Hardening Wind Energy Systems from Cyber Threats-Final Project Report

Technical Report · February 2023

CITATIONS
2

READS
1,197

12 authors, including:

Jay Johnson
DER Security Corp
217 PUBLICATIONS **3,036** CITATIONS
SEE PROFILE

Craig G Rieger
TRECS Consulting
108 PUBLICATIONS **1,968** CITATIONS
SEE PROFILE

Rafer Cooley
University of Wyoming
16 PUBLICATIONS **98** CITATIONS
SEE PROFILE

Jake Paul Gentle
Idaho National Laboratory
24 PUBLICATIONS **388** CITATIONS
SEE PROFILE

SANDIA REPORT
SAND2023-12610
Printed February 2023

Sandia National Laboratories

Hardening Wind Energy Systems from Cyber Threats–Final Project Report

Jay Johnson, Michael McCarty, Bryan Richardson, Craig Rieger, Rafer Cooley, Jake P. Gentle, Bradley Rothwell, Tyler Phillips, Beverly Novak, Megan Culler, Keith Schwalm, and Brian Wright

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185
Livermore, California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods

Hardening Wind Energy Systems from Cyber Threats–Final Project Report

Jay Johnson
Sandia National Laboratories
jjohns2@sandia.gov

Michael McCarty
Idaho National Laboratory
michael.mccarty@inl.gov

Bryan Richardson
DNK Consulting
bryan@activeshadow.com

Craig Rieger
Idaho National Laboratory
craig.rieger@inl.gov

Rafer Cooley
Idaho National Laboratory
rafer.cooley@inl.gov

Jake P. Gentle
Idaho National Laboratory
jake.gentle@inl.gov

Bradley Rothwell
Idaho National Laboratory
brad.rothwell@inl.gov

Tyler Phillips
Idaho National Laboratory
tyler.phillips@inl.gov

Beverly Novak
Idaho National Laboratory
beverly.novak@inl.gov

Megan Culler
Idaho National Laboratory
megan.culler@inl.gov

Brian Wright
Sandia National Laboratories
bjwrigh@sandia.gov

Keith Schwalm
DNK Consulting
keith@dnk.com

SAND2023-12610

ABSTRACT

Sandia National Laboratories and Idaho National Laboratory created multiple network/power co-simulation environments to evaluate the ability of cybersecurity to improve wind energy system resilience. The team studied the impact of encryption, access control, intrusion detection systems, Security Information and Event Management (SIEM), and Security, Orchestration, Automation, and Response (SOAR) tools on multiple physical and cybersecurity metrics when a simulated local and remote adversary conducted a sequence of attack steps against a wind turbine site. This work attempted to quantify cost-benefit tradeoffs and risk reductions when layering different security technologies on wind energy operational technology (OT) networks and endpoint devices. We found that, once programmed, the intrusion detection systems could detect attacks and the SOAR system was able to effectively and autonomously quarantine the adversary prior to impacting the power system. Cyber and physical metrics indicated good network and endpoint visibility were essential to improve the resilience of the system, but each of the hardening features were able to improve the security posture of the wind site.

Acknowledgment

The team would like to thank the U.S. Department of Energy Wind Energy Technologies Office for supporting this research.

CONTENTS

LIST OF FIGURES

Nomenclature

ACL Access Control Lists

ARP Address Resolution Protocol

CIA Confidentiality, Integrity, Availability

CPU Central Processing Unit

DER Distributed Energy Resources

DG Distributed Generation

DHCP Dynamic Host Configuration Protocol

DHS Department of Homeland Security

DMZ Demilitarized Zone

DNP3 Distributed Network Protocol 3

DNS Domain Name System

DoD Department of Defense

EDR Endpoint Detection and Response

EMS Energy Management System

HIDS Host-based Intrusion Detection System

HIPS Host-based Intrusion Prevention System

HMI Human-Machine Interface

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

ICS Industrial Control Systems

IDS Intrusion Detection System

IED Intelligent Electronic Device

IIoT Industrial Internet of Things

IP Internet Protocol

IPS Intrusion Prevention System

IPSEC Internet Protocol Security

IT Information Technology

MAC Media Access Control

MFA Multi-factor Authentication

MODBUS Modicon Communication Bus

NIDS Network-based Intrusion Detection System

NIPS Network-based Intrusion Prevention System

NIST National Institute of Standards and Technology

OT Operational Technology

PKI Public Key Infrastructure

PLC Programmable Logic Controller

PMU Phasor Measurement Units

PV Photovoltaic

RTU Remote Terminal Unit

SCADA Supervisory Control and Data Acquisition

SDN Software Defined Networking

SEM Security Event Monitoring

SFTP Secure File Transfer Protocol

SIEM Security Information and Event Management

SIM Security Information Management

SMTP Simple Mail Transfer Protocol

SOAR Security Orchestration, Automation and Response

SOC Security Operations Center

SSH Secure Shell

SSL Secure Sockets Layer

SQL Structured Query Language

SYSLOG System Logging Protocol

SYSLOG-NG System Logging Protocol Next-Gen

TCP Transmission Control Protocol

TLS Transport Layer Security

TTP Tactic, Technique, or Procedure

UDP User Datagram Protocol

VLAN Virtual Local Area Networks

VPN Virtual Private Network

WAF Web application Firewall

WAN Wide Area Network

WEF Windows Event Forwarding

WTG Wind Turbine Generator

XDR Extended Detection and Response

ZTA Zero Trust Architecture

1. INTRODUCTION

Renewable energy production continues to grow, with wind energy supplying 9.2% of generation in the United States [1] and up to 22.6% of generation in other western countries like Germany [2]. For reference, solar energy is at 2.8% of generation in the United States [1] (for utility-scale installations) and near 10% in Germany [3]. Through diversification and greater distribution system integration, the application of renewable energy promises greater power system resilience from threats that include damaging storms and cyberattack [4, 5].

Renewable energy offers communities the ability to meet critical load demand. Distributed systems can further lift the resilience burden on transmission systems and large-scale generation suppliers to fulfill these needs. Diversification of generation assets can reduce the impact from individual threats because cyber disruptions are likely smaller in scale and less likely to affect all assets. Looking to the future and potential impacts of climate change, distribution and diversification provide practical pathways for resilience and impact reduction.

However, the control systems necessary to integrate distributed, diverse renewable energy systems expands the attack surface via more communications interfaces [6]. As a result, the resilience to cyberattack must be elevated to levels proportional to increasing threat levels to give owners and operators the reliability their mission demands. Advancing a reference architecture that enables secure design across all generation types, large and small scale, is critical to the future of distributed power system resilience.

The application of security technologies and secure applications will underpin next-generation resilient designs for energy applications, informed by research and development (R&D) work, and applied by industry. To inform a reference architecture design and R&D gaps for the renewables industry, a survey [7] was conducted to evaluate the current state of the industry. The survey was sent to cybersecurity vendors and original equipment manufacturers (OEMs) in solar energy, wind energy, and electric vehicle (EV) sectors, discussed more in Appendix A.

The survey highlighted elements of a defense-in-depth cybersecurity approach with several layers of prevention, detection, and response capabilities. Renewable energy security architectures requires multiple elements, including:

1. **Prevent**. Stop adversaries from gaining a foothold in the environment.
2. **Detect**. Monitor network traffic to recognize undesirable traffic.
3. **Analyze**. Methods, including machine learning techniques, to baseline normal traffic and endpoint operations to recognize abnormal or malicious operations.
4. **Decide/Visualize**. Present information to cyber defenders for quick recognition and response.

5. **Mitigate/Recover**. Methods to stop a cyberattack and reverse any negative effects.

6. **Share**. Provide indicators of cyberattack that can be securely shared and benefit the defenses of other organizations.

These security architecture elements are provided through the following security tools–note that many of the tools provide multiple functions:

- *Operational technology encryption*–This adds confidentiality to OT communications, but at the expense of network-based intrusion detection (NIDS) deep packet inspection visibility.

- *Access control*–Security tools that regulate who can view, create, or manipulate resources. This is often built using a role-based access control (RBAC) paradigm.

- *Network-based intrusion detection/prevention system (NIDS/NIPS)*–Uses network data to identify anomalous communications and alert (NIDS) or respond (NIPS) to adversary actions.

- *Host-based intrusion detection/prevention system (HIDS/HIPS); endpoint detection and response (EDR)*–These identify anomalous actions on endpoints (e.g., user logons, account creation/modification, binary execution, etc.) and alert (HIDS) or autonomously take defensive actions (HIPS).

- *Security information and event management (SIEM) system*–A single interface, typically in a Security Operations Center (SOC), with alert information from different security monitoring and detection tools, threat feeds, etc., and potentially integrated analytics for detailed analysis.

- *Extended detection and response (XDR); security orchestration, automation, and response (SOAR)*–Technologies that ingest NIDS/HIDS data and use automated response tools to defend the system assets with pre-programmed playbook rules.

Based on the survey, the team selected or programmed representative tools for each of these cyber hardening technologies in the cyber range environment, as shown in Fig. 1-1 [1]. The OT Modbus traffic was encrypted using Secure Modbus/Transmission Control Protocol (TCP) [8] implemented in the SunSpec Wind Turbine Generator (WTG) controllers and in a custom RBAC proxy. The proxy authenticated a user via mutual Transport Layer Security (TLS) authentication and queried a lightweight directory access protocol (LDAP) server for access control policies to give users limited, role-based access to read and write actions on the the WTG Modbus server holding registers. Nozomi Networks Guardian [9] was used for the NIDS and Wuzah was used for the HIDS [10]. The SIEM was two Grafana dashboards that pulled data from the Elasticsearch database associated with Wuzah. This project used Palo Alto Cortex XSOAR as the SOAR tool[11]. A bash script called pbtrigger was created to scan for NIDS/HIDS alerts in the SIEM, and then issue a call to a XSOAR webhook to trigger the associated playbook [2].

[1] The inclusion of these tools in the cyber range should not be considered an endorsement by the U.S. Government or the national laboratories.

[2] Alternative SOAR implementations would regularly poll ElasticSearch directly.

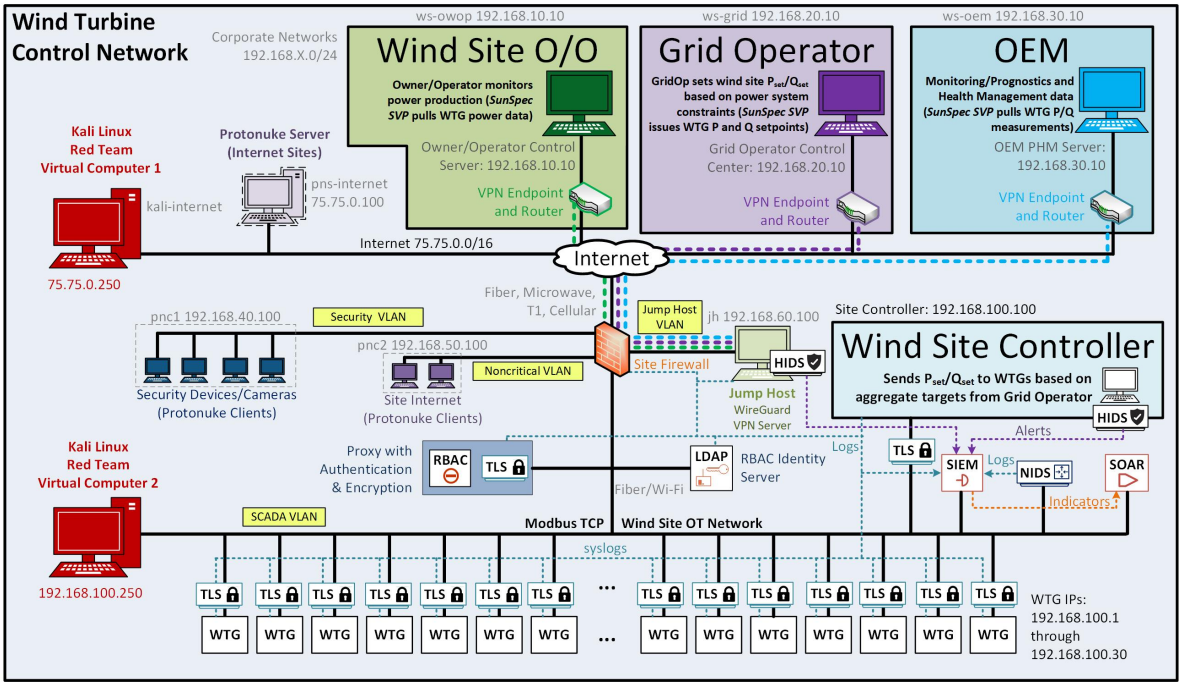

Figure 1-1. Virtualized cyber-physical environment

The primary contributions of this work were (a) creating a quantitative environment for evaluating cyber-physical metric improvements with different cybersecurity investments, and (b) establishing and calculating cyber-resilience metrics for wind generation assets. We created a real-time, high-fidelity power/networking co-simulation cyber range to study the security improvements when layering different cyber technologies onto a wind site network. This effort expanded on prior work to harden photovoltaic communications networks [12] by applying the approach to wind communications and power generation co-simulation environments with different cybersecurity defense and remediation technologies.

2. NETWORK AND POWER SYSTEM CO-SIMULATION DESIGN

This section details our approach to designing cyber-secure architectures for wind energy systems. The virtualized environment was created using multiple Sandia National Laboratories-developed Emulytics (emulation + analytics) tools:

1. minimega [13]–a tool for launching and managing virtual machines (VMs) distributed across a compute cluster.
2. phēnix [14]–an orchestration tool allowing easy configuration, access, and interaction with experiments and VMs in minimega. An image of the phēnix dashboard is shown in 2-1.
3. bennu [15]–a tool for simulating control system devices backed by physical system simulators.

