Pacific Northwest
NATIONAL LABORATORY

Cybersecurity: Challenges and Opportunities

January 18, 2023

Mark Rice, Jim Ogle, Chris Bonebrake, Chance Younkin, Jereme Haack

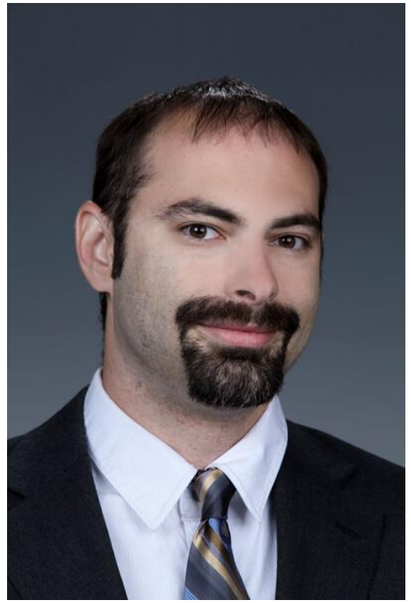
U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

PNNL-SA-181205

Presentation Overview

James Ogle



Chris Bonebrake

Chance Younkin

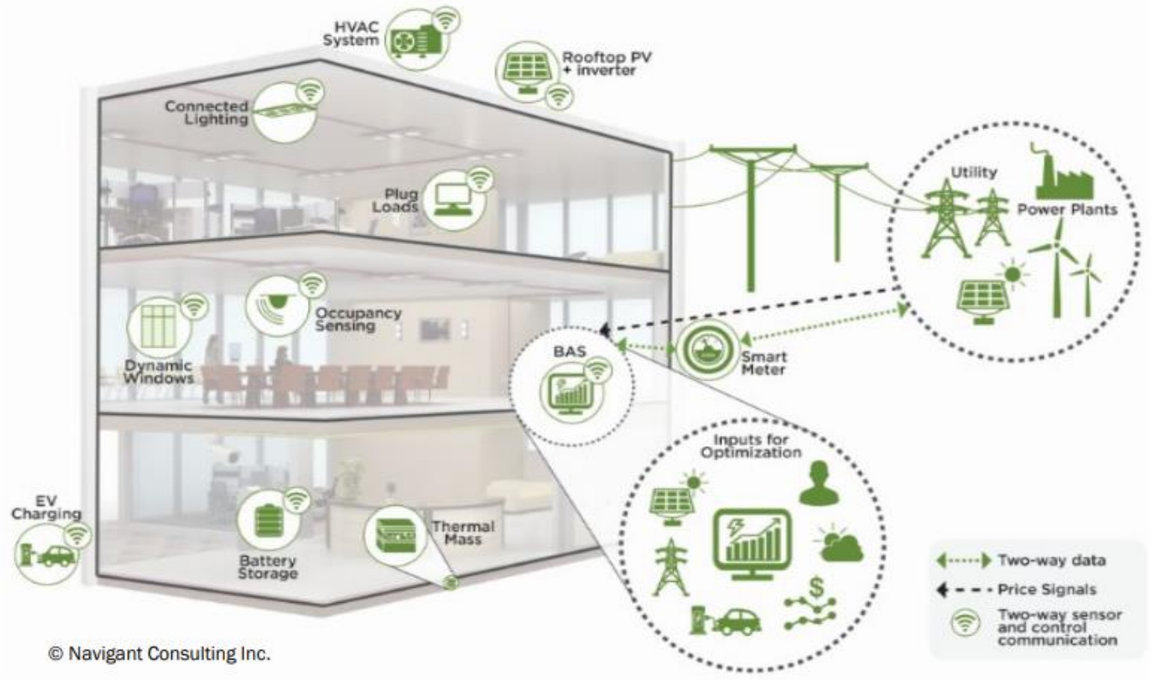
Jereme Haack

Pacific Northwest
NATIONAL LABORATORY

Introduction

Grid Interactive Efficient Buildings (GEB) Vision

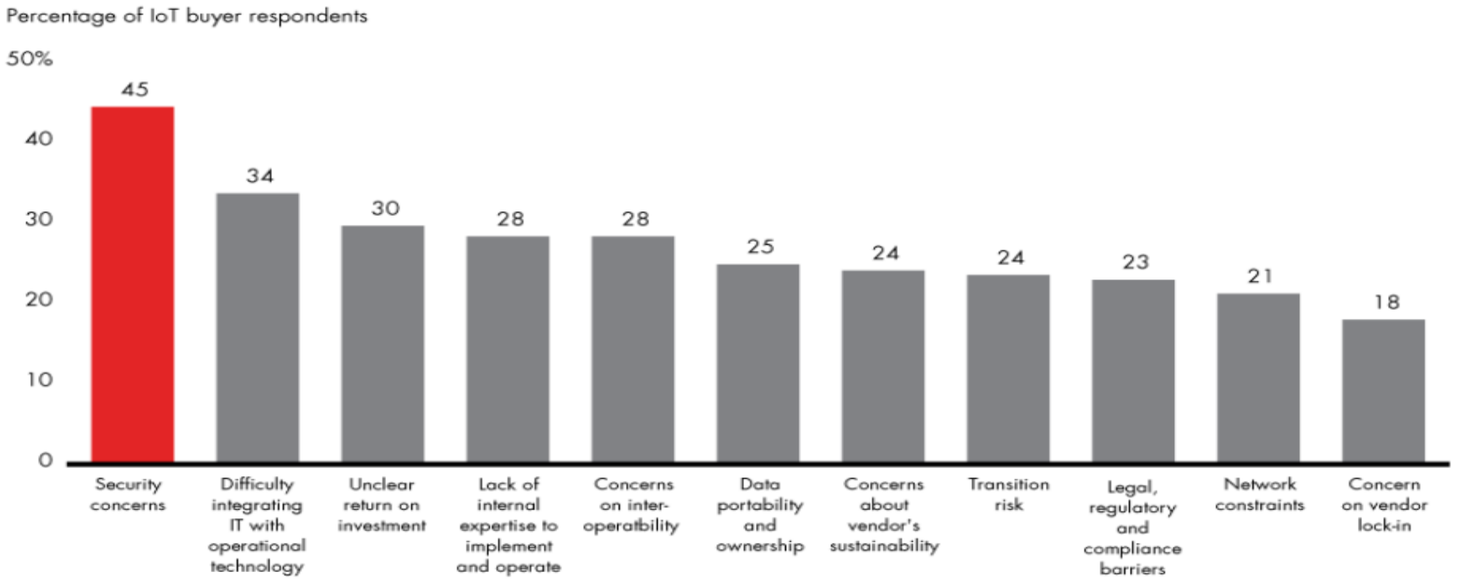
- DOE has established a goal of tripling energy efficiency and demand flexibility in residential and commercial buildings by 2030
- GEBs offer a $100-200B value proposition over the next two decades[1]
- National roadmap cites cybersecurity as a key deployment challenge and research and development need



