3D power device to which it is connected. This sphere represents the local network or subnet used to connect the devices together. Each device is represented by a marked node in the sphere. The network traffic generator, NetFlow, records between them are represented as individual packets flowing along the white lines between the nodes.

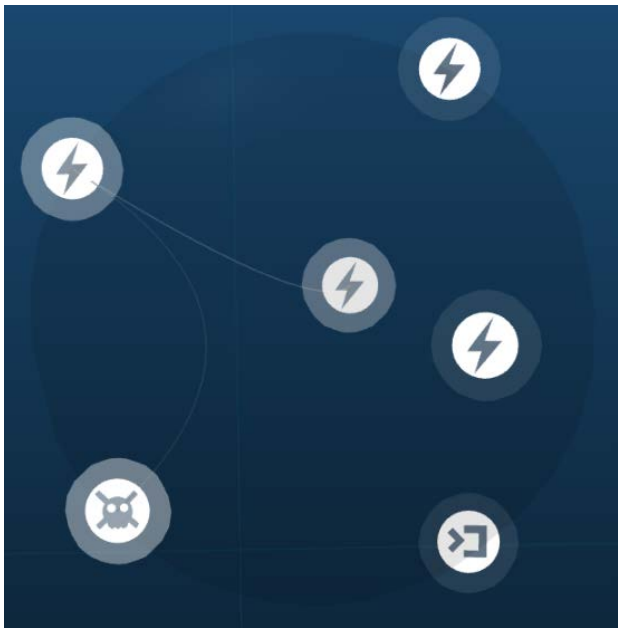


**Figure 7. A 3D network visualization**

The network visualization can also showcase real-time alerts from the internal IDS. Any record of an alert produced by the IDS is captured and overlaid onto the network visualization as a colored and elevated network flow. The nodes will also flash with the color of the severity of the alert that was received. In the test bed, high-severity alerts are red, and lower severity alerts and warnings are orange and yellow, respectively. See Figure 8.

**Figure 8. An IDS alert in the 3D network visualization**

Details and specific fields from the alert are captured and visualized as tiles in the event log of the device or node. The event log stores all the alerts seen by the visualization for that device in the local cache, and the user can scroll through to find historical alerts, even after the real-time communications and alert have passed. See Figure 9.


**Figure 9. Viewing alert details in the visualization**

## 4.3 Grid Visualization Dashboard

The threat detector can be deployed in NREL's Cyber Range, which provides real-time visualization capabilities of the network flow, power flow, device architecture, and IDS or SMP alerts, as shown in Figure 10.


**Figure 10. Example of the cyber range grid visualization dashboard**

The 3D visualization is a capability of NREL's Cyber Range and uses simple representations for both the network and power flows. Each network device is represented by a white node within the sphere representing the local network. Real-time network communication activity is represented by small white packets flowing between the nodes. These local networks, in the combined view, hover over the power system elements with which they are geographically co-located. The power flow between these elements is represented by blue spheres moving along the

lines to indicate the direction of the flow. In this manner, the combined power and network view provides a significant level of visibility into the scenario conditions.

## 4.4 Detector Service Dashboard

The threat detector is managed through a dashboard deployed with the Django Python web framework. Restful commands are used to communicate with the detector service. When an event is sent to the detector from the SMP and IDS parser, the signature is compared against predefined signatures in the detector dashboard, and the signature is mapped to a scenario. A report containing a decision is created based on the of the scenario relationship mapping of the run time events. See Figure 11. The detector and decision tree processes are further explored in Appendix A.4.

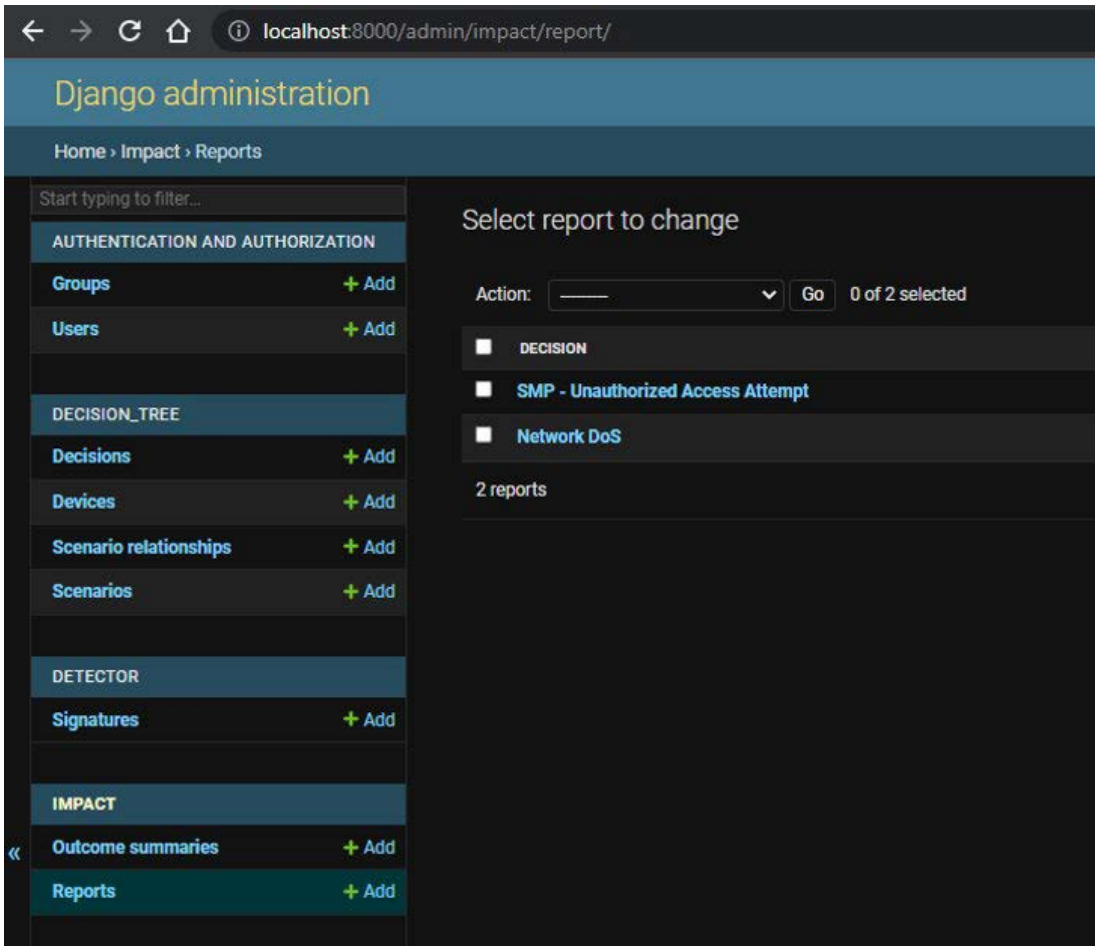



**Figure 11. Detector service dashboard**

## 4.5 Event Parser Dashboard

The parser, which runs as a container, takes alerts and alarms from the power monitor (SMP application programming interface) and IDS logs and restfully sends them to the detector as signatures. The detector then makes decisions based on the defined rules for the parser-generated signatures.

# 5 Experimental Testing and Evaluation

As a part of the deployment pipeline for the advanced OT detector, GitLab, GitLab Runners, and Ansible technologies were used to orchestrate and deploy the container. The minimum necessary steps to deploy the detector can be run using other methods available for containers, such as Docker Command Line Interface (CLI) or Docker Compose. These individual steps are shown in the Ansible Yet Another Markup Language (YAML), Ain't Markup Language (.yml) file, which is used to deploy containers. See Figure 12.

```
---
- hosts: master
  tasks:

  - name: Deploying detector service...
    become: false
    become_user: tcf
    shell: docker run -d --rm --name detector --network host 192.168.99.41:5000/detector-service:v1.1
           Hupp, William, 3 months ago • reverting headmismatch …
  - name: Copying database to detector service...
    become: false
    become_user: tcf
    shell: docker cp {{project_path}}/detector-configs/db.sqlite3 detector:/detector-docker/db.sqlite3

  - name: Pause for 10 seconds to start detector
    pause:
      seconds: 30

  - name: Deploying parser service...
    become: false
    become_user: tcf
    shell: docker run -d --rm --name parser -v /tmp/experiments/:/tmp/experiments/ --network host 192.168.99.41:5000/parser-service:v1.0

  - name: Training decision tree...
    become: false
    become_user: tcf
    shell: docker exec -it detector python3 manage.py shell -c 'from decision_tree.models import DecisionTree; DecisionTree.load().train()'
```

**Figure 12. AOT detector deployment steps**

The steps can be reduced to:

1. Run the container for the detector service.
2. Start the detector database.
3. Deploy the parser.
4. Deploy the detection model.

## 5.1 Attack Vectors

### *5.1.1 DOSAttack*

One method of executing a DoS attack is to have an attacker run the hping3 using a Kali Linux virtual machine to send packets and saturate the bandwidth of the connection between the IEDs. The IDS would detect the DoS network attack using the defined signature-based rule and flag it as an alert. The generated alert signature would help inform the SMP of the impact that resulted in the loss of observability. IViz-OT generates the DoS attack report and outcome summary from the signature generated from the parser IDS logs. See figures 13–15.