These tools work in concert to easily deploy and tear down the cyber range as well as provide researchers access to virtual equipment.

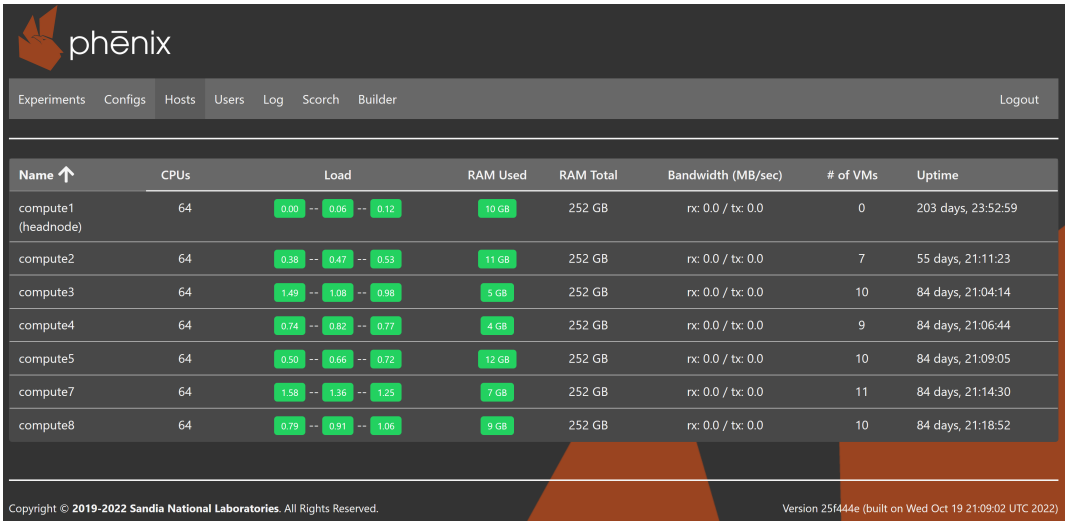

Figure 2-1. Phēnix dashboard showing experiments

2.1. Power System Model

The power system model was based on the ACTIVSg2000 synthetic 2000-bus ERCOT model [16, 17, 18], modified to include 30 WTGs. The WTGs replaced a single wind generator in the original ACTIVSg2000 model on bus 2100, which mostly impacted the voltage at the point of common

coupling when adjusting the turbine output from zero to rated power. This model was run in real-time on a separate Windows VM in the cyber range using PowerWorld Dynamics Studio (PWDS) and integrated with the bennu PWDS provider to relay measurements and setpoints between other bennu VMs acting as wind turbine controllers over the common management network.

2.2. Wind Site Network Designs

There were a total of five experiments utilized in the co-simulation environment to score the topologies against cyber and physical metrics. Each experiment was composed of the same base topology, shown in Figure 2-2. The base topology comprised four distinct networks with supporting infrastructure representing a fictional wind turbine control network topology. The four networks were a wind site owner/operator (OWOP), grid operator (GRID), original equipment manufacturer (OEM), and the wind site (WS). The OWOP, GRID, and OEM networks had independent connections to the WS network through a dedicated IPSEC tunnel. These three networks connect to the WS network to interact or control the wind site controller based on their given role. Each of those private networks comprised a private router and a workstation VM running Windows 10 and the SunSpec System Validation Platform (SVP).

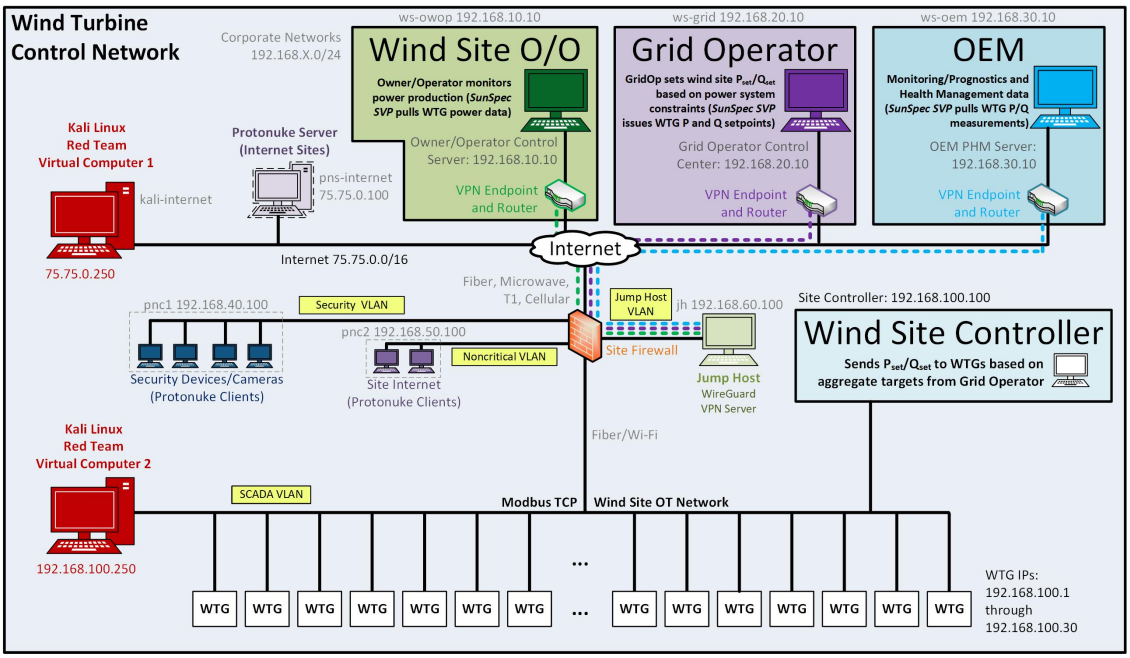

Figure 2-2. Baseline wind network architecture

The SunSpec SVP was used because it allowed easy scripting of wind site controller functions; i.e., reads and writes to monitoring and control data points. The team configured the WTGs to include SunSpec Modbus servers so that pySunSpec and other tools could interact easily with the turbine equipment. This represented basic OT communication traffic between the OWOP, GRID, and OEM workstations to the WS controller–though the communication protocol will vary site-to-site.

This protocol was also selected because it supported public key infrastructure-based encryption and certificate-based role-based access control (RBAC).

Each of the four private networks was connected to a network representing the internet. At the edge of each private network was a private router connected to an ISP router, which provided fictional internet connectivity. In the internet space was a Kali VM and a protonuke[1] server. The latter generates HTTP, HTTPS, and SMTP traffic to Protonuke clients on the WS network. In addition, a VM was meant to represent a "mobile" technician laptop accessing a jump host on the WS network. This connection was supported using a Wireguard VPN connection.

The WS network was the largest and meant to represent a wind site with 30 wind turbines. Two of the sub-networks on the WS network were for administrative functions. For example, one network was a Protonuke client VM intended to represent the security devices or cameras on the site and the traffic they may pass out of the WS network. The other was a Protonuke client VM, representing a workstation available to access specific network services. The WS private router had Access Control Lists (ACLs) limiting access to various VLANs to prevent each of the sub-networks from accessing the OT systems. A third sub-network was the jump host server for connection from mobile technicians. Finally, the fourth sub-network was for the OT systems, including the fictional 30 wind turbines. One of the VMs was the wind site controller, also running Windows 10 and the SunSpec SVP. An additional Kali VM on the OT VLAN represented an internal attacker.

Each of the private routers on the four networks had ACLs that first supported the IPSec VPN connections, tying private networks together for direct access to the OT devices from the various SVPs. Next, the ACLs prevented direct access from systems on the internet. Finally, within the WS network, ACLs stopped direct access from the WS sub-networks to the OT VLAN; or, where relevant in some of the experiments, the ACLs allowed access from specific VMs.

Additional VMs were added to the WS network based on the topologies that tested various defensive approaches. One experiment included an LDAP and proxy VM to process role-based access control. When a "user" attempted to access systems on the WS network, the LDAP and proxy VMs validated their credentials and then granted access based on their role through these VMs. Next, a HIDS VM was added to monitor the WS network's jump host and wind site controller. Finally, another experiment included a NIDS VM monitoring the WS network traffic. These latter two VMs passed log collection to a SIEM VM, which, when combined with the previous two VMs, would provide alerts to a SOAR VM for an automated response.

The above experiments and related phēnix topologies can be found at the GitHub repository [2].

2.3. Hardening Technologies

Several tests were performed to demonstrate the cyber-physical benefits of different cybersecurity technologies. Each test included a different cyber range topology that incorporated these technologies as they would be fielded at a wind site. By phasing in the cybersecurity technologies, the

[1] https://minimega.org/articles/protonuke.article

[2] `https://github.com/sandia-minimega/phenix-topologies/tree/main/renewables/wind/plant`.

team was better able to quantify the resilience improvements from individual technologies. The five different wind site security topologies are provided in Table 2-1. The baseline topology only included basic perimeter controls that exist at most wind sites. Encryption and access control were added in the second topology because they provide well-known confidentiality and authentication protections. Topology 3 included a NIDS, which provided sensing of potential malicious behavior on the network and a SIEM that provided analysis and visualization for the cyber defenders. Topology 4 employed the SIEM with the HIDS installed on the jump host and the wind site controller. Finally, in Topology 5, a NIDS, HIDS, SIEM and SOAR were integrated with the system. The SOAR enabled the environment to autonomously respond to NIDS and HIDS alerts to block the attacker's IP address.

Table 2-1. Phased introduction of a cybersecurity reference architecture

Topology	Encryption	Access Control	SIEM	HIDS	NIDS	SOAR
1 (baseline)						
2	X	X				
3			X		X	
4	X		X	X		
5			X	X	X	X

2.4. Cyber-Physical Metrics

Cyber and physical impact metrics were created to correlate security technologies to resilience improvements. The physical impacts were calculated based on the impact on the wind site power production and local voltage measurements. The cyber metric provided a basis for the alignment or threat to the communications infrastructure based on *a priori* knowledge of the two attacker kill chains [19]–or sequences of adversary actions to reach their objective.

The physical resilience score was the result of two penalty measurements based on the voltage of the system and the active power production of the wind assets. The WTG wind profiles were set to produce full nameplate power (0.8 MW) for the experiments in PWDS. Because there were 30 turbines, the site was anticipated to produce 24.0 MW under normal operations. If a cyberattack reduced production, the generation penalty was represented by,

$$Pen_{gen} = \frac{P_{nameplate} - \sum_{i=1}^{N} P_{WTG_i}}{P_{nameplate}} \tag{2.1}$$

where $P_{nameplate}$ is the production of the wind site and N is the total number of WTGs, 30, at the site. This resulted in a score of 0 when the site was operating as expected and a score of 1 when the site had lost 100% of the generation due to a cyber incident. Notably, with real wind sites, the generation is not fixed at $P_{nameplate}$, so this term would need to be replaced with $P_{forecast}$ based on local anemometer measurements or some other out-of-band prediction of production.

The voltage resilience metric was calculated based on a quadratic penalty function based on the deviation from the nominal voltage (1.0 pu). The voltage metric was calculated using,

$$Pen_{volt} = \alpha(V_{PCC} - V_{nominal})^2 \tag{2.2}$$

where α was a scaling factor, V_{PCC} is the voltage of the wind site at the point of common coupling and $V_{nominal}$ is the voltage at the site without any cyber events. When the V_{PCC} was at $V_{nominal} = 1.0$ pu, the score was 0. The α term was selected to be 100 to bound the result to [0, 1] within a 0.90-1.10 pu voltage deviation. When voltage deviates from nominal voltage, the penalty increases until reaching 1 at ± 0.10 pu deviation. Small deviations are expected in Pen_{volt} under normal operating conditions due to changes in generation and loads. However, larger deviations can be caused by physical degradation of components or loss of components from a cyber or physical event. Therefore, larger deviations from the baseline voltage result in a reduction of the physical score.

The physical resilience score, R_{phys}, was determined based on the root sum squared value of Pen_{gen} and Pen_{volt} through the following relationship,

$$R_{phys} = 1 - \sqrt{Pen_{gen}^2 + Pen_{volt}^2} \tag{2.3}$$

where a score of 1 is good and a score of 0 is bad and means that both the generation has dropped to 0 and voltage is significantly outside of normal ANSI C84.1 Range B limits.

The cyber resilience was a measure of the system to resist pre-programmed local and remote cyberattacks. A cyber resilience score of 100 indicated the system had prevented all cyberattack steps for both the local and remote attack sequences. A resilience score of 0 indicated all attacks were successful and the system did not stop any of the attack steps. During the cyber attacks, the success or failure of the attack was pushed to the centralized Elasticsearch server based on custom response characteristics. The cyber resilience metric on the Grafana dashboard then pulled the number of successful attacks from the Elasticsearch database to calculate the current cyber resilience score,

$$R_{cyber} = 1 - \frac{\sum \Theta_{remote}^{successful} + \sum \Theta_{local}^{successful}}{\sum \Theta_{remote} + \sum \Theta_{local}} \tag{2.4}$$

where Θ represents the attacker steps, denoted with $remote$ or $local$ subscripts. $\Theta^{successful}$ are the steps that fully executed on the cyber range. There are eight steps in the remote kill chain and five steps in the local kill chain for a total of 13 steps, i.e., the cyber resilience score denominator. Successful execution of each attack step reduces the cyber resilience score by 0.077, so if all attacks are successful the resilience score will go from 1 to near zero.

While this approach worked well for this cyber range, alternative cyber resilience metrics are also possible that do not rely on *a priori* knowledge of attacker behaviors. These could include control or communication availability of WTGs, level of adversary access to site VLANs or systems, or number of malicious WTG commands/packets. We recommend future work to continue to investigate cyber-physical metrics for wind systems.