1. https://gebroadmap.lbl.gov/

Motivation

- Commercial customers cite security as the number one concern in adopting IoT technology
- Cybersecurity reputation and remediation risks could far exceed the benefits in productivity and energy efficiency in smart buildings
- **<u>Cyber resiliency needed to address non-malicious threats as well!</u>**



Source: Bain 2018 IoT customer survey (n=521)

https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things

Current Cybersecurity Posture

- **Sites are not well protected:** Half of the sites assessed by Intelligent Buildings had devices directly exposed to the internet and 95% had no disaster recovery plan or had not changed default configurations and ports[1].
- **Practitioners do not know how to prioritize:** A survey of over 300 practitioners showed that "*23 BACS vulnerabilities were [considered] to be equally critical with limited variance. Mitigation strategies were no better, with respondents indicating poor threat diagnosis*." This was in contrast to security professionals who showed an ability to differentiate and prioritize vulnerabilities and mitigation strategies[2].
- **Buildings are being targeted:** Analysis of 40,000 servers used by building automation servers showed that 37.8% of these computers had been targeted by a mix of malware, phishing scams and ransomware[3]. *"The majority of threats came from the internet … with 26% of infection attempts being web-born".*

1. http://automatedbuildings.com/news/apr19/articles/ib/190318022808ib.html
2. Brooks, D. J. , et al. "Intelligent building systems: security and facility professionals' understanding of system threats, vulnerabilities and mitigation practice" ISSN: 0955-1662 , 1743-4645;
3. https://memoori.com/37-8-of-smart-building-automation-systems-were-attacked-in-h1-2019-kaspersky-reports/

Cybersecurity IS risk management

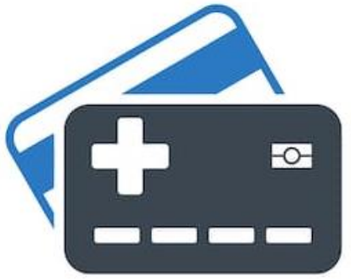
Best Practices

Hygiene

Response Protocols

First Responders

Subject Matter Experts



Risk Underwriters

People

Processes

Technology

NIST Cybersecurity Framework Functions

Recovery:
System functionality returned
Key lessons-learned incorporated

Need to identify:
- Physical and software assets
- Risks and vulnerabilities
- Organizational R&Rs

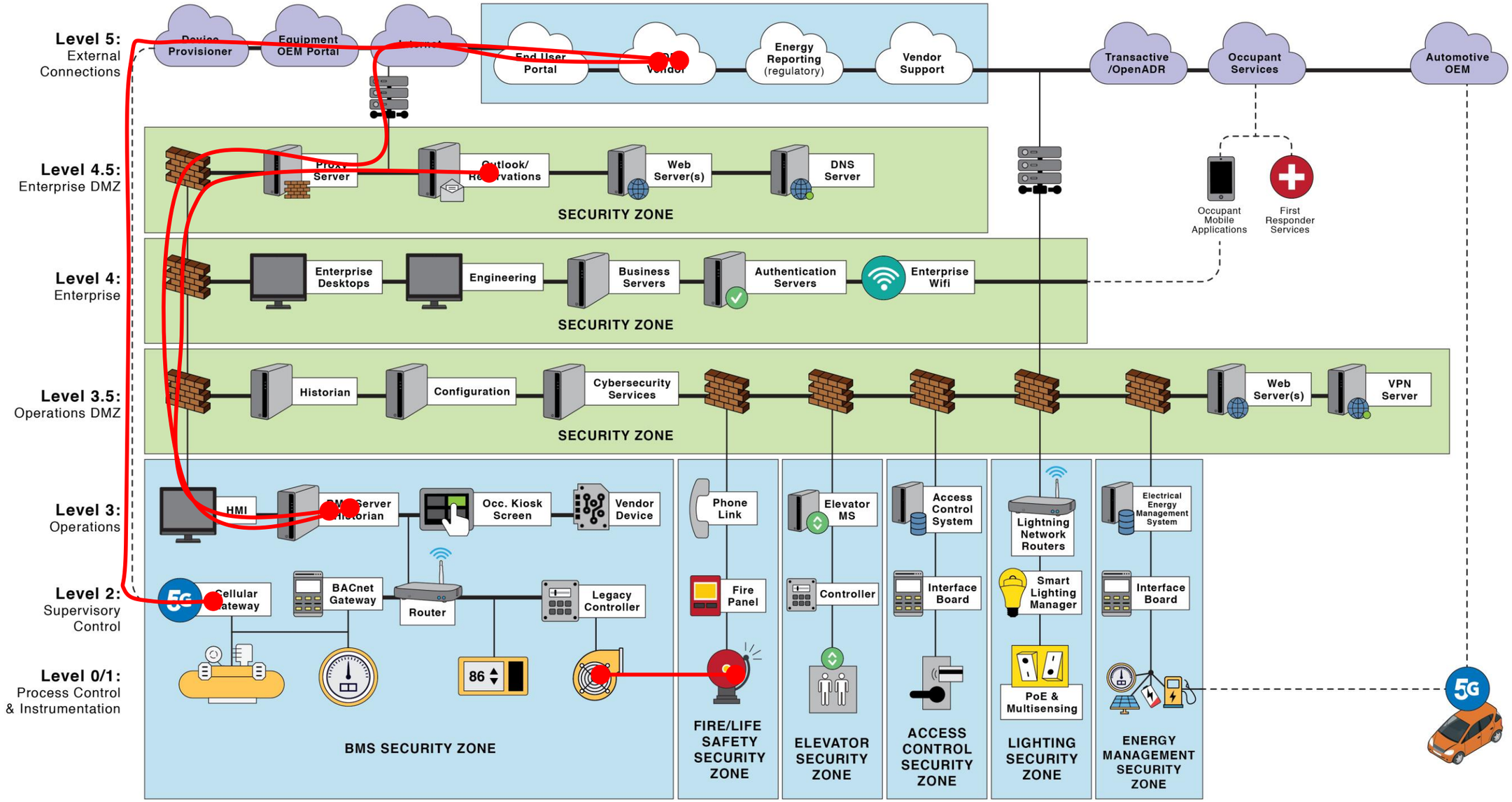
Response plan:
Detected events are reported, contained and mitigated

