SAND2021-4140PE

Hardening Wind Energy Systems from Cyber Threats – Project Briefing

Jay Johnson, Sandia National Laboratories

Jake Gentle and Craig Rieger, Idaho National Laboratory

Wind Consortium Meeting

7 April 2021

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.

Project Overview

GOAL:

Recommend cybersecurity defenses for wind sites
using adversary-based assessments of virtualized wind site networks

"Hardening Wind Energy Systems from Cyber Threats" Project

- $1.5M, 3-year project funded by the DOE Wind Energy Technologies Office
- Team: Sandia National Laboratories and Idaho National Laboratory

Project Plan

- Build power system and networking co-simulation environment where cyber -attacks are reflected on the power simulation
- Implement different cybersecurity defenses in the network emulation
- Conduct adversary-based (red team) assessments of different defenses to score their effectiveness against different attacks

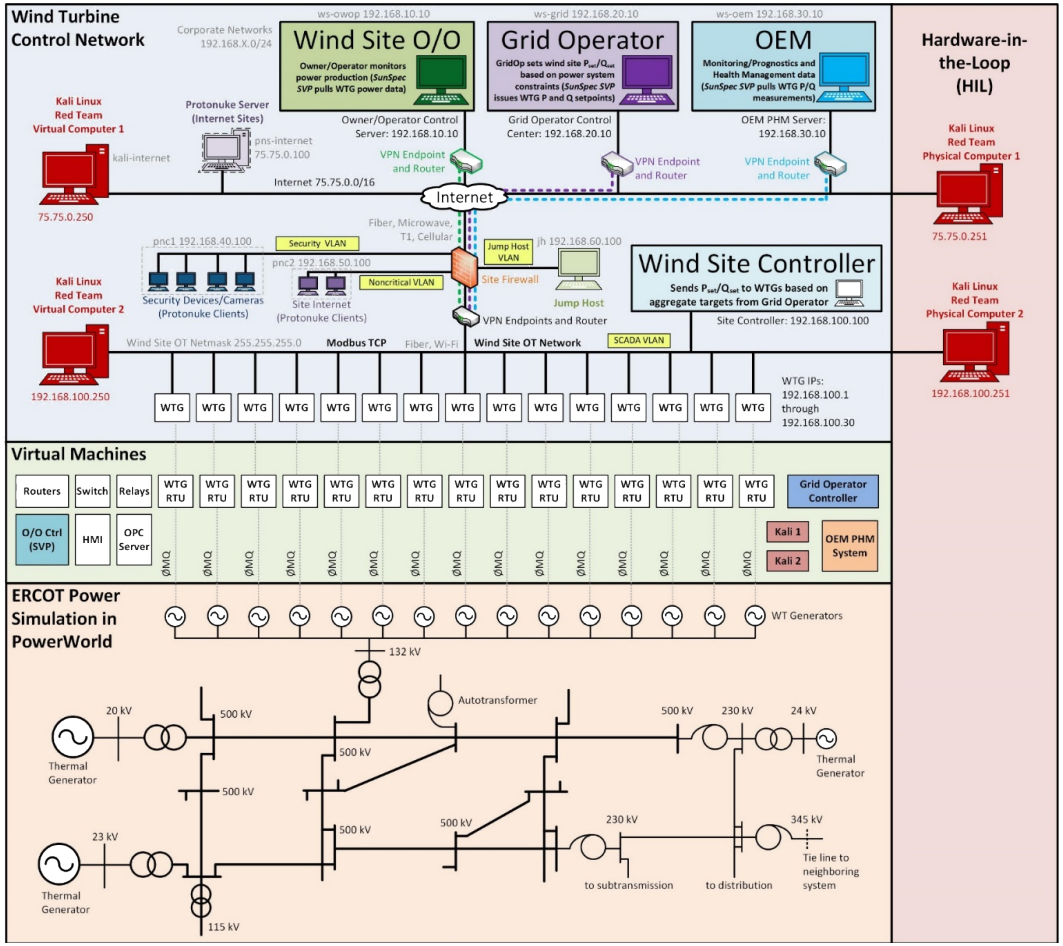
Agenda

- Co-simulation environment
- Hardened wind site architectures
- Details on hardening features
- Real-time power system resilience metric (scoring tool)
- Cybersecurity survey
- Automated security assessments using test scripts

SCEPTRE

- Cyber security assessments use realistic communication networks and power system simulations in the SCEPTRE platform
- SCEPTRE uses network emulation and analytics (Emulytics™) to model, simulate, emulate, test, and validate control system security and process simulations
- SCEPTRE is part of an Emulytics suite developed over a decade at Sandia for government agencies and military applications
- In this project, SCEPTRE will assess the cybersecurity posture of the different cyber security architectures/defenses with a red team

SCEPTRE
scada-as-a-plafform™



SIMULATION ENVIRONMENT

Networking Design

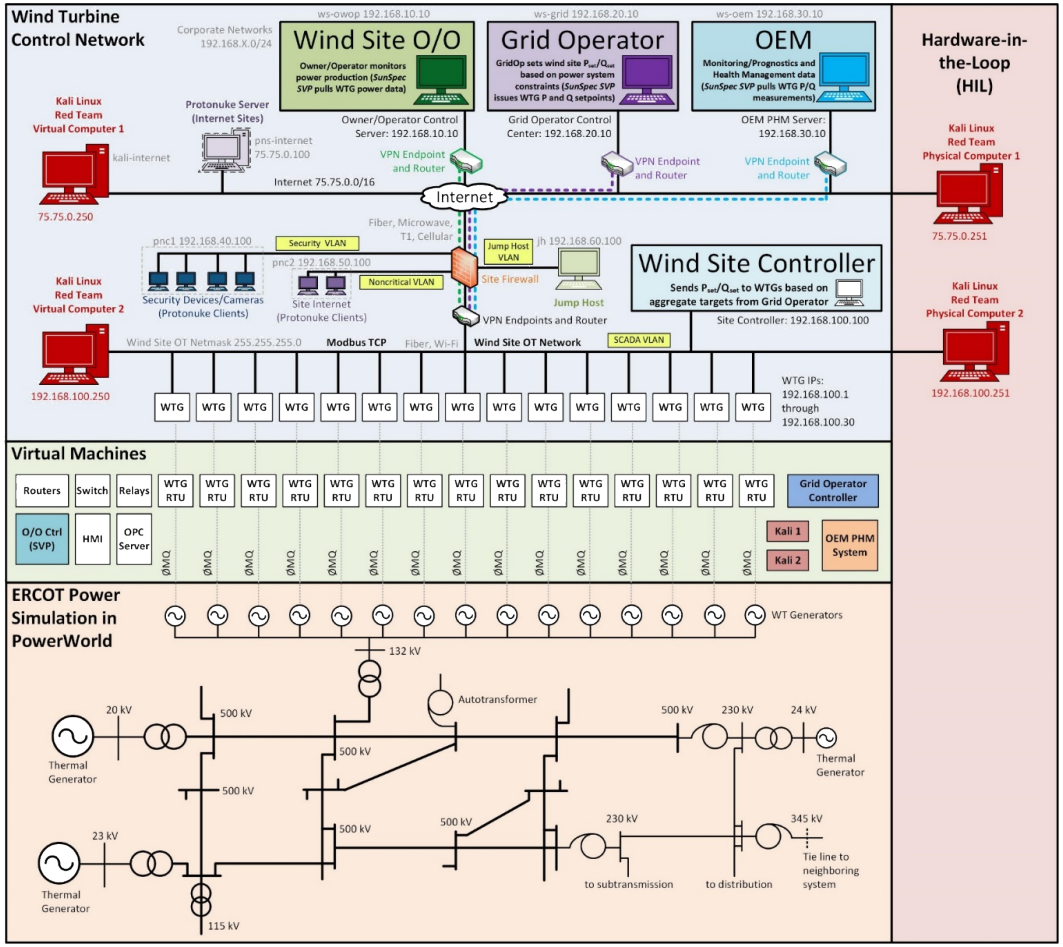
- Representative communications from OEMs, O/Os, and the utility/grid operator to wind site
- Wind Site segmentation using VLANs with dedicated network for OT traffic