**Figure 13. A malicious packet in the cyber range visualization**

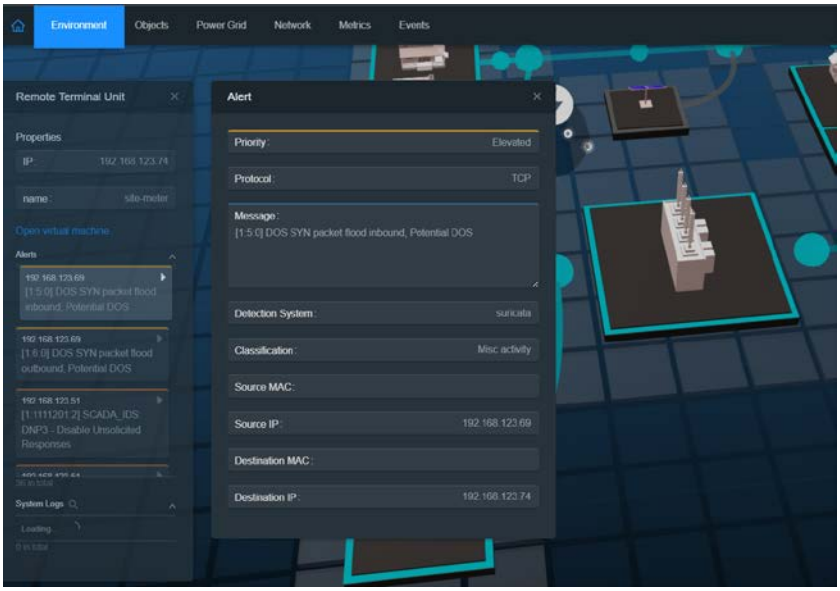



**Figure 14. An alert received in the cyber range visualization**

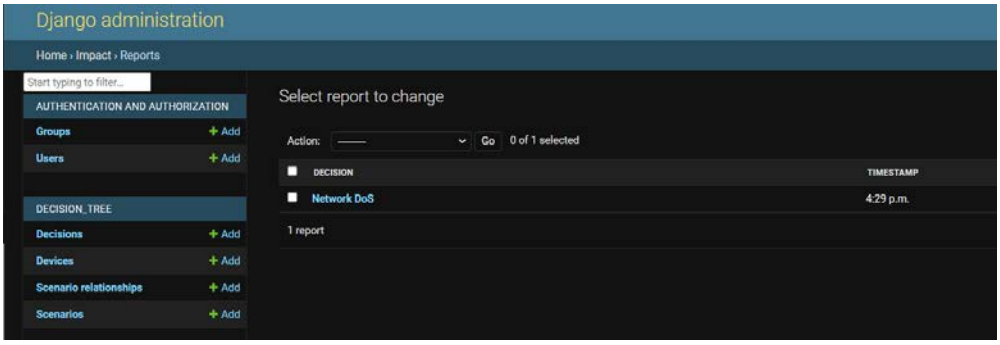



**Figure 15. An IDS alert in the detector**

### 5.1.2 DNP3 MITM Attack

An attacker having eavesdropped on unencrypted DNP3 communications between the site meter and the SMP can see how to target the site meter and send a malicious command to disable the device. In this case, we assume that the attacker has the necessary credentials and was sending a tripping packet through a separate session. The malicious command—which caused the breaker of the substation to open, resulting in the loss of power to the site—is flagged as it is executed. IViz-OT will generate a report related to the defined scenario. In this case, a "Site Meter Power Sag" signature was generated from the parser's power alert received from the SMP, and a "Site Meter Possible MITM" parser signature was generated from the IDS logs. See figures 16–19.

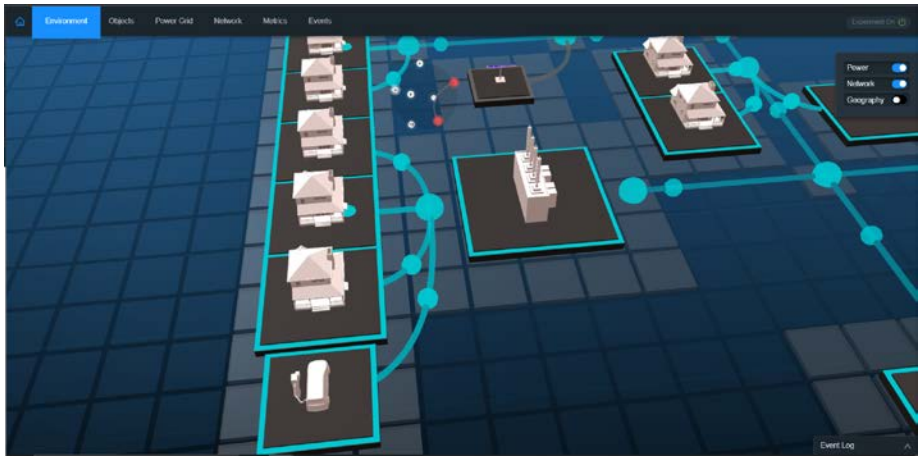



**Figure 16. An MITM attack on a substation in the cyber range visualization**

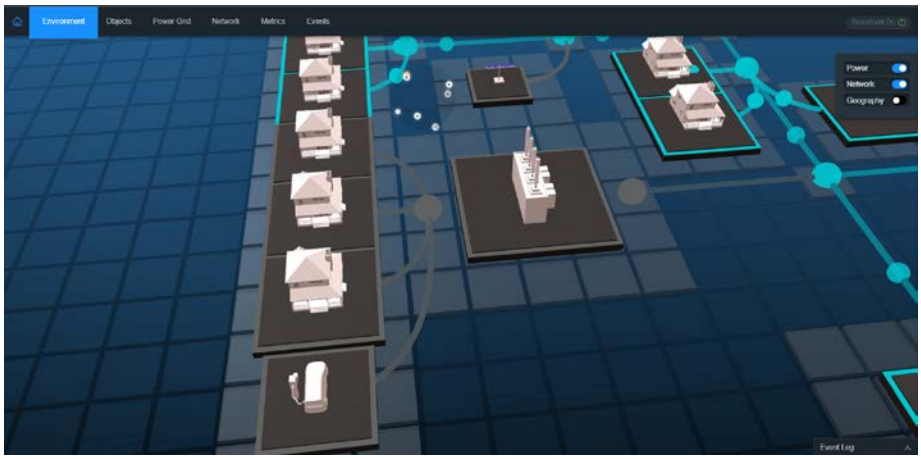



**Figure 17. The substation power-off after an MITM attack**

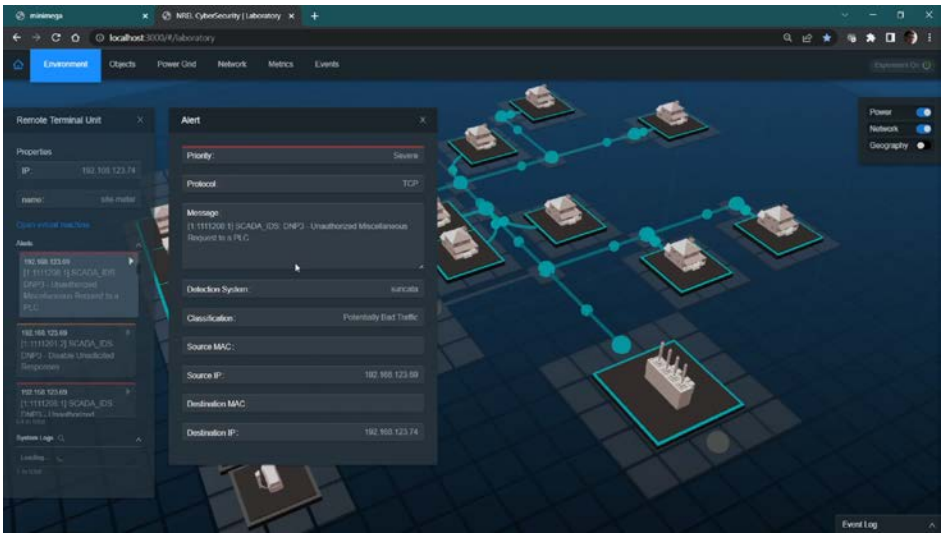



**Figure 18. A DNP3 alert received in the cyber range visualization**

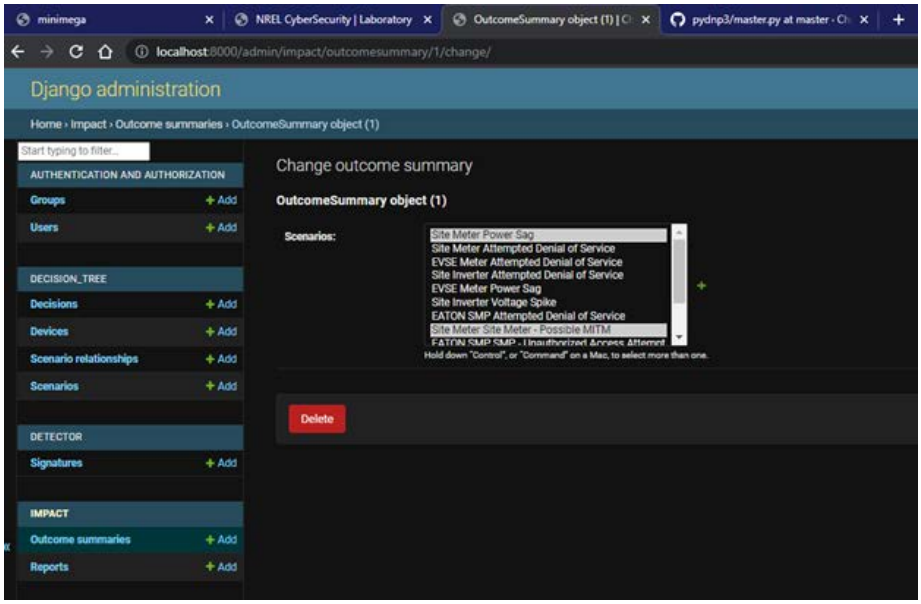



**Figure 19. An MITM report in the detector combining the SMP and IDS signatures**

### *5.1.3 SSH Brute Force Attack*

Metasploit is used an attempted brute force attack on the password to access the SMP. Metasploit is a penetration software that is used to analyze and probe existing vulnerabilities in the system, network, and servers. This attempted unauthorized access event can be detected using the defined signature rule in the IDS. The communication flows related to the SSH brute force attempt are flagged by the IDS and made visually distinct using color and arc height in NREL's Cyber Range visualization dashboard. A drastic system impact after this type of communication traffic would indicate that the adversary was able to gain unauthorized access. IViz-OT will generate a report for the logged event based on the signature generated from the parser and IDS logs. See Figure 20 and Figure 21.

