Facility Cybersecurity Framework Training Game

Asteroids Scenario Report

This Asteroids report was generated on Monday, October 13, 2025 at 21:52:26.

Table of Contents

Summary

Congratulations! You've completed the Asteroids scenario of the Facility Cybersecurity Framework (FCF) training game. As you worked through the scenario, you had the opportunity to implement your decisions and analysis of how to use resources around functions to ***Identify***, ***Protect***, ***Detect***, ***Respond***, and ***Recover*** from the imposed cyber threat(s) to the facility.

Learning Objectives

In Asteroids,

The players will experience and get familiarized with the following key terms:

1. Bring Your Own Device (BYOD)
2. Building Automation System (BAS)
3. BACnet building controller
4. Lateral movement

External organizations often have the crucial role of information sharing when new threats are discovered. The following organizations are introduced to the player in this scenario:

1. MITRE
2. National Institute of Standards and Technology (NIST)
3. National Vulnerability Database (NVD)

The course of actions taken by threat actors is determined by which tools are in their skillset. This scenario details how the following tools are being used:

1. Reverse Shell
2. USB Drive

Communication protocols dictate how threat actors can transmit information between compromised devices. This scenario discusses the following communication protocols:

1. BACnet

Techniques used between various threat actors often differ even when trying to accomplish the same goal. The players will be faced with the following cyber-attack tactics:

1. Replication through Removable Media
2. Remote Code Execution
3. Buffer Overflow
4. Resource Destruction
5. Stuxnet Attack

Common Vulnerabilities and Exposures (CVEs) are a standard method to identify and classify threats that occur on a large scale. The following CVE-ID is discussed through this scenario:

1. CVE-2019-9569

Training Game

The training game and the results reported in this document will teach you how to implement the FCF framework's five concurrent and continuous functions to Identify, Protect, Detect, Respond, and Recover from cyber threats and vulnerabilities to facilities. As you move forward from the training game to implementing the FCF framework for your organization the ***FCF Framework Background*** will act to guide you in your cybersecurity knowledge.

FCF Framework Background

The five functional domains outlined in ***Figure 1*** and defined below can be easily adopted by facility operators to enhance facility security. These domains are not intended to form a serial path or lead to a static desired end state. Instead, the domains can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. The essence is captured in a set of "how-to" instructions for facility operators to adopt, adapt, and apply to their facilities.

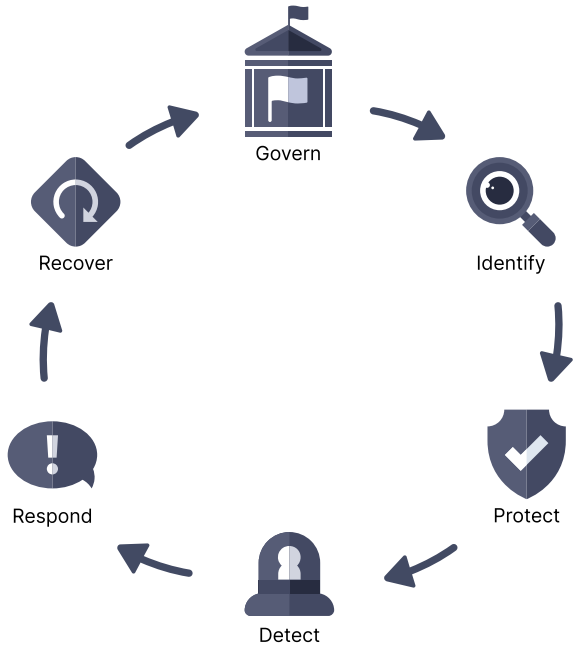

Figure 1: Outline of Facility Cybersecurity Framework

Govern

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

Identify

The goal of this domain is to identify and inventory critical cyber assets (CCAs) and develop the facility's capacity to manage cybersecurity risk to systems, assets, data, and capabilities. To realize that goal, this domain provides an overview of various critical cyber assets found in different facility types and demonstrates various risk management techniques to develop a risk characterization and risk registry QRA. Activities in this domain help facility operators focus and prioritize efforts, consistent with the facility's risk management strategy and business needs.