Wind Turbine Emulation

- Simplified Modbus RTU wind turbine controller includes P/Q setpoints and power system measurements

Power Simulation

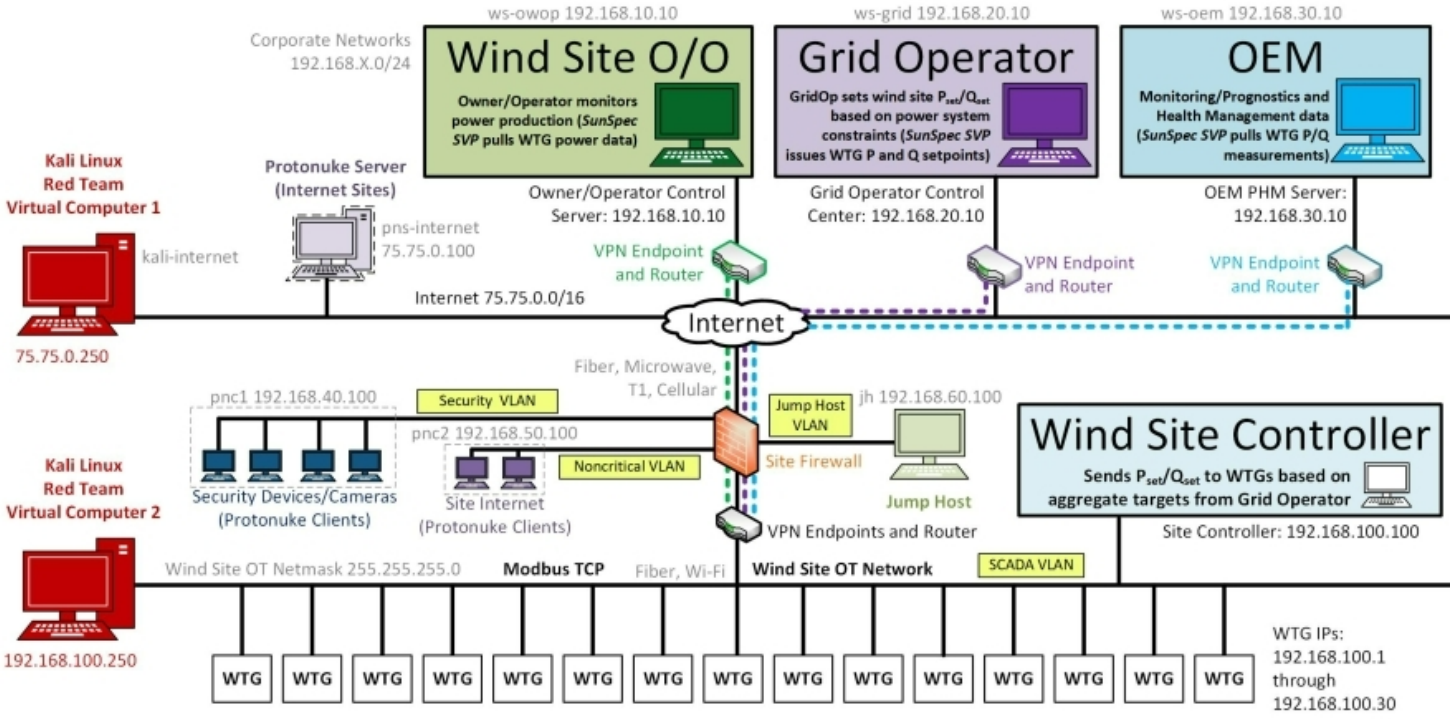
- ERCOT power simulation executed in PowerWorld to measure cyber-attack impact



SCEPTRE scada-as-a-platform™

Initial Reference Architecture (Based On Multiple Site Visits)

- Wind Site VLANs are isolated from the internet using a Site Firewall
- VPNs to the OT network are available for O/O, Grid Operator, and OEM
- Security VLAN for site cameras
- Noncritical VLAN is site Wi-Fi for operators (e.g. webinars)
- Jump host allows remote users or local operator access to the OT VLAN



Our Requests to the Wind Industry
(feedback still welcome)

Asked during the Protect our Power Best Practices in Utility Cybersecurity Conference
Jan 2020 and ESIG O&M 2020 Spring Meeting

- Recommendations for the **Baseline Reference Architecture**
  - Is our reference architecture reasonable?
  - Can you share reference architectures and security recommendations with the team? (We can sign NDAs)
  - Is segmentation widely used? Is it typically done using VLANs?
  - Are there VPNs for the O/O, OEM, and grid operators?
  - Are jump hosts common?
  - What firewall rules are used at the site perimeter?
  - What role-based access controls exist at these sites?
  - What protocols are used on the site and within the turbines?

- Certain **attack vectors** should we investigate?
  - Denial of Service
  - MITM/Data Injection/Replay attacks
  - Escalation of Privilege
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure

- What **defensive strategies** should we implement?
  - Segmentation/VLANing
  - Moving Target Defense
  - Encryption
  - IDS/IPS/Anomaly Detection
  - Firewall rules
  - Access controls/RBAC
  - SIEM/CPS analysis

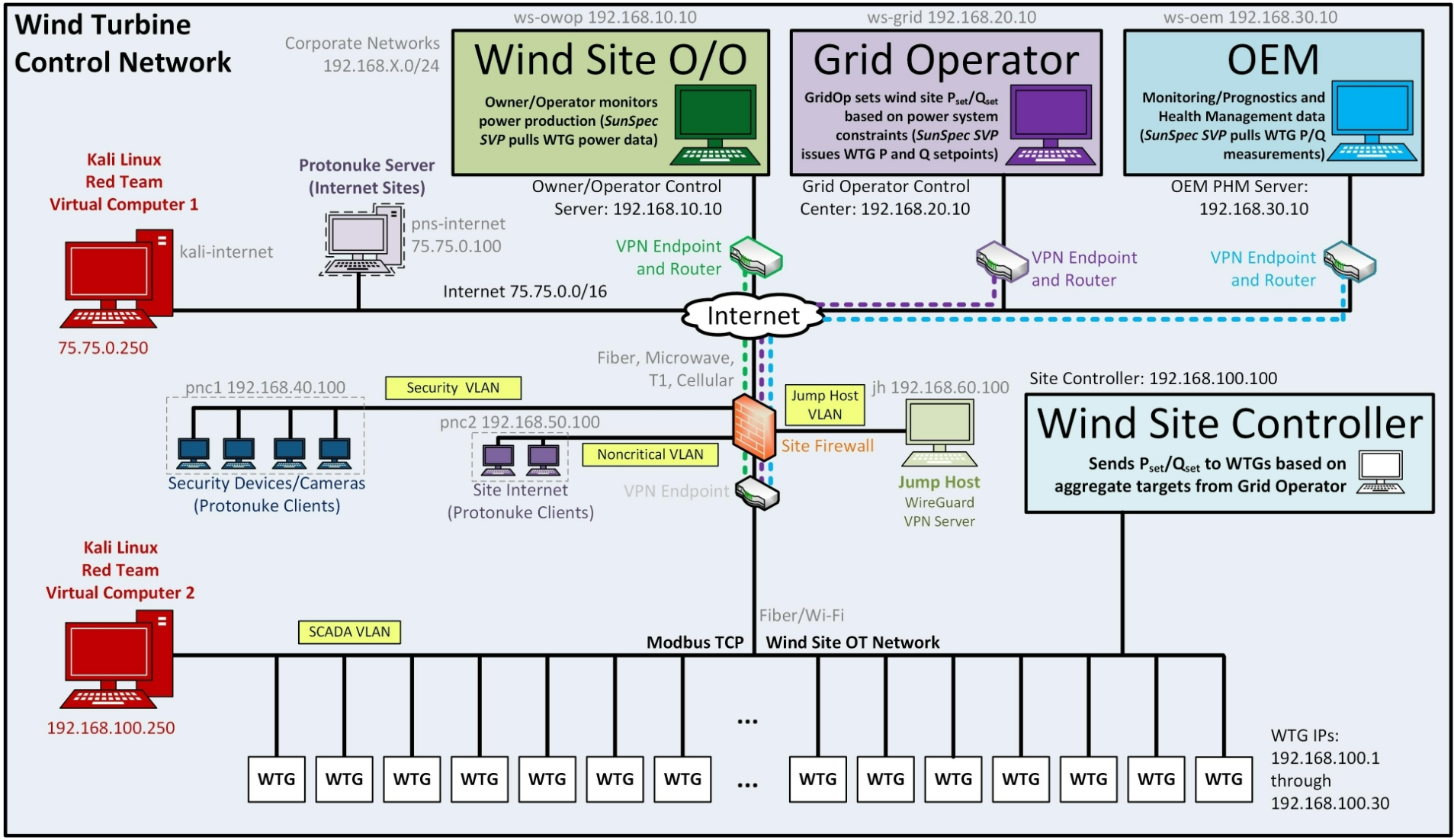
- What **consequences of concern** should we investigate?
  - Cyber
    - Confidentiality
    - Integrity
    - Availability
  - Physical
    - Adaptive Capacity (Impact to Reserves)
    - Turbine Damage (e.g., Damage Equivalent Loads)
  - Financial
    - Market Prices

