Seeing the Unseen: An Evaluation of Active Scanning in ICS Environments

Jennifer Guerra
DEFCON ICS Village
August 10, 2024

Photo from iStock-627281636

Clean Energy Cybersecurity Accelerator

Our Purpose

Advance cyber innovation to defend modern, renewable energy technologies against high-priority cybersecurity risks to the energy sector.

Track 1

Address utilities' most urgent security interests by assessing market-ready cybersecurity solutions in a representative testing architecture.

Track 2

Help developers improve pre-market cybersecurity technologies and bridge the "valley of death" between innovation and commercialization.

Track 1 Cohorts

Cohort 1

Strong Authentication and Authorization

Status: Complete

Tested three solution providers to address risks related to authentication and authorization within distributed energy resource (DER) environments.

Evaluated capabilities such as user management of field devices, interconnection of DER systems, and authentication and authorization of commands.

Cohort 2

Hidden risks due to incomplete system visibility, device security, and configuration

Status: In Progress

Evaluating two solution providers that actively identify all industrial control system (ICS) assets connected to a utility's infrastructure—physically and virtually—to understand the totality of assets that need to be monitored and protected within the environment.

Selected solutions support the identification of unauthorized, unmanaged, or compromised assets to be removed or remediated.

Key Takeaways from Cohort 1

Move Beyond Perimeter Security

Heavy focus on perimeter: insufficient security approach for modern hyper-connected systems.

Internal defensive devices: provide higher visibility, improve understanding of network topology, and effective placement of security assets.

Enable Multifactor Authentication

This best practice can defend against an attacker's lateral movements through a compromised network.

Invest in Defense-in-Depth Security

Signature-based detections alone will fail to defend networks. No single solution can protect against all threat scenarios.

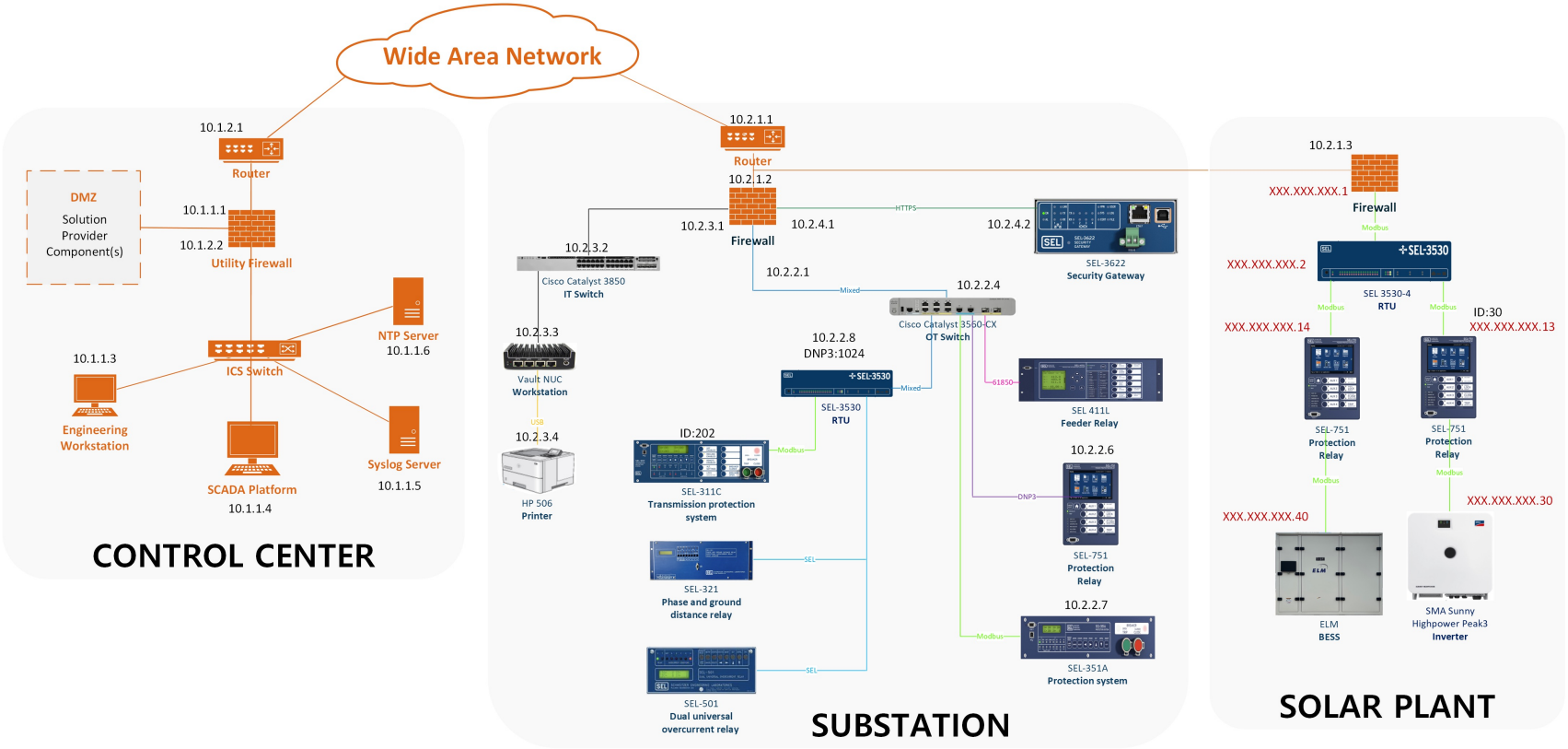
Living-off-the-Land Techniques Difficult to Defend