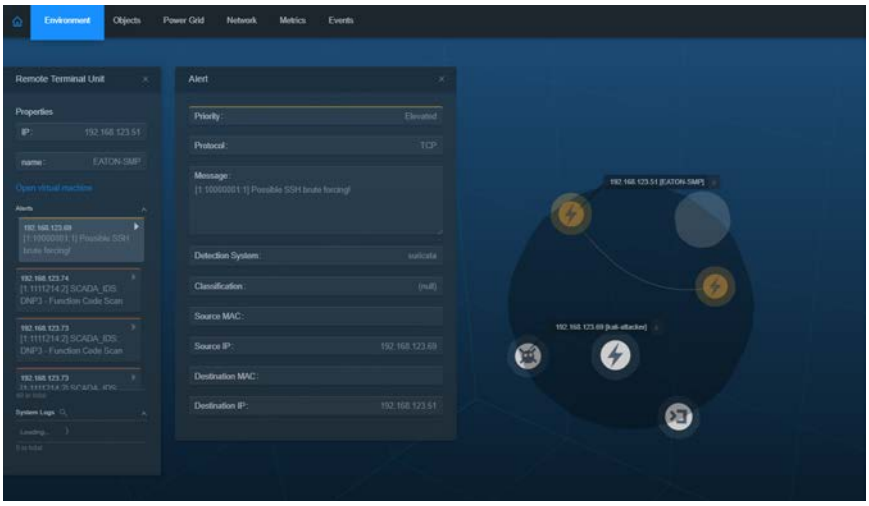



**Figure 20. An SSH alert received in the Ccyber range visualization**

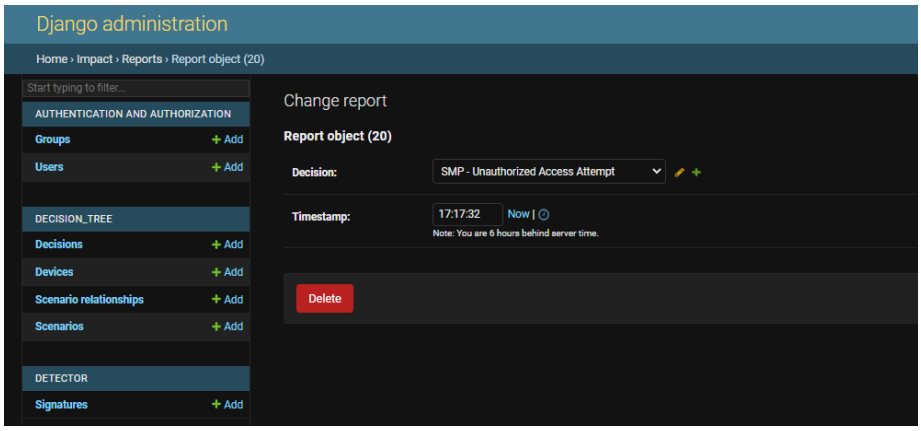



**Figure 21. An SSH alert in the detector**

## 5.2 Results and Discussion

Multiple runs of the scenario and demonstrations have been performed to show the capability of the developed software to correctly detect and raise an alert for a specific type of cyberattack. Under the emulated conditions, the system responded as expected each time and sufficiently alerted the user to the occurrence of the attack. The following screenshots show that the detector dashboards after each attack indicate a successful alert. Figure 22 and Figure 23 show the results while performing a network DoS attack.

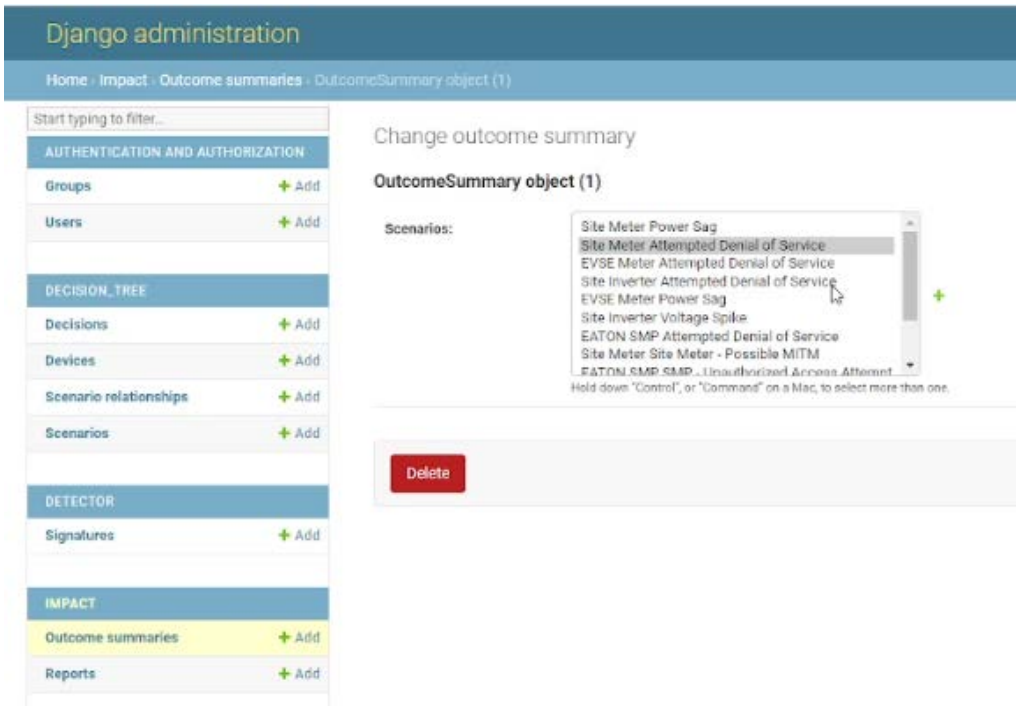



**Figure 22. A screenshot of the IViz-OT dashboard during a DoS attack**

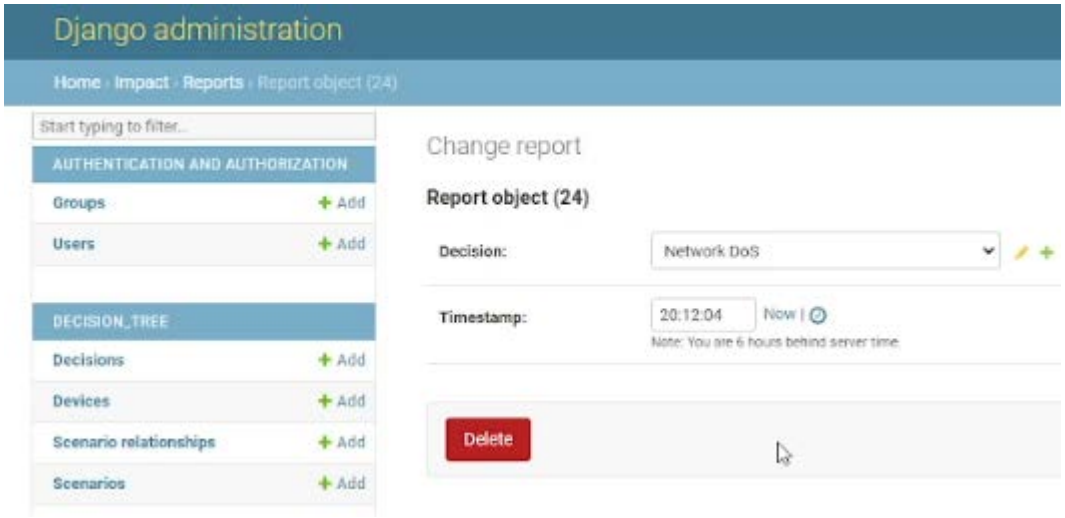



**Figure 23. A screenshot of the IViz-OT dashboard showing the generated report during a DoS attack**

Next, a brute force attack was run against the SMP 4/DP device. See Figure 24 and Figure 25.

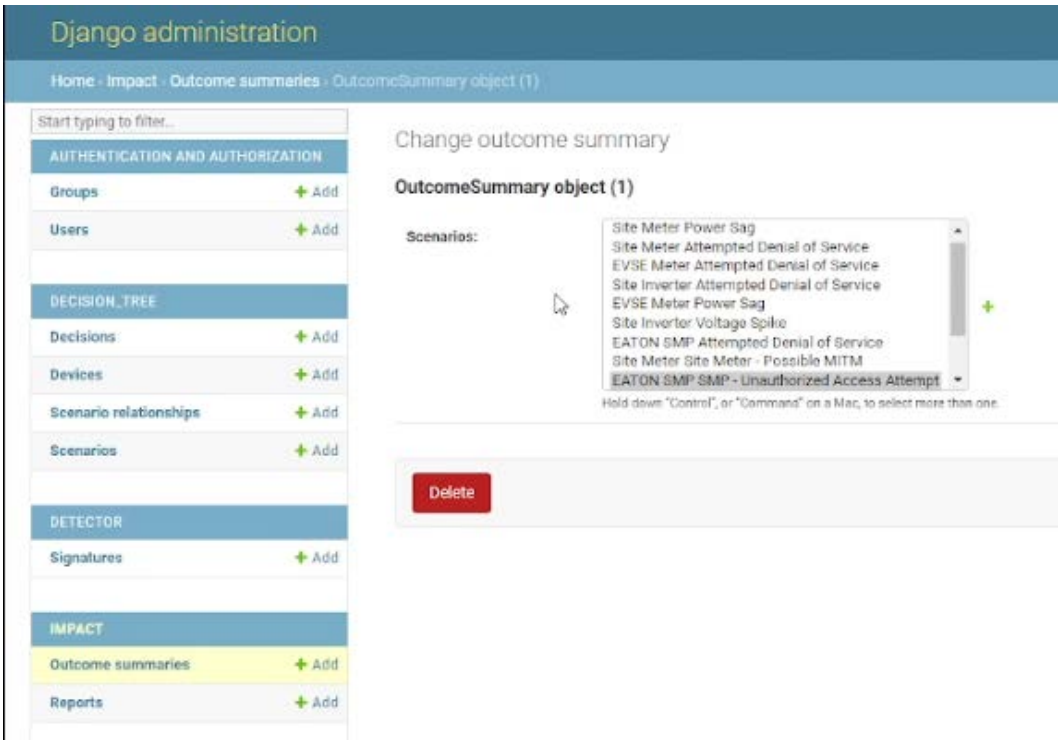



**Figure 24. A screenshot of the IViz-OT dashboard during brute force attack**

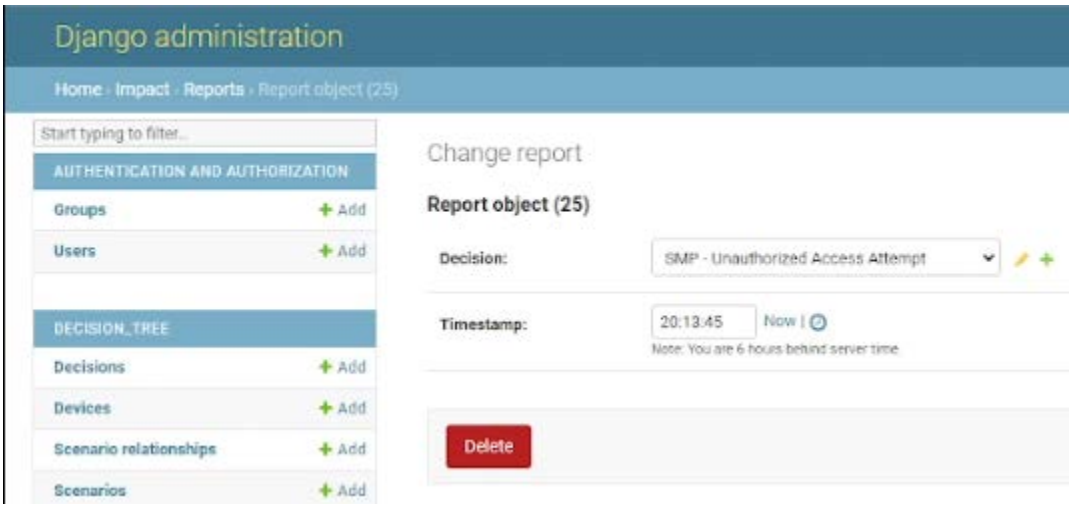



**Figure 25. A screenshot of the IViz-OT dashboard showing the generated report during a brute force attack**

The final attack evaluated was the malicious command from the attacker to the IED, as shown in Figure 26.

