C2M2 | Cybersecurity Capability Maturity Model

Cybersecurity Threat Profile Development Guide

Version 1.0

July 2026

U.S. DEPARTMENT of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The United States Department of Energy (DOE) thanks the organizations and individuals who provided the critiques and recommendations necessary to produce this document.

Program Lead

Fowad Muneer
Office of Cybersecurity, Energy Security, and Emergency Response
United States Department of Energy

Development Team and Contributors

Brian Benestelli
Axio

Shawn Bilak
Southern Company

Jonathan Bransky
Dominion Energy Services, Inc.

Kaitlin Brennan
Edison Electric Institute

Richard Caralli
Axio

Jason Christopher
Energy Impact Partners

Timothy Corum
Knoxville Utilities Board

Cory Faust
Axio

Tricia Flinn
Carnegie Mellon University Software Engineering Institute

John Fry
Axio

Clifford Glantz
Pacific Northwest National Laboratory

Nicholas Harrison
Salt River Project

Daniel Kambic
Carnegie Mellon University Software Engineering Institute

Lindsay Kishter
Nexight Group

Daniel Komnick
Carnegie Mellon University Software Engineering Institute

Annabelle Lee
Nevermore Security

Fowad Muneer
United States Department of Energy

Jason Pearlman
Nexight Group

Jennifer Peters
Nexight Group

Alexander Petrilli
Carnegie Mellon University Software Engineering Institute

Justin Pascale
Dragos

Lynn Pope
Idaho National Laboratory

Jeremy Poynton
Carnegie Mellon University Software Engineering Institute

David White
Axio

Virginia Wright
Idaho National Laboratory

1. SCOPE AND USE OF THIS DOCUMENT

1.1 Intended Audience

This publication is intended for energy sector organizations and other organizations that want to create a new threat profile or improve an existing one. Threat profiles and their development are part of Cybersecurity Threat Management. Some organizations may refer to threat profile development and related activities as threat modeling, threat intelligence, threat management, or risk management.

This guide aligns with and builds upon concepts discussed in the United States Department of Energy (DOE) Cybersecurity Capability Maturity Model Version 2.1 (C2M2). Some references in this document are specific to the C2M2 [DOE 2022]; however, any cybersecurity practitioner may benefit from the practices described in this document.

1.1.1 Disclaimer

The guidance provided in this document is intended to be informative and not prescriptive. The development approach and information included in a threat profile should be tailored to each organization's unique operating conditions and cybersecurity challenges.

This publication is not intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Additionally, this publication is not part of a regulatory framework, nor is it intended for regulatory use. It is anticipated that entities subject to compliance requirements would use this guidance, but it does not in any way alter compliance requirements.

The United States Department of Energy does not endorse any commercial entity, product, company, or service, including any entities, products, or services mentioned in this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the United States Department of Energy.

2. INTRODUCTION

A cybersecurity threat is defined as “any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.” [NIST 2018] Examples of common cyber threats include ransomware, malware, social engineering, denial-of-service, or malicious actions performed by insiders.

A cybersecurity threat profile is a means to describe the range of potential cyber threats to an organization. In the Cybersecurity Capability Maturity Model, a threat profile is defined as:

> *A characterization of the likely intent, capability, and targets for threats to the function. It is the result of one or more threat assessments across the range of feasible threats to the IT, OT, and information assets of an organization and to the organization itself, identifying feasible threats, describing the nature of the threats, evaluating their severity, and determining their priority.* [DOE 2022]

This guide describes development and use of a cybersecurity threat profile. These terms are used interchangeably in this guide and have the same meaning: “cybersecurity threat profile,” “threat profile,” and “profile.”

2.1 Why Develop a Cybersecurity Threat Profile?

Understanding cybersecurity threat is essential to effectively responding to cybersecurity risk. However, developing such an understanding is difficult. The threat environment is vast, complex, and constantly changing. Threat information comes as a constant flow of alerts, advisories, news articles, reports and other sources. Often, this information is fragmented, lacks context, and varies in fit, form, and function.

A threat profile helps simplify and prioritize cybersecurity threat information. This is an essential component of several key cybersecurity activities, including:

- Identifying and responding to cybersecurity risks
- Communicating with organizational leaders
- Coordinating with enterprise risk management
- Setting cybersecurity program strategy
- Detecting and responding to incidents
- Tailoring training and awareness
- Developing a cybersecurity architecture
- Managing assets
- Patching and mitigating vulnerabilities
- Threat hunting

Profile Development Tip

Cybersecurity threat information is a powerful tool for communicating with leaders and other stakeholders. Threat profiles can help amplify messages about the significance of cyber risk and bring topics to life for those less familiar with the potential impacts of a cyber attack.

2.2 Relationship of Cybersecurity Threat to Enterprise Risk

Cybersecurity threat is a component of cybersecurity risk. Cybersecurity risk is, in turn, a component of enterprise risk—the overall risk to the organization. The relationships between cybersecurity threat scenarios, cybersecurity threat profiles, cybersecurity risk, and enterprise risk are detailed in the following paragraphs.