Attackers abusing native protocols and legitimate device relationships are difficult to detect and stop.

Cohort 2 Theme

Hidden risks due to incomplete system visibility, device security, and configuration.

Cohort 2 Baseline Operation Environment

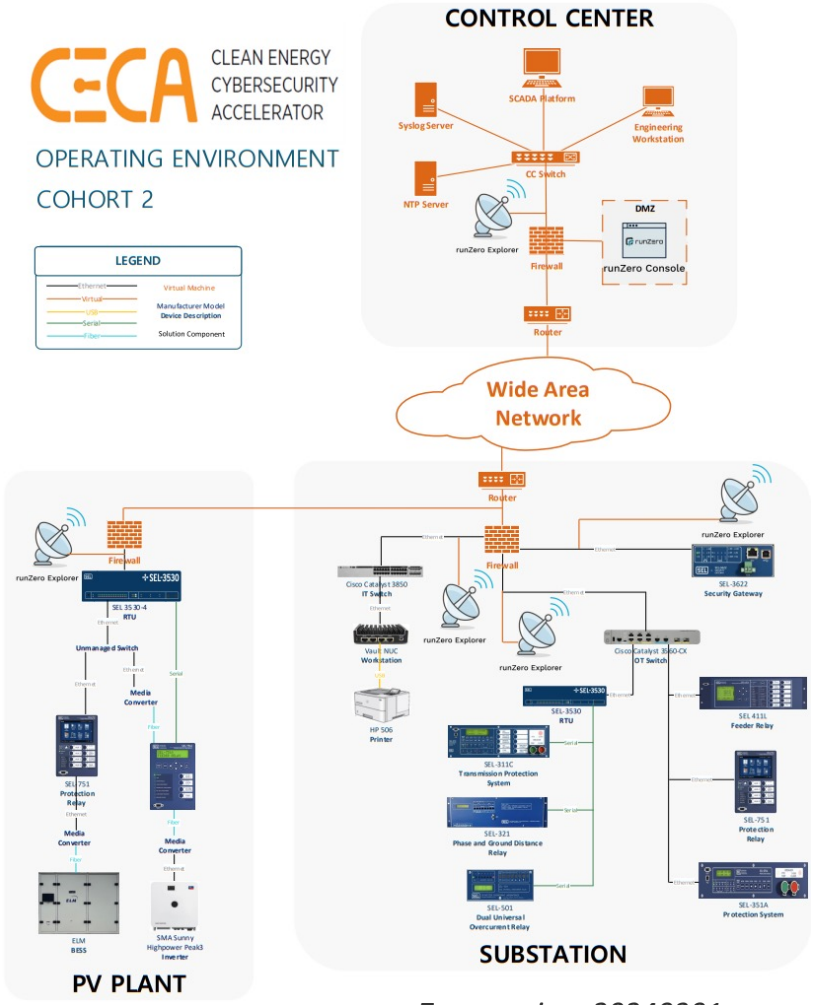


Cohort 2 Evaluation Topics

Evaluation Topic		Description
1	**Initial Discovery** 	How does the solution perform during initial scan of environment?
2	**Change Discovery** 	How does the solution identify changes to the environment?
3	**Passive Discovery** 	What can the solution identify passively?
4	**Scale Discovery** 	How does the solution perform at scale?
-	**Interruption to Operations** 	Does the solution affect the normal operation of devices?

Scenario 1:
Initial Discovery

- Deployed as self-hosted, on-premise, and air-gapped
- runZero Console on DMZ in control center
- Explorers on virtual machines hosted behind the firewall in each subnet of interest