Hardened Wind Site Topologies

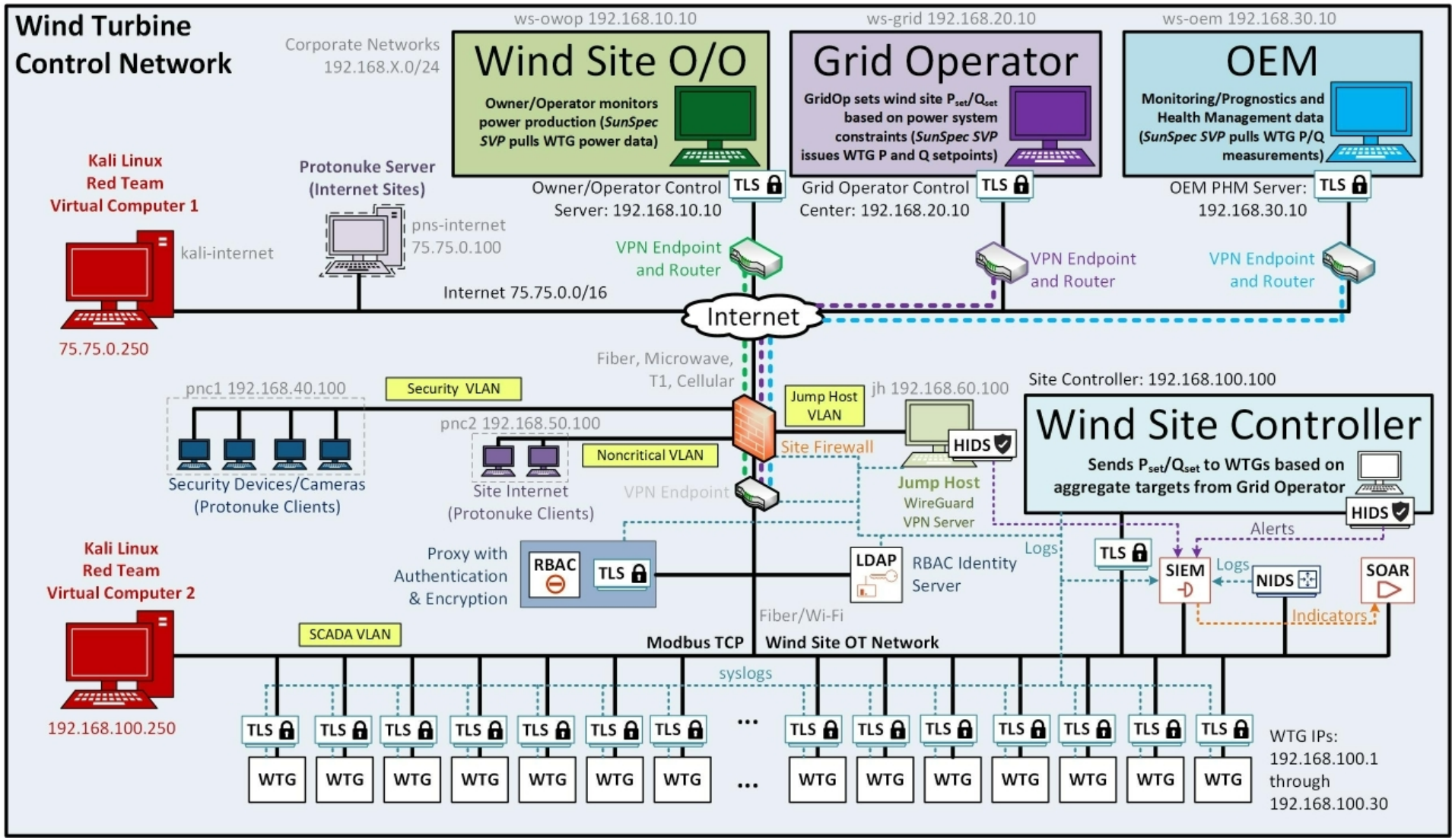
- Five topologies are proposed to demonstrate the spectrum of wind site security from baseline security to heavily fortified.
  - Topologies are designed to show the relative improvements to cyber-physical metrics from each of the technologies.
- Technologies include:
  - **OT Encryption**: encrypts traffic to the wind turbine network (or devices).
  - **Role-based access control (RBAC)**: requires users to be authenticated/ authorized before making changes to wind turbine setpoints.
  - **SIEM**: security information and event management (SIEM) system collects log data to alert admins of potentially malicious cyber activities
  - **NIDS**: network-based intrusion detection system (NIDS) uses deep-packet inspection to alert admins and/or SIEM system to anomalous network traffic.
  - **HIDS**: host-based intrusion detection system (HIDS) that alerts admins, SIEM, or SOAR system to changes to the server by monitoring logs, directories, files, and registries.
  - **SOAR**: Security Orchestration, Automation, and Response collects alerts and automates responses to threats.