Protections in place for:
Access control, training, data security, system configuration and maintenance

Detection of:
Anomalous data flows and malicious software for baseline operation

Pacific Northwest
NATIONAL LABORATORY

Abstract Smart Building Reference Architecture



Industry Resources and Activities

- **RealComm**: Real Estate Cyber Consortium (RECC) has developed best practices for OT security, vendor sourcing, and contract language.
- **BOMA**: Has developed self-assessment checklists as a function of site risks.
- **CABA**: Published whitepapers on preventing vulnerabilities as well as reviewing potential IoT cybersecurity standards
- **ASHRAE**: has developed BACnet Secure Connect and promoted increased understanding of smart building cybersecurity issues through seminars and ASHRAE Journal articles
- **RE-ISAC:** The Real Estate Information Sharing and Analysis Center Group (RE-ISAC)
- **NEMA:** The National Electrical Manufacturers Association (NEMA) plans to roll-out a building system cybersecurity certification program.

Pacific Northwest
NATIONAL LABORATORY

Challenges, Gaps, and Strategic Needs

Deployment Challenges and Barriers

1. Cybersecurity value proposition is hard to quantify
2. Cybersecurity must address a variety of requirements
3. Legacy systems present unique challenges
4. Workforce and end-user education and training
5. Validation: how to test components and commission and certify systems?

Pacific Northwest
NATIONAL LABORATORY

Key Recommendations

1. Curation and development of **tailored cybersecurity resources and tools** for the building community

2. Continued **education and engagement of the building community** to establish clear expectations, roles, and responsibilities

3. The continued research and development in tools and technologies to increase cybersecurity, particularly when it comes to the **detection and response/recovery to attacks**