- ***Cybersecurity threat scenarios*** are the building blocks of a cybersecurity threat profile. Cybersecurity threat scenarios describe what could happen if a cybersecurity threat is realized. For example, a threat scenario may describe what could happen in the event of a ransomware attack.
- ***Cybersecurity threat profile*** refers to a collection of all *cybersecurity threat scenarios* of significant concern to an organization. Cybersecurity threat profiles define how cybersecurity threats could result in harm to an organization. Thus, they are a core element of cybersecurity risk [CMU 2007].
- ***Cybersecurity risks*** are similar to cybersecurity threat scenarios. Both describe what could happen if a cybersecurity threat is realized. Cybersecurity risk analysis may go beyond the threat development processes discussed in this guide. For example, it may include estimates of likelihood or the quantification of cybersecurity risks. For many organizations, a cybersecurity threat profile alone may provide ample information to manage and communicate cybersecurity risks. While other organizations may use a threat profile to support further risk analysis.
- ***Enterprise risks*** are the most significant risks to an organization's mission and goals. Examples include financial risk, operational risk, or legal risk. Cybersecurity is one of many potential causes of enterprise risks. Other examples of causes are natural disasters, war, regulatory changes, or shifts in customer demand.

  Modern organizations rely heavily on technology to support business and operational processes. As a result, cybersecurity attacks can significantly impact those processes as well as dependent processes. Cybersecurity threat scenarios describe how that could occur and what the impacts might be. This information enables leaders to compare cybersecurity risks with other sources of risk and make informed decisions regarding risk tolerance, resource allocation, and strategic planning.

The relationship between cybersecurity threat scenarios, threat profiles, cybersecurity risk, and enterprise risk is depicted in Figure 1.

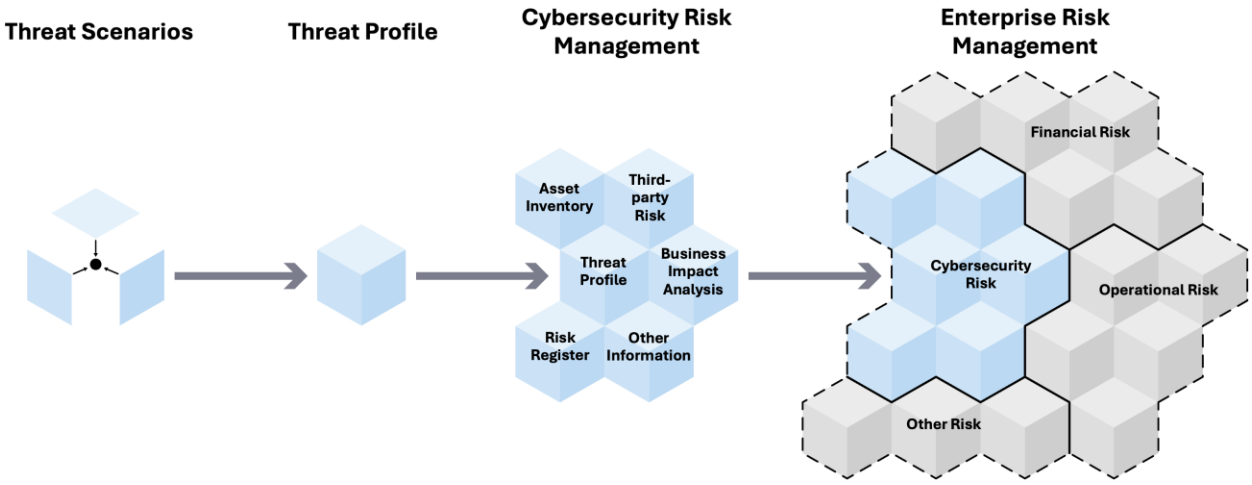

Figure 1: Relationship of Cybersecurity Threat, Cybersecurity Risk, and Enterprise Risk

2.3 Process for Development and Use of a Threat Profile

The process for developing and using a threat profile varies significantly from organization to organization. However, at a high level, the process involves four steps: Plan, Develop, Use, and Maintain.

1. ***Plan*** includes engaging stakeholders, setting objectives, and other considerations that are useful to address in advance of development.
2. ***Develop*** includes identifying, prioritizing, documenting, and validating threat scenarios.
3. ***Use*** includes applying the threat profile to improve decision-making and protecting the profile.
4. ***Maintain*** includes developing organizational processes to ensure that the profile is kept up to date with current threat intelligence, adjusted for organizational changes, and reviewed periodically for completeness, relevance, and manageability.

Figure 2 summarizes the steps in the process. These steps are discussed in detail in Section 5 (Plan), Section 6 (Develop), Section 7 (Use), and Section 8 (Maintain).