	Encryption	RBAC	SIEM	NIDS	HIDS	SOAR
1 (baseline)						
2	x	x				
3			x	x		
4	x				x	x
5	x	x	x	x	x	x

Baseline Wind Site Topology

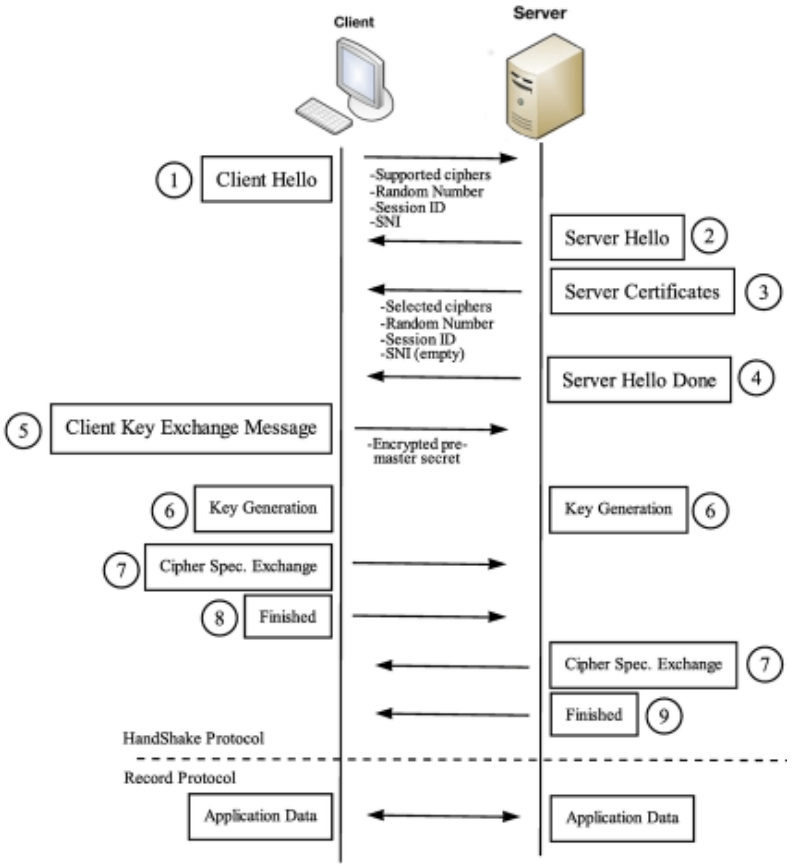


Hardened Wind Site Topology



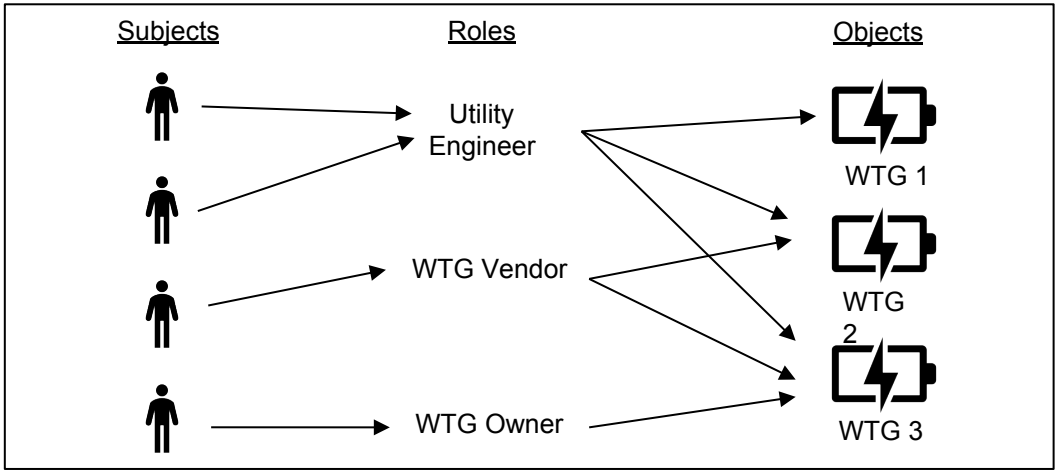
OT Encryption

- **Secure Modbus Proxy (using new Modbus TLS specification)**
  - Proxy deployed on same network as Wind Turbine Generator (WTG) controllers
- **All Modbus connections from external clients are proxied**
  - Clients use same IP address for each WTG controller, but different Modbus Unit ID
  - Proxy forwards Modbus connections based on Unit ID <--> device IP address mapping
- **All traffic between external clients and proxy is authenticated and encrypted via TLS**
  - Additionally, all clients are authenticated using certificate-based authentication as per the Modbus TLS specification
- **All traffic between internal clients (including the proxy) and Modbus WTG controllers is also authenticated and encrypted via TLS**



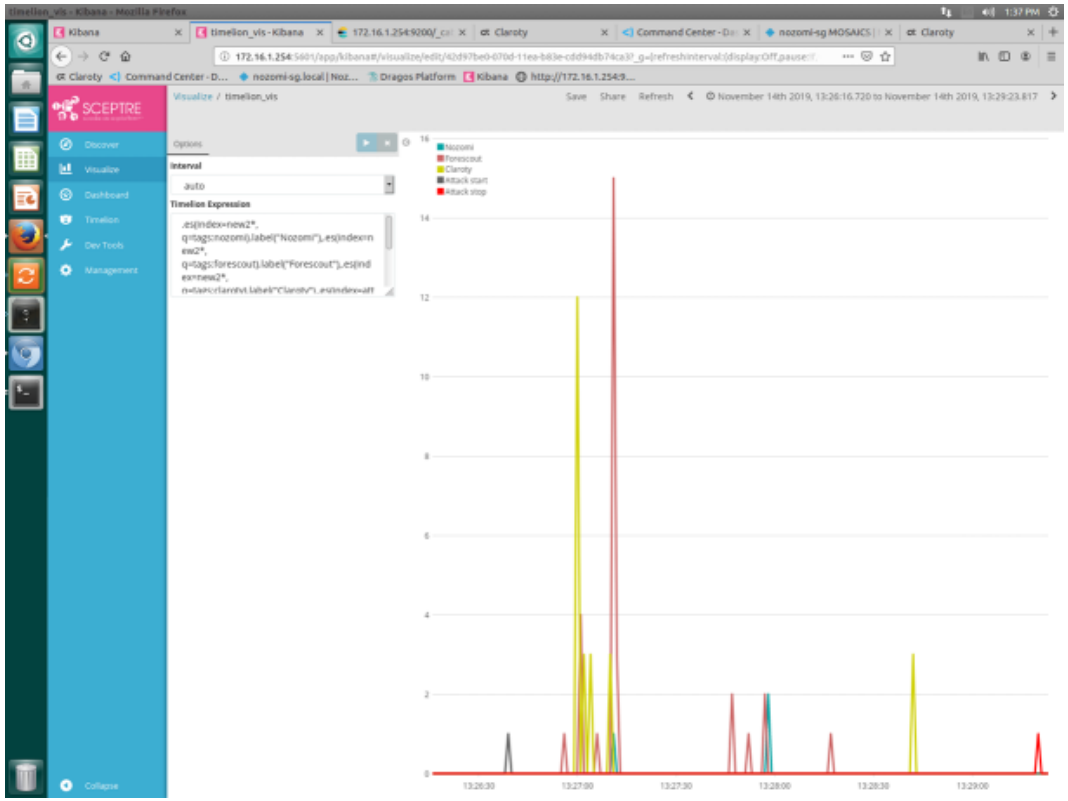
Role-Based Access Control

- Role-based Access Control (RBAC) within Secure Modbus Proxy
- Provides fine-grained control over what a Modbus client can do
  - Policies based on Modbus function codes and register addresses
  - Modbus function code policies allow for limiting based read-only vs. read/write, as well as data type (binary, analog)
  - Modbus register address policies allow for limiting access to actual physical sensors and actuators
- Modbus TLS specification calls for client role embedded in authentication certificate
  - Each client connection to Secure Modbus Proxy authenticated using client certificate
  - Once certificate is validated, role name pulled from certificate
  - Role name maps to zero or more RBAC policies (using local configuration or LDAP)
  - Client Modbus request(s) compared to role policies to allow/deny
- Role policies centrally managed using LDAP