Pacific Northwest
NATIONAL LABORATORY

DOE/PNNL Initiatives and Resources

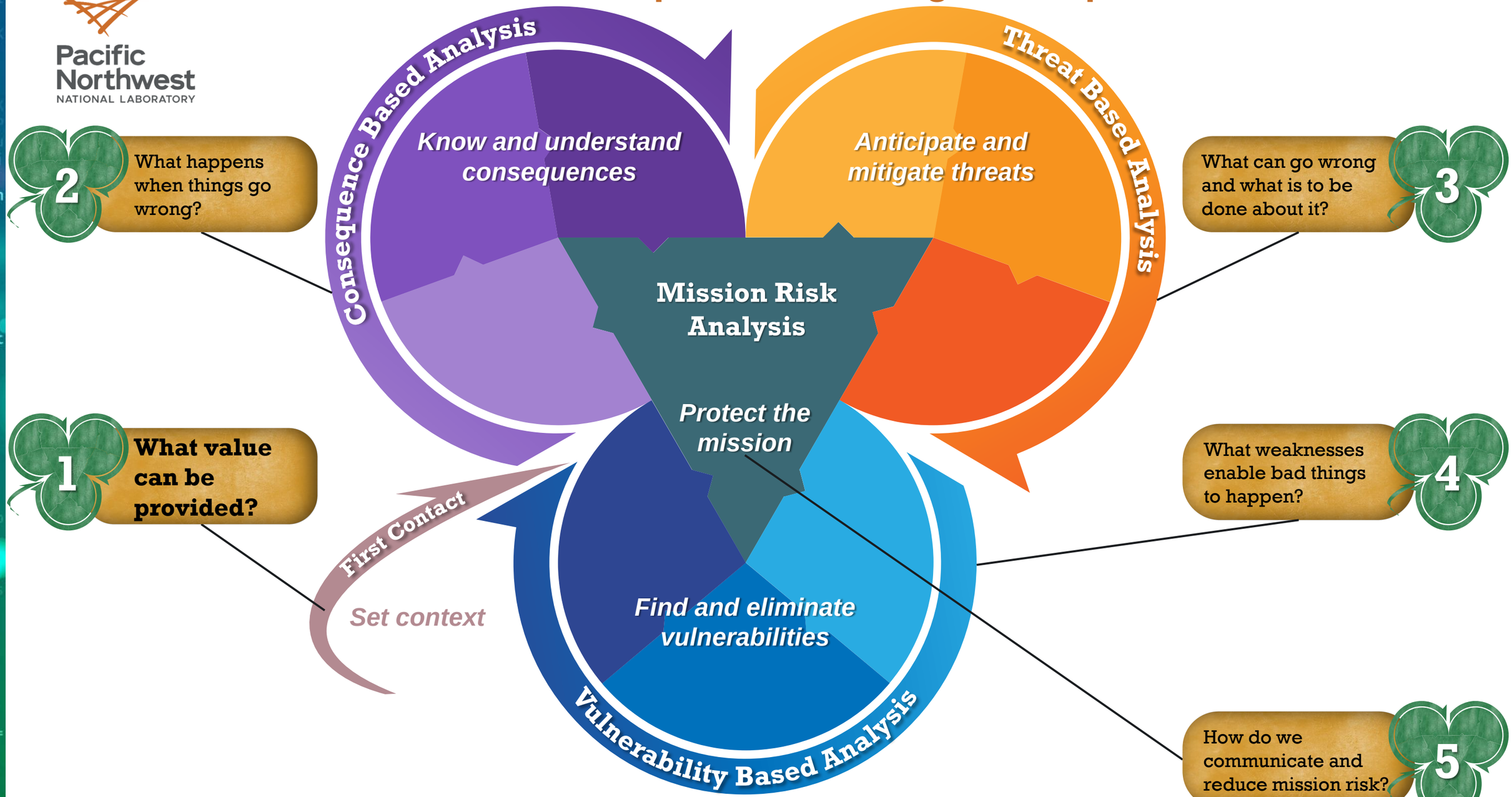
Stakeholder Engagement and Assessments

- DOE and national labs have engaged commercial building stakeholders to define key cybersecurity needs and priorities[1]
- PNNL has identified the building cybersecurity landscape, reference architectures, relevant organizations, and resources[2]
- With UL, evaluated access control protections on lighting systems[3]. Developed facility and lighting system factsheets[4-5]

1. https://buildings.lbl.gov/sites/default/files/Cyber%20Roundtable%20Summary%20Report%202019%2011%2019%20%282%29.pdf
2. https://www.energy.gov/sites/default/files/2021-04/bto-pnnl-29813-securing-buildings-cyber-threats-040821.pdf
3. https://www.energy.gov/sites/prod/files/2020/04/f73/ssl-cls-authentication-vulnerability-mar2020.pdf
4. https://www.energy.gov/sites/prod/files/2018/01/f46/cyber_securing_facilities.pdf
5. https://www.energy.gov/sites/prod/files/2018/06/f52/cyber_security_lighting.pdf

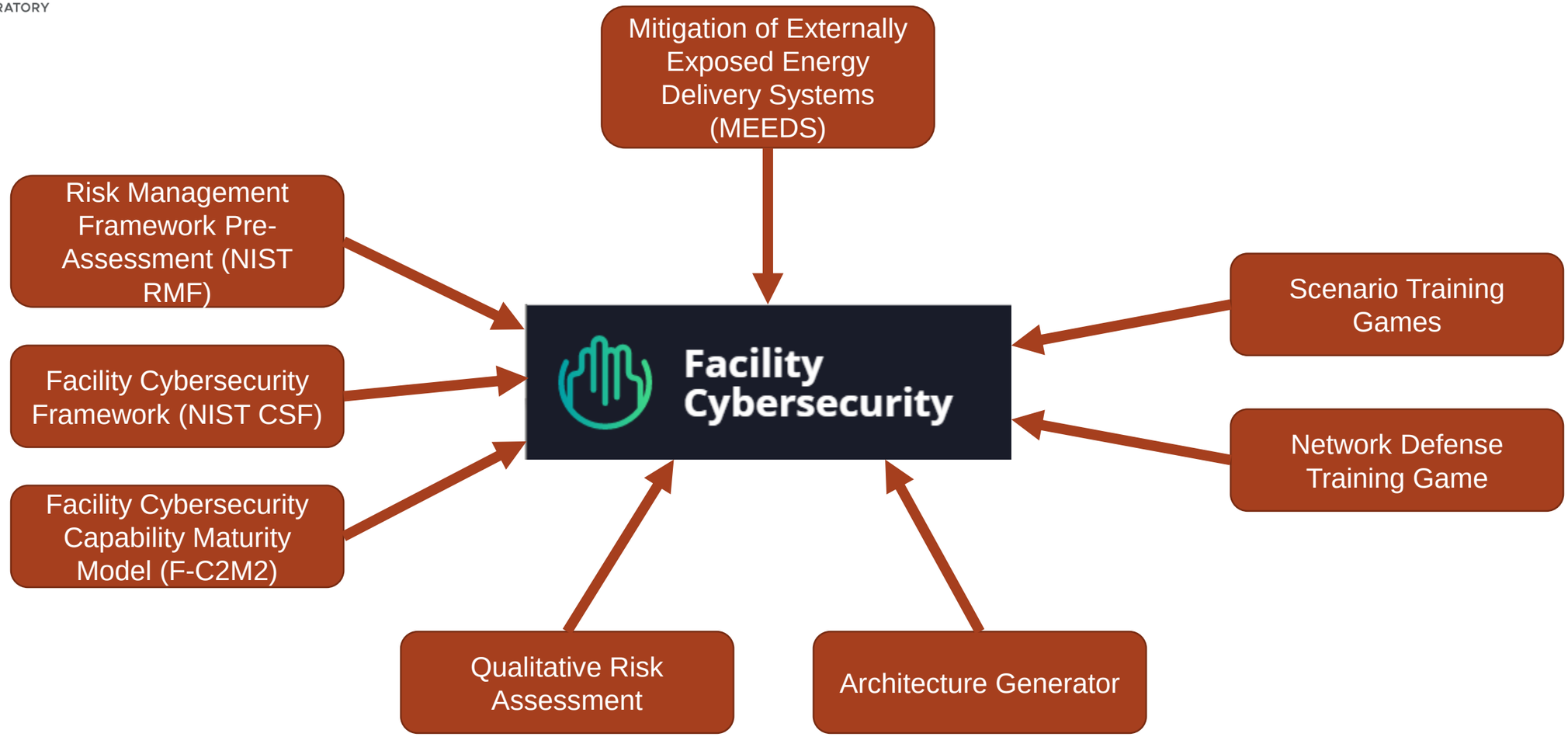
The Shamrock concepts – answering basic questions