Protect

The goal of this domain is to introduce facility operators to cyber protection techniques that enable risk control through risk avoidance. This domain will help facility owners and operators develop and implement the appropriate safeguards to increase buildings cybersecurity posture and protect their critical cyber assets. The protect

domain supports the ability to limit or contain the impact of a potential cybersecurity event. Key takeaways from this function include: **Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology**. The protect domain is meant to supplement, improve, and/or help facility owners enhance their cybersecurity posture, not replace existing cybersecurity policies.

Detect

The goal of this domain is to introduce facility owners and operators to cyber detection techniques that will help them develop and deploy the appropriate detection systems to increase their facility's cybersecurity defense and detect any cyber attacks and anomalies.
The detect domain supports the ability to monitor the network, alert an intrusion in an attempt to nullify or minimize the impact due to a potential cybersecurity event. Key takeaways from this function include: **Anomalies and Events, Security Continuous Monitoring, and Detection Processes**.
This domain provides details about cybersecurity detection systems, which focuses on securing critical cyber assets in a facility. While facility technology varies significantly in different facility types, those detection systems can be used in residential, small commercial, large commercial, and federal facilities. Once those systems are defined, more detailed steps should be followed to configure those systems based on the need. The detect domain is meant to supplement, improve, and/or help facility owners enhance their cybersecurity posture, not replace existing cybersecurity policies but to enhance them using the findings of detection system.

Respond

The goal of this domain is to introduce facility owners and operators to

response techniques that will help them develop the facility's response plans, jump kits, etc. to ensure prompt response during a successful cyber attack on critical cyber assets. The respond domain supports the ability to react to a cyber attack and ensure that the business processes are restored quickly. Key takeaways from this function include: **Response Planning, Communications, Analysis, Mitigation, and Improvements**. This domain illustrates the content of a response plan and roles and responsibilities of a response team. The illustrated response plan and methodology is relevant to residential, small commercial, large commercial, and federal facilities. This domain also provides detailed steps to perform analysis, help identify communication strategies, and facilitate mitigation means. In addition, this domain provides an approach to improve the response plan based on lessons learned. The respond domain is meant to supplement, improve, and/or help facility owners to effectively respond to cyber attacks and to enhance the existing cybersecurity policies by using the findings of response analysis methodologies.

Recover

The goal of this domain is to introduce facility owners and operators to recovery techniques that will help them to ensure a prompt restoration and reintegration of the facility’s critical cyber assets (CCAs). The recover domain supports the ability to react to a cyber attack and ensure that the business processes are restored quickly. Key takeaways from this function include: **Recovery Planning, Improvements, and Communications** The domain illustrates the content of key attributes of a recovery plan. The illustrated recovery plan and methodology is relevant to residential, small commercial, large commercial, and federal facilities. The domain also provides detailed steps to reintegrate the systems in a facility to ensure business continuity. The recover domain is meant to supplement, improve, and/or help facility owners to effectively recover from a cyber attack and to enhance the existing cybersecurity policies by using the findings of recovery analysis

methodologies.

Maturity Indicator Levels

The FCF defines three maturity indicator levels (MILs), MIL1 through MIL3, which apply independently to each domain in the FCF. There are four aspects of MILs that are important to understand and apply the FCF:

1. Because the maturity indicator levels apply independently to each domain an organization using the FCF may be operating at different MIL ratings for different domains. For example, an organization could be operating at MIL1 in one domain, MIL2 in another, and MIL3 in a third.

2. The MILs are cumulative within each domain; to earn a MIL in a given domain, an organization must perform all of the practices in that level and the levels preceding it. For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization would have to perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.

3. Establishing a target MIL for each domain is an effective strategy for using the FCF to guide cybersecurity program improvements. Organizations should become familiar with the practices in the FCF prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those target levels.

4. Practice performance and MIL achievement need to align with business objectives and the organization's cybersecurity strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL against potential benefits. However, the FCF was

developed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

Scoring

Unlike a traditional assessment the training game does not focus on implementation levels for each control. Instead, scoring uses a star based system based on how well you were able choose the right course of action to take and recover from incorrect choices that may have come previously.