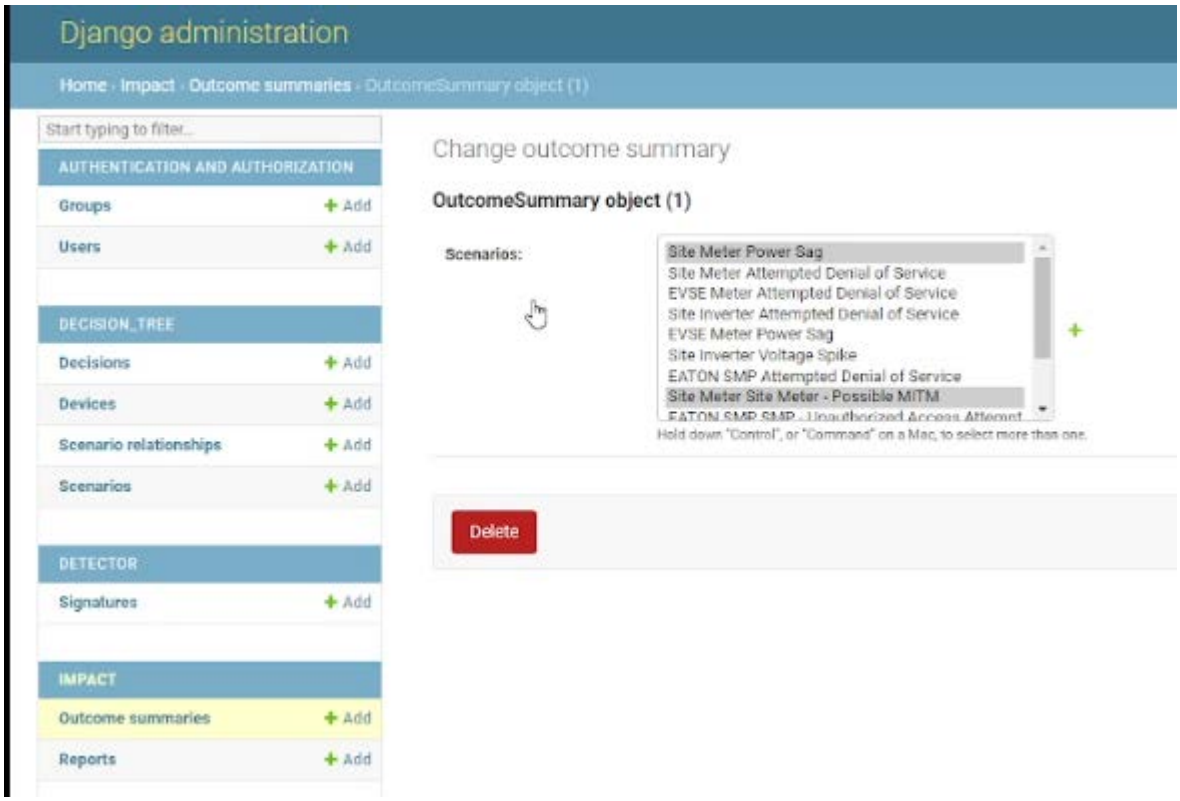



**Figure 26. A screenshot of the IViz-OT dashboard during a malicious tripping attack**

The alerts were correctly observed after the occurrence of each attack, with no false positives. These alerts were observed with a high rate of accuracy because of the capability of the detector to ingest custom-tuned signatures from the IDS and alerts based on user-defined thresholds from the SMP 4/DP. Using this capability, the specific IDS signatures and decision model were tuned to minimize false positives for the specific attacks. This implies that when the detector is deployed in a well-understood environment, in which custom signatures can be developed and the detector is well-tuned, the accuracy can be maximized. Further, using test beds or experiment environments to tune the tools for specific attacks is a good way to continually improve a site's security posture and to keep it current with the latest attack signatures and patterns.

# 6 Steps Toward Commercialization

## 6.1 Commercialization Plan

This project seeks advance the nation's critical infrastructure readiness to tackle cybersecurity and resilience concerns for both the legacy power infrastructure and newly deployed systems. The target market for commercialization mainly consists of utility companies that operate and maintain transmission and distribution systems, with a focus on assets that support other critical sectors, i.e., hospitals, military, and government. Eaton regularly conducts market analysis research to determine and prioritize required and anticipated cybersecurity measures for their customers. Reports mentioned that most utility chief executive officers showed concern that becoming a victim of a cyberattack is a matter of "when" and not "if," and not all are prepared. 50% of their organizations have experienced at least one attack against OT infrastructure that resulted in downtime in the past 24 months, and 90% have experienced damaging attacks.

Current markets for such technologies are bound by standardization and regulation. The U.S. Department of Energy has published a roadmap to prioritize the cybersecurity requirements for critical infrastructure. This effort aligns with the roadmap and targeting an implementation plan that supports standardization for future commercially available products.

Eaton plans to embed the transferred technology into the next-generation SMP product line. The containerized firmware enables such technology to run without impeding the normal operation for the platform. Eaton conducted an initial market study with customers, and it has been determined that they see this as an added value to their controllers. The challenge remaining is attaching the capabilities of such technology to the current configuration mechanism used for the SMP. Also, the SMP has a web interface that is used for monitoring purposes that could be embedded with the proposed tools.

One aspect of the commercialization is the cost of the technology and the overall added cost to the SMP platform. Eaton is considering various theories on these additional costs if any. Given the novelty of the technology and the amount of effort associated with the configuration for different system topologies, Eaton is considering a type of service associated with the cost to the customer, including long-term support.

The end state for the commercialization plan is to deliver the following: (1) Answer the question about where the OT-based intrusion detection is going to reside physically within the system domain. The goal is to clear the way toward standardization and, potentially, regulation, (2) Develop an alarm generation system that can identify and visualize cyber-attacks, and 3) Demonstrate a pilot deployment in an OT environment.

# 7 Conclusion

Detailed event visualization and comprehensive situational awareness are necessary to harden the cybersecurity of grid-edge devices. This project delivered an intrusion visualization tool, IViz-OT, that works seamlessly and in coordination with HIDES tool to detect, visualize, locate, and understand the detected anomalies and generated logs in the grid network. The generated logs from the signature-based IDS (HIDES) are difficult for system operators to comprehend ; training and long-term experience are required to process the information. Therefore, the IViz-OT tool categorizes the alert logs into human-readable scenarios that are easy to understand and provide more information to understand the complexity of attacks.

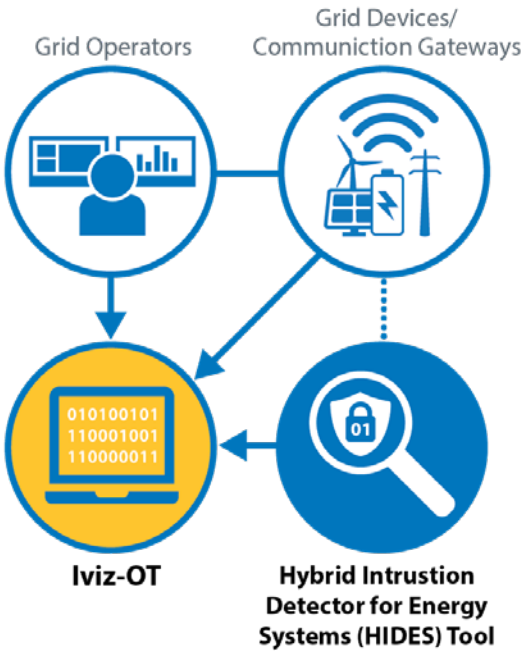



**Figure 27. A generic flowchart of integrated IViz-OT and HIDES tools**

Fig. 27 presents a generic flowchart of integrated IViz-OT and HIDES tools that are compatible with grid edge devices and communication gateways. In general, this tool operates as an advanced threat finder that interprets various types of cyber and physical events on the grid network. It allows cyber and physical monitoring to deliver real-time awareness to system owners and operators. The current market lacks such a technology, which can provide defense-in-depth visualization using analytical approaches.

This report demonstrated the working operation of proposed tool for different attack scenarios that included IT and SCADA-specific attacks. We also mapped these attacks with the NESCOR vulnerability classes and NERC CIP standards while describing the potential impact on the power grid. The proposed tool was tested and validated in the HIL-integrated cyber range environment. The experimental results validated the effectiveness of the proposed tool against different types of cybersecurity threats with clear 3D visualizations of power flows and cyber communications.

