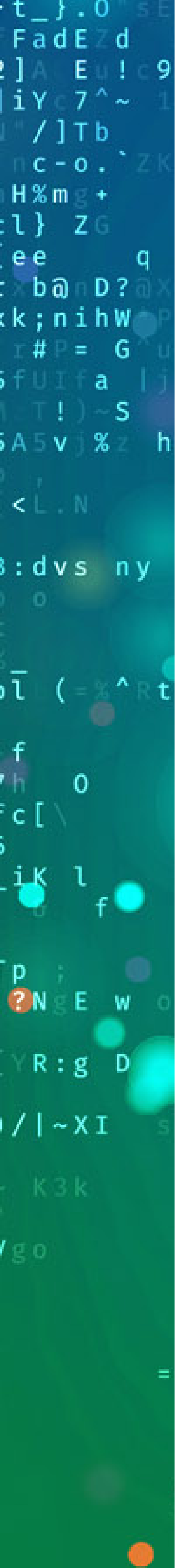


FEMP Facility Related Control System Cyber

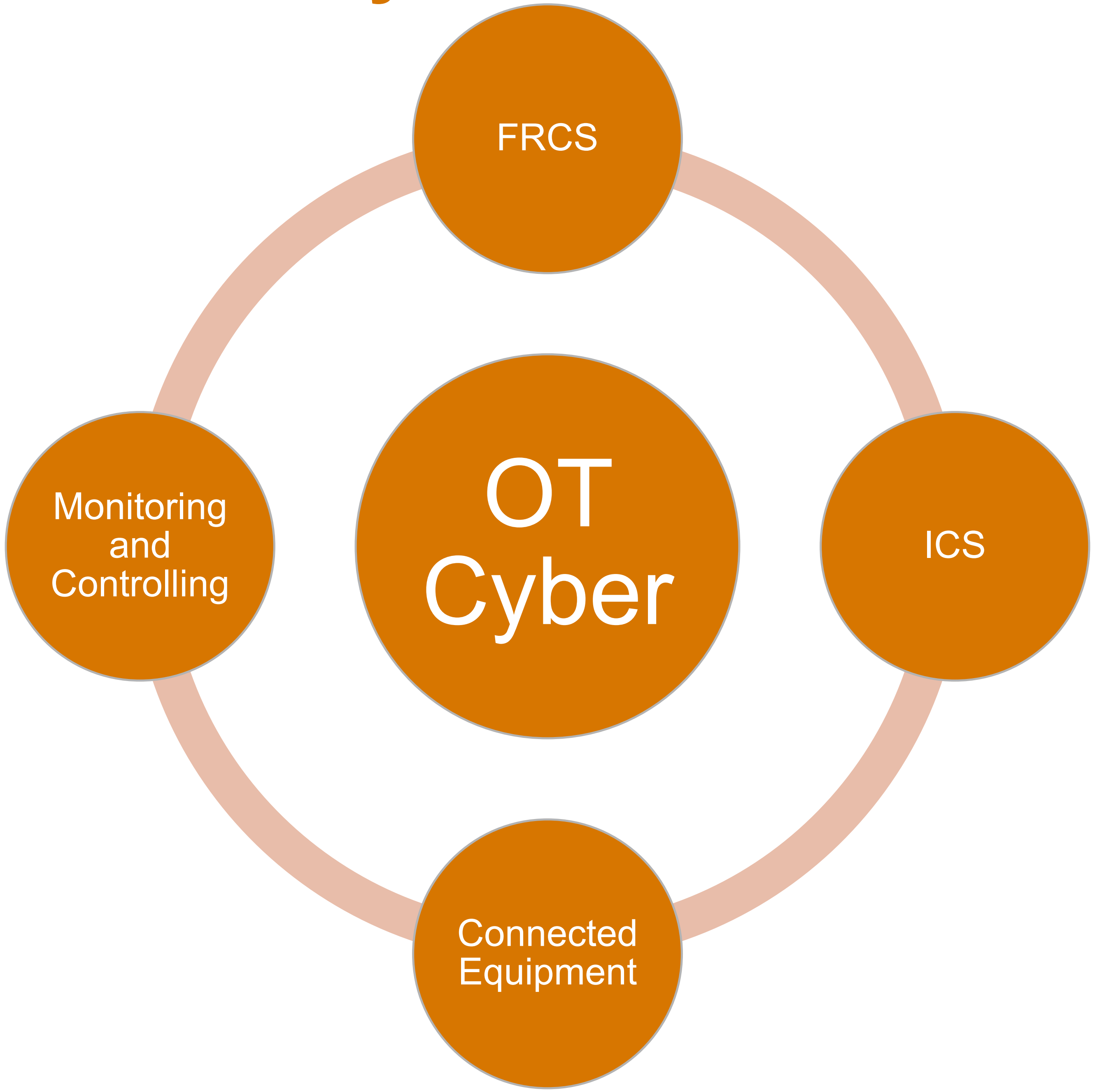
October 22, 2020

Sri Nikhil Gupta Gourisetti, Julia Rotondo
Pacific Northwest National Laboratory

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

What is OT Cybersecurity?