Pacific Northwest NATIONAL LABORATORY



Breaking down the Shamrock Cyber concepts…

Pacific Northwest
NATIONAL LABORATORY



PNNL Energy Cyber Security at a Glance

NIST Cyber Security Framework Perspective

PNNL supports DOE with:

- Information Sharing/ Situational Awareness
- Best Practices
- Research

IDENTIFY

- Cybersecurity Plans
- Procurement Language
- Cyber Capability Maturity Models
- Maturity Model Assessment Tools
- NIST Cybersecurity Framework
- Risk Reduction

- Internet Scanning for Exposed ICS

PROTECT

- Distributed Sensors
- Secure Serial
- Cyber Security Manager
- GPS Security
- Utility Security Roles / Certifications
- IEC 61850 Cybersecurity Acceleration
- Facilitate Secure ICCP
- Secure Coding
- Load Drop Security Study
- Secure Protocol Integration
- Substation Secure Switching
- Secure MicroGrids
- Secure Multipeak Toolkit
- Situational Awareness

- Block Chain, Software Defined NW

RECOVER

- OT Forensics

- Collaboration

RESPOND

- NERC E-ISAC GridEx
- Federated Modeling
- LiveWall Video Conferencing
- Emergency Response Tools

- Universal Utility Data Exchange

DETECT

- Cybersecurity for EMS Decision Support
- Supply Chain
- Cybersecurity Information Sharing
- Traffic Visualization
- Traffic based Analytics
- Sensor Fusion

- Continuous OT Scanning

Advanced Distribution System Operations and Secure Communications

Pacific Northwest NATIONAL LABORATORY

Related PNNL Efforts

Grid Architecture Transformation
Methods, tools, and references to view and analyze complex intertwined electrical, cyber, industry structures

Resilient Distribution Systems
Distributed architecture and controls to coordinate response to natural or cyber threats

Sensor Data Anomaly Detection
AI/ML and model-based methods to detect suspect operational data and quantify data confidence

Secure Grid Data Assurance
Standardized Secure SCADA Communication, Universal Utility Data Exchange for secure comms between entities

Software Defined Networking for Grid Operations
Robust and flexible grid-aware communications for secure networks

Greater Uncertainty

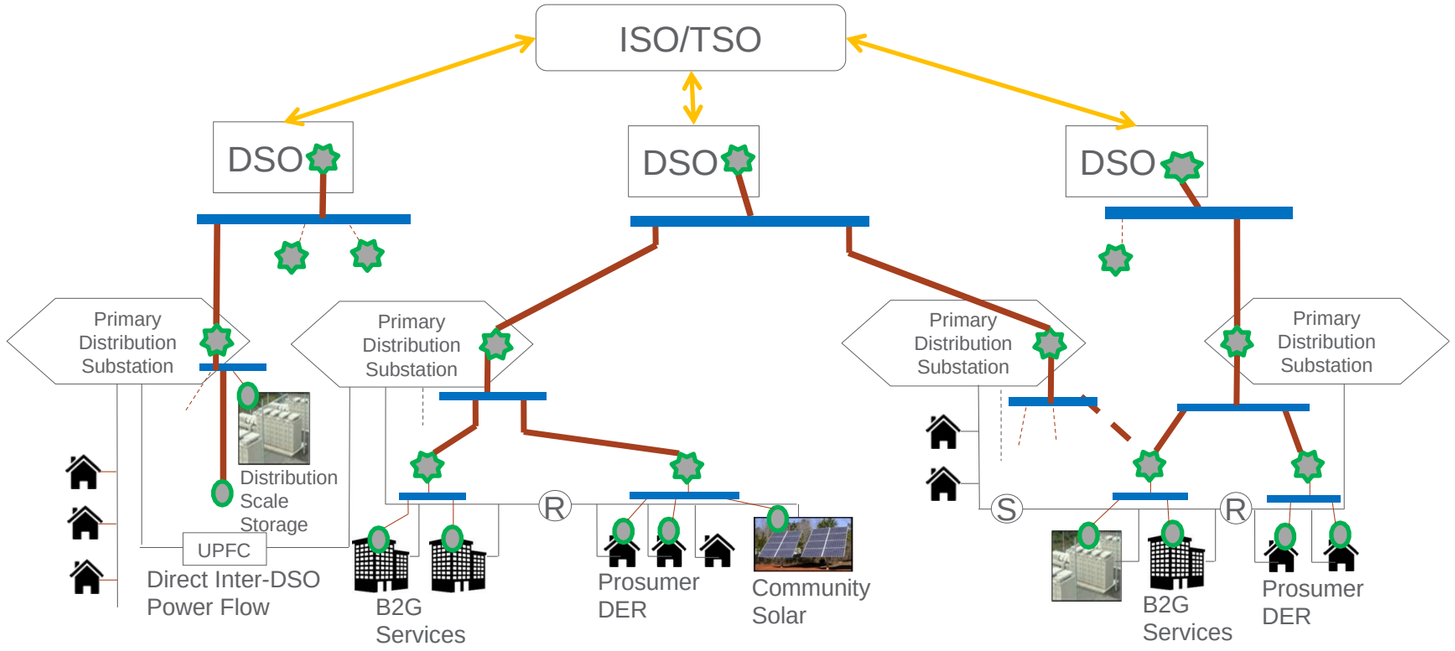
Variable, renewable energy resources
Transportation electrification