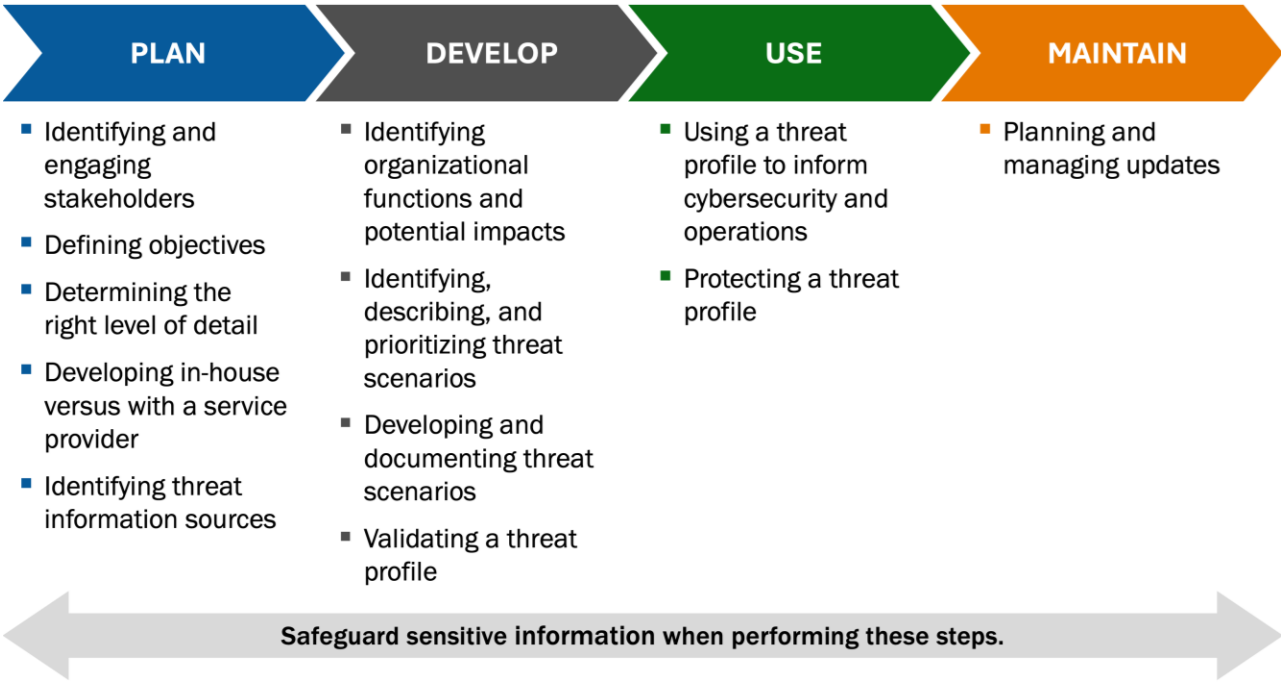

Figure 2: Steps in the Process for Developing and Using a Threat Profile

2.4 Threat Profiles in the Cybersecurity Capability Maturity Model

The establishment of a threat profile is a prominent component of C2M2 as well as many other commonly used cybersecurity frameworks, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [NIST 2024]. This is because an accurate understanding of cybersecurity threat is essential to prioritizing and mitigating cybersecurity risk effectively.

Several practices in the C2M2 depend upon successful development and implementation of a threat profile. For example, if the threat profile is incomplete and does not inform the cybersecurity architecture, the intent of practice ARCHITECTURE-1j—*The cybersecurity architecture is guided by the organization's risk analysis information and threat profile*—is unlikely to be achievable.

Figure 3 shows the relationship of C2M2 practices associated with threat profiles.