2.5. Security Information and Event Management (SIEM)

Situational awareness of OT systems is critical for threat hunting and forensics. Security Information and Event Management (SIEM) tools provide a real-time, single-pane view of event information. A notional dashboard (Fig. 2-3) for tracking cyber-physical resilience on a "single pane" was created that integrated alerts, trends, and cyber-physical metrics. The diversity of the dashboard ensured a cross-role perspective on how cyber and physical impacts were tied, easily displayed the level of impact, and tracked the overall resilience of the power and communications systems against threats. For this effort, this represented the recognition of the benefits of introducing cybersecurity tools.

In the cyber range, the dashboard utilized Grafana software [20] to visualize and monitor the system by querying the Elasticsearch database. This software lends properties and capabilities similar to most monitoring solutions utilized by OT fields to manage their physical equipment readings. Representing information in a manner that is understood by operators from both specialties allows for easier communication, understanding, and cooperation between these specialties, resulting in a more efficient operating environment.

The dashboard was arranged into three distinct sections that utilize common cybersecurity metrics and monitoring to understand the risk and resilience posed to physical assets within the testing environment. The top of the dashboard consisted of metric panels detailing the number of physical log events for different severity levels. This gave operators monitoring the system detailed information about how severe and/or persistent a threat to the system may have been. Showing the number of log events, grouped by severity level over time can allow operators to notice the attacks that may be more calculated or methodical by performing actions over set time intervals. Next on the dashboard is a network diagram that associates NIDS and HIDS log events to specific devices within the test environment. The desktop computer icons represent workstations, servers, and OT devices. The icons were color shaded according to the maximum severity of the NIDS and HIDS log events on a 0-10 range following these rules:

- Severity < 4 = Green
- $4 \leq$ Severity < 7 = Yellow
- Severity ≥ 7 = Red

Finally, in the bottom pane is a line-graph panel displaying cyber-physical metrics defined in the previous section over a period. The combination of panels displaying event logs grouped by severity and resilience metrics over time gives operators a visual correlation capability to view how different system events may impact the resilience of the testing environment.

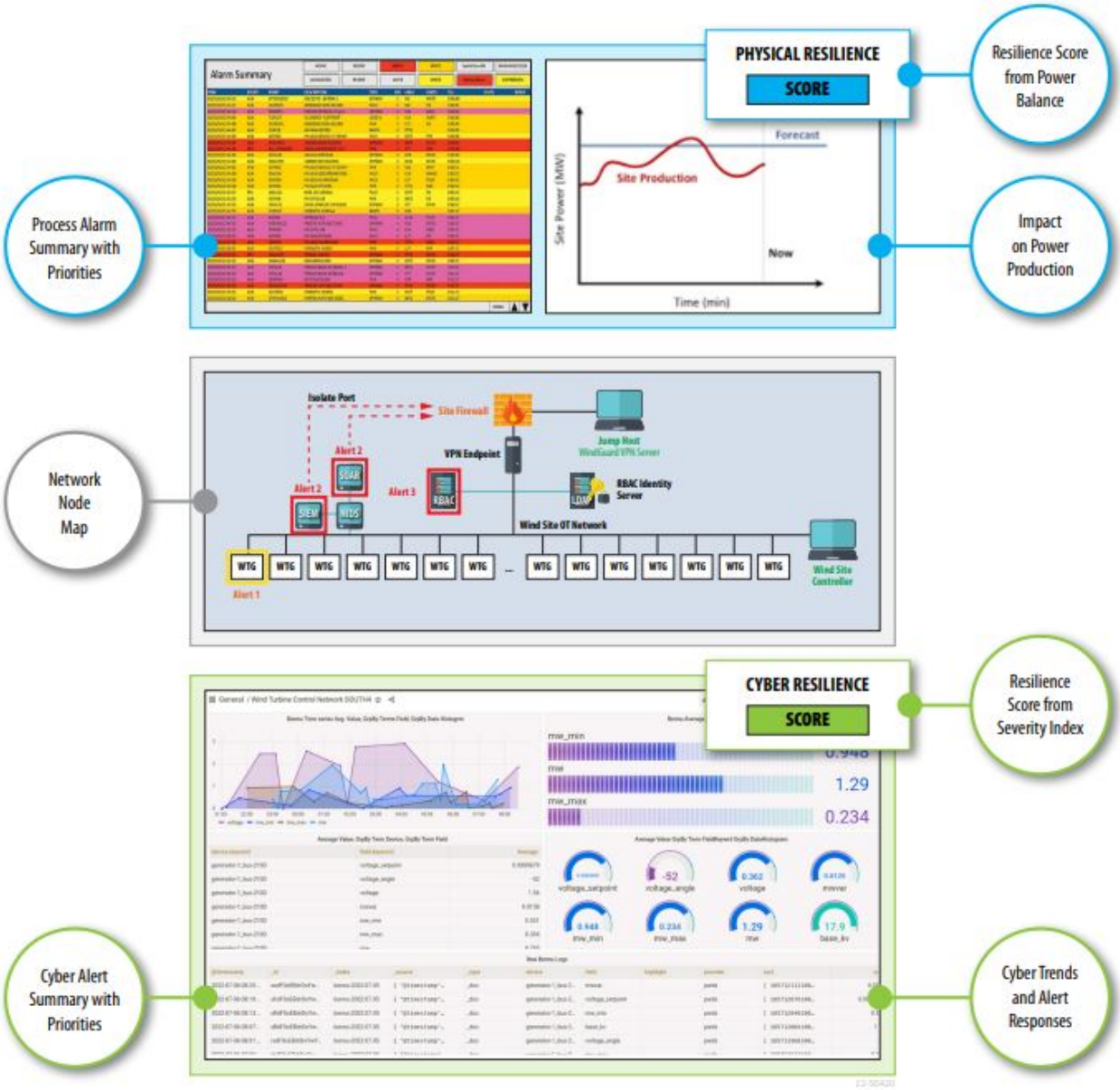

Figure 2-3. Conceptual design of a cyber-physical dashboard for wind sites

3. LOCAL AND REMOTE ATTACK SEQUENCES

The threat actors noted in this experiment can be considered having the capabilities of advanced persistent threats. Two attack vectors were considered: one originating from the internet and other via a local OT system, as depicted in Fig. 1-1. The attack steps are provided for the remote adversary in Table 4-1 and in Table 4-2 for the local adversary. Each of the steps of the kill chain was correlated with a Technique from the MITRE adversarial tactics, techniques, and common knowledge (ATT&CK) framework [21] or ATT&CK for ICS Framework [22]. The fourth column of the tables includes possible NIDS and HIDS alerts that could be generated from the adversary actions. These alerts could then be acted upon by a cyber defender or a SOAR tool, as indicated in the last column of the tables.

3.1. Automated Testing

The team used an INL-developed attack test harness (ATTAR) [25] to automate testing and provide for reproducibility. The ATTAR is a set of small, simple bash scripts designed to run in the virtualized environment for automated testing. The ATTAR included several features:

- Provides processing daemon for running tests and/or attacks across the entire network
- Allows scripting and automation mechanism
- Has ability to call Python, web browsers, file sharing, Scapy [26], robot framework [27] and others
- Works well with metasploit framework, goART [28] atomics, and other attack frameworks
- Employs a centralized location from which to view report and test results

The execution time and room for error were greatly reduced because the attacks were automated via the test harness. In fact, by using the ATTAR tool the entire remote kill chain could be executed in 206 seconds and the local kill chain could be executed in 49 seconds. This was helpful in quickly iterating over red team-blue team scenarios and refining the cyber defense tools as part of the project.

3.2. Test Harness Implementation

Using the test harness framework, targeted attack steps were scripted for the remote and local kill chains. The remote attacks used the metasploit framework; custom created metasploit modules, and specialized python scripts were used to deploy a realistic attack on the wind site. In short, the remote ATTAR attack sequence included the following:

1. Establishing the VPN connection to the jump host and starting the metasploit framework remote procedure (startup operation) daemon [23]
2. Nmap scanning to ensure the wind site controller target was online
3. Deploying the EternalBlue payload, which gave remote control of the Windows 7 wind site controller
4. Migrating the meterpreter session into the *explorer.exe* process to disguise the adversary's presence
5. Exfiltrating password hashes from the site controller's security account manager (SAM) database
6. Adding a backdoor user to the target site controller
7. Adding a scheduled task to the target site controller that would call back to a remote command and control (C2) server in case the meterpreter session died
8. Creating port forwarding rules on the wind site controller to reach the WTG Modbus servers
9. Sending Modbus writes to change 20 out of 30 windfarm WTGs to 20% active power through the Site Controller
10. Disconnecting from the VPN and shutdown the daemons (cleanup operation)

While the first and last items were simply to build up and tear down the connections, the other operations could be theoretically detected by NIDS and HIDS tools that were properly configured (and trained in the case of machine-learning based IDSs), as shown in Table 4-1. Attack steps that sent traffic over the network, like the Nmap scan and EternalBlue attack, could be detected by NIDS systems that were monitoring network traffic connected to network taps or switched port analyzer/mirror ports. In the case of the operation on endpoints, such as the process migration and creation of scheduled tasks, these can only be detected by HIDS devices on systems with the appropriate host logging functions enabled. Additionally, attacks that impact physical operations, such as the Modbus WTG writes that change site production, can be detected in changes in the power output of the wind farm. This highlights the need to have good cyber-physical data analytics and visualization tools. Further, installing diverse physical protection technologies (e.g., safety-instrumented systems, hardened control/fault logic, etc.) can reduce the impact of cyberattacks.

The local network attack sequence targeted the wind site like an adversary who had gained local OT network access. This attack kill chain was noisy with network scanning, denial of service attacks, and ultimately reduction of WTG power output. All of the attacks generated plain text network traffic that could easily be ingested by a NIDS except the brute force password attack on the remote desktop protocol (RDP) service. The ATTAR sequence included the following steps:

1. Perform an Nmap scan on the network to discover hosts
2. Hydra [29] brute force password attack on remote desktop service running on wind site controller
3. Hping3 [30] denial of service attack on wind site controller

4. Hydra brute force password attack on wind site PLC's telnet service
5. Custom python Modbus-based attack, which changes settings on the WTGs to reduce active power output to 20% of nameplate capacity

Creating these attack steps took several human-days but the automated execution only took a few minutes. As a human defender, it would not be possible to react to the automated sequence but in a real cyberattack it is likely the adversary would require several hours or days to complete these steps, in which time a human operator could block or otherwise isolate the adversary.

Table 3-1. Remote attacker kill chain

Step	Adversary Action	MITRE ATT&CK or ATT&CK for ICS TTP	Potential Cyber Alerts	Possible Cyber Defender or SOAR Response
0	Phishing attack on Wind OEM company gives attacker wind site VPN credentials.	T0865 - Spearphishing Attachment	Assumed starting place for attack.	N/A - Not in scope.
1	Adversary logs into wind network with VPN credentials.	T0822 - External Remote Services	NIDS or jump host HIDS detects VPN access from unexpected IP and posts alert to SIEM	Change firewall rule to prevent inbound traffic from attacker IP.
2	Adversary performs wind site reconnaissance (Nmap scan, etc.)	T0841 - Network Service Scanning	NIDS detects port scan	Change firewall rule to prevent inbound traffic from attacker IP.
3	Metasploit [23] EternalBlue exploit [24] with Remote Administration Trojan (RAT) payload sent to wind site controller.	T0866 - Exploitation of Remote Services	If exploit is known, NIDS or HIDS alerts on attack signature/behavior.	Block traffic to/from IP sending exploit. Temporarily prevent connections to wind site controller.
4	Privilage escalation using Metasploit to migrate to a process operating as NT Authority\SYSTEM.	T1055 - Process Injection	Advanced HIDS may be able to detect this.	Log into wind site controller and terminate process.
5	Exfiltrate hashed passwords using memory hashdump (then crack them offline)	T1003 - OS Credential Dumping, T1041 - Exfiltration Over C2 Channel	NIDS alerts on outbound traffic to unexpected IP	Firewall updated to block future data exfiltration.
6	Create new user on wind site controller and change permissions to superuser	T1136.001 - Creating new local accounts	HIDS alerts on new user account creation and modification.	Remove user from wind site controller and initiate forensics/threat hunting.
7	Establish persistence on wind site controller with scheduled task	T1053 - Scheduled Task	HIDS detects new scheduled task.	Remove scheduled task from wind site controller.
8	Port forward Modbus traffic through wind site controller to write 20% power setpoints to 20 WTGs	T0831 - Manipulation of Control, T0818 - Engineering Workstation Compromise	NIDS sees new/unexpected Modbus traffic.	Isolate wind site controller, reset WTG setpoints.

Table 3-2. Local attacker threat scenarios

Step	Adversary Action	MITRE ATT&CK or ATT&CK for ICS TTP	Potential Cyber Alerts	Possible Cyber Defender or SOAR Response
0	Three options: adversary cuts lock on wind turbine tower and plugs into network switch; adversary has site operator open malicious attachment on engineering laptop; adversary compromises local wireless OT network.	T1566.001 - Spearphishing Attachment, T0863 - User Execution, T0860 - Wireless Compromise	Assumed starting place for attack.	N/A - Not in scope.
1	Adversary performs wind site reconnaissance (Nmap scan, etc.)	T0841 - Network Service Scanning	NIDS detects port scan	Change firewall rule to prevent inbound traffic from attacker IP.
2	Brute force attack on remote desktop service of the wind site controller.	T0812 - Default Credentials, T0859 - Valid Accounts	NIDS or HIDS alerts on brute force attack.	Block traffic from offending IP.
3	Denial of Service (DoS) attack on wind site controller	T0814 - Denial of Service, T0826 - Loss of Availability	NIDS can quickly detect this.	Block attacking machine with new site and host-based firewall rules.
4	Brute force attack on WTG telnet service.	T0812 - Default Credentials, T0859 - Valid Accounts	NIDS alerts on brute force attack. If HIDS is included on WTGs, this could also alert on multiple failed logons.	Block traffic from adversary IP.
5	Attacker sends unencrypted Modbus active power setpoints to 30 WTGs	T0831 - Manipulation of Control	NIDS sees new/unexpected Modbus traffic.	Isolate adversary with firewall rules or other segmentation mechanisms. Reset WTG operations to normal.