More Threats

More frequent natural threats
Cyber-Physical Security threats

Increasing Scale

Distributed energy resources with non-utility owners
Fast-acting power electronics



Control and coordination approaches evolving

More Information: https://gridarchitecture.pnnl.gov/

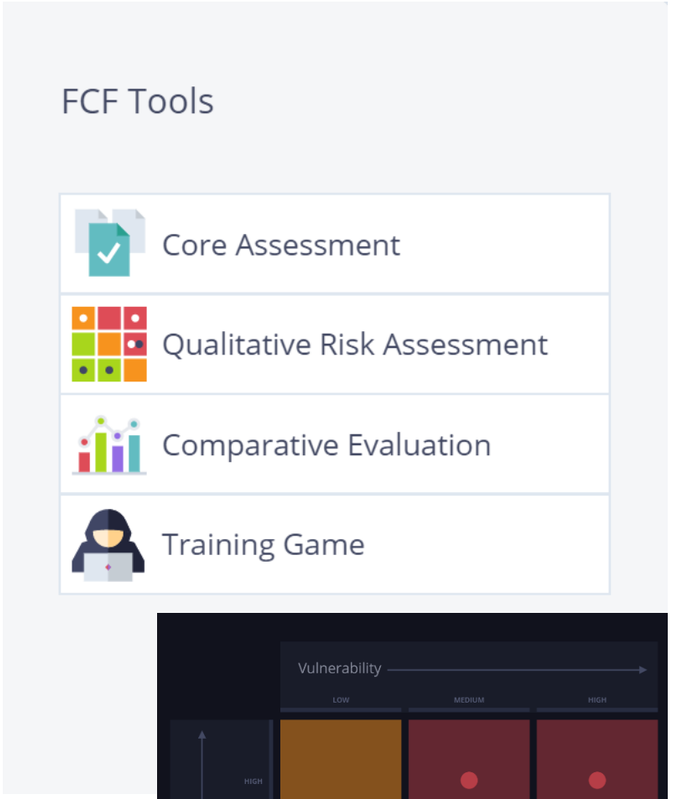
Pacific Northwest
NATIONAL LABORATORY

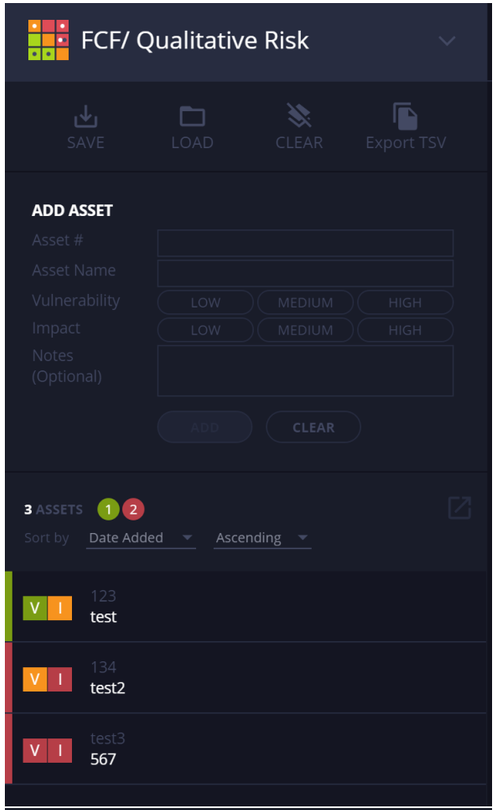
Thank you

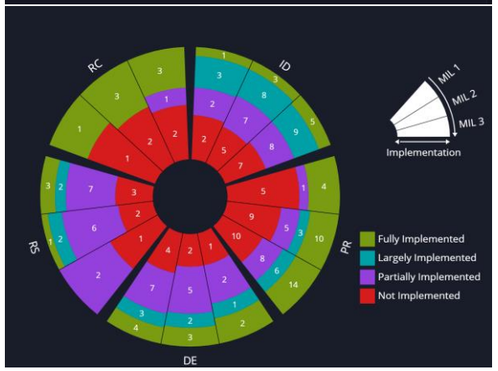
Facility Cybersecurity Framework (FCF)

FCF provides a set of **voluntary, risk-based, standards and best practices** to help facility owners and operators better manage cybersecurity risks by:

- Describing their current posture
- Describing their current target state
- Identifying and prioritize improvement opportunities
- Assessing progress towards the target state