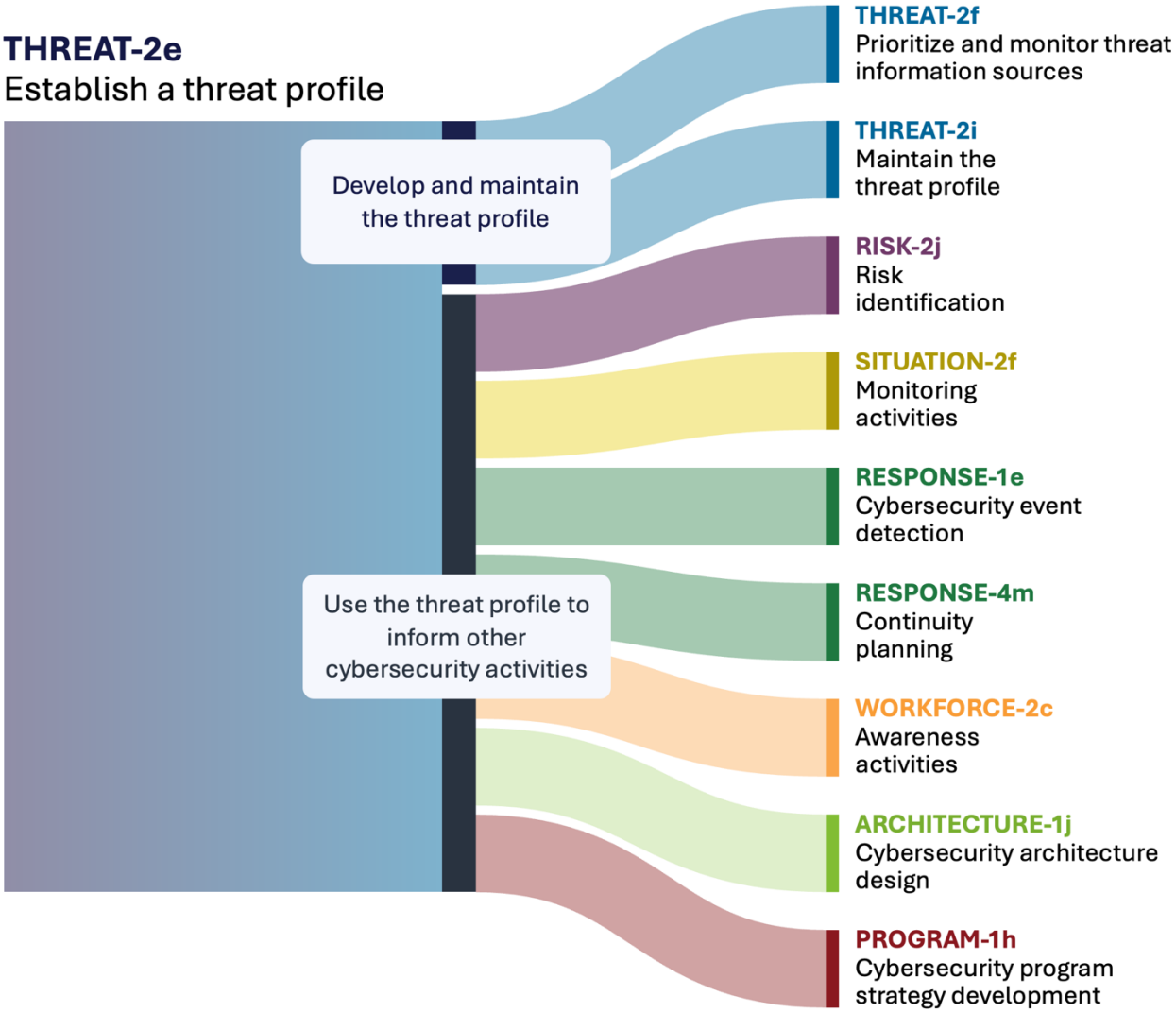

Figure 3: Establishing a Threat Profile and Its Relationship to other Cybersecurity Practices

Table 1 provides the text for each C2M2 practice related to Threat Profiles.

Table 1: C2M2 Practices Related to Threat Profiles

Practice	MIL	Practice Text
THREAT-2e	MIL 2	A threat profile for the function is established that includes threat objectives and additional threat characteristics (for example, threat actor types, motives, capabilities, and targets)
THREAT-2f	MIL 2	Threat information sources that collectively address all components of the threat profile are prioritized and monitored
THREAT-2i	MIL 3	The threat profile for the function is updated periodically and according to defined triggers, such as system changes and external events
RISK-2j	MIL 3	Threat management information from THREAT domain activities is used to update cyber risks and identify new risks
SITUATION-2f	MIL 2	Monitoring activities are aligned with the threat profile
RESPONSE-1e	MIL 3	Cybersecurity event detection activities are adjusted based on identified risks and the organization's threat profile
RESPONSE-4m	MIL 2	Continuity plans are aligned with identified risks and the organization's threat profile to ensure coverage of identified risk categories and threats
WORKFORCE-2c	MIL 2	Cybersecurity awareness objectives are aligned with the defined threat profile
ARCHITECTURE-1j	MIL 3	The cybersecurity architecture is guided by the organization's risk analysis information and threat profile
PROGRAM-1h	MIL 3	The cybersecurity program strategy is updated periodically and according to defined triggers, such as business changes, changes in the operating environment, and changes in the threat profile

3. OVERVIEW OF CYBER THREAT SCENARIOS

3.1 Threat Scenario Definition

A threat scenario describes a situation in which a threat is realized. A threat scenario details important characteristics of a threat, such as potential actors; potential motives; targeted assets; tactics, techniques, and procedures (TTP); vulnerabilities; or potential impacts.

For example, an activist *(potential actor)* wants to make a political statement *(potential motive)* by stealing customer data (*targeted asset*). The activist sends phishing emails containing malware *(TTP)* that takes advantage of a recently published software bug in a critical application that may not yet have been patched *(vulnerability)*. The activist publishes the email addresses of key employees on the dark web *(potential impact).*

Profile Development Tip

Threat actors are creative problem-solvers and do not operate under the same constraints as defenders. They are free to experiment and may test many potential vulnerabilities—including unconventional ones—to achieve their goals. Developing a robust threat profile requires a shift in perspective to "think like a hacker" and spot opportunities that otherwise may go unnoticed.