4. RESULTS

Five different wind site network topologies were scored in accordance with the cyber and physical resilience metrics described previously. The results of the experiments are summarized in Table 4-1 and Table 4-2. Prior to running the local and remote attacks and getting the scores, each environment had the Elasticsearch database cleared by erasing all alerts, power data, and ATTAR data–which were parsed to generate the SIEM dashboard and track kill chain progress.

4.1. Resilience Metrics

In the baseline test, Topology 1, no protections or orchestration were enabled. As expected, the results represented a worst case scenario, where all adversary attacks were successful. As a result, the remote attack reduced the cyber resilience to 38.5% and the local attack reduced the cyber resilience to 61.5% taking both attacks at the same time reduced the cyber resilience to 0.0%, meaning all attacks were successful. The remote attack took approximately 1 minute to run seven of the eight attacks, gaining complete control of the system; total time to run all eight attacks was about 2 minutes.

In Topology 2, access control and Modbus encryption were added and the same battery of tests was executed. The cyber resilience score increased to 46.2% for the remote attack scenario and 69.2% for the local attack scenario. Because the adversary was unsuccessful in manipulating the WTG power setpoints without the correct TLS credentials, the physical resilience score was 96.0% for both scenarios because the voltage at the wind site point of common coupling is 1.02 pu when the turbines are operating at rated power. However, if the adversary had used their access to the wind site controller to extract certificates, they would have been able to impact the WTG generation and the physical resilience would have dropped to 46.4% and 17.2% for the remote and local attacks–or even worse if the adversary set the turbine active power curtailment to 0% of nameplate.

Topology 3 included the SIEM and NIDS. The NIDS alerted on the reconnaissance, EternalBlue, and WTG Modbus write kill chain steps of the remote attack. If a human actor was closely monitoring the SIEM, they may be able to block the attacker before Step 3 was executed. This would have increased R_{cyber} from 38.5% to 84.6% and R_{phys} from 46.0% to 96.0%. Similarly, the NIDS picked up the reconnaissance and WTG Modbus write kill chain steps of the local attack. Again if a human cyber defender was quick, they could have isolated the attack before Step 2 and increased R_{cyber} from 61.5% to 92.3% and R_{phys} from 17.2% to 96.0%.

In Topology 4, encryption, SIEM, and HIDS cybersecurity defensive tools were incorporated. Without human intervention, there was no difference between the cyber resilience score from Topology 2. The encryption again blocks all attempts to reduce the resilience of the wind turbine network just as in Topology 2. In this topology, the HIDS alone does not stop or block the

attack, but if a human actor investigated the HIDS alerts they would have been able to stop the kill chain sequence before Step 7 of the remote attack and before Step 3 of the local attack–bumping R_{cyber} from 46.2% to 53.8% for the remote attack and 61.5% to 84.6% for the local attack.

Last, Topology 5 included the NIDS, HIDS, SOAR and SIEM. In the event of a NIDS alert with a severity of $\geq$9, the script would trigger the remote attacker defense playbook, which would confirm that "EternalBlue" was in the NIDS message with a call to the Elasticsearch. The playbook would then continue and take the source IP from the NIDS message and Secure Shell (SSH) into the wind site firewall to restrict access to the SCADA VLAN by blocking the VPN IP address to the wind network. The second orchestration playbook was designed to handle a local brute force attack. If there was an alert from the HIDS with a severity >5, the script would call the local attacker defense script that would confirm multiple "failed logins" messages with the Windows 7 wind site controller. At that point, the playbook would find the offending source MAC address and SSH into the OT switch to disable the switch port the MAC address was connected to (simulated with a change in the Open vSwitch configuration).

This configuration resulted in a significant increase in cyber resilience because of the automatic reaction of the playbooks. In the case of the remote attack, the EternalBlue attack succeeds, but then the attacker is blocked from the network. For the local attack, the RDP brute force attack is terminated before it can finish. To calculate response times for the SOAR playbooks, each attack was run five times. The EternalBlue SOAR playbook executed in 2, 3, 8, 8, and 8 sec (5.8 sec average) and the local attack RDP playbook completed in 11, 8, 18, 17, 15 sec (13.8 sec average). The difference is because the RDP playbook looked for eight failed logins before triggering the playbook. As a result of the SOAR response, the cyber resilience score is 76.9% for remote attack because EternalBlue completes and 84.6% for local attack because the RDP brute force is prevented by the SOAR tool. The physical impacts are prevented to produce a score of 96.0%. If a human were to respond to the reconnaissance alerts, the cyber resilience score could be increased by 7.7% for the remote and local attacks.

The signature-based SOAR approach produced a zero false-positive rate for the experimentation, however this is a specially tailored defensive response based on known alert messages. In a field installation, the playbooks would not be fully tuned to the HIDS and NIDS alerts. Instead, it is more likely a human would need to take appropriate response actions.

4.2. SIEM Dashboards

As described earlier and shown in Fig. 2-3, the SIEM dashboards were designed to provide insights into what wind site cyber-physical data a cybersecurity defender in a Security Operations Center would see. Using data from the Elasticsearch database, a representation of the cyber and physical scores were created as shown in Fig. 4-1. This dashboard shows the site production and voltage, resilience scores, and the severity of the NIDS alerts.

The second dashboard shown in Fig. 4-2 shows a collection of NIDS and HIDS alerts. This shows the importance of detecting the attack early. This dashboard also shows the number of NIDS alerts of a given severity versus time. For the time frame shown there are two severity 9 alerts, related to

Table 4-1. Cyber hardening technology impact on remote kill chain. Red indicates adversary completed step, teal indicates the adversary was detected and an attentive human could potentially block them after this step, and green means the adversary was blocked by the SOAR tool as a result of this step.

Step	Topo 1 (Base)	Topo 2 (Encrypt, RBAC)	Topo 3 (SIEM, NIDS)	Topo 4 (Encrypt, SIEM, HIDS)	Topo 5 (SIEM, NIDS, HIDS, SOAR)
0 - VPN Access	Step Complete	Step Complete	Step Complete	Step Complete	Step Complete
1 - VPN Login	Step Complete	Step Complete	Step Complete	Step Complete	Step Complete
2 - Reconn	Step Complete	Step Complete	Complete but detected by NIDS	Step Complete	Complete but detected by NIDS
3 - EternalBlue	Step Complete	Step Complete	Complete but detected by NIDS	Step Complete	Blocked by SOAR after NIDS detects attack
4 - Privilege escalation	Step Complete	Step Complete	Step Complete	Step Complete	N/A - Adversary removed from network
5 - Exfil password hashes	Step Complete	Step Complete	Step Complete	Step Complete	N/A - Adversary removed from network
6 - Create new superuser	Step Complete	Step Complete	Step Complete	Complete but HIDS detects new user	N/A - Adversary removed from network
7 - Scheduled task	Step Complete	Step Complete	Step Complete	Complete but HIDS detects new task	N/A - Adversary removed from network
8 - WTG power attack	Step Complete	Modbus attack on WTGs is prevented with TLS encryption	Complete but NIDS detects new Modbus write operation	Modbus attack on WTGs is prevented with TLS encryption	N/A - Adversary removed from network
V_{PCC}	0.979 pu	1.020 pu	0.979 pu (1.02 pu if mitigation after step 2)	1.02 pu	1.02 pu
$\sum P_{WTG}$	11.2 MW	24.0 MW	11.2 MW (24.0 MW if mitigation after step 2)	24.0 MW	24.0 MW
Pen_{volt}	0.044	0.040	0.044 (0.040 if mitigation after step 2)	0.040	0.040
Pen_{gen}	0.533	0.000	0.533 (0.000 if mitigation after step 2)	0.000	0.000
Physical Resilience	46.4%	96.0%	46.4% (96.0% if human mitigation after step 2)	96.0%	96.0%
Cyber Resilience	38.5%	46.2%	38.5% (84.6% if human mitigation after step 2)	46.2% (53.8% if human mitigation after step 6)	76.9% (84.6% if human mitigation after step 2)

the EternalBlue attack, and one severity 7 alert, related to the Nmap scan. There is also a network map with color coding associated with alert severity. This screenshot was taken immediately after the local attack Modbus writes, where "New global function code" and the "New global variable producer" severity 5 NIDS alerts, related to the new Modbus traffic, were detected by the NIDS. Based on the destination IP addresses, the dashboard showed that all WTGs were targeted in this attack. As described earlier, we found that Nozomi did not consistently alert on Modbus events, especially if this traffic had been seen previously.

4.3. Study Limitations

As shown in the cyber and physical metrics in Tables 4-1 and 4-2, there are clear beneficial trends when including security technologies. But the benefit of the cybersecurity technologies depend on the type of attack vector and adversary tactics, techniques, and procedures (TTPs). For instance, TLS encryption protected the OT network traffic from being intercepted by malicious intruders and TLS mutual authentication foiled attempts to write to Modbus holding registers in the WTGs. In comparison, the RBAC implementation did not increase the cyber or resilience metrics because the adversary did not incorporate the Modbus proxy as part of the kill chains by, for example, using compromised TLS certificates from the OEM, O/O, or grid operator controllers. For Topology 2 and 4, based on the level of access by the adversary, additional steps could have been taken to bypass the encryption and access control protections. The NIDS and HIDS worked well to sense abnormal traffic and host actions but there was noise in the signal. Some of the false positives–defined as alerts that were unrelated to the cyberattacks–included HIDS alerts for normal user

Table 4-2. Cyber hardening technology impact on local kill chain. Red indicates adversary completed step, teal indicates the adversary was detected and an attentive human could potentially block them after this step, and green means the adversary was blocked by the SOAR tool as a result of this step.

Step	Topo 1 (Base)	Topo 2 (Encrypt, RBAC)	Topo 3 (SIEM, NIDS)	Topo 4 (Encrypt, SIEM, HIDS)	Topo 5 (SIEM, NIDS, HIDS, SOAR)
0 - Get OT Access	Step Complete	Step Complete	Step Complete	Step Complete	Step Complete
1 - Reconn	Step Complete	Step Complete	Complete but detected by NIDS	Step Complete	Complete but detected by NIDS
2 - RDP Brute Force	Step Complete	Step Complete	Step Complete	Complete but detected by HIDS	Adversary blocked by SOAR after HIDS detects failed logins
3 - WTG DoS	Step Complete	Step Complete	Complete but detected by NIDS	Step Complete	N/A - Adversary removed from network
4 - WTG Telnet Brute Force	Step Complete	Step Complete	Complete but detected by NIDS	Step Complete	N/A - Adversary removed from network
5 - Change WTG Power	Step Complete	Modbus attack on WTGs is prevented with TLS encryption	Complete but NIDS detects new Modbus write operation	Modbus attack on WTGs is prevented with TLS encryption	N/A - Adversary removed from network
V_{PCC}	0.954 pu	1.020 pu	0.954 pu (1.02 pu if mitigation after step 2)	1.02 pu	1.02 pu
$\sum P_{WTG}$	4.8 MW	24.0 MW	4.8 MW (24.0 MW if mitigation after step 2)	24.0 MW	24.0 MW
Pen_{volt}	0.212	0.040	0.212 (0.040 if mitigation after step 2)	0.040	0.040
Pen_{gen}	0.800	0.000	0.800 (0.000 if mitigation after step 2)	0.000	0.000
Physical Resilience	17.2%	96.0%	17.2% (96.0% if human mitigation after step 2)	96.0%	96.0%
Cyber Resilience	61.5%	69.2%	61.5% (92.3% if human mitigation after step 1)	61.5% (84.6% if human mitigation after step 2)	84.6% (92.3% if human mitigation after step 1)

logons and logoffs and NIDS alerts for packets with the same IP source and destination. Examples of false positives alerts are outlined in Table 4-3

After careful construction, the SIEM dashboard provided cyber defenders awareness of appropriate mitigative actions. Configuring these displays would be challenging for field installations because only critical information should be displayed in the SOC. Depending on the wind site design, there could be substantial differences in the layout and data presented on the SIEM dashboards. Also, depending on the cybersecurity team, different information or displays may be preferred.

A SOAR tool introduces automated playbooks that provide a step-by-step flow of actions to expediting response. The playbook designed to respond to the EternalBlue attack is shown in Fig. 4-3 and the playbook designed to respond to the password bruteforce attack from the local attacker is shown in Fig. 4-4.

Unfortunately, playbooks take hours to create and test, and they must be created for each type of suspected attack. These playbooks would not provide any security improvements for zero day vulnerabilities or attacks with unknown signatures because the NIDS or HIDS would not detect these attacks.