- Operational Technology (OT) directly monitors or controls physical devices, processes or events
  - Frequently incorporate IT components
- Common OT at federal facilities: facility related control systems (FRCS) & industrial control systems (ICS)
- Why is OT Cyber a concern?
  - Traditional IT solutions may not work for OT
  - If compromised, OT technologies could have both cyber and physical impacts



Importance of Facility Related Control Systems Cybersecurity

- Increasingly connected devices and system (IoT)
  - Offer building owners, managers, and occupants increased performance, physical security, productivity, energy management options, and value across a host of products.
  - However, proliferation of these technologies presents new cyber threats and vulnerabilities to buildings and their business and residential occupants.
  - Concern on the seam of operational technology (OT) and informational technology (IT); traditional cybersecurity focused on IT – with more IoT, OT increasingly an attack surface.

- The average amount of time it takes an organization to realize they have been hacked is reported to be more than 180 days

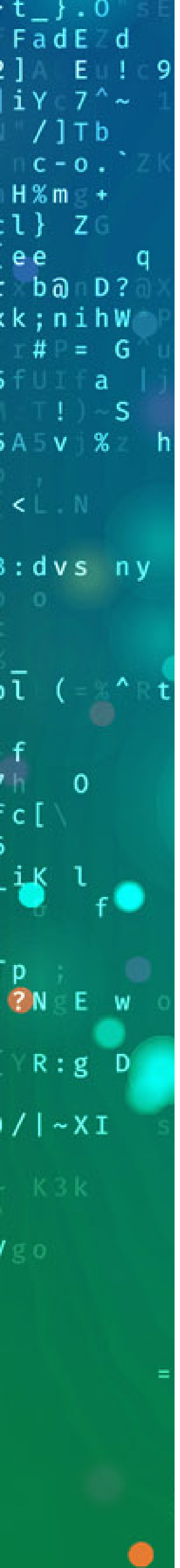
Current Cybersecurity Posture

- **Facilities need to be 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].

- **Buildings are being targeted**: Analysis of 40,000 servers used by building automation systems showed that 37.8% of these computers had been targeted by a mix of malware, phishing scams and ransomware[2]. “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] https://memoori.com/37-8-of-smart-building-automation-systems-were-attacked-in-h1-2019-kaspersky-reports/



Pacific Northwest
NATIONAL LABORATORY

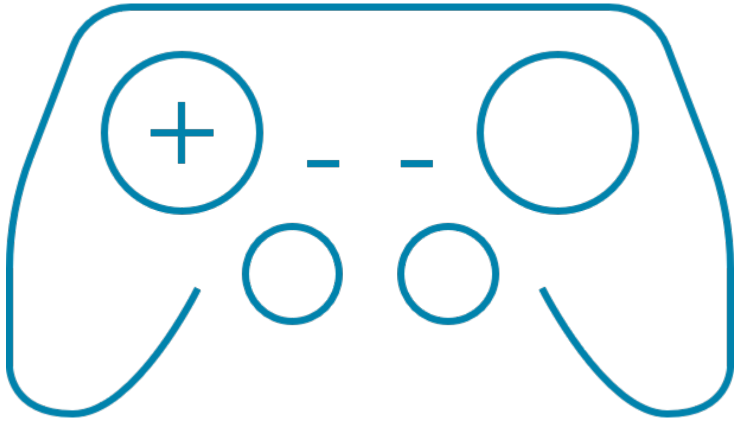
FEMP
Federal Energy Management Program

FEMP FRCS Cyber Program

Goal: Help stakeholders…

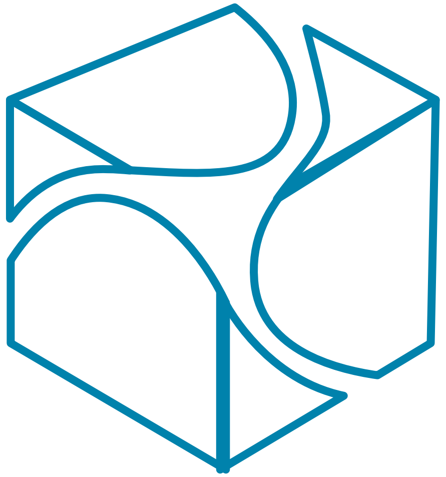
- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Evaluate their current state for physical security
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk
- Enhance their understanding and application of cybersecurity concepts and best practices