# 8 Future Work

Many areas are considered for additional improvement of this technology because it is in the process of commercialization and integration with Eaton's devices. Some immediate areas for improvement are:

- **Artificial intelligence-based decisions**: A good area for future work is to implement artificial intelligence-based decision making (Singh et al. 2021). The decision tree needs to be configured with the necessary decision parameters and conditions; however, this makes it necessary to frequently tune it, and it will require maintenance to stay current to the latest attacks. A more intelligent decision-making paradigm that is capable of learning new network conditions and attack patterns would greatly extend the detection capabilities of this tool.
- **Validated rule sets**: Should the tool be integrated into and deployed on Eaton's devices in a manner that is like this design, the rules, alert thresholds, and decision tree configurations will become valuable configurations to achieve a similar detection performance to the validated performance on the test bed (Singh et al. 2020). This allows the generation, maintenance, optimization, and validation of these configurations to be useful intellectual property that can be provided to customers as validated configurations to protect against specific attacks that have been tested and for which performance metrics can be provided.
- **Additional alerting mechanisms**: This tool combines alerts from an IT-oriented IDS tool and an OT-oriented device using the concept of hybrid intrusion detection to produce a more valuable alert to the operator. This concept is not limited to only these two tools, however, and it can be extended using additional alerting mechanisms. Using an event analysis framework, either instead of or in addition to the implemented IDS could allow more complex analysis and alerting to be performed.

# References


Cleveland, F. M. 2008. "IEC 62351-7: Communications and Information Management Technologies—Network and System Management in Power System Operations." *2008 IEEE/PES Transmission and Distribution Conference and Exposition*: 1–4. https://doi.org/10.1109/TDC.2008.4517189.

DNSstuff. 2020. "7 Best Intrusion Detection Software and Latest IDS Systems." February 18, 2020. www.dnsstuff.com/network-intrusion-detection-software.

Ghafir, Ibrahim, Vaclav Prenosil, Jakub Svoboda, and Mohammad Hammoudeh. 2016. "A Survey on Network Security Monitoring Systems." *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*: 77–82. https://doi.org/10.1109/W-FiCloud.2016.30.

Hasandka, Adarsh, Joshua Rivera, and Josh Van Natta. 2020. *NREL's Cyber-Energy Emulation Platform for Research and System Visualization*. Golden, CO: National Renewable Energy Laboratory. https://doi.org/10.2172/1659978. https://www.osti.gov/biblio/1659978.

W. H. Kersting, "Radial distribution test feeders," 2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.01CH37194), 2001, pp. 908-912 vol.2, doi: 10.1109/PESW.2001.916993.

National Electric Sector Cybersecurity Organization Resource (NESCOR). 2014. *Electric Sector Failure Scenarios and Impact Analyses*. Palo Alto, CA: Electric Power Research Institute. https://smartgrid.epri.com/doc/NESCOR%20failure%20scenarios%2006-30-14a.pdf.

North American Reliability Corporation (NERC). 2022. "Standards, Compliance, and Enforcement Bulletin." July 25–31, 2022. https://www.nerc.com/pa/comp/news/Documents/2022_07_25_StandardsCompliance_Bulletin.pdf.

Singh, Vivek K., and Manimaran Govindarasu. 2021. "A Cyber-Physical Anomaly Detection for Wide-Area Protection Using Machine Learning." *IEEE Transactions on Smart Grid* 12 (4): 3514–26. https://doi.org/10.1109/TSG.2021.3066316. https://ieeexplore.ieee.org/abstract/document/9380576.

Singh, Vivek Kumar, Evan Vaughan, Joshua Rivera, and Adarsh Hasandka. 2020. "HIDES: Hybrid Intrusion Detector for Energy Systems." *2020 IEEE Texas Power and Energy Conference (TPEC)*: 1–6. https://doi.org/10.1109/TPEC48276.2020.9042544. https://ieeexplore.ieee.org/document/9042544.

V. K. Singh, E. Vaughan, and J. Rivera. 2020. "SHARP-Net: Platform for Self-Healing and Attack Resilient PMU Networks," 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2020, pp. 1-5, https://doi: 10.1109/ISGT45199.2020.9087796. https://ieeexplore.ieee.org/abstract/document/9087796

# Appendix A: Power System Modeling

This section shows the line of codes for running the power system model in OpenDSS.