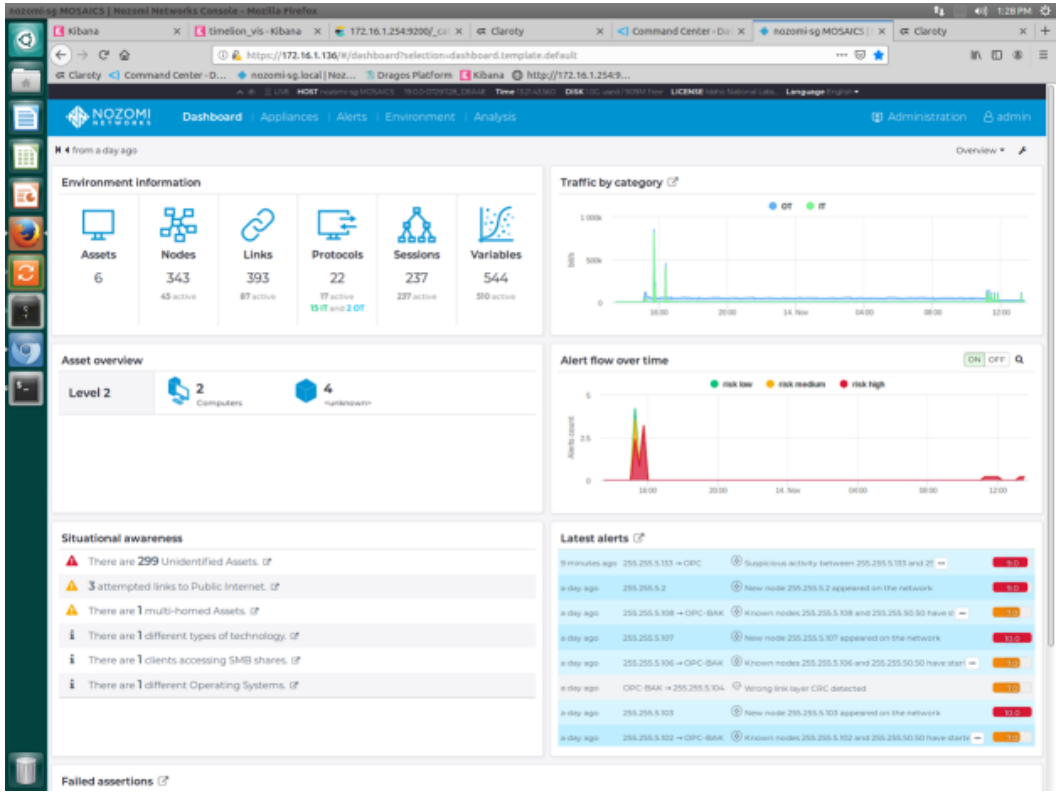
Security Information and Event Management (SIEM): ELK

- **Several Modules**
  - Logstash (Log Collection)
  - Elastic Search (Database)
  - Kabana (Visualization/Analytics)
- **Ingests logs from other systems**
- **Uses Indexes**
  - Can configure Logstash to combine multiple systems reporting to one index
- **Open Source Package that has Flexibility, but Greater User Learning Time**
  - Splunk is a competitor that has substantial built in capability, but also high investment cost



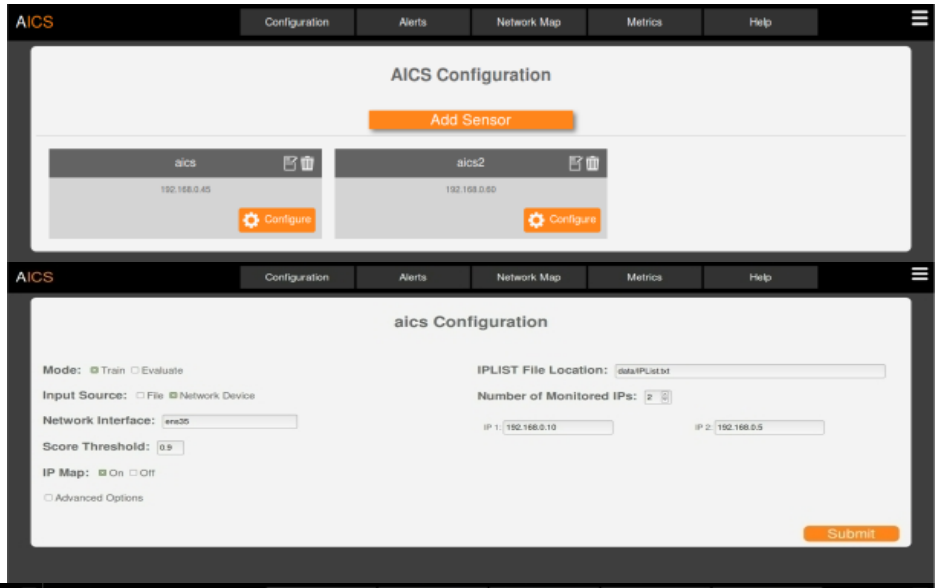
NIDS#1: Nozomi

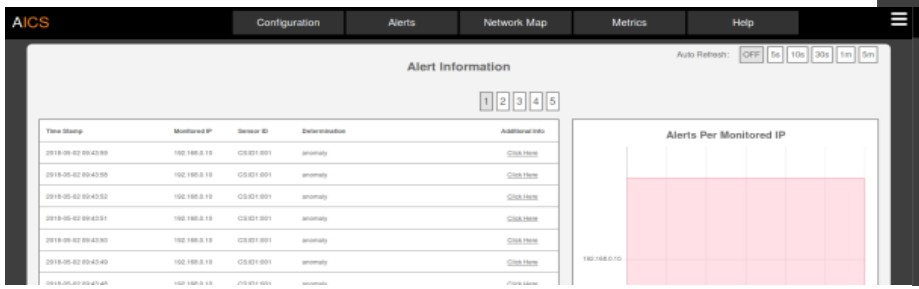
- Guardian – Industrial strength OT and IoT Intrusion Detection
- IDS modes
  - Machine learning mode
  - Protection Mode
- Elk Connection
  - Json File
  - SysLog
- Configuration
  - Data forwarding
  - System Setup
  - Licensing
- GUI
  - Shows snap shots
    - Alerts
    - Traffic
    - Assets
    - Environment information

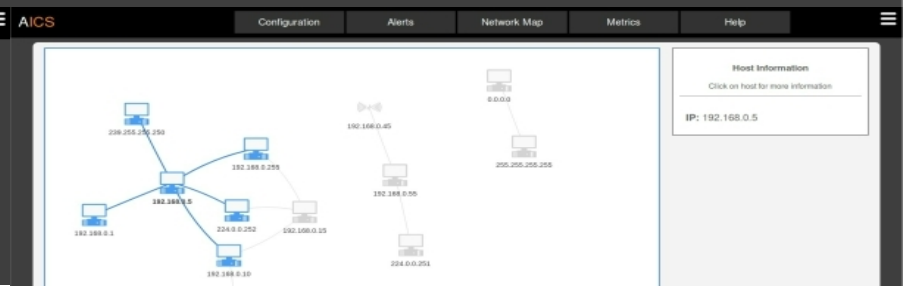


NIDS#2: Autonomic Intelligent Cyber Sensor (AICS)

- **Easily configurable**
  - Control files
  - Hosts to monitor
  - Logs to send to Elk
- **IDS Modes**
  - Machine learning
  - Protecting
- **Monitors**
  - OT & IT systems
- **Developed at the INL**
- **Commercialized by Trust Automation**