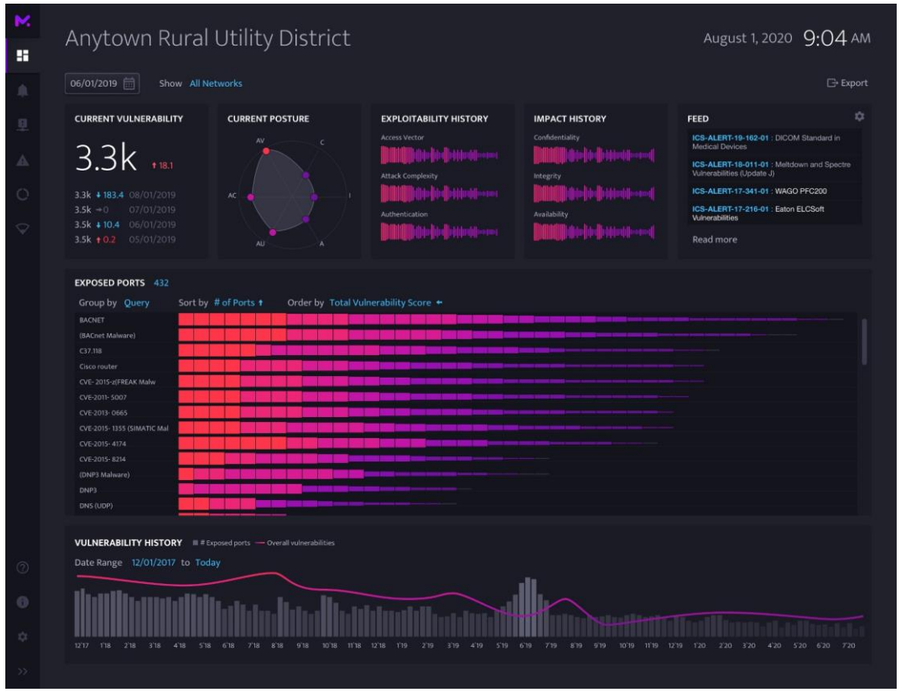


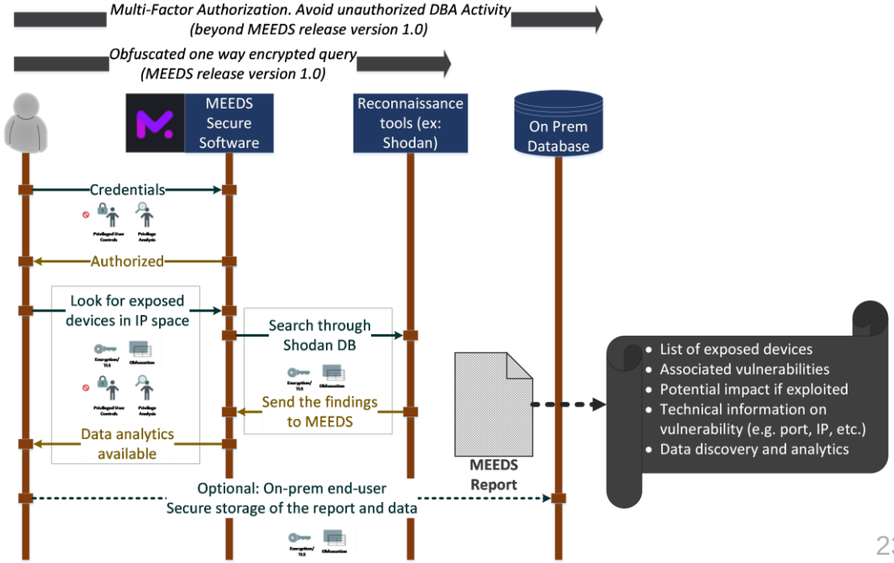


https://facilitycyber.labworks.org/

Mitigation of External Exposure of Energy Delivery System (MEEDS)

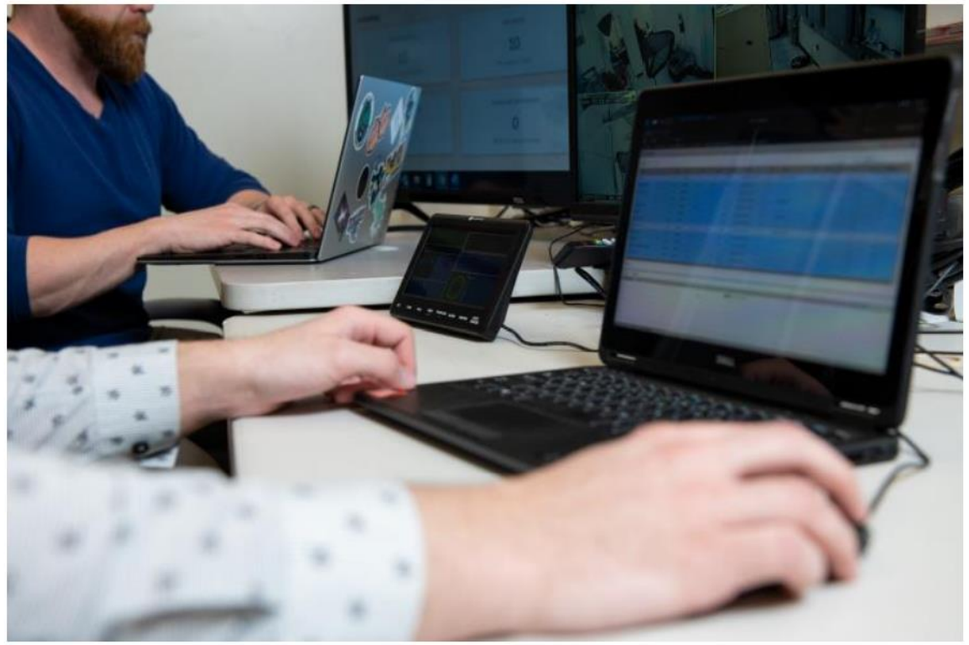
- Initially funded by CEDS. FEMP funding additional data sources and building specific queries
- MEEDS is an easy-to-use tool that identifies, detects, and mitigates vulnerable devices that are inadvertently exposed to the public internet
- MEEDS uses web spider databases such as Shodan that gathers information about critical systems exposed to the internet