## A.1 A Screenshot of OpenDSS Model Script

```
Clear
Set DefaultBaseFrequency=60
! This script is based on a script developed by Tennessee Tech Univ students
! Tyler Patton, Jon Wood, and David Woods, April 2009

new circuit.IEEE13Nodeckt
~ basekv=115 pu=1.0001 phases=3 bus1=SourceBus
~ Angle=30                    ! advance angle 30 deg so result agree with
published angle
~ MVAsc3=20000 MVASC1=21000    ! stiffen the source to approximate inf source

!SUB TRANSFORMER DEFINITION
! Although this data was given, it does not appear to be used in the test case
results
! The published test case starts at 1.0 per unit at Bus 650. To make this happen,
we will change the impedance
! on the transformer to something tiny by dividing by 1000 using the DSS in-line
RPN math
New Transformer.Sub Phases=3 Windings=2   XHL=(8 1000 /)
~ wdg=1 bus=SourceBus   conn=delta  kv=115  kva=5000   %r=(.5 1000 /)
~ wdg=2 bus=650             conn=wye    kv=4.16  kva=5000   %r=(.5 1000 /)

! FEEDER 1-PHASE VOLTAGE REGULATORS
! Define low-impedance 2-wdg transformer

New Transformer.Reg1 phases=1 bank=reg1 XHL=0.01 kVAs=[1666 1666]
~ Buses=[650.1 RG60.1] kVs=[2.4  2.4] %LoadLoss=0.01
new regcontrol.Reg1  transformer=Reg1 winding=2  vreg=122  band=2  ptratio=20
ctprim=700  R=3   X=9

New Transformer.Reg2 phases=1 bank=reg1 XHL=0.01 kVAs=[1666 1666]
~ Buses=[650.2 RG60.2] kVs=[2.4  2.4] %LoadLoss=0.01
new regcontrol.Reg2  transformer=Reg2 winding=2  vreg=122  band=2  ptratio=20
ctprim=700  R=3   X=9

New Transformer.Reg3 phases=1 bank=reg1 XHL=0.01 kVAs=[1666 1666]
~ Buses=[650.3 RG60.3] kVs=[2.4  2.4] %LoadLoss=0.01
new regcontrol.Reg3  transformer=Reg3 winding=2  vreg=122  band=2  ptratio=20
ctprim=700  R=3   X=9
```

```
!TRANSFORMER DEFINITION
New Transformer.XFM1  Phases=3   Windings=2  XHL=2
~ wdg=1 bus=633       conn=Wye kv=4.16    kva=500    %r=.55     XHT=1
~ wdg=2 bus=634       conn=Wye kv=0.480    kva=500    %r=.55   XLT=1

!LINE CODES
// these are local matrix line codes
// corrected 9-14-2011
New linecode.mtx601 nphases=3 BaseFreq=60
~ rmatrix = (0.3465 | 0.1560 0.3375 | 0.1580 0.1535 0.3414 )
~ xmatrix = (1.0179 | 0.5017 1.0478 | 0.4236 0.3849 1.0348 )
~ units=mi
New linecode.mtx602 nphases=3 BaseFreq=60
~ rmatrix = (0.7526 | 0.1580 0.7475 | 0.1560 0.1535 0.7436 )
~ xmatrix = (1.1814 | 0.4236 1.1983 | 0.5017 0.3849 1.2112 )
~ units=mi
New linecode.mtx603 nphases=2 BaseFreq=60
~ rmatrix = (1.3238 | 0.2066 1.3294 )
~ xmatrix = (1.3569 | 0.4591 1.3471 )
~ units=mi
New linecode.mtx604 nphases=2 BaseFreq=60
~ rmatrix = (1.3238 | 0.2066 1.3294 )
~ xmatrix = (1.3569 | 0.4591 1.3471 )
~ units=mi
New linecode.mtx605 nphases=1 BaseFreq=60
~ rmatrix = (1.3292 )
~ xmatrix = (1.3475 )
~ units=mi

New linecode.mtx601 nphases=3 BaseFreq=60
!!!~ rmatrix = (0.0674673 | 0.0312137 0.0654777 | 0.0316143 0.0306264 0.0662392 )
!!!~ xmatrix = (0.195204  | 0.0935314 0.201861 | 0.0855879 0.0760312 0.199298 )
!!!~ cmatrix = (3.32591   | -0.743055 3.04217 | -0.525237 -0.238111 3.03116 )
~ rmatrix = [0.065625    | 0.029545455  0.063920455  |
0.029924242  0.02907197  0.064659091]
~ xmatrix = [0.192784091 | 0.095018939  0.19844697   |
0.080227273  0.072897727  0.195984848]
~ cmatrix = [3.164838036 | -1.002632425  2.993981593 | -0.632736516  -
0.372608713  2.832670203]
New linecode.mtx602 nphases=3 BaseFreq=60
!!!~ rmatrix = (0.144361 | 0.0316143 0.143133 | 0.0312137 0.0306264 0.142372 )
!!!~ xmatrix = (0.226028 | 0.0855879 0.230122 | 0.0935314 0.0760312 0.232686 )
!!!~ cmatrix = (3.01091  | -0.443561 2.77543  | -0.624494 -0.209615 2.77847 )
```

```
~ rmatrix = [0.142537879 | 0.029924242  0.14157197   |
0.029545455  0.02907197  0.140833333]
~ xmatrix = [0.22375     | 0.080227273  0.226950758  |
0.095018939  0.072897727  0.229393939]
~ cmatrix = [2.863013423 | -0.543414918  2.602031589 | -0.8492585  -
0.330962141  2.725162768]
New linecode.mtx603 nphases=2 BaseFreq=60
!!!~ rmatrix = (0.254472 | 0.0417943 0.253371 )
!!!~ xmatrix = (0.259467 | 0.0912376 0.261431 )
!!!~ cmatrix = (2.54676  | -0.28882 2.49502 )
~ rmatrix = [0.251780303 | 0.039128788  0.250719697]
~ xmatrix = [0.255132576 | 0.086950758  0.256988636]
~ cmatrix = [2.366017603 | -0.452083836  2.343963508]
New linecode.mtx604 nphases=2 BaseFreq=60
!!!~ rmatrix = (0.253371 | 0.0417943 0.254472 )
!!!~ xmatrix = (0.261431 | 0.0912376 0.259467 )
!!!~ cmatrix = (2.49502 | -0.28882 2.54676 )
~ rmatrix = [0.250719697 | 0.039128788   0.251780303]
~ xmatrix = [0.256988636  | 0.086950758  0.255132576]
~ cmatrix = [2.343963508 | -0.452083836 2.366017603]
New linecode.mtx605 nphases=1 BaseFreq=60
!!!~ rmatrix = (0.254428 )
!!!~ xmatrix = (0.259546 )
!!!~ cmatrix = (2.50575 )
~ rmatrix = [0.251742424]
~ xmatrix = [0.255208333]
~ cmatrix = [2.270366128]
New linecode.mtx606 nphases=3 BaseFreq=60
!!!~ rmatrix = (0.152193 | 0.0611362 0.15035 | 0.0546992 0.0611362 0.152193 )
!!!~ xmatrix = (0.0825685 | 0.00548281 0.0745027 | -0.00339824 0.00548281
0.0825685 )
!!!~ cmatrix = (72.7203 | 0 72.7203 | 0 0 72.7203 )
~ rmatrix = [0.151174242 | 0.060454545  0.149450758 |
0.053958333  0.060454545  0.151174242]
~ xmatrix = [0.084526515 | 0.006212121  0.076534091 | -
0.002708333  0.006212121  0.084526515]
~ cmatrix = [48.67459408 | 0  48.67459408 | 0  0  48.67459408]
New linecode.mtx607 nphases=1 BaseFreq=60
!!!~ rmatrix = (0.255799 )
!!!~ xmatrix = (0.092284 )
!!!~ cmatrix = (50.7067 )
~ rmatrix = [0.254261364]
~ xmatrix = [0.097045455]
~ cmatrix = [44.70661522]
```

```
!LOADSHAPE DEFINITIONS
new loadshape.load_loadshape0 npts=604800, interval=0.00027777778,
mult=(file=load_loadshape.csv, col=1, header=no)
new loadshape.load_loadshape1 npts=604800, interval=0.00027777778,
mult=(file=load_loadshape1.csv, col=1, header=no)
new loadshape.pv_loadshape0 npts=604800, interval=0.00027777778,
mult=(file=pv_loadshape.csv, col=1, header=no)

!LOAD DEFINITIONS
New Load.671 Bus1=671.1.2.3  Phases=3 Conn=Delta Model=1 kV=4.16   kW=1155
kvar=660 duty=load_loadshape0
New Load.634a Bus1=634.1     Phases=1 Conn=Wye  Model=1
kV=0.277  kW=160   kvar=110 duty=load_loadshape1
New Load.634b Bus1=634.2     Phases=1 Conn=Wye  Model=1
kV=0.277  kW=120   kvar=90 duty=load_loadshape0
New Load.634c Bus1=634.3     Phases=1 Conn=Wye  Model=1
kV=0.277  kW=120   kvar=90 duty=load_loadshape1
New Load.645 Bus1=645.2       Phases=1 Conn=Wye  Model=1
kV=2.4      kW=170   kvar=125 duty=load_loadshape0
New Load.646 Bus1=646.2.3    Phases=1 Conn=Delta Model=2
kV=4.16    kW=230   kvar=132 duty=load_loadshape1
New Load.692 Bus1=692.3.1    Phases=1 Conn=Delta Model=5
kV=4.16    kW=170   kvar=151 duty=load_loadshape0
New Load.675a Bus1=675.1    Phases=1 Conn=Wye  Model=1 kV=2.4  kW=485   kvar=190
duty=load_loadshape1
New Load.675b Bus1=675.2    Phases=1 Conn=Wye  Model=1 kV=2.4  kW=68   kvar=60
duty=load_loadshape0
New Load.675c Bus1=675.3    Phases=1 Conn=Wye  Model=1 kV=2.4  kW=290   kvar=212
duty=load_loadshape1
New Load.611 Bus1=611.3      Phases=1 Conn=Wye  Model=5 kV=2.4  kW=170   kvar=80
duty=load_loadshape0
New Load.652 Bus1=652.1      Phases=1 Conn=Wye  Model=2 kV=2.4  kW=128   kvar=86
duty=load_loadshape1
New Load.670a Bus1=670.1    Phases=1 Conn=Wye  Model=1 kV=2.4  kW=17    kvar=10
duty=load_loadshape0
New Load.670b Bus1=670.2    Phases=1 Conn=Wye  Model=1 kV=2.4  kW=66    kvar=38
duty=load_loadshape1
New Load.670c Bus1=670.3    Phases=1 Conn=Wye  Model=1 kV=2.4  kW=117  kvar=68
duty=load_loadshape0
! additional load
new load.ev0 bus1=634 phases=3 kv=0.277 kw=50 model=1 class=1 status=fixed
duty=load_loadshape0
new load.commload0 bus1=692 phases=3 kv=4.16 kw=500 model=1 class=1 status=fixed
duty=load_loadshape0
```

```
! PV system
new pvsystem.pv0 bus1=692 phases=3 kv=4.16 kva=100 pf=0.98 pmpp=75
duty=pv_loadshape0 %cutin=1 %cutout=1 irradiance=1
new xycurve.pv0curve npts=6 xarray=[0.5,0.95,0.96,1.04,1.05,1.5]
yarray=[0.4503,0.4503,0,0,-0.4503,-0.4503]
new invcontrol.pv0control pvsystem=pv0 mode=voltvar vvc_curve1=pv0curve
vv_refreactivepower=varmax_watts deltaq_factor=0.1 !voltagechangetolerance=0.0001

!CAPACITOR DEFINITIONS
New Capacitor.Cap1 Bus1=675 phases=3 kVAR=600 kV=4.16
New Capacitor.Cap2 Bus1=611.3 phases=1 kVAR=100 kV=2.4

!Bus 670 is the concentrated point load of the distributed load on line 632 to
671 located at 1/3 the distance from node 632

!LINE DEFINITIONS
New Line.650632    Phases=3 Bus1=RG60.1.2.3   Bus2=632.1.2.3  LineCode=mtx601
Length=2000 units=ft
New Line.632670    Phases=3 Bus1=632.1.2.3    Bus2=670.1.2.3  LineCode=mtx601
Length=667  units=ft
New Line.670671    Phases=3 Bus1=670.1.2.3    Bus2=671.1.2.3  LineCode=mtx601
Length=1333 units=ft
New Line.671680    Phases=3 Bus1=671.1.2.3    Bus2=680.1.2.3  LineCode=mtx601
Length=1000 units=ft
New Line.632633    Phases=3 Bus1=632.1.2.3    Bus2=brkr633.1.2.3  LineCode=mtx602
Length=500  units=ft
New Line.632645    Phases=2 Bus1=632.3.2      Bus2=645.3.2    LineCode=mtx603
Length=500  units=ft
New Line.645646    Phases=2 Bus1=645.3.2      Bus2=646.3.2    LineCode=mtx603
Length=300  units=ft
New Line.692675    Phases=3 Bus1=692.1.2.3    Bus2=675.1.2.3  LineCode=mtx606
Length=500  units=ft
New Line.671684    Phases=2 Bus1=671.1.3      Bus2=684.1.3    LineCode=mtx604
Length=300  units=ft
New Line.684611    Phases=1 Bus1=684.3        Bus2=611.3      LineCode=mtx605
Length=300  units=ft
New Line.684652    Phases=1 Bus1=684.1        Bus2=652.1      LineCode=mtx607
Length=800  units=ft

New line.sitebreaker633 Phases=3 Bus1=brkr633  Bus2=633 Switch=y r1=1e-4
x1=0  r0=1e-4 x0=0 c1=0 c0=0 normamps=500

!SWITCH DEFINITIONS
New Line.671692    Phases=3 Bus1=671   Bus2=692  Switch=y  r1=1e-4 r0=1e-4
x1=0.000 x0=0.000 c1=0.000 c0=0.000
```

```
! BusCoords IEEE13Node_BusXY.csv
Set Voltagebases=[115, 4.16, .48]
calcv
Solve

set maxcontroliter=1000
set mode=duty

! run initial solve
set number=1 stepsize=1s hour=10 sec=0 controlmode=static
solve

set controlmode=time
solve
```

## A.2 Suricata Rules

The following rules were added to the default rules available for the Suricata intrusion detection system deployed within the test bed. Most Distributed Network Protocol 3 (DNP3)-related rules were obtained from the public set provided by the Digital Bond IDS community.

alert tcp any any -> any any (msg:"DOS SYN packet flood inbound, Potential DOS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:5;)

alert tcp any any -> any any (msg:"DOS SYN packet flood outbound, Potential DOS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:6;)

alert tcp any any -> any 22 (msg:"Possible SSH brute forcing!"; flags: S+; threshold: type both, track by_src, count 5, seconds 30; sid:10000001; rev: 1;)

alert tcp any any -> any 20000 (flow:from_client,established; content:"|15|"; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Disable Unsolicited Responses"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:1111201; rev:2; priority:2;)

alert tcp any any <> any 20000 (flow:established; pcre:"/(?!\x05\x64)/iAR"; msg:"SCADA_IDS: DNP3 - Non-DNP3 Communication on a DNP3 Port"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:non-standard-protocol; sid:1111202; rev:2; priority:2;)

alert tcp any 20000 -> any any (flow:established; content:"|82|"; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Unsolicited Response Storm"; threshold: type threshold, track by_src, count 5, seconds 10; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:1111203; rev:1; priority:2;)

alert tcp any any -> any 20000 (flow:from_client,established; content:"|0D|"; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Cold Restart From Authorized Client"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:1111204; rev:1; priority:2;)

alert tcp 192.168.123.69 any -> any 20000 (flow:from_client,established; content:"|0D|"; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Cold Restart From Unauthorized Client"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:denial-of-service; sid:1111205; rev:1; priority:1;)

alert tcp 192.168.123.69 any -> any 20000 (flow:from_client,established; content:"|01|"; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Unauthorized Read Request to a PLC"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:1111206; rev:1; priority:2;)

alert tcp 192.168.123.69 any -> any 20000 (flow:from_client,established; content:"|05 64|"; depth:2; pcre:"/[\S\s]{10}(\x02|\x04|\x05|\x06|\x09|\x0A|\x0F|\x12)/iAR"; msg:"SCADA_IDS: DNP3 - Unauthorized Write Request to a PLC"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:1111207; rev:1; priority:1;)

alert tcp 192.168.123.69 any -> any 20000 (flow:from_client,established; content:"|05 64|"; depth:2; pcre:"/[\S\s]{10}(\x03|\x07|\x08|\x0B|\x0C|\x10|\x11|\x13|\x14|\x15|\x16|\x17|\x18|\x19|\x1A|\x1B|\x1C|\x1D|\x1E)/iAR"; msg:"SCADA_IDS: DNP3 - Unauthorized Miscellaneous Request to a PLC"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:1111208; rev:1; priority:1;)