Self-Assessment Tools



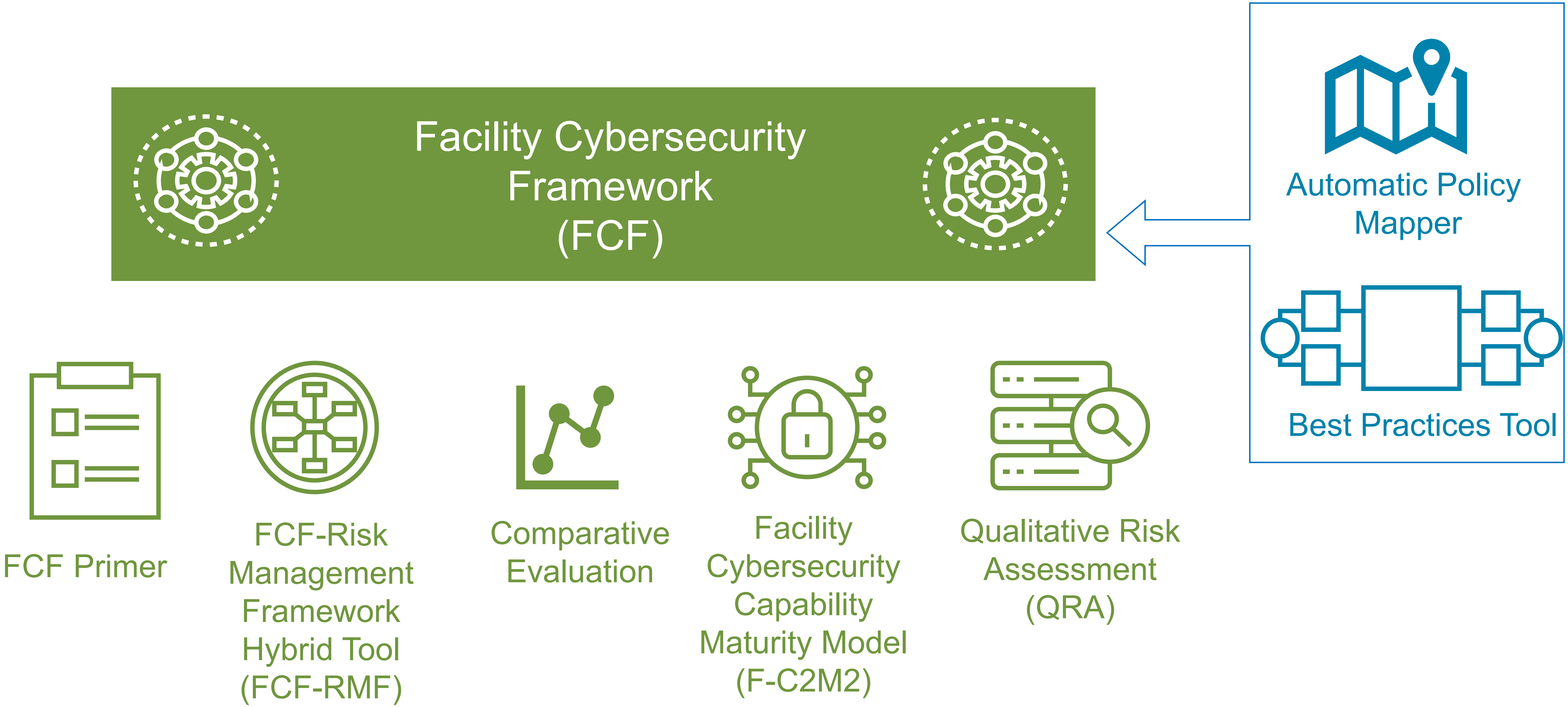
Interactive Training

Best Practices & Threat Identification



Vulnerability Discovery

TECHNICAL ASSESSMENT



Facility Cybersecurity Framework (FCF)

Automatic Policy Mapper

Best Practices Tool

FCF Primer

FCF-Risk Management Framework Hybrid Tool (FCF-RMF)

Comparative Evaluation

Facility Cybersecurity Capability Maturity Model (F-C2M2)