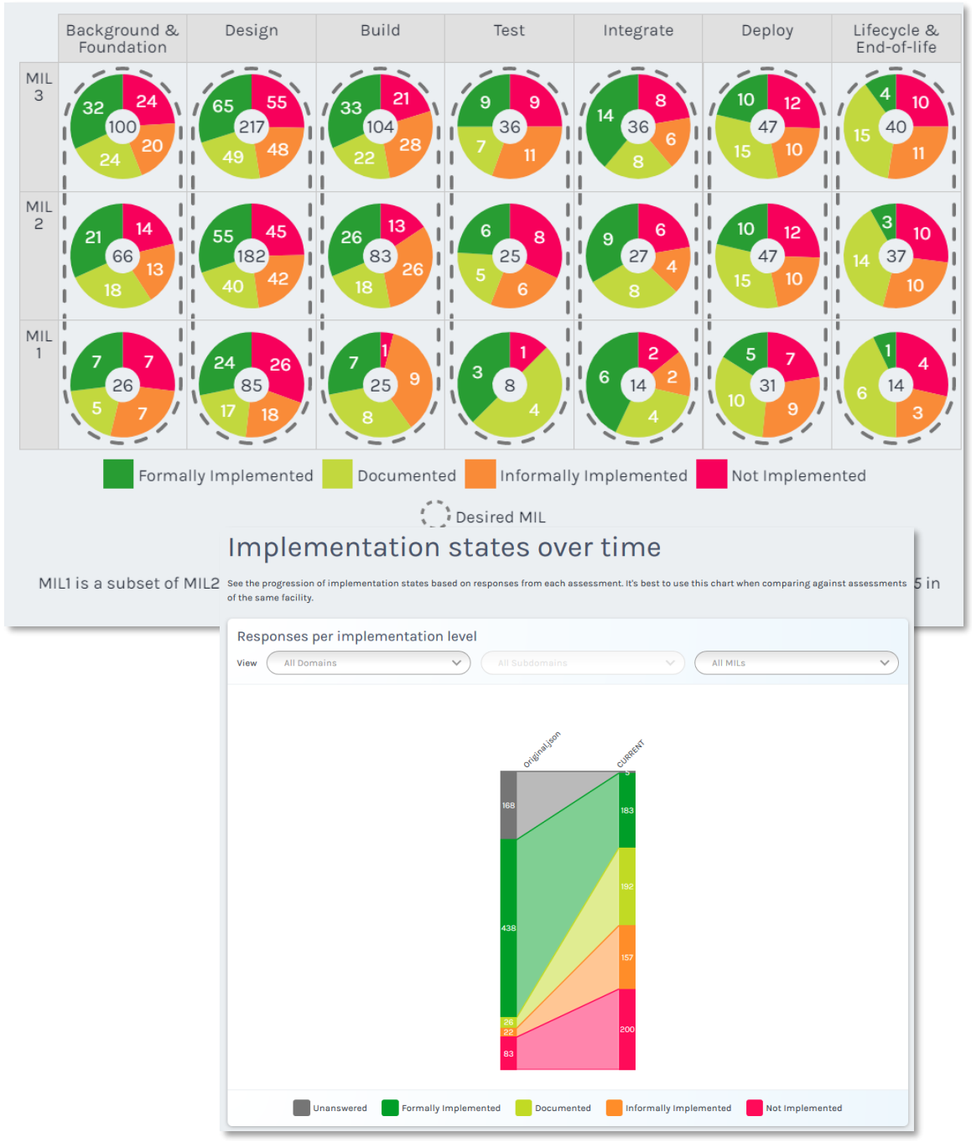
IoT Lab

- To address IoT/IIoT security, PNNL established the Internet-of-things Common Operating Environment (IoTCOE). The IoTCOE is a facility designed for IoT device testing that focuses on providing research and operations capability to both government and private organizations by collecting, producing, and analyzing device and network data.
  - Device-level behavioral analysis
  - IoT communications
  - Cybersecurity + Data Science
  - IoT/IIoT data analytics
  - IoT/IIoT device testing and evaluation



Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2)

- SD2-C2M2 provides an easy-to-use tool that facilitates the adoption of cybersecurity in the design and deployment process
- This tool helps to improve security in the design and development procedures used by vendors for critical systems in U.S. critical energy infrastructure
- Enables tracking of process maturation over time



More information: https://www.pnnl.gov/pnnl-maturity-models

Resource Gap Analysis

- While PNNL assessment tools cover entire NIST framework, building industry resources are primarily focused on ‘identify’ and ‘protect’ domains
- Capability is required to detect intrusions, mitigate attacks, and speed recovery. This aligns well with diagnostics and control disciplines.

	Identify						Protect						Detect			Respond					Recover		
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management	Supply Chain	Access Control	Awareness & Training	Data Security	Information Protection	Maintenance	Protective Technology	Anomalies & Events	Continuous Monitoring	Detection Processes	Response Planning	Communication	Analysis	Mitigation	Improvements	Recovery Planning	Improvements	Communications
FCF	6	5	4	6	3	5	6	5	8	12	2	5	5	8	5	1	5	4	3	2	1	2	3
NIST Man. Profile	12	9	4	8	3	0	17	7	18	26	5	12	10	14	8	1	7	7	4	2	2	2	5
RECC	4	0	1	6	0	10	11	2	6	5	3	2	0	0	0	0	0	0	0	0	0	0	0
BOMA	7	7	7	10	0	1	44	4	2	22	5	11	1	15	2	4	0	0	1	2	0	0	0

Pacific Northwest
NATIONAL LABORATORY

Summary and Conclusions

- Cybersecurity and resilience is critical to enabling the deployment of smart solutions
- PNNL is developing and applying cybersecurity processes and tools to its own R&D
- Providing significant support to federal building operators to assess and mature their posture
- Making tools available for assessing the maturity of operational and development environments