Table 2 lists the data elements that make up a threat scenario. Section 3.3 describes each data element in detail.

Table 2: Threat Scenario Data Elements

Threat Scenario Data Element	Description
Threat scenario title and description	A unique name and summary of the nature of the threat scenario.
Targeted organizational function and related assets	Major operational process or activity important to an organization and the associated assets that may be affected if the scenario were realized.
Potential impacts	The consequences of a cyber attack. This includes effects on an organization's mission, goals, functions, or assets. Examples include loss of human life, operational disruption, or destruction of hardware. For C2M2 users, potential impacts are synonymous with threat objectives.
Resilience and cybersecurity priorities	The fundamental requirements necessary to achieve the mission and maintain the operating state of an organization.
Tactics, techniques, and procedures	The actions that may be executed by a threat actor in the pursuit of a cyber attack.
Vulnerabilities	A weakness or flaw in IT, OT, or communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a threat [DOE 2022].
Key controls	Important actions to help prevent or reduce the impact of the scenario. This may include current and planned controls.
Potential actors	Individuals or groups that may execute the cyber attack described in the threat scenario.
Potential motives	The reasons potential actors may have for attempting the actions in the scenario.

3.2 Components of a Threat Profile

A threat profile is composed of threat scenarios. The number of scenarios to include in a threat profile varies by organization. The goal is to develop a profile that is comprehensive enough to be useful without being difficult to create and manage. A threat profile is not intended to document all the individual threats to which an organization may be exposed. Instead, it should summarize a range of scenarios that characterize high-priority threats.

At a minimum, a profile should address the threat scenarios that could have a significant impact on an organization's mission and objectives. This helps align cybersecurity program priorities to organizational priorities. Large organizations—particularly those that participate in multiple industry sectors or operate different lines of business—may require more than one profile to account for the unique threat scenarios that diverse operating conditions pose. For example, an integrated natural gas company that both produces natural gas and operates pipeline infrastructure may decide to create separate threat profiles that align to the unique threats and risk appetites of each line of business.

3.3 Threat Scenario Data Elements

Threat scenario data elements describe the characteristics of a threat, such as its title, targeted assets, potential impacts, or likely threat actors.

A threat profile may require only a few data elements to be effective. The data elements identified in this document are examples. Not all may be needed. For example, some elements may not be knowable. Others may not apply to the intended purpose of the profile.

Profile Development Tip

Threat profiles are a tool to improve decision making—include only those elements that directly support a specific decision.

Data elements for consideration include:

- Threat Scenario Title and Description
- Targeted Organizational Function and Related Assets
- Potential Impacts
- Resilience and Cybersecurity Priorities
- Tactics, Techniques, and Procedures
- Vulnerabilities
- Key Controls
- Potential Actors
- Potential Motives

3.3.1 Threat Scenario Title and Description

The threat scenario title and description should create a common understanding of the threat. For example, a threat scenario describing a denial-of-service (DoS) attack that results in disruption of payment processing services on a utility's website could be given the title "Denial-of-Service Attack on Customer Payment Processing Website." This title describes a cyber attack method *(DoS)* focused on a specific organizational function *(customer payment processing)* that may result in a negative impact *(disruption of an asset—the organization's website)*.

3.3.2 Targeted Organizational Function and Related Assets

This data element supports one of the most important uses of a threat profile—informing the organization which critical functions—and related assets—could be affected if a threat scenario is realized.

- ***Functions*** are major operational processes or activities important to an organization. Disruption of a function may lead to many potential impacts including loss of human life, economic loss, or collateral harm to other functions. In a threat scenario, the function defines the targets of the attack. In a scenario titled "Denial-of-Service Attack on Customer Payment Processing Website," the associated function is "customer payment processing." Consider that functions may cross organizational boundaries.
- ***Assets*** are the people, technology, facilities, and data [CMU 2016] that enable organizations and functions to carry out their mission. Disruption of assets may affect the operation of a function. In a scenario titled "Denial-of-Service Attack on Customer Payment Processing Website", "Website" is a key asset that facilitates the "customer payment processing" function.

3.3.3 Potential Impacts

Potential impacts are the possible consequences of a cyber attack. This includes effects on an organization's mission, goals, functions, or assets.

- ***Impacts on an organization's mission and goals*** are effects on what the organization values most. Examples include loss of human life, disruption of critical services, or financial loss.
- ***Impacts on functions and assets*** are the immediate effects of a cyber attack. Examples include operational disruption, loss of communications, or destruction of hardware. When brainstorming, remember that these impacts may lead to impacts on the mission and goals of the organization.

Potential impacts may also include secondary impacts such as collateral damage to assets, functions, or external parties that were not the direct target of an attack. In general, focus on identifying the impacts posing the greatest potential harm to the organization and its stakeholders.