Table 4-3. False positive examples from the HIDS and NIDS tools

Alarm Source	Alarm Message
NIDS	Under high load
	Src and dst IP are equal
	Known nodes 192.168.100.100 and 192.168.100.100 have started anomalous communications
HIDS	Faulting application name: spoolsv.exe, version: 6.1.7600.16385, time stamp: 0x4a5bd3d1 Faulting module name: ntdll.dll
	Fault bucket, type 0 Event Name: APPCRASHResponse: Not available Cab Id: 0 Problem signature: P1: spoolsv.exe
	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name:WS-OT Account Domain:WORKGROUP ...
	Print Spooler terminated unexpectedly
	Windows Application error event

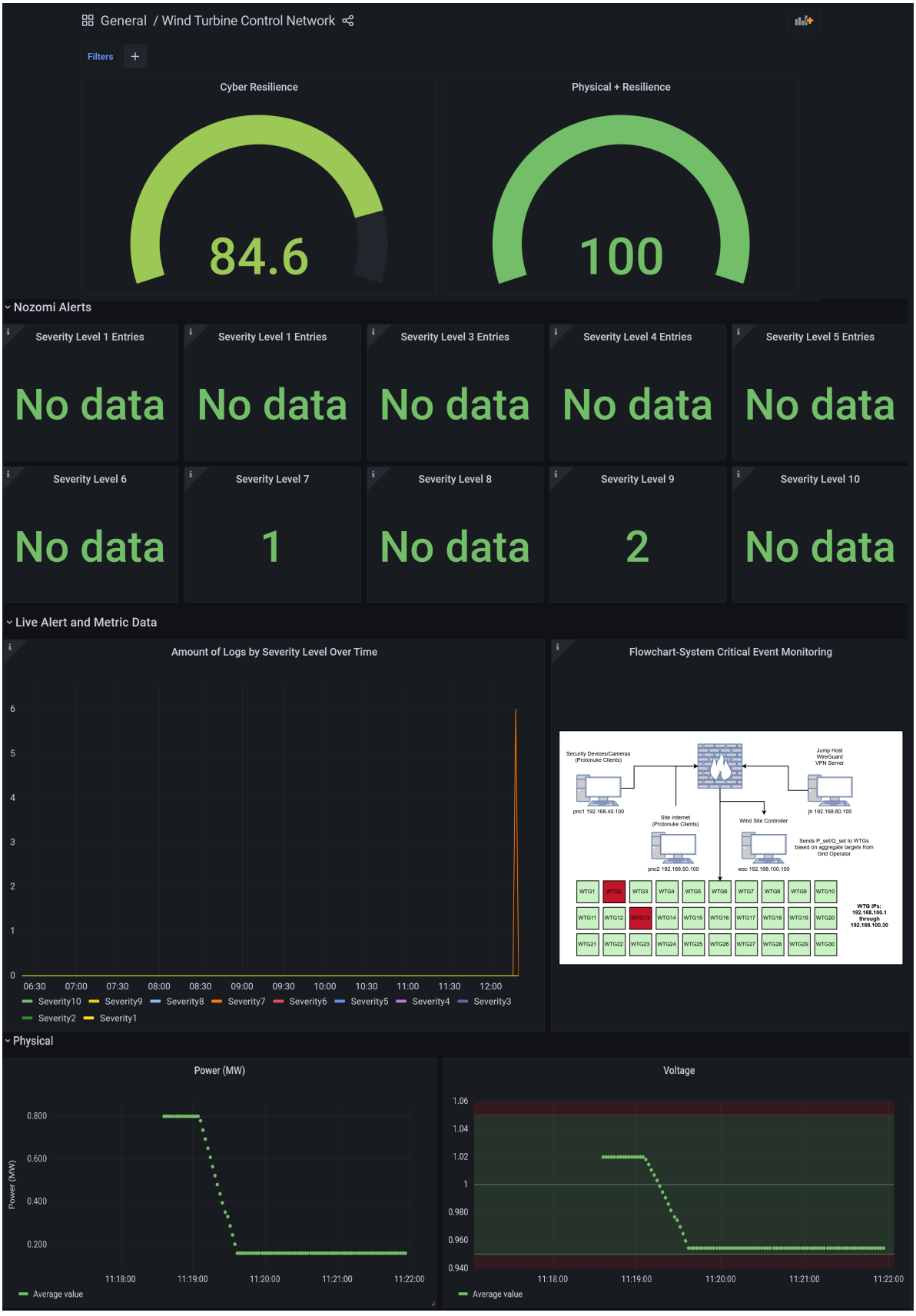

Figure 4-1. Grafana SIEM dashboard showing wind site power and PCC voltage

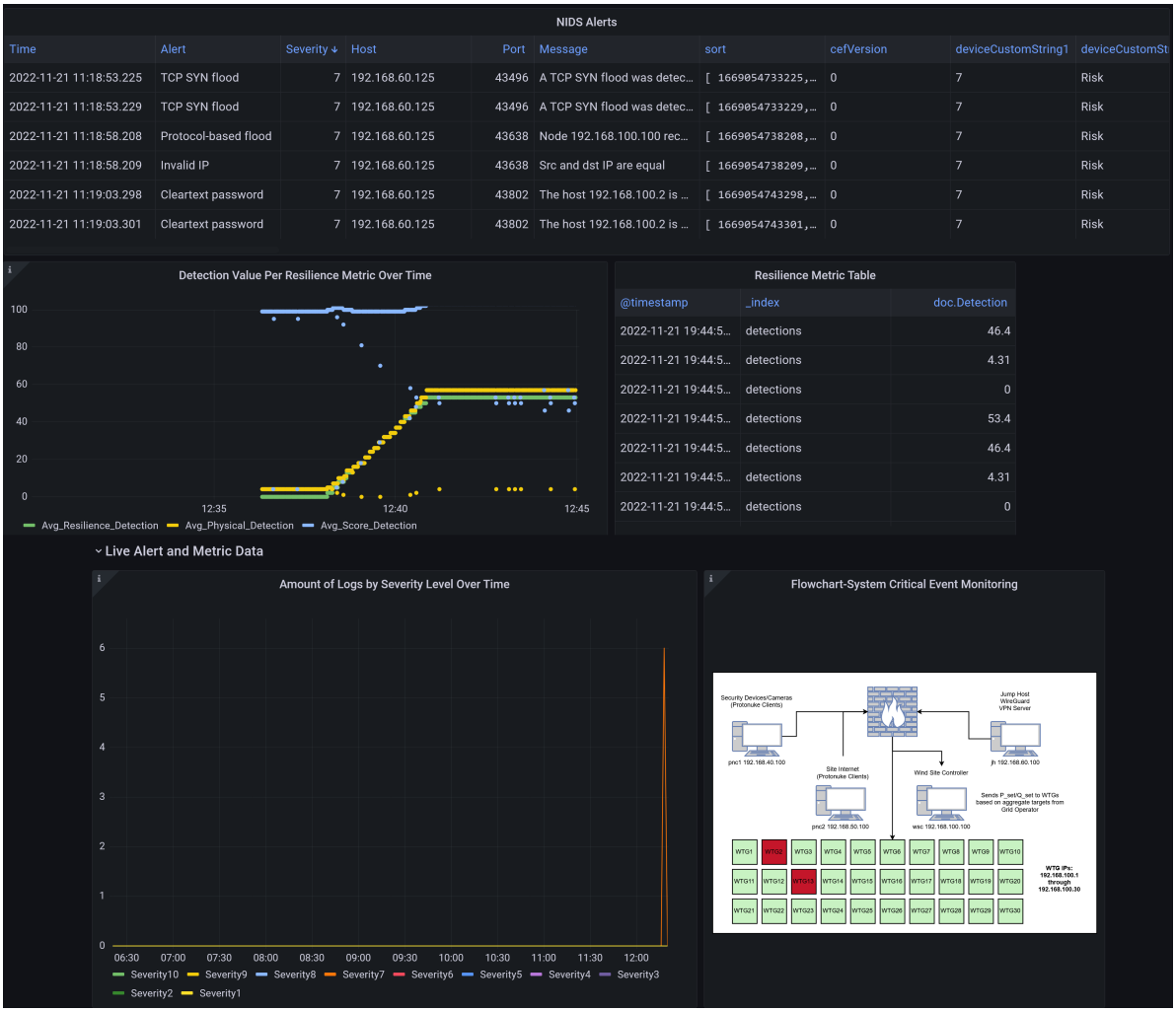

Figure 4-2. Grafana SIEM dashboard showing live NIDS alerts, severity levels, and locations of alerts based on destination IP addresses

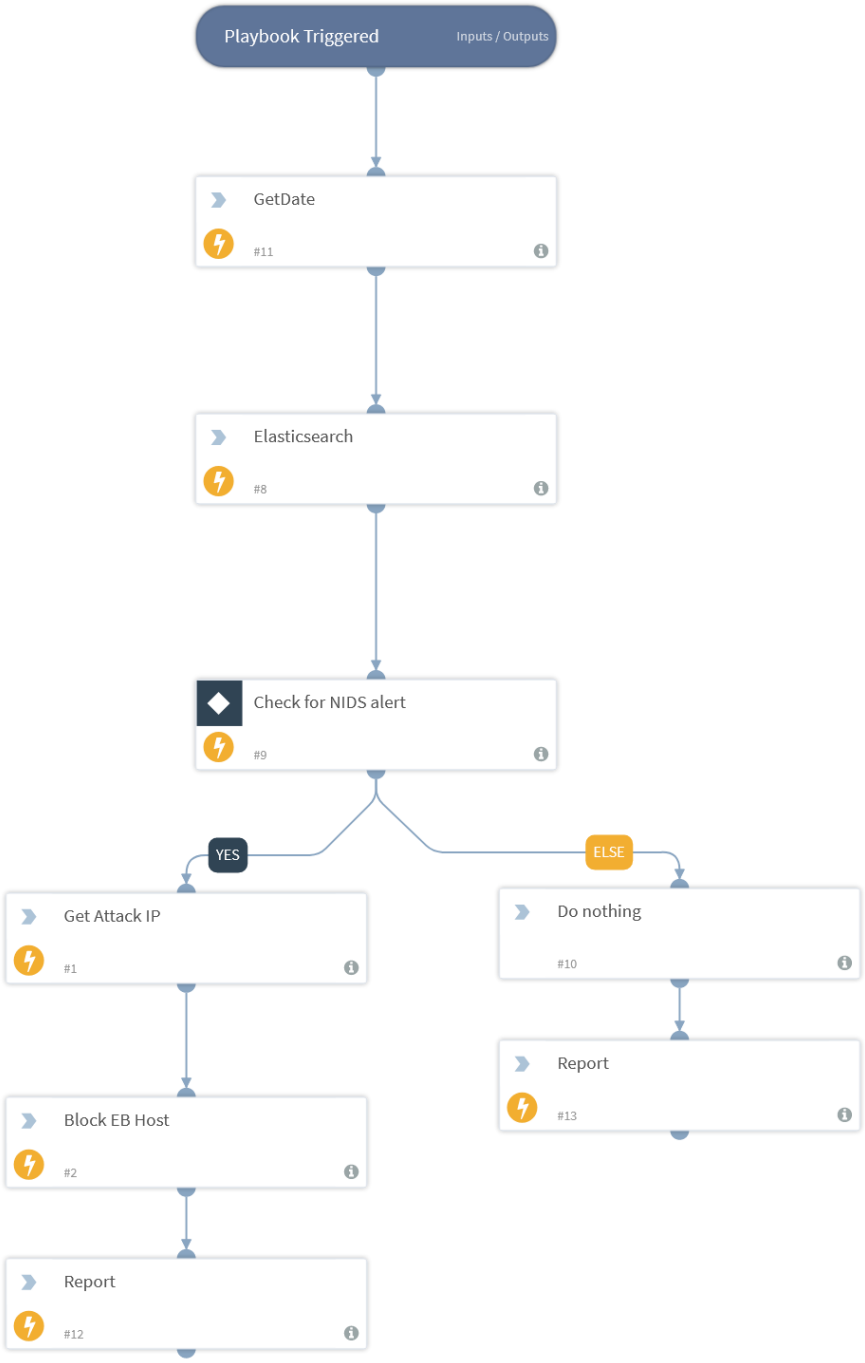

Figure 4-3. Remote XSOAR Playbook

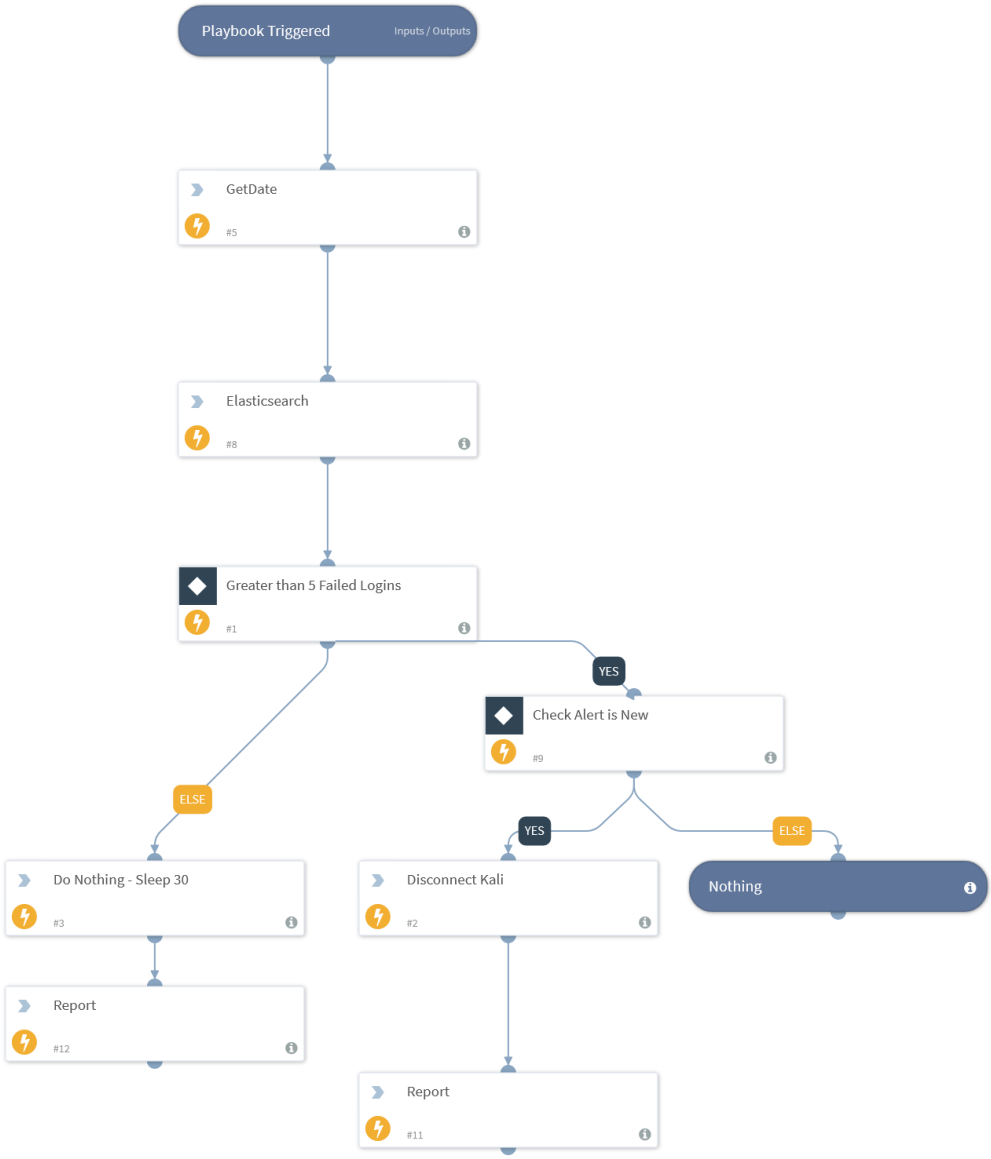

Figure 4-4. Local XSOAR Playbook

4.4. Configuring Cyber Hardening Technologies

The cyber resilience of the wind site is based on its ability to prevent, recognize, and mitigate cyberattacks. Each of the security technologies provide features to more effectively defend the wind system but only when configured correctly. Operational environments are likely to require further refinement. The following are a set of considerations when configuring and relying on these technologies in ICS networks.