The stars based system awards one of the three stars in ***Figure 1***. A copper star is awarded in the event that the desired outcome isn't achieved at the end of an event but a majority of the controls were correctly chosen. Silver is awarded when the desired outcome is achieved successfully. The gold star is awarded for achieving the desired outcome with almost all of the controls correctly chosen.

Figure 1: Training Game success stars

Control Graphs

The control graphs show the various paths available and what decisions are necessary to move closer to success. The controls are listed in a real-life sequence where controls and gates colored green have been satisfied. Any AND gates, see ***Figure 1***, require all controls to be satisfied to satisfy them while OR gates, see ***Figure 2***, can supersede prior AND gates assuming the required controls are satisfied.

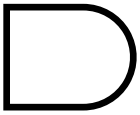

Figure 1: AND gate

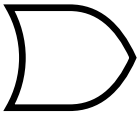

Figure 2: OR gate

In the example in ***Figure 3*** there are three success paths shown. The first path, teal, requires Control 1 and Control 2 to be chosen to satisfy the AND gate which then allows the teal path to proceed past the OR gate. The second path, purple, only requires Control 3 to be satisfied to proceed past the OR gate. The third path, red, is similar to the second path in that only Control 4 must be satisfied ro proceed past the OR gate.

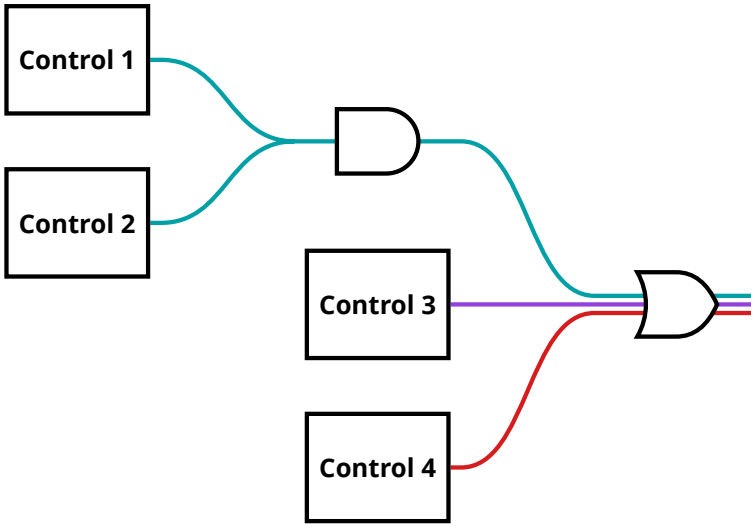

Figure 3: Control Gate Example

Results

You are now presented with the results of your selections measured against the ideal responses. Upon successfully finishing this cybersecurity training game scenario, you've gained experience to:

Identify critical cyber controls

Know Common Vulnerabilities and Exposures (CVE) and how to use the CVE information to identify and document internal and external threats against facility assets.

Protect critical cyber assets

Recognize and assess potential shortfalls associated with normal responses to a given CVE (e.g., scanning, human error) and use appropriate measures to protect against those risks (e.g., manage permissions and authorizations, provide only essential capabilities).

Detect non-linear cyber threats

Employ the use of automated alerts from trusted organizations and baseline data to recognize anomalous network or personnel activity or data flows.

Respond promptly to cyber events and anomalies

Synthesize information from automated alerts and unusual activity to develop and implement a coordinated plan to mitigate or document as an accepted risk any newly identified vulnerabilities.

Recover successfully from the cyber event

Evaluate the sequential best practices to recover from cyber event.

Analysis Description

Your training game results are identified in the Results. Each heading will provide you details and what the results mean to them (and how they can apply what they learned here to FCF assessment reports or their facilities.)

Success

The node at the end of each control map represents whether you were successful in mitigating the attack during the event. The ultimate goal is to implement every control in the control map completely for optimal coverage and doing so will increase your score and star earned in that event.