runZero version: 20240301

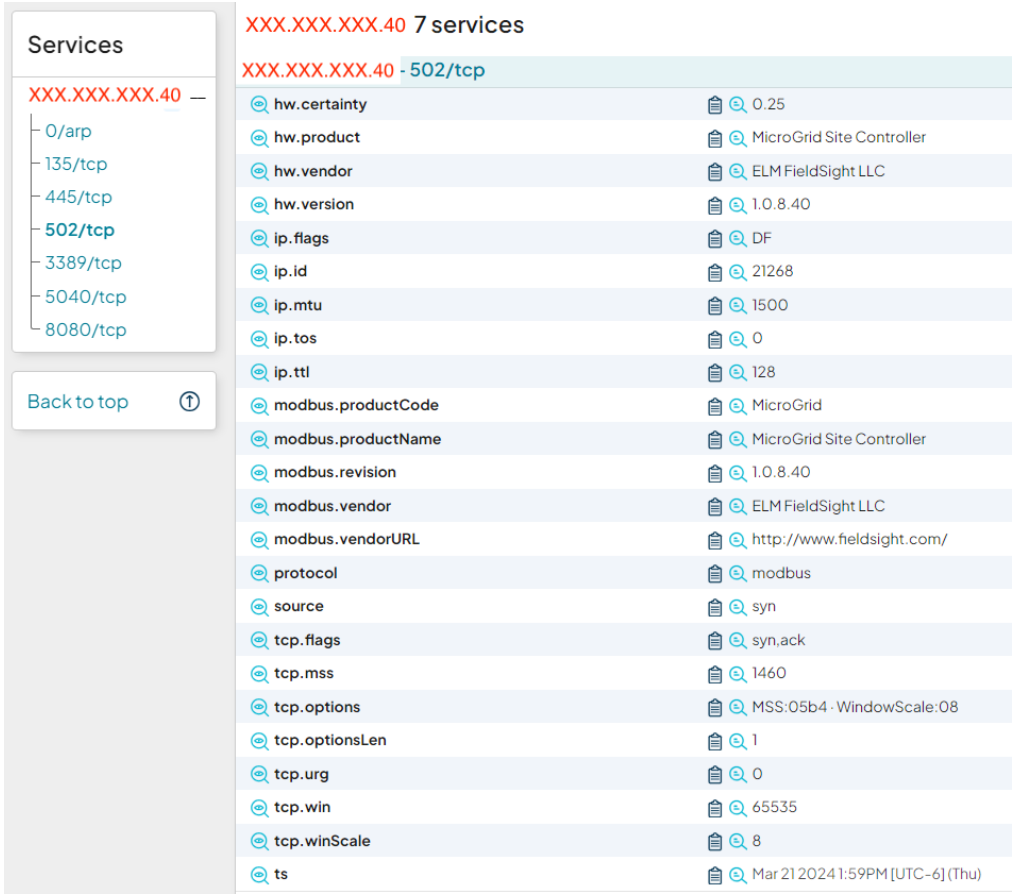
Scenario 1:
Results

- Identified any services available, and ports open for probes enabled in the scan
- Identified Transmission Control Protocol port 20,000 as open on the operational technology (OT) devices communicating via a Distributed Network Protocol 3 (DNP3) but did not identify a DNP3 service.

Device	Hostname	IP Address	MAC Address	MAC Vendor	OS	OS Version
Substation OT (11 devices)						
Sub firewall	✓	✓	✓	✓	✓	✓
OT switch	✓	✓	✓	✓	✓	✓
Sub-ot admin vm	✓	✓	✓	✓	✓	✓
Sub-ot runZero vm	✓	✓	✓	✓	✓	✓
SEL 3530 RTAC	✓	✓	✓	✓	✓	
SEL 411L		✓	✓	✓		
SEL 751		✓	✓	✓		
SEL 351A		✓	✓	✓		
***SEL 311C**						
***SEL 321**						
***SEL 501**						
Substation OT gateway (3 devices)						
Sub-ot-gateway admin vm	✓	✓	✓	✓	✓	✓
Sub-ot-gateway runZero vm	✓	✓	✓	✓	✓	✓
SEL 3622	✓	✓	✓	✓	✓	
PV plant (8 devices)						
PV firewall	✓	✓	✓	✓	✓	✓
PV admin vm	✓	✓	✓	✓	✓	✓
PV runZero vm	✓	✓	✓	✓	✓	✓
SEL 3530 RTAC	✓	✓	✓	✓	✓	
SEL 751		✓	✓	✓		
SEL 751		✓	✓	✓		
SMA Sunny Highpower	✓	✓	✓	✓	✓	
ELM BESS	✓	✓	✓	✓	✓	✓