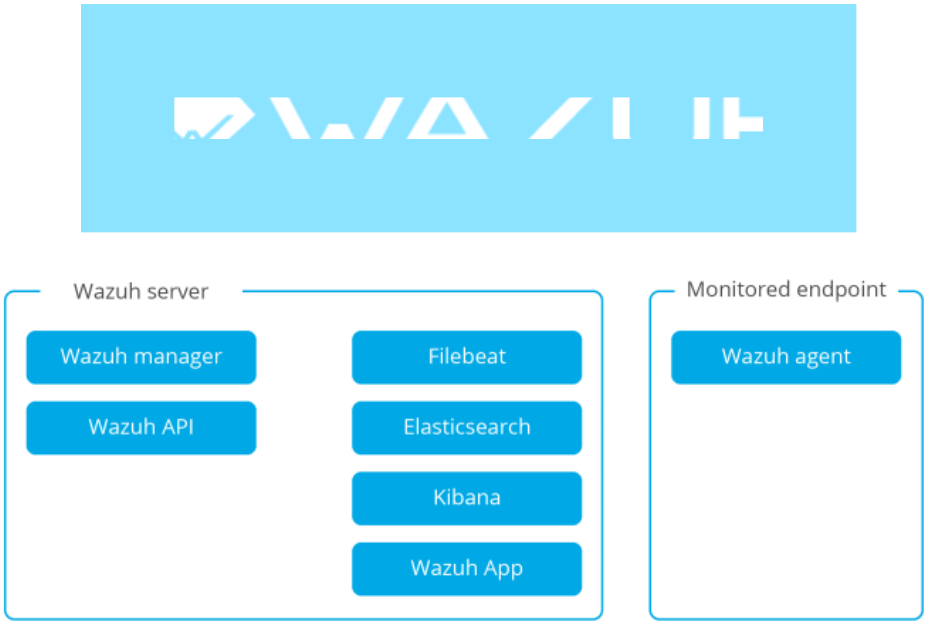






HIDS#1: Wazuh

- Security Analytics
- Intrusion Detection
- Log Data Analysis
- File Integrity Monitoring
- Vulnerability Detection
- Configuration Assessment
- Incident Response
- Regulatory Compliance



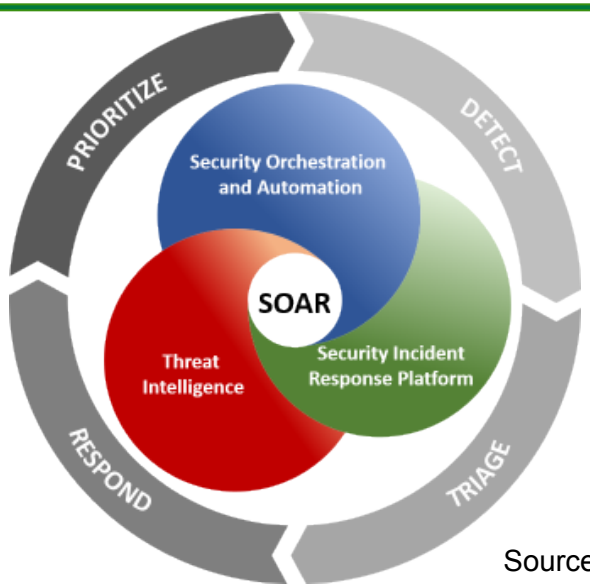
- Agent must be installed on machine it is monitoring
- Wazuh uses (requires) filebeat, elasticsearch and kibana
- Server can be split into manager portion and database portion if desired
- Open source and based/forked from OSSEC.
  - Whereas OSSEC is a small single application, Wazuh adds a database and front end to be able to parse raw alert and logs into meaningful data providing the full SIEM

HIDS#2: OSSEC

- Worlds most widely used host intrusion detection system
- Open source, lightweight
- Log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response.
- It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows.
- Uses secure connection to server to forward messages
- Active response system allows for running of commands on host
- Generally, all alerts and data are forwarded to a server where they are logged
- Will run integrity and other checks and create report of any security issue it finds on the host

SOAR: Orchestrator

- System Orchestration, Automation and Response
- Interfaces with SIEM data and evaluation analytics
  - Provides evidence/confidence
- Integrates playbooks
  - Defined steps for evaluation of evidence
  - Defined, appropriate responses
- Reduces time from alert to response
- DeMisto/XSOAR is one implementation



Source44.net

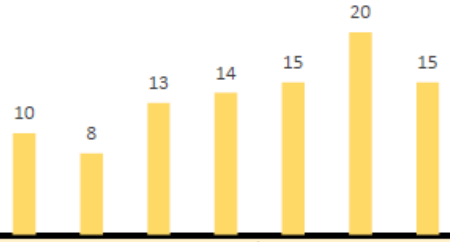
thesoftwarereport.com

Cybersecurity Surveys: What security products are out there?

- **Goal: determine what tools exist on the market and what tools are currently deployed on wind systems, PV systems, and EV charger networks.**
- **Five Questionnaires**
  - One for cybersecurity vendors, wind asset owners and operators, wind original equipment manufacturers, PV service providers/operators, EV charging network operators.
  - Asked about their experience with:
    - Industrial Control System Encryption
    - Access control or role-based access control (RBAC)
    - Security Information and Event Management (SIEM)
    - Network-based Intrusion Detection System (NIDS)
    - Host-based Intrusion Detection System (HIDS)
    - Security Orchestration, Automation, and Response (SOAR)
- **Initial Survey and Summary Completed in Q2**
- **Sharing of Appropriate Information for Community Benefit in Q3**
- **Follow-on in-person workshop could be planned for Fall 2021**

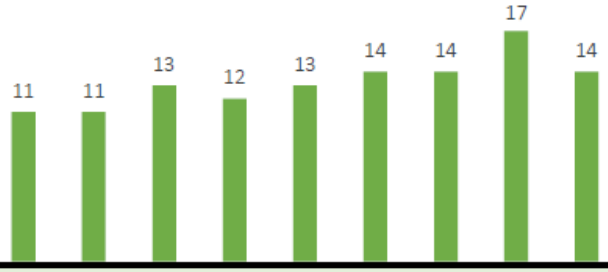
- **Please enter your information!**
  - **Wind OEM:** https://inlhrfedramp.gov1.qualtrics.com/jfe/form/SV_aYwJmf6pYssa99P
  - **Owners/Operators:** https://inlhrfedramp.gov1.qualtrics.com/jfe/form/SV_72MuS6S8psMDHbn

Example Results – Access Control



Company	Solar	Wind	Electric Vehicles	Length of time on the market	Access Control Features						
					Check for multiple logins with the same credentials	Check for default passwords	Protect data egress	Custom API for development/application	Monitor unauthorized access	Control local and remote user access to networks and devices	Other
Bivio Networks, Inc.	X	X		5 years	X		X	X	X	X	X
Claroty	X	X		5+ years						X	
Dragos	X	X		5 years				X	X	X	X
Dragos	X	X		5				X	X	X	X
Fend Incorporated	X	X	X	1 year			X				X
Fend Incorporated	X	X	X	8 Months			X			X	X
HP Inc.	X	X	X	81 years							X
InZero Technologi	X	X	X	3-6 months			X	X		X	X
Mantis Networks	X	X	X	12 months					X		X
Optiv Federal	X	X	X	10 years+	X	X	X	X	X	X	X
Owl Cyber Defense	X	X	X	Ten to Twenty Years	X	X	X			X	
Owl Cyber Defense	X	X	X	1 Year		X	X			X	
Qubitekk	X	X	X	6 months			X			X	X
R&K Cyber Solutions LLC	X	X	X	5months					X	X	
SecureFLO	X	X	X	10	X			X	X	X	
SNC	X	X	X	6 years			X	X	X		X
Templar Shield	X	X		15 years				X		X	X
Templar Shield	X	X		15 years	X	X	X	X	X	X	
Templar Shield	X	X		10 years	X	X	X	X	X	X	
Templar Shield	X	X		10 Years	X	X		X	X	X	
Verve Industrial Protection	X	X		5+ years	X	X		X	X	X	X
Xage Security	X	X		3 years	X	X	X	X	X	X	X
Itron Inc.	X		X	10+			X		X	X	
Verica			X	2+ years	X			X	X	X	X