4.4.1. Encryption

Encryption was provided using Secure Modbus/TCP [8] for the SunSpec protocol. This functionality was added to pySunSpec [31] to provide confidentiality in the SunSpec Modbus communications. One of the downsides of encrypting the Modbus (or any other OT traffic) is the inability for deep packet inspection tools to work on these connections. That is, if there is a malicious command or other message sent over an encrypted channel, it is not possible for NIDS tools to detect that operation and send an alert.

4.4.2. Role-Based Access Control

The RBAC was implemented in a custom Modbus proxy that authenticated users via mutual TLS authentication and queried an LDAP server for access control policies based on the role extension present in the Modbus client TLS certificate. The role-based access control policies were enforced at the proxy and would permit Modbus WTG read/write actions for the user based on their role. Alternatively, less granular approaches to this implementation include restricting access to the OT VLAN based on roles or "all-or-nothing" access to the WTG controllers, in turn, based on a role present in the certificate.

4.4.3. Network-Based Intrusion Detection System

Nozomi Networks Guardian requires a training period to learn normal network patterns. This training data set needs to include a full range of operations or there is the risk of false positives once it is switched into protecting mode. For the wind simulations, the NIDS was trained with 1 hour of network data that included normal wind site controller interactions with the WTGs. If other actions are likely in the environment, such as remote access by owners or OEMs, this traffic should be included in the training data set. While that initial training set was used to generate alarms, the system continues to learn. Therefore, if an adversary is interacting with the system over an extended period, the likelihood of detecting their actions decreases over that period because the machine learning NIDS tool begins to recognize this traffic as normal. An example of the NIDS interface with alerts is provided in Fig. 4-5.

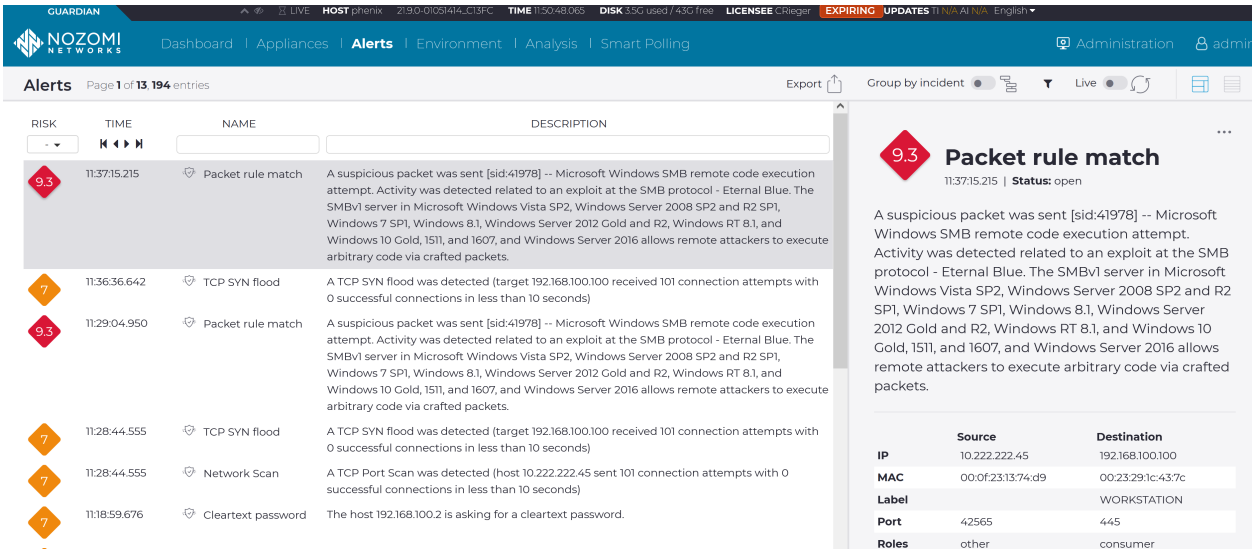

Figure 4-5. The Nozomi alerts dashboard. The highlighted alert was for the malicious Windows SMB Eternal-Blue packet.

4.4.4. Host-Based Intrusion Detection System

HIDS endpoint tools, like Wuzah agents, forward local logs to a centralized server. It is essential that appropriate logging is enabled on the endpoints so that HIDS tools can detect adversary actions. For instance, the Wuzah agent was not able to detect the creation of a new user or brute force attack on the Windows 7 wind site controller until system audit policies were modified. Critical systems should be carefully configured to ensure appropriate logging information is available. It is also helpful to perform penetration testing of these systems to validate they are configured and operating as intended. A screenshot of the HIDS GUI is provided in Fig. 4-6.

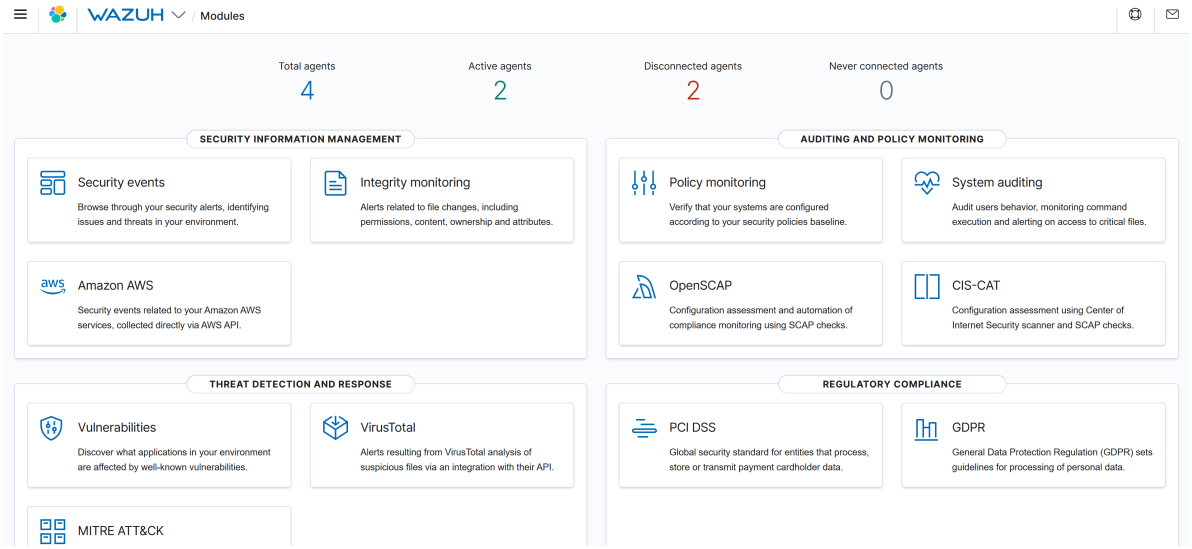

Figure 4-6. WAZUH HIDS dashboard indicating that there are two active agents. These were located on the jump host and wind site controller.

4.4.5. Security Information and Event Management

The SIEM system is designed to provide a single location to visualize corporate-wide threats. This means that critical logs and alerts need to be captured by the associated database, shown in Fig. 4-7, and easy-to-use tools need to be created to visualize and interact with this data. SIEM industry leaders have mechanisms to quickly pivot through massive data sets to perform threat hunting operations. In the case of the wind systems, not all the IDS and SOAR tools had easy Elasticsearch integrations, so custom code was created to push data and pull data from the database.

4.4.6. SOAR Implementation

The XSOAR playbooks were created using drag and drop graphical programming methods to create flow diagrams. There were two playbooks created to stop attacks. One blocked the remote adversary after detecting EternalBlue on the network and the other blocked the local attacker after detecting the RDP brute force logons. Normally, NIDS and HIDS tools would be configured to

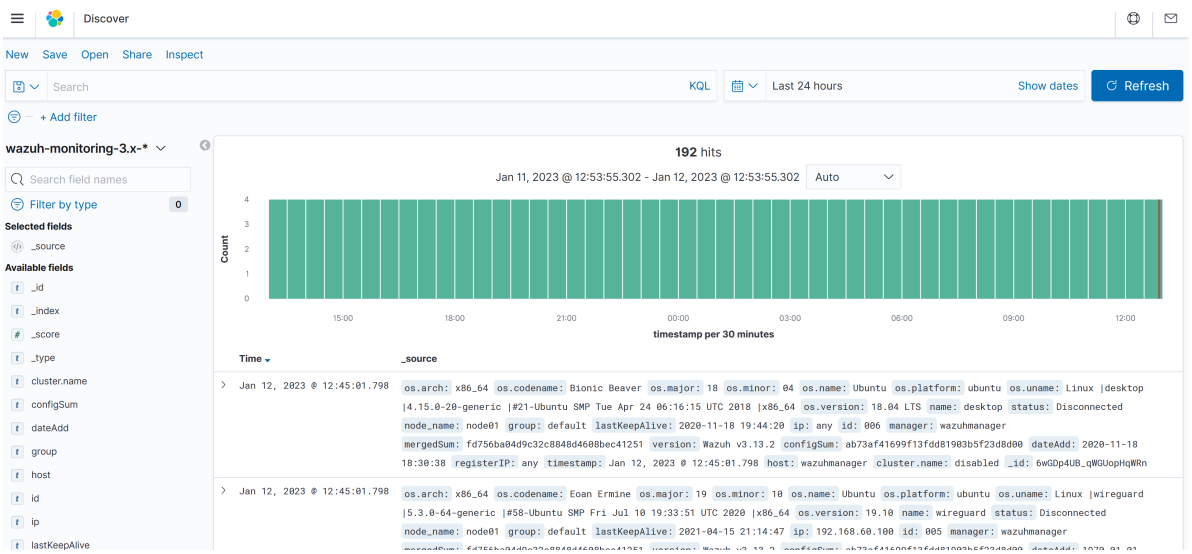

Figure 4-7. Elasticsearch SIEM database that was used to create the Grafana SIEM dashboards.

trigger SOAR playbooks, but these capabilities were not possible with the tools used in this project. To get around this barrier, we created a playbook trigger script to poll the Elasticsearch database looking for specific messages in the alerts and call the SOAR playbooks via webhooks. A better solution for triggering SOAR playbooks would be creating direct connections within Nozomi and Wuzah to directly trigger SOAR playbooks with webhooks or using RabbitMQ [32] or Kafka [33] to establish a pipeline for analyzing the severity of the alert and to determine if it rises to the level of direct, immediate action from the SOAR system.

We found that the learning curve for the SOAR tools was steep. Incorporating these technologies into wind systems will require substantial time for highly qualified security defenders. However, once configured correctly, the SOAR tool quickly and accurately isolated the adversary and prevented physical impacts to the system.

5. EXPERIMENTAL RESULTS REPLAY CAPABILITY

To enable other researchers to work with the attack, detection, and response datasets, a separate simulation environment was created capable of simulating the flow of data into the Elasticsearch database and the associated visual representation in the Grafana dashboard. This environment was created to replay results gathered by the SIEM during the experiments so alternative SOAR playbooks or other wind hardening technologies could be developed. By providing a method to replay the collected data we hope to be able to enhance the understanding of different experimental hypothesis and results with external collaborators who may not have access to the original simulation environment. It also provides the capabilities for collaborators to be able to view the Grafana dashboard from the SIEM and see what the different attacks would look like to cyber defenders and incident responders as if the attacks were happening in real-time.

5.1. Environment Details

The environment attempts to mimic the SIEM in the original simulation environment. The containerization technology, Docker, and its Docker Compose tool were utilized to define specific technologies and to deliver an easily reproducible environment. This environment was developed using Docker V20.10 and should work with any version close to or greater than that. The version of docker compose was originally targeted as V2.12 to make use of the profiles feature. However, V2+ of Docker Compose was not widely adopted at the time of the project. Therefore, a setup was configured where V1.29 of the Docker Compose tool, the last version with a publicly available container, was itself run inside of a docker container.