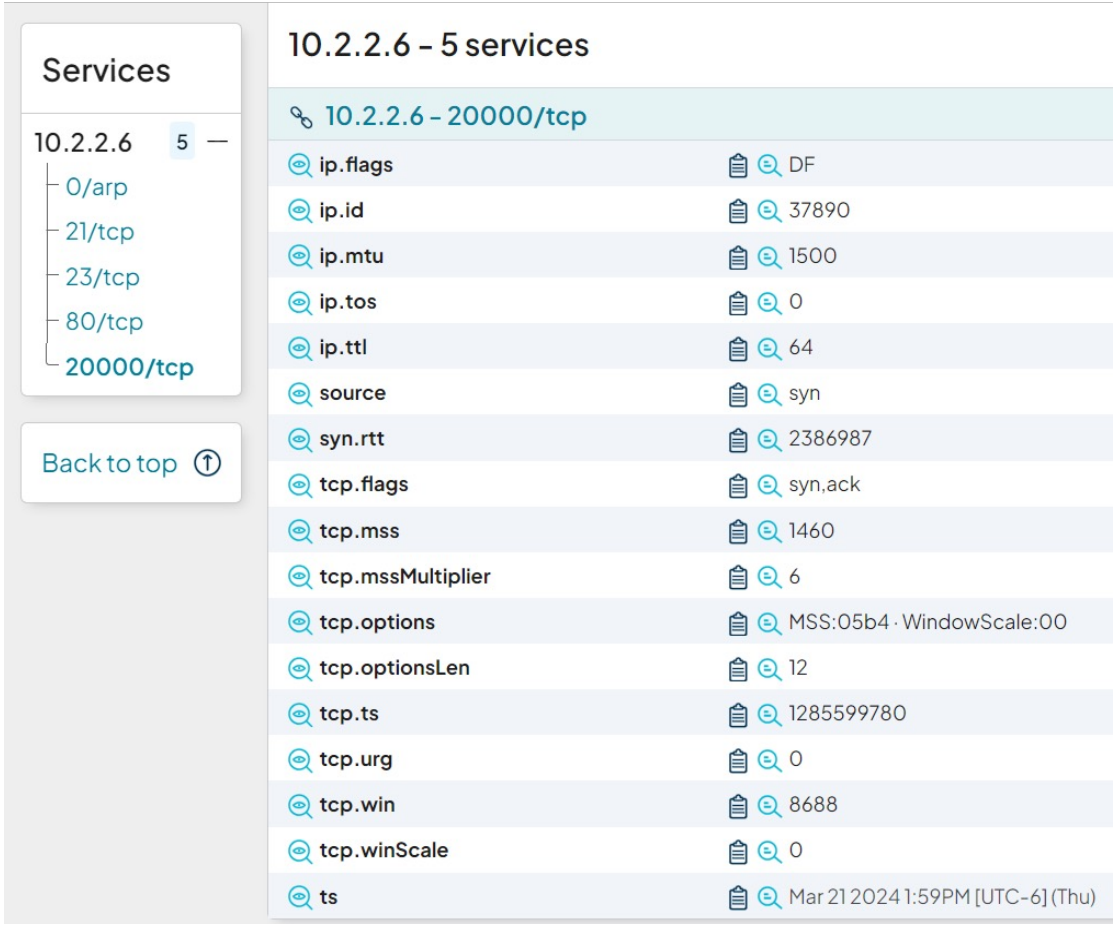
Scenario 1: Results

- Port 502
- Modbus protocol
- Vendor



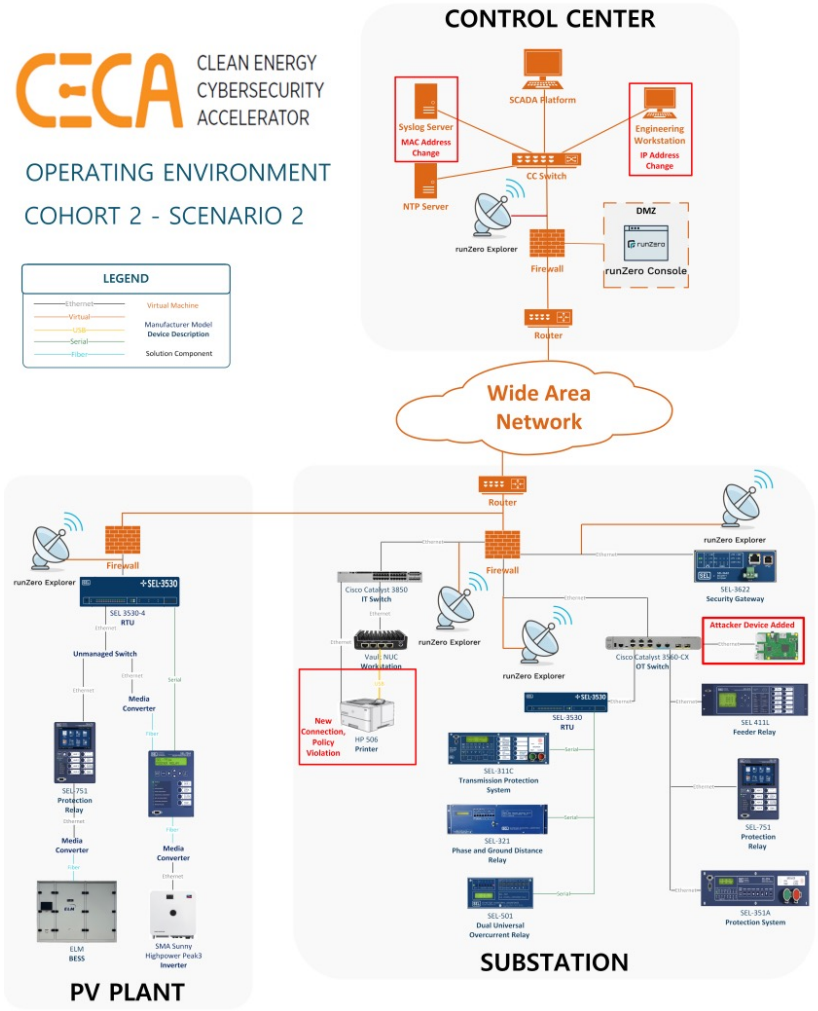
Scenario 1:
Results

- Port 20,000 – identified as open on OT devices communicating via DNP3
- Did not identify a DNP3 service.



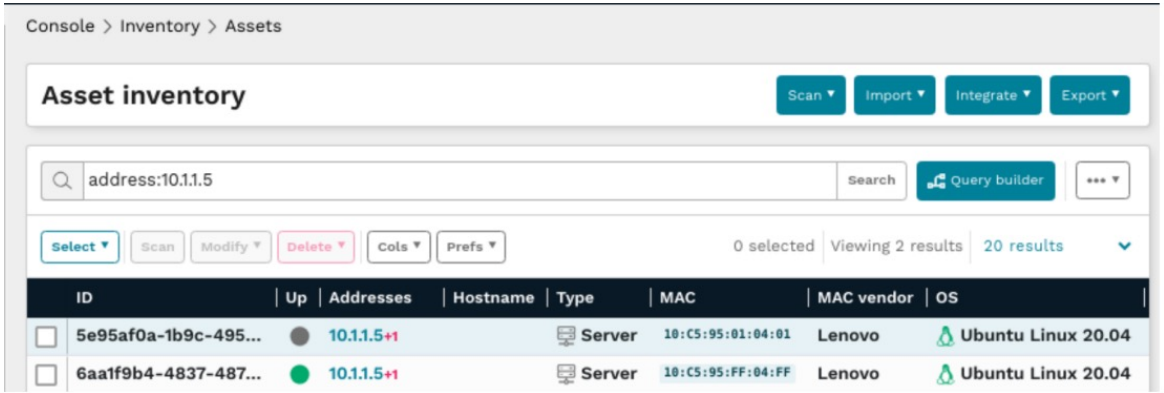
Scenario 2:
Change Discovery

- Connected a Raspberry Pi running Kali Linux OS in the substation OT subnet
- Plugged the printer into the switch via ethernet
- Changed IP address of the engineering workstation in the control center
- Changed MAC address of the syslog server in the control center