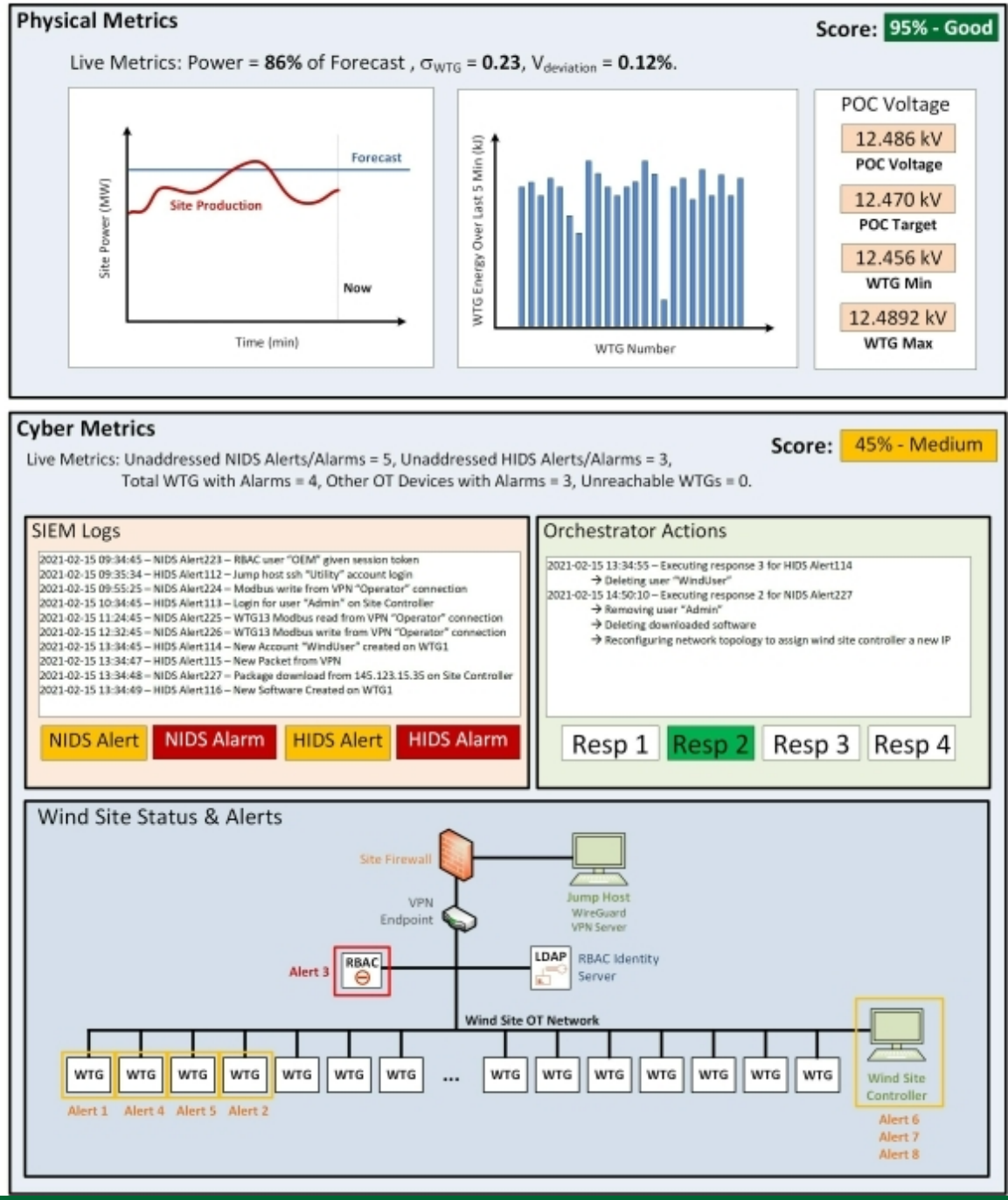
Example Results – SIEM



Company	Solar	Wind	Electric Vehicles	Length of time on the market	SIEM Features								
					Visualize networks and devices	Recommend courses of action	Automatic categorization	Web-based interface	Decision support	Centralized analysis	External timing for log stamps	Information sharing	Other
Bivio Networks, Inc.	X	X		5 years	X	X	X	X	X	X	X	X	X
Dragos	X	X		5			X					X	X
Dragos	X	X		5 years		X						X	X
HP Inc.	X	X	X	81 years									X
InZero Technologi	X	X	X	3-6 months			X	X	X	X		X	X
Mantis Networks	X	X	X	12 months							X	X	X
New Context	X	X		Still in R&D	X	X	X	X	X	X	X	X	X
Optiv Federal	X	X	X	10 years+	X	X	X	X	X	X	X	X	X
Owl Cyber Defense	X	X	X	10-20 years					X	X	X	X	
Owl Cyber Defense	X	X	X	1 Year							X	X	
SecureFLO	X	X	X	10	X	X	X	X	X	X	X	X	
Splunk	X	X	X	12 years	X	X	X	X	X	X	X	X	X
Templar Shield	X	X		15 years	X	X	X	X	X	X	X	X	
Templar Shield	X	X		10 Years	X	X	X	X	X	X	X	X	
Verve Industrial Protection	X	X		5+ years	X		X	X	X	X	X		X
Waterleaf International LLC	X	X	X	1 year	X	X	X	X	X	X	X	X	X
Elastic			X	2012	X	X	X	X	X	X	X	X	
Tanium	X			10+ years						X		X	X
Verica			X	2+ years									X
Waterleaf International	X			4 months	X	X	X	X	X	X	X	X	X

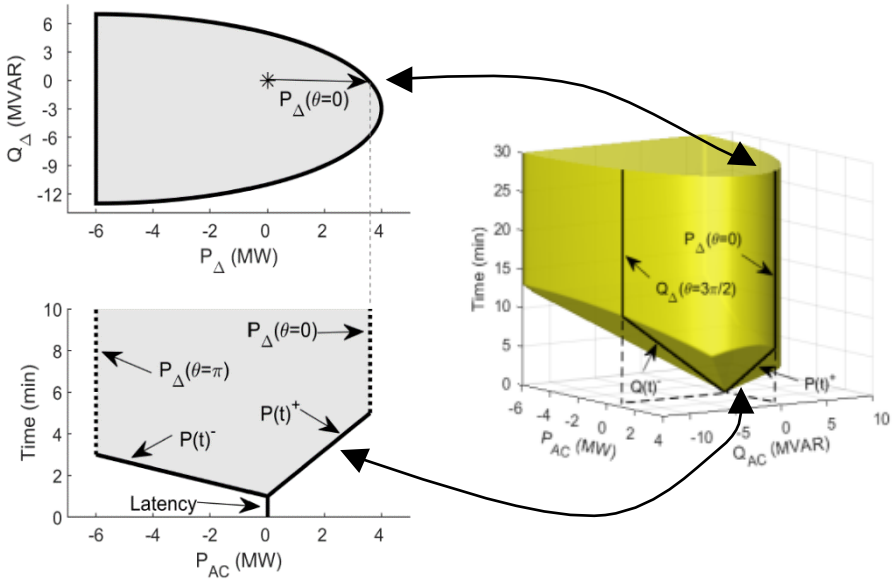
Metrics

- How do we quantify the cybersecurity performance for each of the topologies?
- We've been working on creating dashboards that capture the cyber and physical performance of the system
- Can compare the results for each of the topologies during and after the automated cybersecurity attacks to determine the "score"
- Provides a novel prototype on a security operations center (SOC) that would be hosted by both cyber defenders and physical domain experts
- Based on this "big picture" information, responses can be orchestrated through SOAR and human-in-the-loop responses.