Qualitative Risk Assessment (QRA)

For more information, visit https://facilitycyber.labworks.org/

Approach: FEMP Solution Technical Architecture

Web-based software application
- Modern browser (Chrome, Firefox, Edge, etc.)
- No specific hardware requirements

Advanced user-friendly data analytics
- Integrated code-based with security by design
- zero external reach-outs, plethora user options

Compatible with user's data protection
- TLS encryption: Data-in-transit protected
- Data-at-rest protection per user policies

Built-in Checklist tracker
- Lets user track mitigation progress over time
- Facilitates on-the-fly mitigation plan enhancements

Built-in Comparative analyzer
- Compare progress over time/years
- No limit on data comparison from assessments

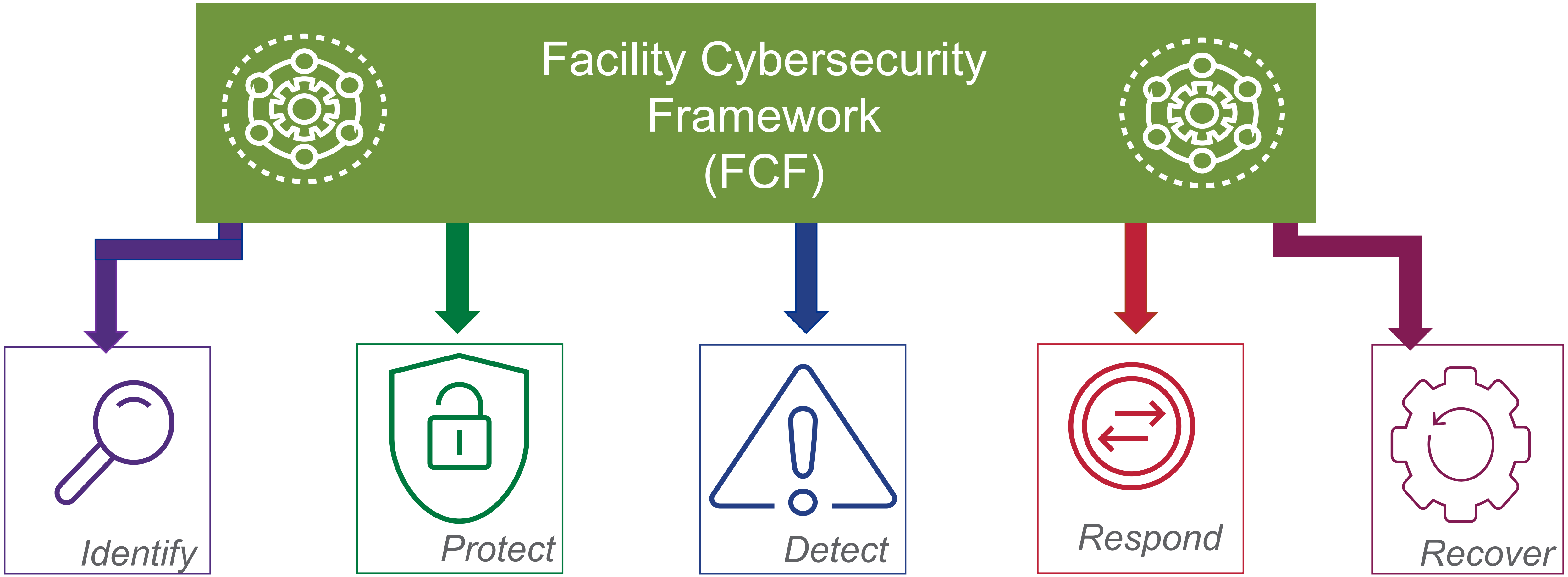
PDF based report
- Standardized report to share the results
- Establish communication path with stakeholders

Non-intrusive tool patching and updates
- No need to install patches, automated upgrades
- Ability to share feedback, suggest enhancements

Built-in trainer game
- Real-world attack-based training game
- Use current assessment against known events

Built-in Risk Registry
- Maintain risk-based asset management
- Use tool's controls to identify, protect, and defend

Widely sharable
- Use save/load to share the data with peers
- Establish organizational wide policy adoption



Facility Cybersecurity Framework (FCF)

Identify

Protect

Detect

Respond

Recover

Architecture Generator (ArcGen)

Mitigation of Externally Exposed Delivery Systems (MEEDS) for Facilities

Pitfall Scenario

Centipede Scenario

Airlock Scenario

Red Team / Blue Team

Red Team Blue Team Game

Asteroids Scenario

Berzerk Scenario

FEMP Cyber Training (Games)