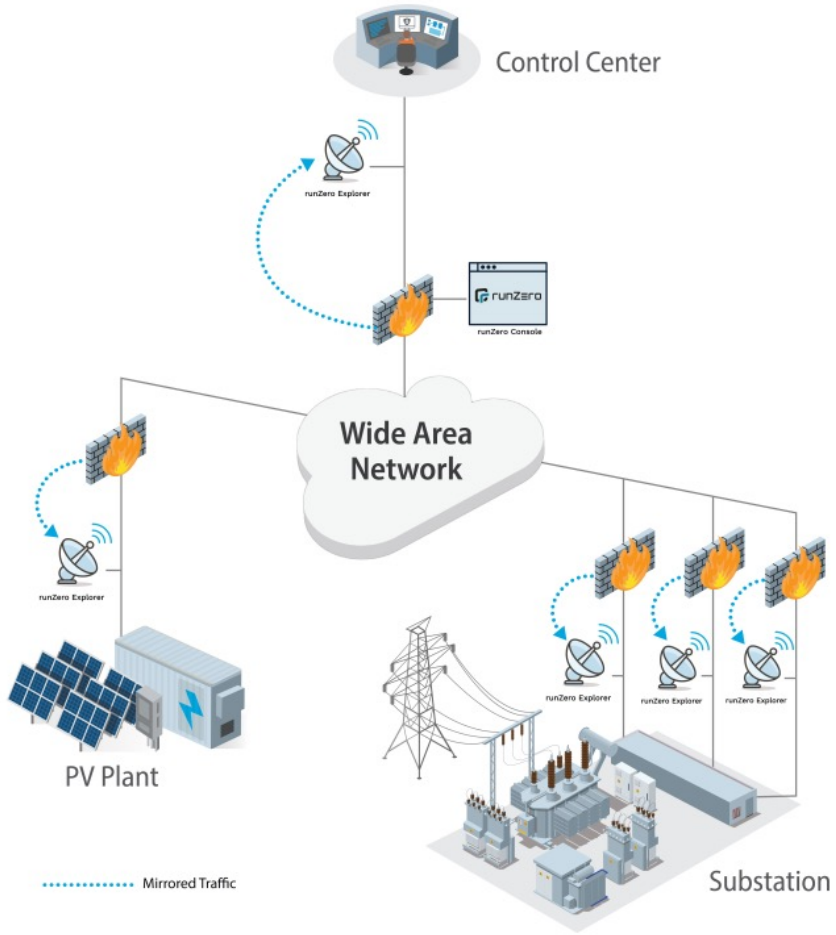
Scenario 2:
Results

- Identified each of the four changes introduced into the environment. Profiled just as in-depth as other devices.
- Changed IP address tracked; updated device entry for the engineering workstation with the new IP
- With the changed MAC address for the syslog server, runZero platform created new device entry in the inventory database, and marked the "old" syslog server as "offline"



Scenario 3:
Passive Discovery

- Traffic collection point sampling via a mirror port on firewall interface
- Each Explorer configured to listen to any broadcast traffic on its subnet