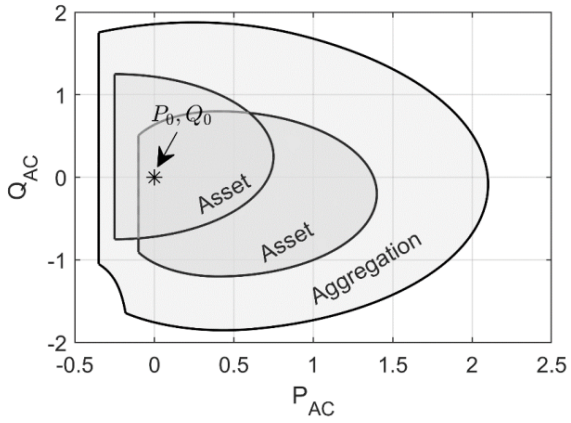


Real Time Power System Resilience Metric

- **Operational metric based on assets adaptive capacity**
- **Captures generation limit and operating points**
- **Includes temporal constraints**
  - Latency, ramp rates, energy limits



- System resilience is based on aggregation of the system assets
- Aggregation from operating point at all power factor angles
- Defines the limits of the system with temporal constraints



Scripted attacks will produce consistent results for each topology

MITRE ATT&CK for ICS (https://collaborate.mitre.org/attackics/) is a community-sourced framework for identifying malicious threat behaviors, specifically the tactics and techniques of the adversaries in industrial control systems (ICS). Our techniques include the following:

- T0841 - Recon (nmap scan, etc.)
- T0831 - Modbus active/reactive power holding register adjustments
- T0866 - Eternal Blue attack on Wind Site Controller – assume the wind site controller is a windows box, can gain admin shell
- T0812/T0859 - Windows SMB/RDP check and brute forces password
- T0812/T0859 - SSH brute force – Linux machines (WTGs?) on network
- T0812/T0859 - Telnet brute force
- T0814 - DOS hping3 attack – ICMP noise

INITIAL ACCESS	EXECUTION	PERSISTENCE	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Creating adversary scenarios: Threats, tactics, techniques and procedures

- We assume the adversaries:
  - Are “Remote” and have Operational Technology (OT) presence on the O/O system and can access the VPN connection, or
  - Are “Local” and have access to a wind turbine generator (WTG) network switch, wireless network, or onsite controller.

Remote Scenario

Step	Adversary Action	MITRE ATT&CK™ for ICS	Defenses	SOAR Response
0	Phishing attack on Wind OEM company gives attacker access to OEM monitoring system and wind site VPN credentials.	T0865 - Spearphishing Attachment	(Assumed starting place for the attack)	N/A
1	Attacker logs into the wind network with the VPN credentials stolen from the OEM	T0822 - External Remote Services	NIDS detects VPN/jump host access from unexpected IP and posts alert to SIEM	Charge firewall rule to prevent inbound traffic from IP of attacking machine.
2	Reconnaissance (nmap scan, etc.)	T0841 - Network Service Scanning	NIDS detects scan and posts alert to SIEM	Charge firewall rule to prevent inbound traffic from IP of attacking machine.
3	Compromised OEM computer sends adjusts WTG active/reactive power Modbus setpoints through VPNs	T0831 - Manipulation of Contro T0818 - Engineering Workstation Compromise	RBAC will block, NIDS sees unexpected traffic from OEM (if conducting DPI), syslogs report writes from unexpected IP. NIDS and syslog alerts sent to SIEM.	N/A
4	Metasploit Eternal Blue exploit [SMBv1/MS17-010]with Remote Administration Trojan (RAT) payload sent to Wind Site Controller	T0866 - Exploitation of Remote Services	HIDS detects the payload injection and sends alert to SIEM.	Block traffic to/from the Wind Site Controller.
5	Privilage escalation using metasploit to migrate to a PPID operating as NT Authority\SYSTEM	T1055 - Process Injection	N/A	N/A
6	Create new user on Wind Site Controller and change permissions for user to admin on Wind Site Control windows machine	T1136.001 - Creating new local accounts	HIDS alerts SIEM to new user account addition.	Remove user from Wind Site Controller
7	Exfiltrate hashed passwords using memory hashdump (then crack them offline)	T1003 - OS Credential Dumping T1041 - Exfiltration Over C2 Channel	NIDS alerts SIEM to new outbound traffic to unexpected IP.	Firewall updated to block future exfiltration and sever connection to command and control server.
8	Establish persistence on Wind Site Controller (srvany.exe tool installed as a service to permit netcat.exe to run as a service)	T1053 - scheduled task	HIDS alerts SIEM to program modification.	Remove user from Wind Site Controller

Creating adversary scenarios: Threats, tactics, techniques and procedures

- We assume the adversaries:
  - Are “Remote” and have Operational Technology (OT) presence on the O/O system and can access the VPN connection, or
  - Are “Local” and have access to a wind turbine generator (WTG) network switch, wireless network, or onsite controller.

Local Scenario

Step	Adversary Action	MITRE ATT&CK and ATT&CK for ICS	Defenses	SOAR Response
0	Attacker cuts the lock on a wind turbine tower and plugs in their laptop into the network switch.		(Assumed starting place for the attack)	
0	Attacker gets wind site operator to open malicious attachment on the Wind Site Control computer.	T1566.001 - Phishing: Spearphishing Attachment T0863 - User Execution	(Assumed starting place for the attack)	
0	Attacker compromises wireless network to gain access to the OT network.	T0860 - Wireless Compromise	(Assumed starting place for the attack)	
1	Reconnaissance (nmap scan, etc.)	T0841 - Network Service Scanning	NIDS detects scan and posts alert to SIEM	N/A
2	Attacker sends unencrypted Modbus active/reactive power setpoints	T0831 - Manipulation of Control	OT Encryption prevents writes. NIDS sees unexpected (unencrypted) traffic and sends an alert to the SIEM.	Remove attacking machine from network with Open vSwitch reconfiguration.
3	Wind Site Controller (Windows) SMB/RDP password brute force attack	T0812 - Default Credentials T0859 - Valid Accounts	NIDS detects the brute force attack and alerts the SIEM.	Remove attacking machine from network with Open vSwitch reconfiguration.
4	SSH brute force attack on linux-based components in WTGs	T0812 - Default Credentials T0859 - Valid Accounts	NIDS detects the brute force attack and alerts the SIEM.	Block Port 22 traffic, block set of IPs at firewall, or remove attacking machine from network with Open vSwitch reconfiguration.
5	Telnet brute force on WTG PLCs	T0812 - Default Credentials T0859 - Valid Accounts	NIDS detects the brute force attack and alerts the SIEM.	Block port 23 traffic? Remove attacking machine from network with Open vSwitch reconfiguration.
6	DOS attack using hping3 to produce excessive ICMP traffic to WTGs	T0814 - Denial of Service T0826 - Loss of Availability	NIDS detects the ICMP noise and sends alert to SIEM.	Remove attacking machine from network with Open vSwitch reconfiguration.

Automated topology assessments

- **The team is using an INL-developed test harness with Red Canary's Atomic Red Team tool**
- **Test harness is a set of very small, fast virtual machines that are designed to run in the SCEPTRE environment for the purpose of automated testing.**
  - **Test VM Features**
    - Connects all other components together using a simple naming convention
    - Provides a development machine with easy access and several development libraries
      - Including python, web browsers, file sharing, scapi, robot framework and others
    - Centralized location from which to view report and test results
      - Can be viewed over http, smb or scp/ssh
  - **Attack VM Features**
    - A processing daemon for running tests and/or attacks across the entire network
    - Pulls all scripts and automation details from test vm and executes them
    - Includes network scanning and sniffing utilities
    - A docker hypervisor of sorts, can support other docker images
    - Metasploit framework included custom compiled with eternal blue

Future Work

- Team roughly 50% through project.
- Next steps:
  - Complete the virtualized hardening features (including all the IDS training, SOAR playbooks, etc.)
  - Finalize metrics for scoring the hardening topologies
  - Finalize the automated attack tools
  - Conduct assessments and share results with the community
  - Collate and publish survey results with areas for the wind industry to expand their defense tools

For additional questions, please contact us:

Jay Johnson – jjohns2@sandia.gov

Jake Gentle – jake.gentle@inl.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.