alert tcp any any -> any 20000 (flow:from_client,established; content:"|12|"; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Stop Application"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:denial-of-service; sid:1111209; rev:2; priority:2;)

alert tcp any any -> any 20000 (flow:from_client,established; content:"|0E|"; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Warm Restart"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:1111210; rev:2; priority:2;)

alert tcp any any -> any 20000 (flow:from_client,established; content:"|FF FF|"; offset:4; depth:2; msg:"SCADA_IDS: DNP3 - Broadcast Request from Authorized Client"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:misc-attack; sid:1111211; rev:1; priority:2;)

alert tcp 192.168.123.69 any -> any 20000 (flow:from_client,established; content:"|FF FF|"; offset:4; depth:2; msg:"SCADA_IDS: DNP3 - Broadcast Request from Unauthorized Client"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:misc-attack; sid:1111212; rev:1; priority:1;)

alert tcp any 20000 -> any any (flow:established; content:"|81|"; offset:12; depth:1; pcre:"/[\S\s]{1}(\x02|\x04|\x06|\x0a|\x0c|\x0e)/iAR";msg:"SCADA_IDS: DNP3 - Points List Scan"; threshold: type threshold, track by_src, count 5, seconds 30; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-recon; sid:1111213; rev:2; priority:2;)

alert tcp any 20000 -> any any (flow:established; content:"|81|"; offset:12; depth:1; pcre:"/[\S\s]{1}(\x01)/iAR"; msg:"SCADA_IDS: DNP3 - Function Code Scan"; threshold: type threshold, track by_src, count 3, seconds 60; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-recon; sid:1111214; rev:2; priority:2;)

alert tcp any any -> any 20000 (msg:"SCADA_IDS: DNP3 - Disable Unsolicited Responses"; dnp3_cmd_fc:21; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:11112011; rev:1; priority:2;)

alert tcp any any <> any 20000 (flow:established; pcre:"/(?!\x05\x64)/iAR"; msg:"SCADA_IDS: DNP3 - Non-DNP3 Communication on a DNP3 Port"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:non-standard-protocol; sid:1111202; rev:1; priority:2;)

alert tcp any 20000 -> any any (flow:established; content:"|82|"; offset:12; depth:1; msg:"SCADA_IDS: DNP3 - Unsolicited Response Storm"; threshold: type threshold, track by_src, count 5, seconds 10; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:11112031; rev:1; priority:2;)

#alert tcp any any -> any 20000 (msg:"SCADA_IDS: DNP3 - Cold Restart From Authorized Client"; dnp3_cmd_fc:13; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:11112041; rev:1; priority:2;)

#alert tcp 192.168.123.69 any -> any 20000 (msg:"SCADA_IDS: DNP3 - Cold Restart From Unauthorized Client"; dnp3_cmd_fc:13; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:denial-of-service; sid:11112051; rev:1; priority:1;)

#alert tcp 192.168.123.69 any -> any 20000 (msg:"SCADA_IDS: DNP3 - Unauthorized Read Request to a PLC"; dnp3_cmd_fc:1; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:11112061; rev:1; priority:2;)

alert tcp 192.168.123.69 any -> any 20000 (flow:from_client,established; content:"|05 64|"; depth:2; pcre:"/[\S\s]{10}(\x02|\x04|\x05|\x06|\x09|\x0A|\x0F|\x12)/iAR"; msg:"SCADA_IDS: DNP3 - Unauthorized Write Request to a PLC"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:1111207; rev:1; priority:1;)

alert tcp 192.168.123.69 any -> any 20000 (flow:from_client,established; content:"|05 64|"; depth:2; pcre:"/[\S\s]{10}(\x03|\x07|\x08|\x0B|\x0C|\x10|\x11|\x13|\x14|\x15|\x16|\x17|\x18|\x19|\x1A|\x1B|\x1C|\x1D|\x1E)/iAR"; msg:"SCADA_IDS: DNP3 - Unauthorized Miscellaneous Request to a

PLC"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:1111208; rev:1; priority:1;)

#alert tcp any any -> any 20000 (msg:"SCADA_IDS: DNP3 - Stop Application"; dnp3_cmd_fc:18; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:denial-of-service; sid:11112091; rev:1; priority:2;)

#alert tcp any any -> any 20000 (msg:"SCADA_IDS: DNP3 - Warm Restart"; dnp3_cmd_fc:14; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-dos; sid:11112101; rev:1; priority:2;)

alert tcp any any -> any 20000 (flow:from_client,established; content:"|FF FF|"; offset:4; depth:2; msg:"SCADA_IDS: DNP3 - Broadcast Request from Authorized Client"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:misc-attack; sid:1111211; rev:1; priority:2;)

alert tcp 192.168.123.69 any -> any 20000 (flow:from_client,established; content:"|FF FF|"; offset:4; depth:2; msg:"SCADA_IDS: DNP3 - Broadcast Request from Unauthorized Client"; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:misc-attack; sid:1111212; rev:1; priority:1;)

alert tcp any 20000 -> any any (flow:established; content:"|81|"; offset:12; depth:1; pcre:"/[\S\s]{1}(\x02|\x04|\x06|\x0a|\x0c|\x0e)/iAR";msg:"SCADA_IDS: DNP3 - Points List Scan"; threshold: type threshold, track by_src, count 5, seconds 30; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-recon; sid:1111213; rev:1; priority:2;)

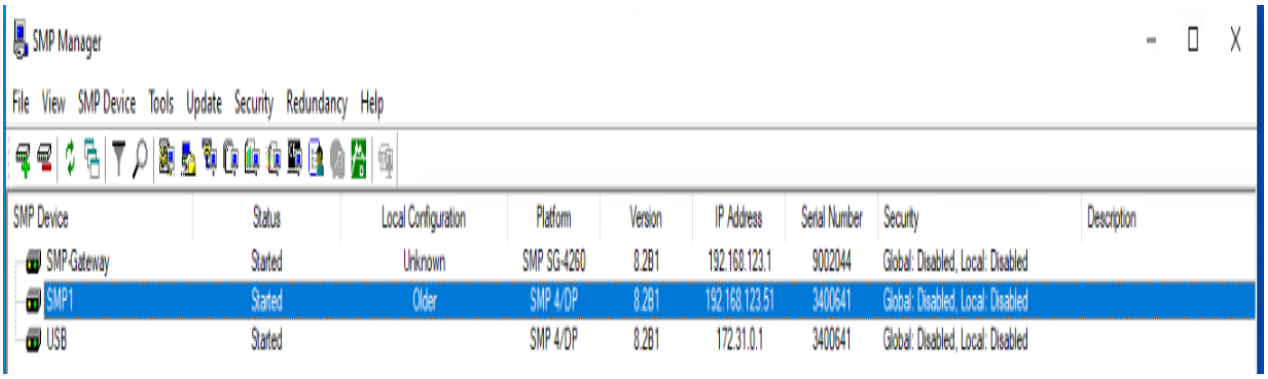
alert tcp any 20000 -> any any (flow:established; content:"|81|"; offset:12; depth:1; pcre:"/[\S\s]{1}(\x01)/iAR"; msg:"SCADA_IDS: DNP3 - Function Code Scan"; threshold: type threshold, track by_src, count 3, seconds 60; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:attempted-recon; sid:1111214; rev:1; priority:2;)

#alert tcp any any -> any 20000 (msg:"SCADA_IDS: DNP3 - Time Change Attempt"; dnp3_cmd_fc:2; dnp3_cmd_ot:50; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:misc-activity; sid:11112151; rev:1; priority:2;)

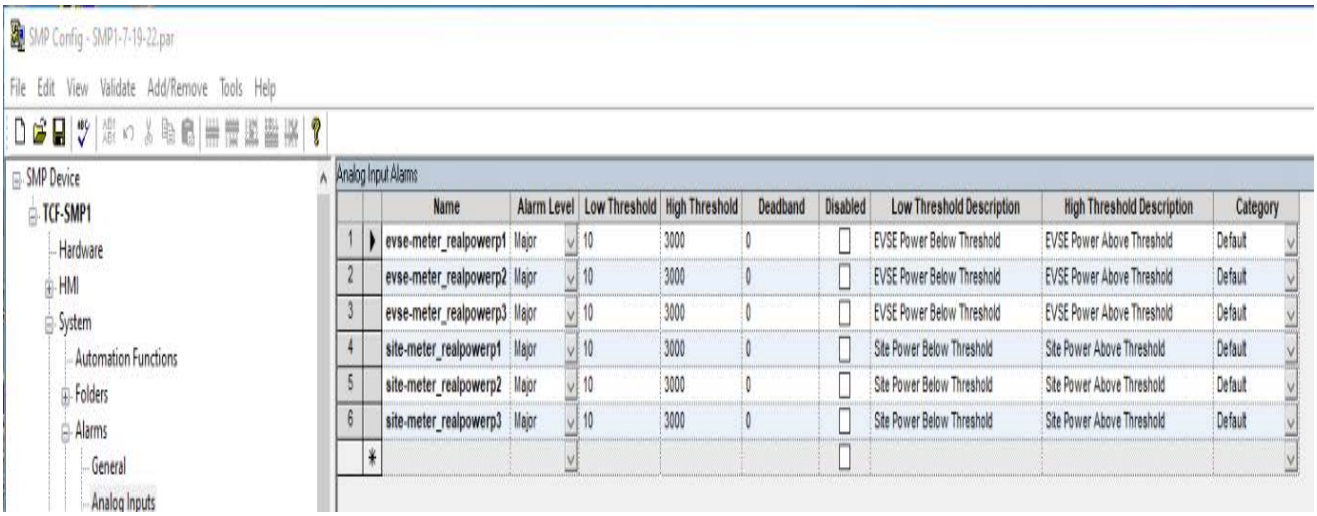
#alert tcp any any -> any 20000 (msg:"SCADA_IDS: DNP3 - Failed Checksum Error"; flags: PA; dnp3_checksum:incorrect; reference:url,digitalbond.com/tools/quickdraw/dnp3-rules; classtype:bad-unknown; sid:11112161; rev:1; priority:2;)

## A.3 SMP 4/DP Alerts

The SMP 4/DP device was configured to monitor the power values. The SMP manager software was used to configure the alarms and other settings for the device.