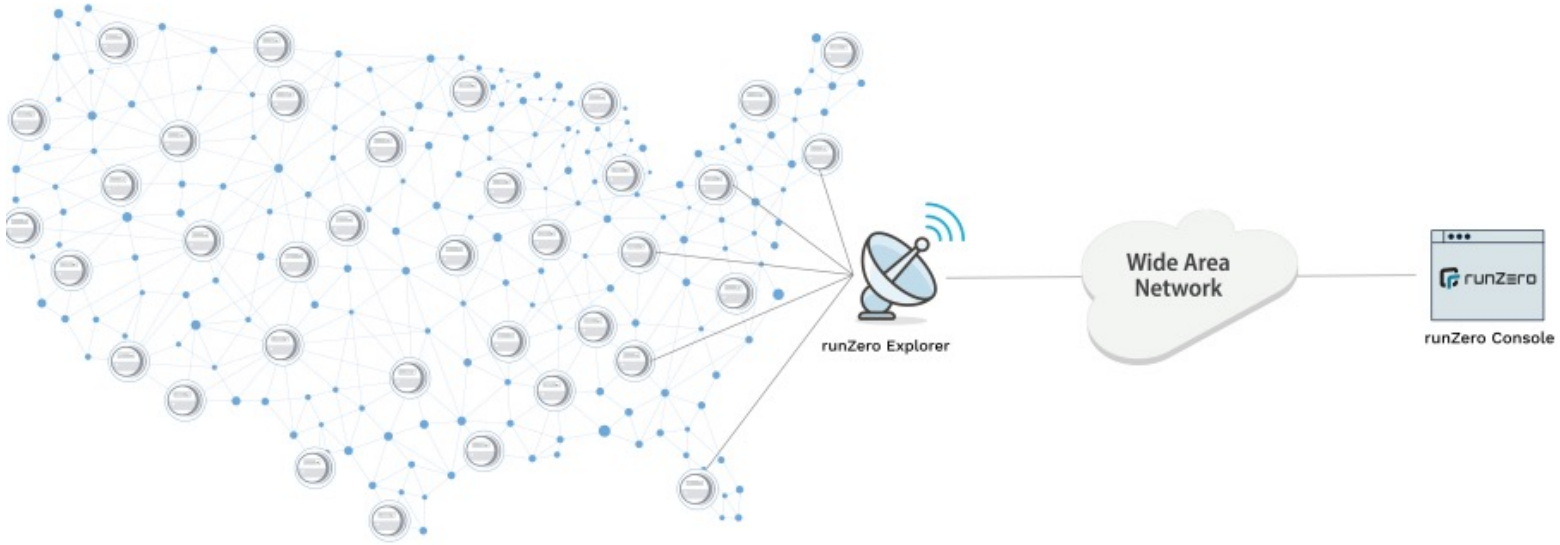


Scenario 3:
Results

- Unable to identify quiet assets as expected with passive detection
- Unable to identify network infrastructure
- Only able to identify signatures that traverse the sampling point

Device	Hostname	IP Address	MAC Address	MAC Vendor	OS	OS Version
Substation OT (11 devices)						
Sub firewall		✓	✓	✓		
***OT switch**						
Sub-ot admin vm	✓	✓	✓	✓		
Sub-ot runZero vm	✓	✓	✓	✓		
SEL 3530 RTAC		✓	✓	✓		
***†SEL 411L**						
SEL 751		✓	✓	✓		
SEL 351A		✓	✓	✓		
***SEL 311C**						
***SEL 321**						
***SEL 501**						
Substation OT gateway (3 devices)						
Sub-ot-gateway admin vm	✓	✓	✓	✓		
Sub-ot-gateway runZero vm	✓	✓	✓	✓		
†SEL 3622						
PV plant (8 devices)						
PV firewall		✓	✓	✓		
†PV admin vm	✓	✓	✓	✓		
PV runZero vm	✓	✓	✓	✓		
SEL 3530 RTAC		✓	✓	✓		
SEL 751						
SEL 751		✓	✓	✓		
SMA Sunny Highpower	✓	✓	✓	✓		
ELM BESS		✓	✓	✓		

Scenario 4: Scale Discovery



The scale environment size represents the number of customers that could be served by a larger substation featuring 3,948 Advanced Metering Infrastructure (AMI) devices on a single flat network within the subnet (10.200.0.0/20).

Scenario 4: Results

- Average time for scans approximately 2 hours, 15 minutes
  - Increasing scan rate settings could have led to faster scan times
- Average network traffic amounted to approximately 170 kB for each device
  - Traffic would change based on probes enabled in the scan profile
- Platform accurately generated an alert when it identified an added device
  - Alerts are highly configurable

Interruption to Operations

- Monitoring throughout testing
  - Verified the Supervisory Control and Data Acquisition (SCADA) Platform for ability to poll downstream devices
  - Internet Control Message Protocol (ICMP) polling apparatus to detect any unresponsive hosts
  - Network captures to track communications and solution traffic
- runZero results
  - Active scanning methods did not measurably affect the deployed ICS assets nor ongoing SCADA process and communications

Note: CECA conclusions cannot be assumed to be generalizable, as the sample of devices and protocols was limited by the time and availability to perform tests

Key Takeaways from Cohort 2 (ongoing)

RunZero

- Tested for its ability to discover detailed information about all **IP-addressable** devices in the environment
- Solution collected **detailed** information about devices, including **all open ports** and some OT protocols like Modbus
- Active scanning methods showed **no impact** on ICS assets' performance nor ongoing SCADA processes and communications

Asimily

- Currently undergoing testing
- Public report due out later in 2024

Thank You

www.nrel.gov

NREL/PR-5T00-90761

This work was authored by the National Renewable Energy Laboratory (NREL), 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. The views expressed in the article do not necessarily represent the views of DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Photo from iStock-627281636

NREL
Transforming ENERGY