- Critical need to enhance the agility and ability of federal cybersecurity capabilities
  - *Experiential learning* helps students to understand how to immediately apply knowledge learned
  - *Gamification* can help engage students and enhance knowledge retention

- PNNL developed cyber training tools to address key cyber competencies from NIST CSF and EERE Cyber Goals

Visit https://facilitycyber.labworks.org/training for all games and https://www.wbdg.org/continuing-education/femp-courses/femp62 for the accredited training game

PNNL worked with Whole Building Design Guide (WBDG) to offer Continuing Education Units (CEUs) for successful completion of games and will be expanding accredited scenarios in FY21

Pacific Northwest NATIONAL LABORATORY

FEMP Federal Energy Management Program

Training Game

- The Facility Cybersecurity Training Game lets you experience and respond cybersecurity events
- You'll use skills, self-assessment tools, and attack scenarios covered by the Facility Cybersecurity Framework to protect your facility from cybersecurity attacks
- The real-world alerts and events you'll face will challenge you and your team to identify threats; protect systems; and detect, respond, and recover from incoming attacks

SCENARIOS

The training game allows users to select a scenario based on potential cybersecurity events and alerts.

Organizational leadership provides information on key priorities and needs at various stages of the scenario. Players must allocate resources appropriately through each scenario.

An assessment report is provided at the end of each game.

Training Game: Centipede

Accredited Training Link: https://www.wbdg.org/continuing-education/femp-courses/femp62

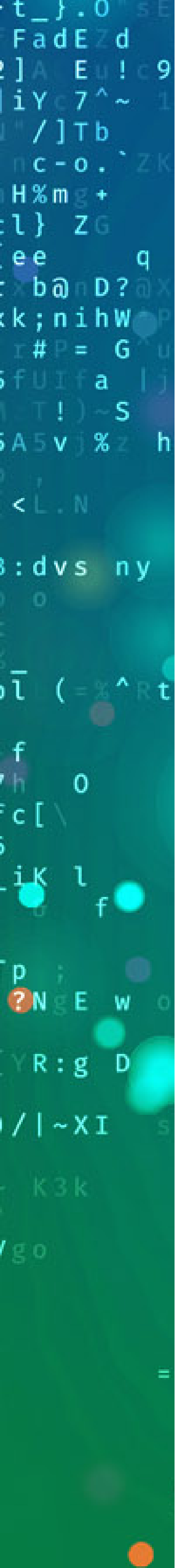
CENTIPEDE

1. Experience and get familiarized with the key cyber terminology (e.g. Personally Identifiable Information (PII))
2. Understand role of external organizational information sharing in light of new cyber threats, such as the United States Computer Emergency Readiness Team (US-CERT)
3. Understand how specific tools are being used, such as spyware like Agent.BTZ
4. Learn how communication protocols impact transmission between compromised devices
5. Gain familiarity with cyber-attack tactics such as Spearphishing and Ransomware
6. Learn about standard methods to identify and classify threats that occur on a large scale

2 modes of gameplay:

- Intermediate
- Expert

Successful completion of the game is eligible for 0.3 CEUs via FEMP's WBDG course catalog