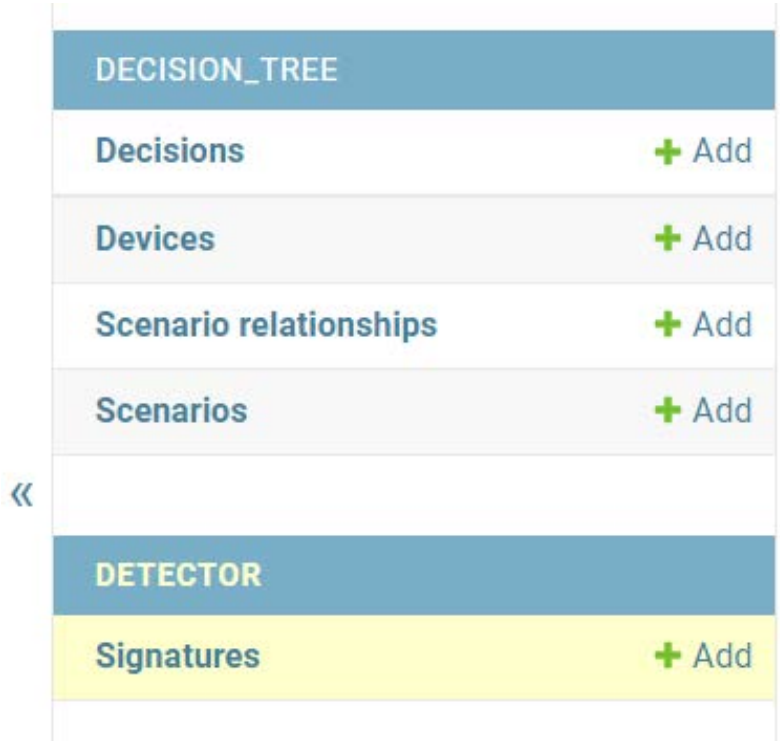



The alarms configured for this scenario were basic threshold-based alerts. Leveraging the capabilities of the SMP 4/DP to generate custom alerts is a good way to improve the detection capabilities of this advanced OT detection tool.

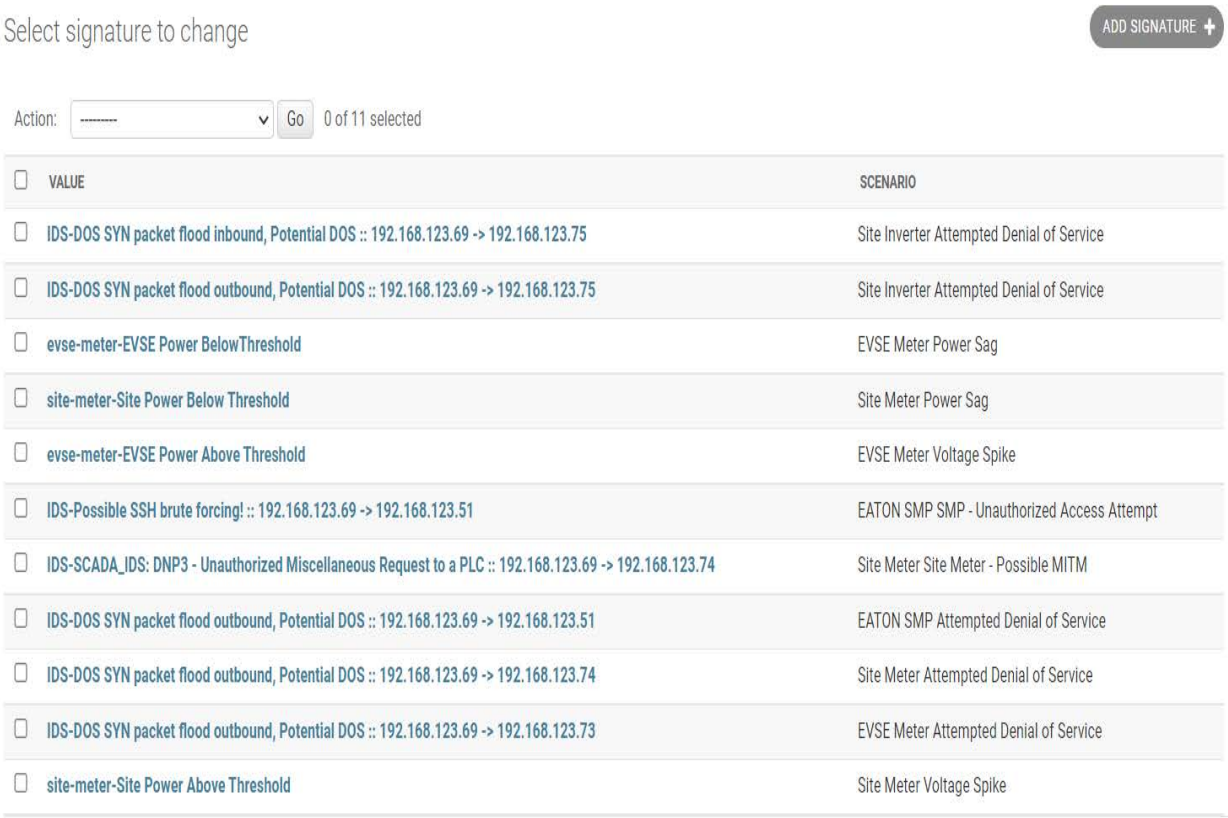


## A.4 Detector Model Update Process

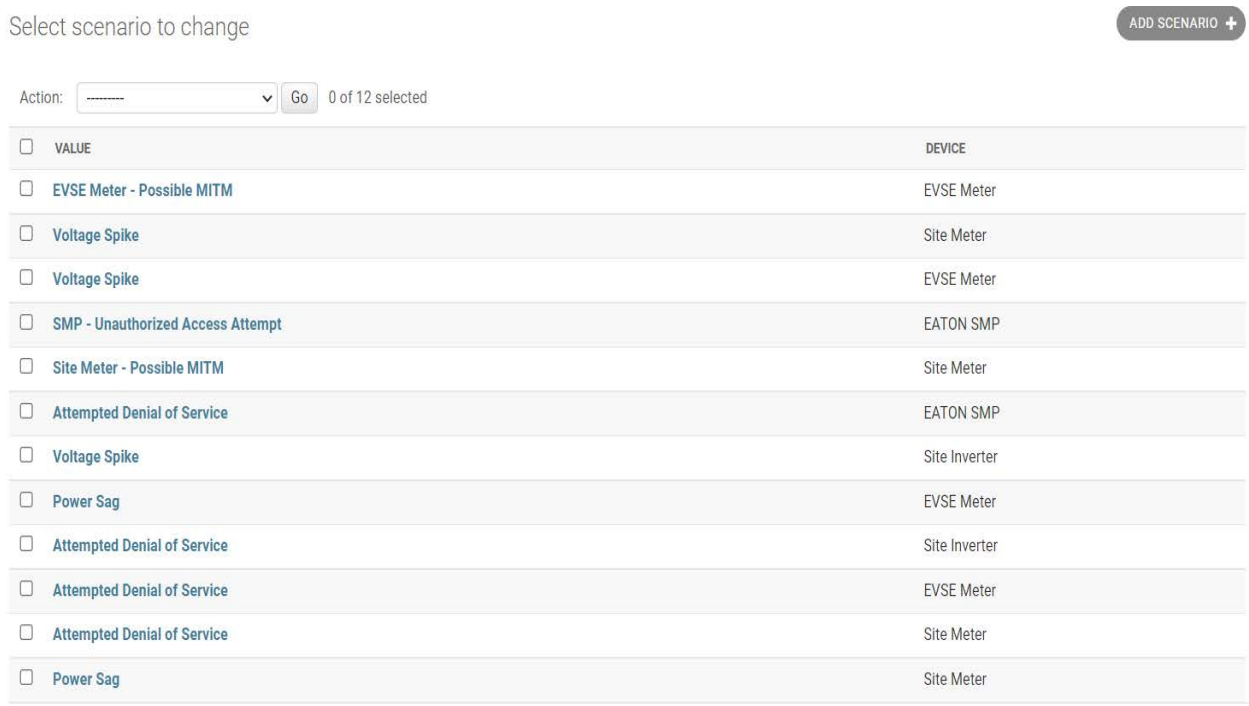
The decision tree and detector can be modified with new signatures, scenarios, decisions, and classifications. These are all contained within the detector database, which is loaded upon the first launch of the detector service. It must be volume-mounted to the container, and any modifications made must be saved in the database on a disk to persist across redeployments.




The Signatures tab contains values to be matched from the IDS and SMP alerts. If the detector receives an alert or log matching a Signature value, the corresponding Scenario is triggered.




The Scenarios tab contains different attack scenarios and their corresponding devices.




The Devices tab contains a list of devices and their importance.

Select device to change

ADD DEVICE +

Action: --------- Go 0 of 4 selected

| NAME | IMPORTANCE |
|---|---|
| EATON SMP | 5 |
| Site Inverter | 5 |
| EVSE Meter | 5 |
| Site Meter | 5 |

4 devices

The Decisions tab contains a list of final decisions that the detector can report.

Select scenario to change

ADD SCENARIO +

Action: --------- Go 0 of 12 selected

| VALUE | DEVICE |
|---|---|
| EVSE Meter - Possible MITM | EVSE Meter |
| Voltage Spike | Site Meter |
| Voltage Spike | EVSE Meter |
| SMP - Unauthorized Access Attempt | EATON SMP |
| Site Meter - Possible MITM | Site Meter |
| Attempted Denial of Service | EATON SMP |
| Voltage Spike | Site Inverter |
| Power Sag | EVSE Meter |
| Attempted Denial of Service | Site Inverter |
| Attempted Denial of Service | EVSE Meter |
| Attempted Denial of Service | Site Meter |
| Power Sag | Site Meter |

The Scenario relationships tab matches scenarios that the decision tree generates based on signatures received from the detector to decisions that the detector can report.

Select decision to change

ADD DECISION +

Action: --------- Go 0 of 9 selected

| VALUE | CLASSID |
|---|---|
| EVSE meter - Possible MITM | 8 |
| SMP - Unauthorized Access Attempt | 7 |
| Site Meter - Possible MITM | 6 |
| EATON SMP - Successful Denial of Service | 5 |
| Network DoS | 4 |
| Site Inverter - Successful Denial of Service | 3 |
| EVSE Meter - Successful Denial of Service | 2 |
| Site Meter - Successful Denial of Service | 1 |
| Benign | 0 |

9 decisions