ENEVO CYBERSEC

DefCamp2024: CRACK the SCADA

CRACK the SCADA

Contents

Malicious Actor

Mission:

Your mission, should you decide to accept it, is to find a way to compromise and to shut down the SCADA: Automatic Transfer Switch of the ABC Energy Utility Company that is serving millions of customers.
As always, should you or any of your Cyber Force be caught, we will deny any knowledge of your actions.
Good Luck!

Background:

You are part of a highly skilled group of cyber adversaries with the role to disrupt the energy infrastructure of ABC Energy Utility Company — a major provider of electricity to millions of customers across the region. Your target is a critical piece of the Infrastructure within ABC's Operational Technology (OT) environment: the **Automatic Transfer Switch (ATS) Platform** integrated into their Supervisory Control and Data Acquisition **(SCADA)** system. The ATS ensures that electricity is consistently and reliably transferred between power sources to keep the grid online during maintenance, faults, or power fluctuations. Compromising the SCADA platform and the OT ecosystem will have devastating effects on power availability. A successful infiltration could cause service outages, cascade failures, and significant chaos, undermining

public trust in ABC Utility's reliability, financial loss, reputational damage, and potentially a massive public safety crisis.

Primary Objective

Gain unauthorized access to the SCADA-controlled ATS Platform and find a way to **manipulate its operational state** to disrupt the electricity distribution managed by ABC Utility Company. To win this exercise, you need to identify and exploit the vulnerabilities in the SCADA (Servers and PLC) environment that controls the ATS Platform, leading to a critical compromise in its ability to manage power transfer seamlessly.

Victory Conditions:

The best malicious actor will be the one who achieves the following:

Successful Compromise – Gain control over the SCADA-controlled ATS Platform and disrupt the platform's normal operation.

Stealth – Maintain covert access to the system, masking your actions to avoid detection by ABC Utility's security team.

Impact – Demonstrate the impact on the ATS system's ability to transfer power, such as delayed response, incorrect switching, or complete shutdown.
Report – Prepare complete and detailed report of the attack method that demonstrates your exploitation approach and compromised infrastructure (snip pictures and logs are mandatory).

The participant with the most sophisticated, stealthy, and impactful attack will be declared the winner of the Enevo Cybersec DefCamp Cybersecurity Exercise.

Working Environment

Each team has access to the following terminals / devices:

-own laptop connected directly to the infrastructure.

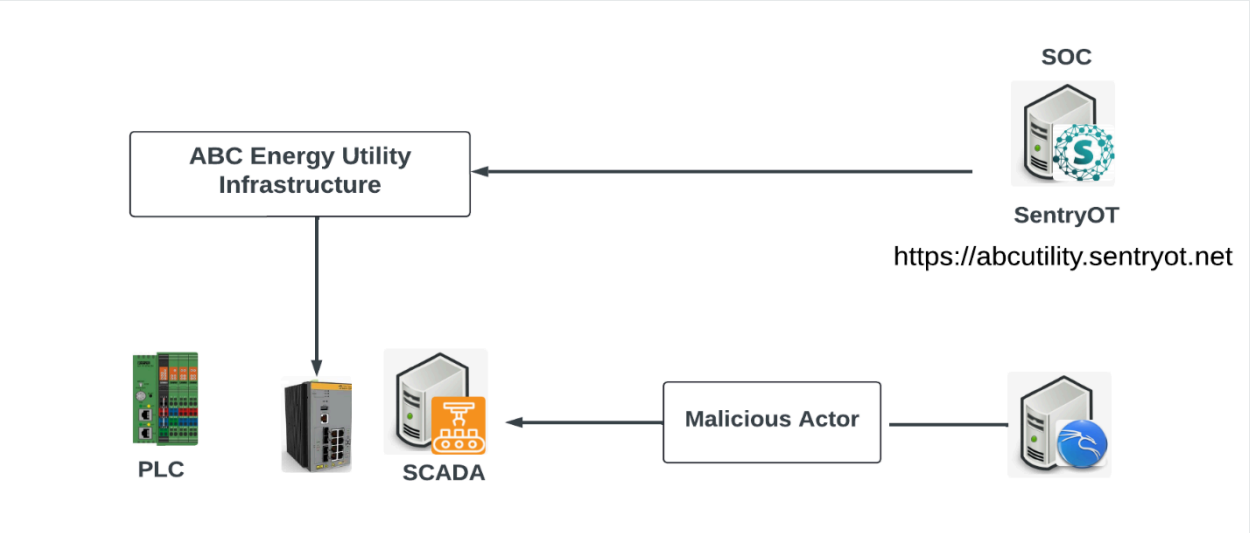
ABC Energy Company Infrastructure

Infrastructure:

ABC Energy Utility Company, leading provider of electricity serving millions of customers, has been compromised by a malicious actor. The role of the ABC Utility Company's Security Operations Center (SOC) Team is to detect and report the actions of the malicious actors. The attack began with a breach of the company's IOT Infrastructure, where the malicious actor carefully navigated through the corporate defenses, gaining unauthorized access to critical

systems. With the initial foothold established, the attacker is now focusing on the SCADA server and the PLCs, key components of the company's OT Infrastructure. By exploiting vulnerabilities in these systems, the adversary seeks to exfiltrate sensitive operational data, manipulate control settings, and send malicious commands to the PLCs. These actions could disrupt power generation, damage critical equipment, and potentially cause widespread outages, threatening the reliability of the energy supply. The attack on ABC Energy Utility Company not only jeopardizes its operations but also highlights the growing risks to national infrastructure posed by cyber threats targeting the convergence of IT and OT environments

Architecture:

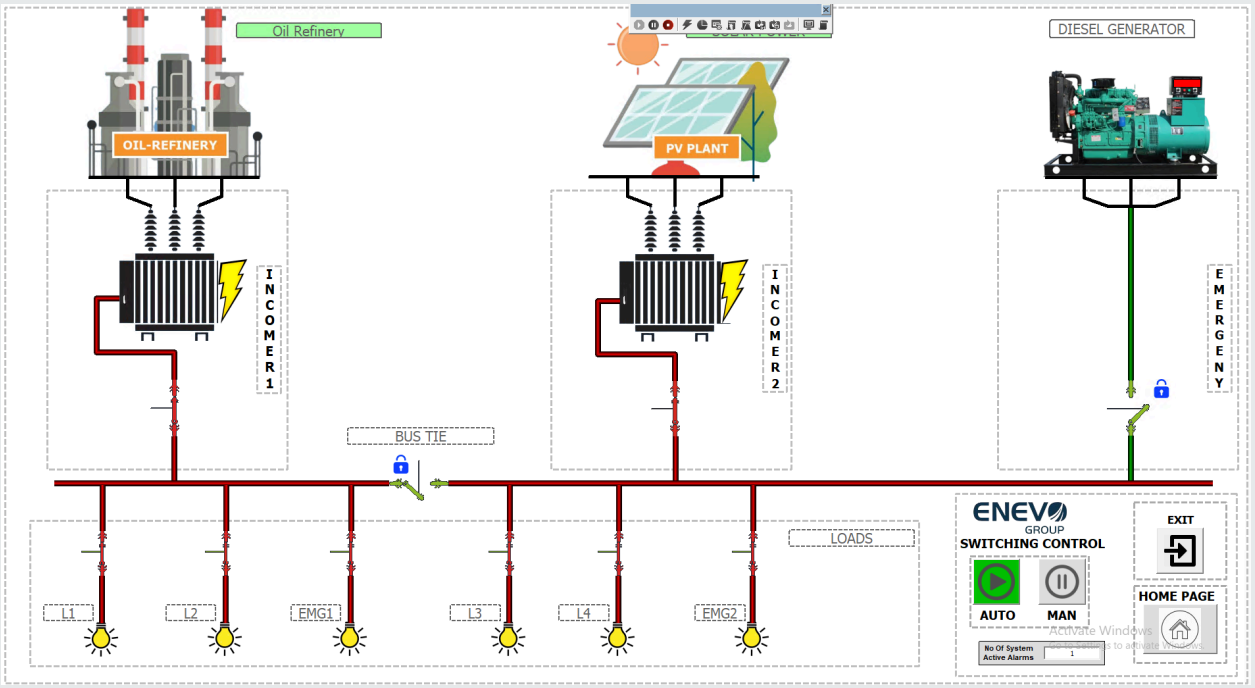


SCADA: ATS

Will be used for gathering, processing and visualizing real-time data from critical infrastructure, such as transformers, circuit-brakers and an entire process of the energy infrastructure. It enables operators to monitor and control substation operations remotely, ensuring the stability and efficiency of power distribution. This server is vital for maintaining system visibility, automating processes, and providing timely responses to faults or abnormal conditions.

Description

- The normal state of the ATS system is Incomer 1 and Incomer 2 are closed, Bus Coupler is opened, Generator is stop and Generator CB is opened. Feeders 1 through 6 are powered.
- If Incomer 1 is tripped the Bus Coupler will close and Incomer 2 will feed power for all feeders.
- If Incomer 2 if tripped the Bus Coupler will close and Incomer 1 will feed power for all feeders.
- If both Incomer 1 and Incomer 2 are tripped the Bus Couper and the Generator CB are closed and the Generator will start. In this case only the emergency feeders will be powered, feeder 5 and 6.



SOC Team:

The Cybersecurity team at ABC Energy Utility Company will play a critical role in identifying and reporting the malicious actor's actions targeting their infrastructure. Utilizing the SentryOT Platform, the SOC team will continuously monitor network traffic, system logs and operational commands to identify suspicious activities and anomalies indicative of the attack. They will analyze alerts and correlate data across OT environment to understand the adversary's tactics, techniques, and procedures (TTPs).
The goal is to identify the attack and to initiate the incident response plan and prepare the incident report.
SentryOT will be used to identify the malicious actors actions:
https://defcamp.sentryot.net

- **SIEM:** Security Telemetry; log collection, correlation, and alerting across IT and OT systems.
- **IDS:** To detect potentially malicious traffic within both IT and OT networks.
- **Operational Visibility:** Comprehensive visibility into the operational process
- **Local agents:** allow tracking commands from application to physical devices

SentryOT will provide real-time monitoring, detection and response to cyber threats targeting critical operational technology inside the ABC Energy Utility Company infrastructure. It ensures the integrity, availability, and safety of industrial control systems (ICS) by identifying anomalies, malware, or unauthorized access.
Industrial Control Systems (ICS): Comprising PLCs (Programmable Logic Controllers), SCADA (Supervisory Control and Data Acquisition) system and Engineering Workstation.

Report Summary

Mission Report Summary

Team [X]		

High-level summary: [insert a two-or-three sentence summary that explains what occurred and what the findings & resolution were]

Initial attack method	

Equipment (PLC/Switch/Server) targeted and compromised	SCADA Server, PLC, Switch
Relevant System Information used to perform the attack	PLC IP, Switch IP, SCADA Process

Attack vector / root cause	Excel file with macro embedded on
Evidence repository	PLC Parameters were modified
Indicators of Compromise	
Environment Information	

Timeline

Date and time	Event

Freeform Notes

Include links to helpful resources whether internal or external, helpful searches/commands, etc.