Critical Dependencies

These are the main options that are critical to a successful path in the game. Using ***Figure 0*** from the last section as an example, if no other controls would result in a successful outcome the two controls (ID.RA.1 and ID.RA.3) would be critical dependencies for the event in question.

Completion

The event's completion score indicates the overall progress made toward full implementation on all questions within the event. This figure informs the user on how close they are to having full implementation for the entire event. The percentage is found using weights for each implementation state to include all implementation states in the

completion percent, shown in the following formula:

$$c\% = \frac{0(n) + 1(p) + 2(l) + 3(f)}{3(t)}$$

Where

c = Total Implemented Percent
n = Number of Not Implemented Questions
p = Number of Partially Implemented Questions
l = Number of Largely Implemented Questions
f = Number of Fully Implemented Questions
t = Total Number of Questions

Event 1 - Initial Access - Replication through Removable Media.

You have successfully safeguarded against this event by correctly implementing enough recommended security controls. You have evaluated the potential actions that attackers would take given specific circumstances and your risk management was ideal. Through your efforts, you have effectively contrived at least one pathway for success according to the event control map. Your response has met the requirements and would have a strong defense against the attacks in this event.

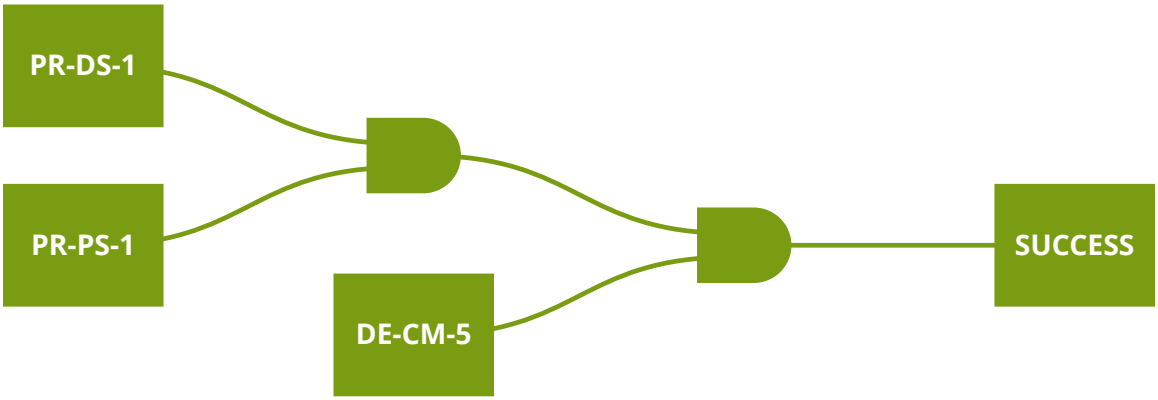

Figure 1: Asteroids - Event 1 - Replication Through Removable Media Control Map

Event 2 - Network Discovery/Persistence - Scripting

You have successfully safeguarded against this event by correctly implementing enough recommended security controls. You have evaluated the potential actions that attackers would take given specific circumstances and your risk management was ideal. Through your efforts, you have effectively contrived at least one pathway for success according to the event control map. Your response has met the requirements and would have a strong defense against the attacks in this event.