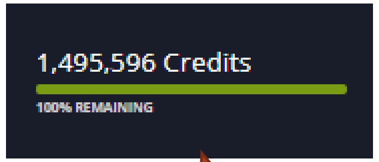
Pacific Northwest
NATIONAL LABORATORY

FEMP
Federal Energy Management Program

Thank you

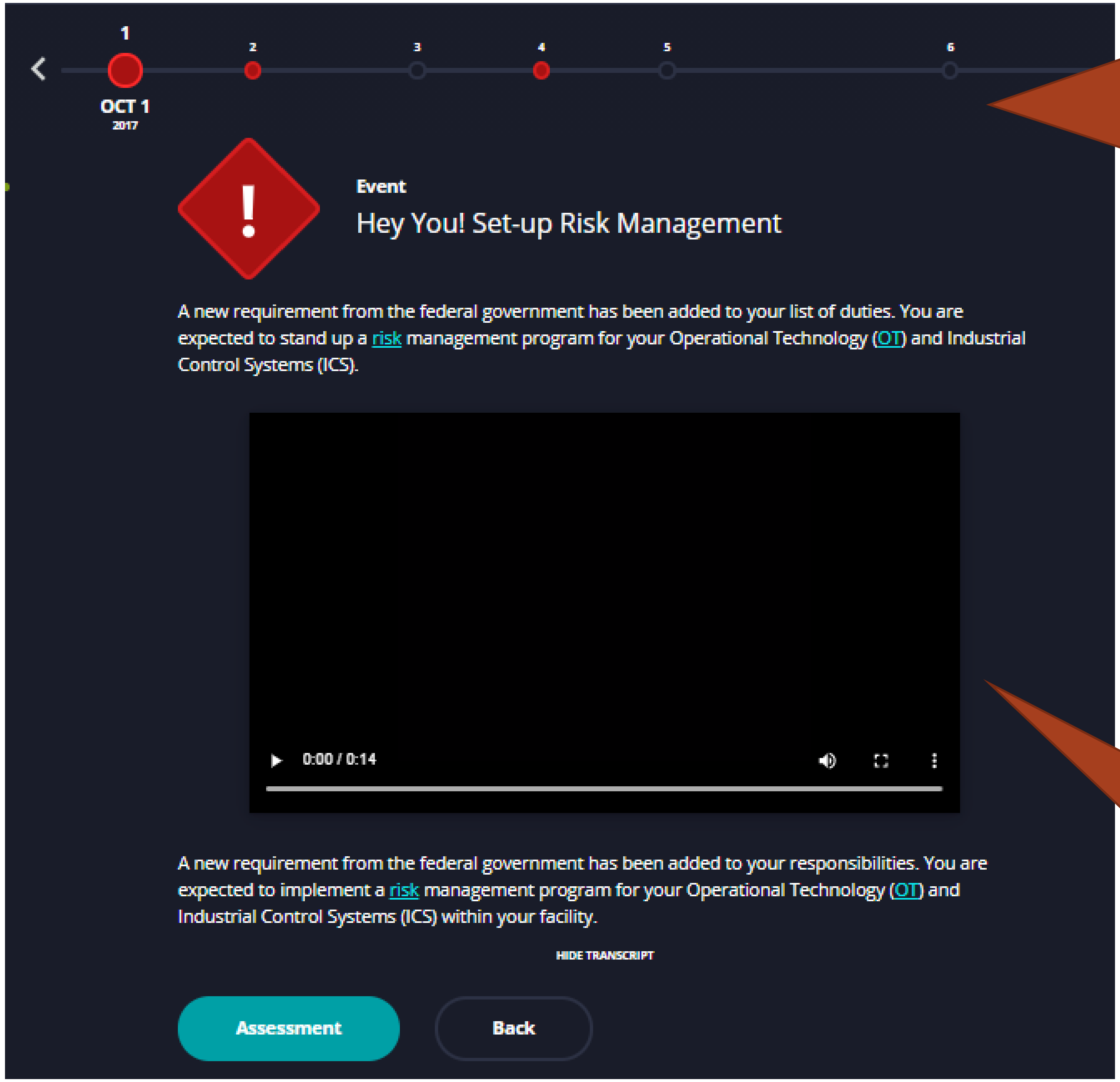
Background (Missed Demonstration)

How it works: Centipede



1,495,596 Credits

Every action has an impact on your budget; as controls are implement, your remaining credits are tracked



Event

Hey You! Set-up Risk Management

A new requirement from the federal government has been added to your list of duties. You are expected to stand up a risk management program for your Operational Technology (OT) and Industrial Control Systems (ICS).

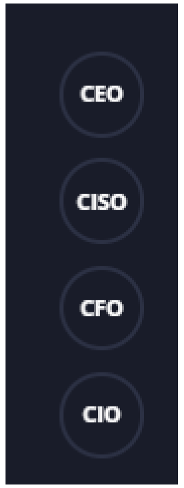
A new requirement from the federal government has been added to your responsibilities. You are expected to implement a risk management program for your Operational Technology (OT) and Industrial Control Systems (ICS) within your facility.