The environment then consists of the following three essential docker containers: Elasticsearch V7.17.3, Grafana V8.5.2, and a custom python V3.10 container. The Elasticsearch and Grafana containers were added to an "infrastructure" profile and the python container was given the "runner" profile. These profiles allowed for the environment to be defined in a single configuration file while allowing for only specific components to be run depending on which command line arguments were provided. The custom python container was built from a separate Dockerfile configuration to use a python script that was developed to read exported simulation data files and to insert the data into the replay environment's Elasticsearch instance. All of processes needed to run the replay environment are managed through a bash script that is run to perform each step of the replay process. More details of the replay tool are provided in Appendix B.

6. BENEFITS AND VALUE PROPOSITION FOR INDUSTRY

Based on discussions with industry, the value proposition for the engineers and scientists responsible for the secure, reliable operation of the wind farm is different from that of the chief information officer and other "C" suite executives, e.g., CEO, CFO, CIO, and CISO. In particular, the engineers and scientists require a technical correlation of the benefits to ensure the security and reliability. However, the C suite will require correlation of the benefits in terms of savings from cybersecurity insurance expenses, probability of losses, etc.

There has been prior analytical work to generate economic models to determine an appropriate level of cybersecurity investment. The Gordon-Loeb (GL) Model [34], for instance, has been used by organizations trying to find the right level of cybersecurity investment. The maximum monetary potential loss of a breach, L, can be calculated from the value of the site equipment, projected repair costs from cyberattack damage, the value of financial data or intellectual property located on the wind site, lost revenue based on the Power Purchase Agreement (PPA), and/or the price of electricity over the anticipated recovery time. The one-period GL Model assumes that organizations are vulnerable to cybersecurity breaches with a vulnerability (defined as a probability of inflicting L costs), v, over some period of time, e.g., 1 year. That means if there is a breach, the attacker will cost the organization a v percentage of maximum loss, known as the expected losses vL. For instance, if the site owner believes every year has a 50% chance an attacker can damage the turbines and a 75% chance an attack can depower the site for 1 day, vL would be the 50% of L for turbine damage and 75% of L for production loss for 1 day. This means the expected (annual) loss from from a cybersecurity breach is vL. However, this value can be reduced with investments in cybersecurity, z. In the GL Model, the Expected Benefit from Cybersecurity Investment (EBC) is defined as:

$$EBC(z) = [v - s(z,v)]L \tag{6.1}$$

where $s(z,v)$ is the productivity function where investments in cybersecurity technologies or personnel reduce the vulnerabilities of the system by reducing the likelihood or impact of a breach. The Expected Net Benefit from an investment in Cybersecurity (EBNC) is defined as:

$$EBNC(z) = [v - s(z,v)]L - z \tag{6.2}$$

Gordon and Loeb [34] showed that for broad classes of security breach probability functions the optimal cybersecurity investment is:

$$z^*(v) \leq vL/e \tag{6.3}$$

where e is 2.7182. This means that organizations should invest $\leq 37\%$ of the expected loss from a cybersecurity breach annually. Unfortunately, it is difficult to estimate v or L for the wind industry, since historical loss and vulnerability information is scarce and proprietary. To provide some numbers for comparison, we can look to corporate losses. Using \$4.82M as the average breach cost for critical infrastructure industries from an IBM "Cost of a Data Breach Report 2022" [35] as the annual expected loss, wind owners and operators should invest $\leq$\$1.78M in cybersecurity each time period the breach occurs. The problem is that we do not know over what time period this applies. Is a wind site breach anticipated every year or every 10 years? If a breach is anticipated every 5 years based on current cybersecurity tools/training, annual corporate wind site cyber investments should be $\leq$\$356k. Another problem is that breaches are becoming more common [1]. This means that breach probability estimates need to be re-evaluated regularly.

As described by Gorbon, Loeb, and Zhou [37], additional cybersecurity investments are not prudent at the point where the expected marginal investment costs are the same as the expected marginal benefits from the investment (e.g., reduced probability of a breach, competitive advantage over competitors, etc.). To link this back to cyber hardening technologies, Table 6-1 includes rough estimates on a cost basis for adding security. This table establishes a baseline to compare upgrading the wind turbine generators as compared to adding new security measures–where the former adds generation capacity but the latter protects that which is currently operating from loss. Within Table 6-1, the estimated technology costs and labor for commercial technologies is based on team experience and information gathered for different installations. Estimates are provided as a range because the cost can vary widely dependent on the technology chosen for the need, the capabilities of the technology, and the size of the site. Labor will vary dependent on the size of the site, network traffic, reporting requirements, etc.

To perform the cost-benefit analysis, we define a breach rate r_{breach}, that is the estimated number of breaches per year. If a company predicted there would be a breach every 2 years, $r_{breach} = 0.5$. A corporation could set this value to a higher value to be more conservative and more easily justify cybersecurity investments. Conversely, a corporation could pick a r_{breach} to be so small that cybersecurity investment is impossible to justify. The break-even point occurs when the annualized breach costs are equivalent to the total cybersecurity technology capital and operations costs–i.e., an organization can justify cybersecurity investments when,

$$\frac{vL}{e} \cdot r_{breach} \geq C_{capital} \cdot r_{breach} + C_{maintenance} + C_{labor}. \tag{6.4}$$

where $C_{capital}$ are cybersecurity capital costs, $C_{maintenance}$ are annual maintenance costs, and C_{labor} are annual labor costs. The left side represents optimal annual cyber investment from the GL Model and the right side is the average annual cybersecurity technology cost when capital costs are necessary. Rearranging and solving for the breach rate at which point investment in a security technology is justified:

$$r_{breach} \geq \frac{C_{maintenance} + C_{labor}}{\frac{vL}{e} - C_{capital}}. \tag{6.5}$$

[1] This is one of the reasons cyber insurance premiums are escalating substantially each year [36].

As an example, let us calculate the breach rate at which point investment of access control technologies is prudent. Using the IBM data, $\frac{vL}{e}$=\$1780k, $C_{capital}$=\$20k, $C_{maintenance}$=\$10k, and C_{labor}=\$50k, we find that if there is a breach rate greater than 0.040 (a breach every 25.2 years), then it is worth the investment in this technology assuming it would help reduce vL losses. If we define the inverse of the breach rate as break-even breach periodicity, τ_{breach}, we can calculate this value for each of the technologies in Table 6-1 using the average values for $C_{capital}$, $C_{maintenance}$, and C_{labor}. One could think of the τ_{breach} number as "the number of years required between breaches necessary to justify not deploying the technology".

Table 6-1. Cost-benefit analysis of adding cyber hardening tools to wind site networks

Hardening Tech	**Capital Cost**[a] (\$k)	**Maintenance Cost**[a] (\$k/yr)	**Labor** (\$k/yr)	**Average Breach Cost** [35] (\$k)	τ_{breach} (Yrs)
Encryption	225[b]	0	0	4820	Never
Access Control	5-25[c]	5-10[c]	25-100[c]		25.21
SIEM	25-1500	25-1500	1000-2000		0.45
NIDS	50-1500	50-1500	500-1000		0.65
HIDS, EDR	0[d]	25-1000	500-1000		1.41
SOAR	0[d]	100-500	1000-2000		0.988

[a] Relative subscription and maintenance cost only for commercial tools.
[b] Calculated for 45 endpoints at \$5k/device. Some vendors offer integrated solutions.
[c] Assuming an on-site LDAP or Active Directory Domain Controller for network access controls with regular maintenance and updates to the users, objects, and associated permissions. Control system devices may include access control features with network security services.
[d] No upfront software cost but there are maintenance/license costs.

7. CONCLUSION

The application of cybersecurity technologies have become commonplace in many sectors. Yet, critical infrastructure comes with unique trade-offs because cybersecurity investments are difficult to quantify, because there are few cyber-resilience metrics or data on costs from cybersecurity threats. The outcomes provided in this R&D project have helped quantify benefits in terms of risk avoidance when making investments in cybersecurity technologies. The results depend significantly on the attacker TTPs, however; if the attack methodology changes, so too will the cyber and physical metric improvements. Running several cybersecurity kill chains in a virtualized environment can illustrate a diverse mitigative benefit to a wide spectrum of attack vectors, and this will point toward a comprehensive solution that tips the cost-benefit scale toward cybersecurity tool and training investment. In this work, we found a quantitative increase in cyber and/or physical resilience metrics when incorporating OT encryption, NIDS, HIDS, SIEM, and SOAR technologies in a virtualized wind site attacked by a local and a remote adversary. We recommend that wind owners, operators, OEMs, and grid operators adopt these technologies to reduce the likelihood of a damaging attack on wind assets.

Furthermore, the reference topologies [38] and Elasticsearch data have been open-sourced to enable others to explore different security technologies and metrics-based benefit comparisons. The team encourages research entities to continue to inform the value proposition for investment by producing results. Follow-on research from this project should include development or refinement of new cyber-physical resilience metrics; conducting red team/blue team scenarios with the wind site cyber range to determine the human response characteristics; and incorporating higher-fidelity WTG and wind site controllers that are more representative of those in the field.

APPENDIX A. Survey Results

Cybersecurity vendors and renewables OEMs were surveyed to confirm the application and adaptation of technologies. Those surveyed were asked about their integration of said tools, and additionally, traditional access controls and encryption-provided perimeter defenses. The survey[7] garnered insightful perspectives from both cybersecurity vendors and OEMs on the technologies listed.

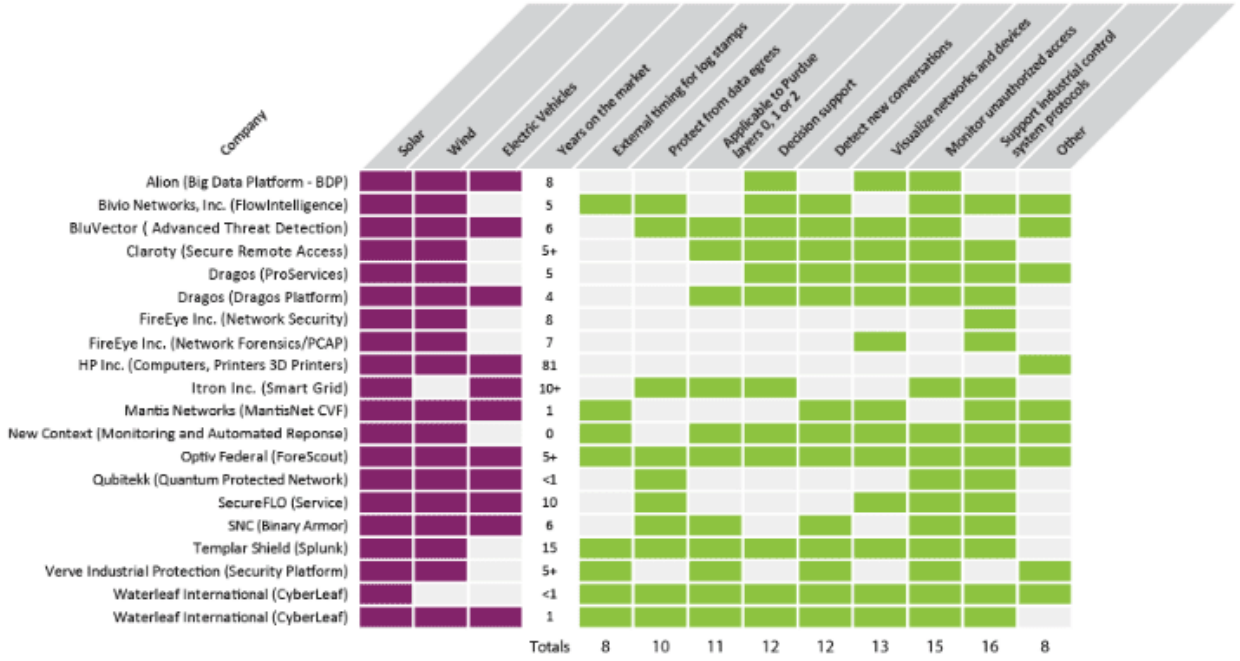

Figure A-1. Example survey results summary for the SIEM security technology

As an example of the results analysis, Fig. A-1 provides a summary example for NIDS from cybersecurity vendors. Each table provides the company, product, renewables domains impacted, and common capabilities of each product. In addition, for each capability (using categories provided), it also shows how many respondents indicated the same capability support.

Many cybersecurity vendors responded to the survey, but only a limited number of OEM renewables vendors chose to participate (shown in Fig. A-2). Evident from the cybersecurity vendors is the belief that their products may provide benefits in this domain. Less evident is a similar level of engagement on and enthusiasm for cybersecurity from the renewables industry OEMs.

Clearly, more discussion on cybersecurity reference architectures is warranted, with more substantial industry participation. Specifically, a greater understanding of the tools, benefits, and costs of

investment would be helpful. While large asset owners have integrated security, further discussion/evaluation is needed on the security of distributed renewables to ensure high-level protection and resilience is designed in. The resulting discussion should illuminate the need for decision-making tools that align benefits with investments. To achieve and maintain a common threat posture between large-scale utilities and renewables, integration of security capabilities that aggregate seamlessly is necessary.