Potential impacts may serve as a useful foundation for additional risk analysis, such as cybersecurity risk quantification. For example, in a scenario titled "Denial-of-Service Attack on Customer Payment Processing Website" the impact of the attack is "disruption of customer payment processing systems" carried out through a DoS attack. The impacts that the organization could face might include reputational damage and lost revenue. The amount of lost revenue may then be estimated as an approximate reduction in revenue of 20% or a loss of $20 million for the organization.

For C2M2 users, consider potential impacts to be the same as threat objectives. The C2M2 defines threat objectives as "the potential outcomes of threat actor activities that are of concern because they would have negative impacts on the organization" [DOE 2022].

3.3.4 Resilience and Cybersecurity Priorities

Resilience and cybersecurity priorities are the fundamental requirements necessary to achieve the organization's mission and maintain its operating state. Regardless of size or maturity, most organizations have a set of commonly understood priorities that provide a foundation for organizational culture and decision making. The purpose of a threat profile is determining how a cyber attack could impact those priorities.

Resilience requirements include:

- Safety
- Reliability
- Performance

Cybersecurity priorities include:

- Confidentiality
- Integrity
- Availability

Keep in mind that resilience and cybersecurity priorities, as well as other important priorities, may be defined in existing documents such as:

- Enterprise risk assessments
- Business impact analysis
- Organizational vision and mission statements
- Organizational strategy documentation
- Financial goals, operations goals, productivity goals, uptime goals, or quality goals
- Service level agreements
- Safety policies, operations policies, or other policies
- Incident response, disaster recovery, or continuity of operations plans
- Regulatory compliance documentation
- Employee codes of conduct

3.3.5 Tactics, Techniques, and Procedures

Tactics, techniques, and procedures are the actions that may be executed by a threat actor in the pursuit of a cyber attack. Organizations can use TTPs to prioritize cybersecurity investments or to inform cybersecurity program operations such as monitoring and threat hunting. The use of an attack framework such as MITRE ATT&CK can facilitate identification of appropriate TTPs for the scenario. Appendix E details how to apply MITRE ATT&CK for threat profile development.

Note that although this document directs users to begin scenario identification by defining potential impacts, TTPs—especially those of concern—are a powerful tool for generating

conversation about threats. Consider how TTPs may support brainstorming and scenario identification.

Seek an appropriate balance between time spent identifying TTPs and the benefit of additional information. For example, a single threat scenario may involve many potential TTPs, and many scenarios may share the same potential TTPs. Moreover, the capabilities of threat actor groups are constantly changing. A basic threat profile need not include a high level of specificity regarding TTPs. An advanced profile may include additional details to help inform the design of mitigations, such as configuring detection tools.

Profile Development Tip

Appendix D – Common Cyber Attack Types is a list of common types of attacks that organizations can use to jumpstart or inform TTP brainstorming discussions.

3.3.6 Vulnerabilities

A vulnerability is a weakness or flaw in information technology (IT), operational technology (OT), or communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a threat [DOE 2022]. When identifying vulnerabilities, remember that "thinking like a hacker" involves using creativity and searching for any potential pathway to a target including unconventional ones. Additionally, involving a diverse set of stakeholders will help identify vulnerabilities that may not otherwise be recognized. Consider scenarios in which a system may be stressed or less secure than normal, such as non-business hours, holidays, peak days, or maintenance periods.

Because vulnerabilities evolve constantly, it may not be practical to document all potential vulnerabilities related to a threat scenario. Limit the vulnerabilities documented in the threat profile to what is necessary for the planned use of the profile.

3.3.7 Key Controls

Controls are actions that an organization may take to help prevent or reduce the impact of cybersecurity incidents. This may include current controls or those planned for the future. In addition to common cybersecurity tools, controls may take the form of:

- Processes
- Plans
- Insurance
- Selecting alternatives that are less vulnerable to cybersecurity threats [DOE 2023]
- Vendors or government entities that may provide response support
- Cybersecurity controls planned for future implementation

Profile Implementation Tip

As a group, the controls identified in the threat profile represent the organization's most important cybersecurity controls.

Include the primary controls deemed important for addressing the threat described in each threat scenario. The following sections highlight some controls to consider when developing or updating a threat profile.

3.3.7.1 Controls Designed to Prevent Incidents Versus Controls Designed to Limit the Impact of Incidents

Controls designed to prevent incidents help avoid the occurrence of incidents altogether. These include things like access controls, awareness training, or firewalls.

Controls designed to limit the impact of incidents help lessen the effects of an incident when one occurs. These controls include logging and monitoring, response plans, exercises, backups, or insurance.

3.3.7.2 Current Controls Versus Controls Planned for Future Implementation

Current controls are controls that are in place and operating when the threat profile is being developed. Current controls are useful to include in a threat profile to support future prioritization and decision making, such as budget decisions, or deciding which controls to prioritize for measurement and metrics reporting.

Controls planned for future implementation are those not currently in place. These may be useful to include in the threat profile to support future budgetary requests for acquiring new technology or to help define requirements for planned implementation projects.