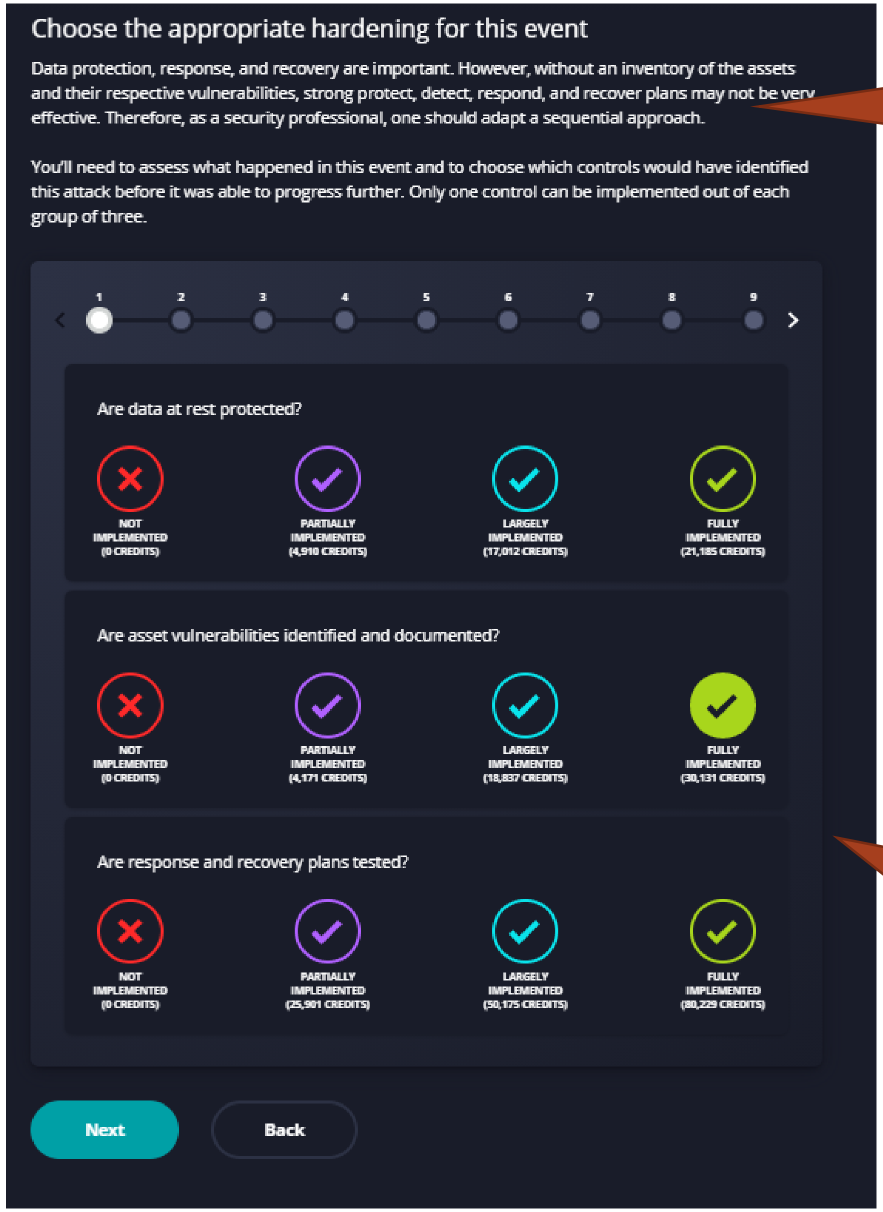
Each scenario begins with an event and is tracked along a timeline. As each scenario progresses, your responses to alerts and events are tracked on a timeline.

Video (and transcript) provide details on what is happening and what action the player needs to take

How it works: Centipede

Players can consult leadership to understand what level of control may be appropriate for their available resources





Choose the appropriate hardening for this event

Data protection, response, and recovery are important. However, without an inventory of the assets and their respective vulnerabilities, strong protect, detect, respond, and recover plans may not be very effective. Therefore, as a security professional, one should adapt a sequential approach.

You'll need to assess what happened in this event and to choose which controls would have identified this attack before it was able to progress further. Only one control can be implemented out of each group of three.

Are data at rest protected?

- ✗ NOT IMPLEMENTED (0 CREDITS)
- ✓ PARTIALLY IMPLEMENTED (4,910 CREDITS)
- ✓ LARGELY IMPLEMENTED (17,012 CREDITS)
- ✓ FULLY IMPLEMENTED (21,185 CREDITS)

Are asset vulnerabilities identified and documented?