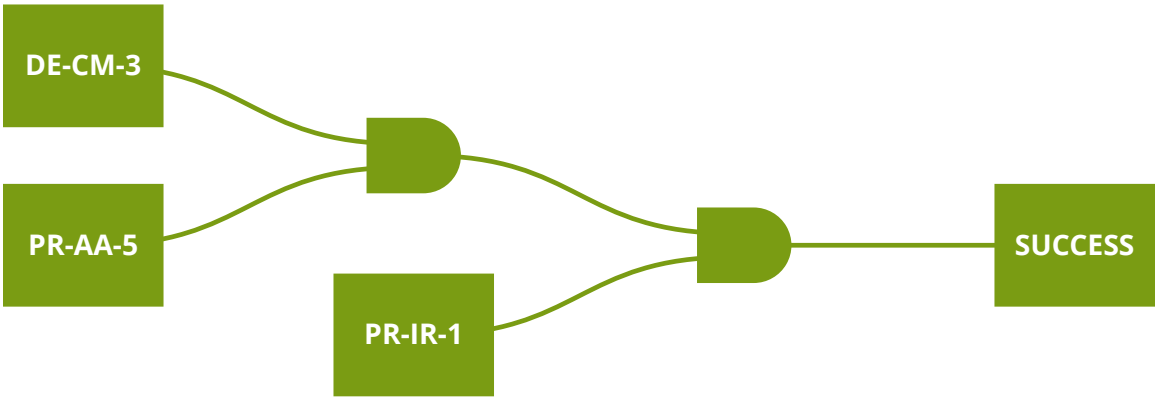

Figure 2: Asteroids - Event 2 - Scripting Control Map

Event 3 - Lateral movement/Command and Control - Communication Through Removable Media

You have successfully safeguarded against this event by correctly implementing enough recommended security controls. You have evaluated the potential actions that attackers would take given specific circumstances and your risk management was ideal. Through your efforts, you have effectively contrived at least one pathway for success according to the event control map. Your response has met the requirements and would have a strong defense against the attacks in this event.

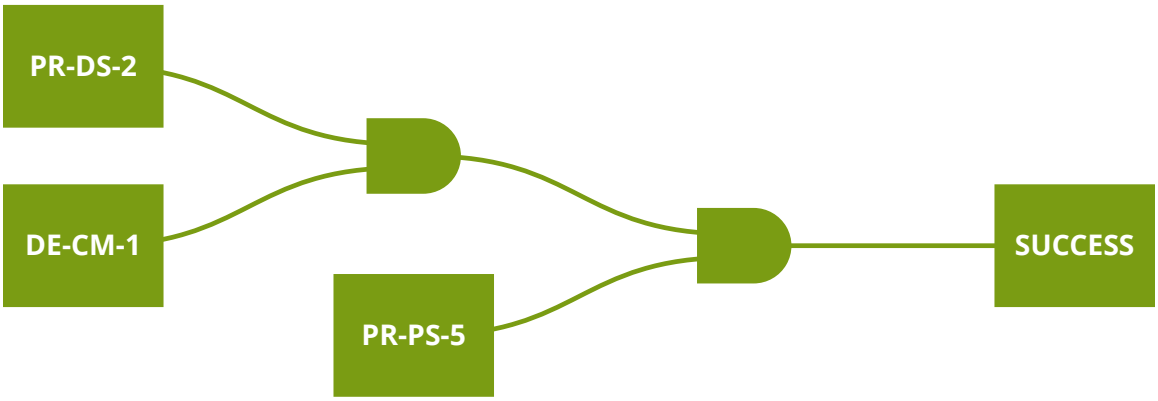

Figure 3: Asteroids - Event 3 - Communication Through Removable Media Control Map

Glossary

Terms

CVE
Common Vulnerabilities and Exposures

FCF
Facility Cybersecurity Framework

MIL
Maturity Indicator Levels

Controls

PR-AA-5

Protect, Identity Management, Authentication, and Access Control, Control 5 – Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

PR-DS-1

Protect, Data Security, Control 1 – The confidentiality, integrity, and availability of data-at-rest are protected

PR-DS-2

Protect, Data Security, Control 2 – The confidentiality, integrity, and availability of data-in-transit are protected

PR-PS-1

Protect, Platform Security, Control 1 – Configuration management practices are established and applied

PR-PS-5

Protect, Platform Security, Control 5 – Installation and execution of unauthorized software are prevented

PR-IR-1

Protect, Technology Infrastructure Resilience, Control 1 – Networks and environments are protected from unauthorized logical access and usage

DE-CM-1

Detect, Continuous Monitoring, Control 1 – Networks and network services are monitored to find potentially adverse events

DE-CM-3

Detect, Continuous Monitoring, Control 3 – Personnel activity and technology usage are monitored to find potentially adverse events

DE-CM-5

Detect, Continuous Monitoring, Control 5 – Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events