3.3.8 Potential Actors

Potential actors are those who may execute a cyber attack. They may be individuals, groups, or categories of threat actors, such as a financial crime gang. Gaining an understanding of the landscape of potential actors is difficult. There are countless numbers of potential actors with different and changing tactics, motivations, locations, and other factors. Many threat

actors go to great lengths to conceal their identity and avoid tracking. Nevertheless, a general understanding of potential actors offers several benefits. Example benefits include helping identify TTPs to defend against and improving threat hunting activities.

A basic profile may only need to identify threat actors by category—such as financial crime gangs. A more advanced profile may specify a selection of named threat actors, such as those known to target similar organizations. When determining the appropriate amount of detail to capture, consider how you will use the profile and how additional information will improve decision-making.

3.3.8.1 Identifying General Types of Threat Actors

A reasonable starting point for identifying threat actors is an existing list of common threat actor types. This is a quick way to create a foundation that may be developed further as needs dictate. Table 3 describes five examples of threat actor types.

Table 3: Examples—Threat Actor Types

Actor	Description
State-sponsored threat actor groups	State-sponsored threat actor groups are supported by government entities to carry out cyber attacks, often performing espionage and intelligence gathering, targeting disruption to critical infrastructure or economic systems, or creating political unrest. Often, these groups are referred to as advanced persistent threats (APTs) or nation-state actors. State-sponsored actors generally have access to extensive resources and can execute extremely sophisticated cyber attacks. State-sponsored actors are difficult to prevent and detect.
Cybercrime gangs	Cybercrime gangs include a wide range of actors and groups motivated by financial gain. They may have extensive technical capabilities. They may employ tools or services, such as ransomware-as-a-service platforms, that facilitate sophisticated attacks with limited investment and technical knowledge.
Hacktivists	Hacktivists use cyber attacks to achieve ideological, political, or social goals, or to damage the reputation of their targets. They may seek to cause physical damage, impact critical infrastructure services, or cause financial damage. Hacktivists include a wide range of actors including terrorist groups and those seeking to draw attention to a particular cause. Hacktivists often use widely available TTPs that require minimal technical investment.
Attention-seekers	Attention-seekers are strongly motivated to execute attacks that increase their popularity or notoriety. Attention-seekers typically have low skill levels and rely on widely available TTPs to execute attacks, primarily against known vulnerabilities and targets. Often referred to as “script kiddies,” they aim to inflict damage and carry out vandalism that is notable and that may result in collateral financial damage.
Insiders	Insiders are current or former employees, contractors, or trusted business partners who intentionally or accidentally misuse authorized access in a manner that affects the organization negatively. Insiders may include employees who are disgruntled or who might be working in collusion with other actors, such as hacktivists.

3.3.8.2 Identifying Specific Threat Actors

If identifying specific threat actors, start with a brief list of five-to-ten groups of high concern. This is a manageable starting point that can provide valuable insights about threat actor behaviors, such as potential TTPs and targets. For example, in 2024, the Cybersecurity and Infrastructure Security Agency (CISA) published an advisory that the state-sponsored threat actor group known as "Volt Typhoon" had "compromised the IT environments of multiple critical infrastructure organizations" including energy companies [CISA 2024].

Profile Implementation Tip

Incorporating specific threat actors helps make stakeholder communications more realistic and tangible.

For some threat actors, it may be useful to create a distinct threat scenario when known TTPs or prior incidents may indicate consistent patterns of behavior.

Consider whether information about potential threat actor groups is:

- ***Relevant*** How closely do TTPs, targets, motivations, and other known characteristics align with the concerns of your organization? How active is the actor? How impactful would a cyber attack from this actor be?
- ***Timely*** Is the threat actor currently active? Is known information about the threat actor up to date?
- ***Actionable*** How will your organization use this information? Will your organization change anything based on this information?

3.3.9 Potential Motives

Potential motives describe why an actor may choose to execute an attack. For example, an activist group may deface a website to raise awareness about a particular cause. For most situations, a high-level list of potential motives will suffice.

Table 4 lists notional examples of motives for a selection of threat actor types.

Table 4: Examples—Threat Actors and Potential Motives

Actor	Potential Motives
State-sponsored threat actor groups	▪ Espionage and intelligence gathering ▪ Political interference ▪ Social unrest ▪ Disruption of critical infrastructure and systems ▪ Building infrastructure for future attacks
Cybercrime gangs	▪ Financial gain ▪ Political unrest or interference ▪ Disruption of critical infrastructure and systems ▪ Contracted operations
Hacktivists	▪ Social activism and change ▪ Political unrest or interference ▪ Spreading an ideology ▪ Retaliation
Attention-seekers	▪ Notoriety ▪ Building skills and testing capabilities ▪ Curiosity and challenge-seeking
Insiders	▪ Espionage ▪ Revenge or retaliation ▪ Reputational damage ▪ Financial gain ▪ Coercion (threatened harm)

4. EXAMPLES OF THREAT SCENARIOS

This section includes three example threat scenarios. The examples are representative of the basic level of detail presented in Section 5.3 and describe the fictional utility company, Anywhere Gas and Electric (AG&E). AG&E provides electricity and natural gas services to residential and commercial customers.