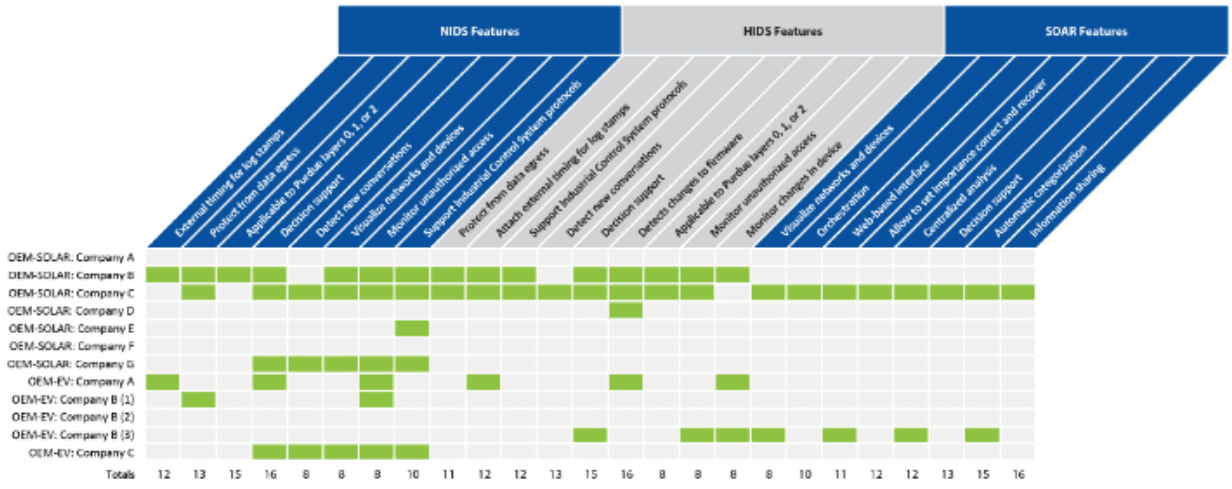

Figure A-2. OEM survey of cybersecurity application

APPENDIX B. Results Replay Features

B.1. Replay Process

All functionality for this simulation environment is achieved through the main setup bash script. It is assumed that this environment is being run from a *NIX system with a Bash shell or compatible alternative. All commands should be run from the root directory of the replay project codebase. The list below details the different high-level actions that are performed during each step of the replay.

- `setup build`: builds and tags the custom python docker container, incrementing the tag number to account for any previous versions to allow for development of the python script.
- `setup start`: starts the infrastructure profile containers using defined configuration files. Once the services are detected to be ready then the python script is triggered to finish initial configuration of the containers.
- `setup list_sim`: runs the python script in the custom container to search for and print out all available simulations from the provided data folder.
- `setup replay <sim_name>`: runs the python script in the custom container to read the data for the set of simulations given as input. The script then determines the time range of all the datapoints for the given set of simulation which it then uses to modify the timestamp of each datapoint before inserting into the Elasticsearch database. The timestamps are modified in a way such that the timestamp of the last data point would occur at the time the script is ran so it appears as though those simulations were just performed.

There is also functionality detailed in the setup file that will clean and prepare newly exported data from the simulation environment. This is to account for an issue where Grafana is unable to provision dashboards from configuration files that contain variables for datasource definitions. Therefore, the cleaning script will print out any datasource variables it finds, then a manual mapping of the variable to a legitimate datasource name is created and stored in a csv file. The csv file is then used as a guide for the second cleaning script that will perform the replacement of the variables.

B.2. Environment Meta-Analysis

Additional functionality was included in the replay environment to visualize the structure and interconnectedness of the docker compose setup as well as generate a report concerning the software used in the setup. Using the docker-compose-viz project created by the PSIH Group [39] we are

able to read the docker compose YAML file that defines this replay environment and generate the graph visualization of how each component works. This visualization helped with understanding which component could communicate with which other component. We also utilized the Syft and Grype tools developed by the Anchore company [40] which will evaluate the layers of a docker container, generate a report of what software is included in each layer and the overall container, and then search for any vulnerabilities associated with the discovered version of that software. This functionality was included to raise awareness of tools that will help researchers evaluate and understand the software they are depending on to develop their research as well as the security of those dependencies.

Bibliography

[1] "What is U.S. electricity generation by energy source?." Available at https://www.eia.gov/tools/faqs/faq.php?id=427&t=3 (2022/11/08).

[2] N. Weekes, "Wind-generated electricity in germany slumps to new low in 2021." Available at https://www.windpowermonthly.com/article/1737041/wind-generated-electricity-germany-slumps-new-low-2021 (2022/01/10).

[3] "Solar power statistics in germany 2021." Available at https://www.solarfeeds.com/mag/solar-power-statistics-in-germany-2021/ (2022/03/16).

[4] J. Schlegelmilch and D. Kushner, "The electrical grid of the future must be built around community need." Available at https://thehill.com/opinion/energy-environment/591233-the-electrical-grid-of-the-future-must-be-built-around-community (2022/01/25).

[5] C. G. Rieger, "Resilient control systems practical metrics basis for defining mission impact," in *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, pp. 1–10, 2014.

[6] IEEE Standards, "Standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," Standard ISO/IEC TR 29110-1:2016, Institute of Electrical and Electronics Engineers, Piscataway, NJ USA, 2018.

[7] "Cybersecurity reference architecture for renewable energy." https://inlbox.box.com/s/qtslosgswmew9g513mqlpm5u4wd7p4nu (2022/04/05).

[8] Modbus.org, "Modbus/TCP Security Protocol Specification." https://modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf, July 2018.

[9] Nozomi Networks, "Guardian Sensors." https://www.nozominetworks.com/products/guardian/, 2022.

[10] "Wazuh - The Open Source Security Platform." https://github.com/wazuh/wazuh, 2022.

[11]

[12] J. Johnson, "Secure scalable control and communications for distributed PV," Jan 2019.

[13] Sandia National Laboratories, "Minimega: A distributed VM management tool." https://minimega.org, 2022.

[14] Sandia National Laboratories, "Phenix Documentation." https://phenix.sceptre.dev, 2022.

[15] Sandia National Laboratories, "bennu," 2022.

[16] Texas A&M, "ACTIVSg2000: 2000-bus synthetic grid on footprint of Texas." https://electricgrids.engr.tamu.edu/electric-grid-test-cases/activsg2000/, 2022.

[17] A. B. Birchfield, K. M. Gegner, T. Xu, K. S. Shetye, and T. J. Overbye, "Statistical considerations in the creation of realistic synthetic power grids for geomagnetic disturbance studies," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1502–1510, 2017.

[18] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid structural characteristics as validation criteria for synthetic networks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3258–3265, 2017.

[19] Lockheed Martin, "The Cyber Kill Chain." https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, 2022.

[20] Grafana Labs, "Grafana." https://grafana.com/, 2022.

[21] MITRE, "MITRE ATT@CK." https://attack.mitre.org/, 2022.

[22] MITRE, "ATT&CK® for Industrial Control Systems." https://collaborate.mitre.org/attackics/index.php, 2022.

[23] "Running Metasploit Remotely." https://docs.rapid7.com/metasploit/running-metasploit-remotely/, 2022.

[24] Multi-State Information Sharing & Analysis Center, "EternalBlue." https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf, Jan 2019.

[25] "Attack Test Harness (ATTAR)." https://github.com/IdahoLabCuttingBoard/ATTAR, 2022.

[26] "Scapy Project." https://scapy.net/, 2022.

[27] "Robot Framework." https://robotframework.org/, 2022.

[28] "Red Canary's Atomic Red Team project." https://github.com/activeshadow/go-atomicredteam, 2022.

[29] van Hauser, "HYDRA." https://github.com/vanhauser-thc/thc-hydra, 2022.

[30] "hPing." https://www.kali.org/tools/hping3/, 2022.

[31] SunSpec Alliance, "pySunSpec." https://github.com/sunspec/pysunspec, 2022.

[32] "RabbitMQ." https://www.rabbitmq.com/, 2022.

[33] "Kafka." https://kafka.apache.org/, 2022.

[34] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, p. 438–457, nov 2002.

[35] IBM, "IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High," July 2022.

[36] GAO, "Rising Cyberthreats Increase Cyber Insurance Premiums While Reducing Availability," July 2022.

[37] L. Gordon, M. Loeb, and L. Zhou, "Investing in cybersecurity: Insights from the gordon-loeb model," *Journal of Information Security*, vol. 07, pp. 49–59, 01 2016.

[38] "sandia-minimega phenix-topologies." https://github.com/sandia-minimega/phenix-topologies, 2022.

[39] "docker-compose-viz." https://github.com/pmsipilot/docker-compose-viz, 2022.

[40] "Syft, grype." https://anchore.com/, 2022.

[41] CISA, "Cost of a cyber incident: Systematic review and corss-validation." Available at https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf (2/3/2023), 10 2020.

[42] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," *Journal of Cybersecurity*, vol. 6, 03 2020. tyaa005.

[43] "EPRI security architecture for the distributed energy resources integration network." https://sunspec.org/wp-content/uploads/2020/01/EPRI-Security-Architecture-for-the-Distributed-Energy-Resources-Integration-Network.pdf (2022/01/25).

[44] EIA, "Wind Explained," March 2022.

[45] N. Weekes, "Wind-generated electricity in Germany slumps to new low in 2021," *Windpower Monthly*, January 2022.

[46] J. Schlegelmilch and D. Kishner, "The electrical grid of the future must be built around community need," *The Hill, Opinion*, January 2022.

[47] J. Yan, C.-C. Liu, and M. Govindarasu, "Cyber intrusion of wind farm scada system and its impact analysis," in *2011 IEEE/PES Power Systems Conference and Exposition*, pp. 1–6, 2011.

[48] J. Staggs, D. Ferlemann, and S. Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 3–14, 2017.

[49] A. Sanghvi, B. Naughton, C. Glenn, J. Gentle, J. Johnson, J. Stoddard, J. White, N. Hilbert, S. Freeman, S. Hansen, and S. Sheng, "Roadmap for wind cybersecurity," 7 2020.

[50] M. J. Culler, J. P. Gentle, C. Velasco, and S. A. Bukowski, "Case study: Applying the inl resilience framework to iowa lakes electric cooperative distributed wind systems," 3 2022.

[51] P. Black, K. Scarfone, and M. Souppaya, *Cyber Security Metrics and Measures*. John Wiley & Sons, Inc., Hoboken, NJ, 2009-03-02 2009.

[52] C. Rieger, J. Gentle, A. Bochman, and J. Miller, "Distributed renewables' cyber resilience," 2021.

[53] Microsoft, "Microsoft Security Bulletin MS17-010 - Critical." https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010, 2017.

[54] SunSpec Alliance, "SunSpec System Validation Platform." https://github.com/sunspec/svp, 2022.

[55] Sandia National Laboratories, "Phenix Topologies." https://github.com/sandia-minimega/phenix-topologies, 2022.

[56] Tom Overbye, "New PowerWorld Modal Analysis Tools." https://www.powerworld.com/files/CC201806_08_ModalAnalysis.pdf, 2018.

[57] R. M. M. Deborah J. Bodeau, Richard D. Graubart and J. Woodill, "Cyber resiliency metrics, measures of effectiveness, and scoring," Standard Dept. No.: T8A2, Project No.: 5118MC18-KA, MITRE, Piscataway, NJ USA, 2018.

[58] R. Geleta, "Cyber security metrics for performance measurement in e-business," in *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 220–222, 2018.

[59] M. Alanzi, H. Challa, H. Beleed, B. K. Johnson, Y. Chakhchoukh, D. Reen, V. K. Singh, J. Bell, C. Rieger, and J. Gentle, "Synchrophasors-based master state awareness estimator for cybersecurity in distribution grid: Testbed implementation & field demonstration," in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–5, 2022.

[60] T. Phillips, T. McJunkin, C. Rieger, J. Gardner, and H. Mehrpouyan, "An operational resilience metric for modern power distribution systems," in *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 334–342, 2020.

[61] K. Eshghi, B. K. Johnson, and C. G. Rieger, "Power system protection and resilient metrics," in *2015 Resilience Week (RWS)*, pp. 1–8, 2015.

[62] A. Zabetian-Hosseini, A. Mehrizi-Sani, and C.-C. Liu, "Cyberattack to cyber-physical model of wind farm SCADA," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 4929–4934, 2018.

[63] ICS CERT, "XZERES 442SR wind turbine vulnerability." https://www.cisa.gov/uscert/ics/advisories/ICSA-15-076-01, August 2018.

[64] "QEMU: A generic and open source machine emulator and virtualizer." https://www.qemu.org/1, 2022.

[65] ICS CERT, "RLE Nova-Wind turbine HMI unsecure credentials vulnerability (update a)." https://www.cisa.gov/uscert/ics/advisories/ICSA-15-162-01A, August 2018.

[66] North American Electric Reliability Corporation (NERC), "Lesson learned: Risks posed by firewall firmware vulnerabilities," Tech. Rep. LL20190901, North American Electric Reliability Corporation (NERC), September 2019.

[67] R. Davidson, "AWEA 2018: Increase in cyber security attacks 'inevitable', expert warns," *Windpower Monthly*, May 2018.

[68] "Episode 22: Mini-stories: Vol 1." Interview by Jack Rhysider. Darknet Diaries (audio blog), September 2018.

[69] B. Sobczak, "Grid leaders clear the air around Russian hacking," *Energywire*, September 2018.

[70] G. Burke and J. Fahey, "AP investigation: US power grid vulnerable to foreign hacks," *AP News*, December 2015.

[71] "Over 95 per cent of WECs back online following disruption to satellite communication." ENERCON, April 2022.

[72] "Third update on cyber incident: News release from Vestas Wind Systems A/S."

[73] V. Petkauskas, "Deutsche Windtechnik hit with a cyberattack, a third on Germany's wind energy sector," *Cybernews*, April 2022.

[74] L. Abrams, "Wind turbine firm Nordex hit by Conti ransomware attack," *BleepingComputer*, April 2022.

DISTRIBUTION

Email—Internal (encrypt for OUO)

Name	Org.	Sandia Email Address
Technical Library	1911	sanddocs@sandia.gov

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.