- ✗ NOT IMPLEMENTED (0 CREDITS)
- ✓ PARTIALLY IMPLEMENTED (4,171 CREDITS)
- ✓ LARGELY IMPLEMENTED (18,837 CREDITS)
- [✓ FULLY IMPLEMENTED (30,131 CREDITS)]

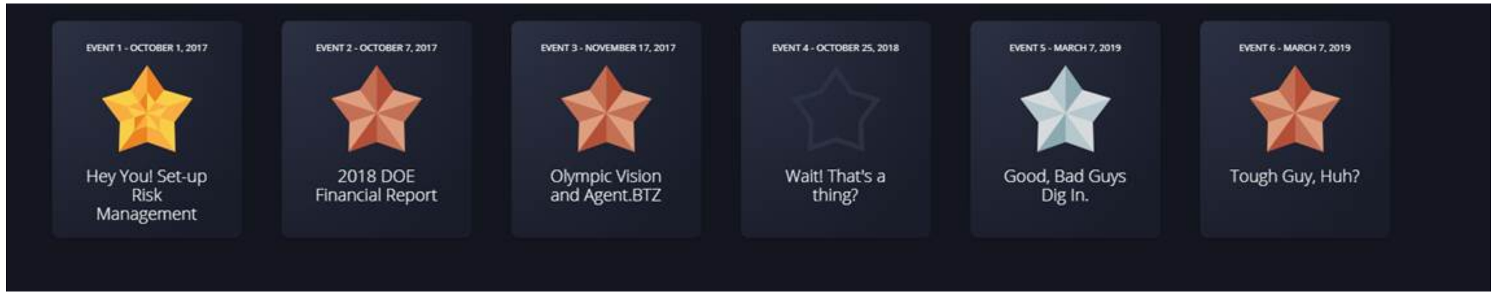
Are response and recovery plans tested?

- ✗ NOT IMPLEMENTED (0 CREDITS)
- ✓ PARTIALLY IMPLEMENTED (25,901 CREDITS)
- ✓ LARGELY IMPLEMENTED (50,175 CREDITS)
- ✓ FULLY IMPLEMENTED (80,229 CREDITS)

Technical information and background is provided for each action

Player selects which control (and what level) is most appropriate

How it works: Centipede



EVENT 1 - OCTOBER 1, 2017
Hey You! Set-up Risk Management

EVENT 2 - OCTOBER 7, 2017
2018 DOE Financial Report

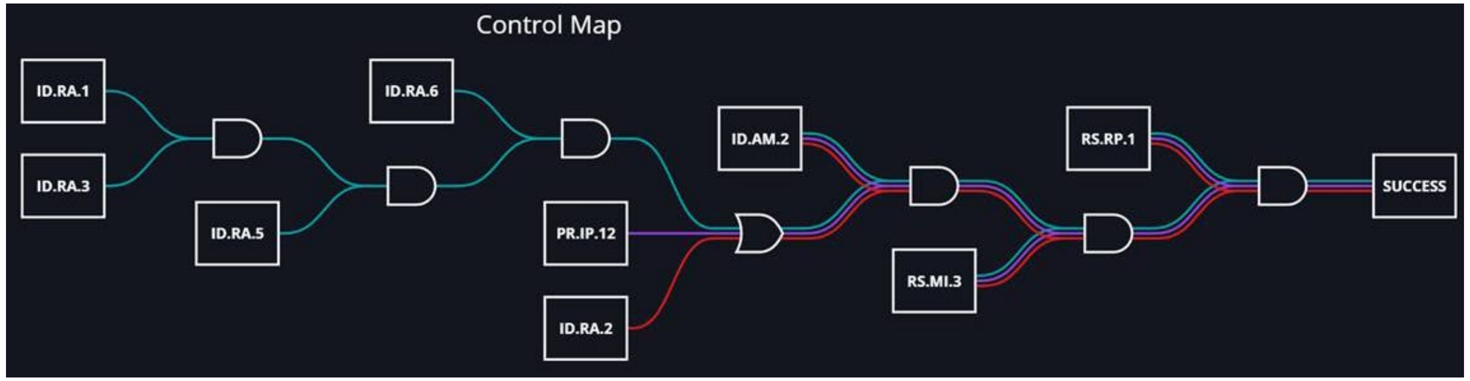
EVENT 3 - NOVEMBER 17, 2017
Olympic Vision and Agent.BTZ

EVENT 4 - OCTOBER 25, 2018
Wait! That's a thing?

EVENT 5 - MARCH 7, 2019
Good, Bad Guys Dig In.

EVENT 6 - MARCH 7, 2019
Tough Guy, Huh?

CEUs will be awarded to players whose overall performance is a silver star (or higher)



The Control map shows how the user should have selected controls to get to the desired outcome as a part of the assessment report provided to users

At the end of the scenario, the player is provided an assessment report. The game uses a star rating system:

- A **bronze star** is awarded when the majority of controls were chosen, but desired outcome isn't reached
- A **silver star** is awarded based on successfully reached the desired outcome of the event
- A **gold star** is awarded for the *ideal path*

A control map is also provided, which shows all FCF controls identified for an event and the correct controls that *should have been* implemented.