The example threat scenarios included in this section are the following:

- Ransomware Impacting Operational Technology Assets—Electricity Distribution
- Denial-of-Service Attack on Customer Payment Website—Business Operations
- Supply Chain Compromise Impacting Gas Control PLCs—Natural Gas Distribution

Note: These examples are fictional and are not based on an actual entity or incident.

4.1 Background: Anywhere Gas and Electric

AG&E is a moderately sized public utility company that provides electricity and natural gas service to approximately 500,000 customers in a mixed urban and rural area of the United States. The company serves both residential and commercial customers, but no military or federal government customers. AG&E purchases its electricity from a nearby, large power utility.

AG&E owns and operates all assets used for delivery of utility services and manages on-premises assets for core business operations, including a public website, customer payment processing, and communications with its electricity supplier. For example, customers access account information and initiate payment for services through the AG&E website. The company has long-standing relationships with several third parties that provide services, including OT asset maintenance, landscaping, and software development.

To improve cybersecurity defenses, AG&E is developing a threat profile. The following sections document three scenarios from AG&E's threat profile.

4.2 Example 1: Ransomware Impacting Operational Technology Assets—Electricity Distribution

AG&E has several contracts with third-party vendors to service its electricity distribution equipment. One vendor, who was conducting routine inspection and maintenance activities, unwittingly introduced ransomware into the system by plugging an infected portable storage device into an asset connected to the electricity distribution OT network. The ransomware spread rapidly and encrypted the hard drives of most of the servers and workstations on the network. Visibility and remote connectivity to substations were rendered unavailable within an hour of the initiation of this attack. AG&E was able to switch to manual operation and maintain delivery of power to all customers. AG&E had previously pre-arranged for cybersecurity incident response and recovery from a local company. The initial incident

response team estimated that the response could take weeks. A full recovery would require several months to limit the potential for a disruption to power service and to leverage existing service windows where possible.

Table 5: Example 1—Threat Scenario

Element	Scenario Details
Threat scenario title and description	▪ **Title:** Ransomware Impacting Operational Technology Assets—Electricity Distribution ▪ **Description:** Ransomware introduced to the OT network with the potential to spread to all or most connected servers and workstations. Impacts include loss of connectivity to remote sites and the need to switch to manual operation of the distribution grid. Devices are restorable without the need to replace affected hardware.
Targeted organizational function and related assets	▪ **Function**: Electricity distribution ▪ **Assets**: OT Servers, OT Workstations
Potential impacts	▪ Operational impacts for planned maintenance and upgrade projects due to response efforts necessary to operate in manual mode and restoration of remote connectivity ▪ Financial impacts resulting from overtime pay for staff assigned to response efforts and extended support required from third-party vendors ▪ Increased expenses, as the response and restoration effort is expected to take several months with the highest costs occurring initially and decreasing linearly until restoration is complete
Resilience and cybersecurity priorities	▪ **Primary:** Continued operation of electricity distribution substations ▪ **Secondary:** Control and monitoring via communication between control center and remote substations
Tactics, techniques, and procedures	▪ A vendor performing routine service and maintenance unintentionally introduced ransomware to the OT network via portable storage device connected to a workstation. ▪ The ransomware spreads rapidly affecting servers and workstations.
Vulnerabilities	▪ Limited segmentation on the OT network ▪ Limited disabling of physical ports on devices ▪ Access to the network by vendor partners and devices owned and managed by those partners ▪ Homogeneity in the type of operating system used for OT servers and workstations

Element	Scenario Details
Key controls	**Current controls** ▪ Policies and procedures related to use of portable media ▪ Limited segmentation on the OT network ▪ Limited disabling of physical ports on devices **Planned controls** ▪ Begin planning for implementation of micro-segmentation project on the OT network. ▪ Initiate a project to disable physical ports on servers and workstations. ▪ Develop training and other enforcement mechanisms for removable media and other vendor-managed assets. ▪ Investigate potential benefits of leveraging differing operating systems to help limit the impact of a malware infection.
Potential actors	▪ Financial crime gangs
Potential motives	▪ Financial crime gangs may target critical infrastructure due to a perception that it will increase the likelihood of payment from victims. Threat actors may coordinate the disruption of electricity with other attacks such as data exfiltration.

4.3 Example 2: Denial-of-Service Attack on Customer Payment Website—Business Operations

AG&E purchases its electricity from a nearby, large power utility. That power utility is increasingly dependent on natural gas to generate supply. This has been associated with expanded fracking activity in the region, including construction of additional natural gas pipelines. Although AG&E is not the direct cause of additional fracking, it is concerned that anti-fracking hacktivist groups might target its assets with the intention of raising awareness about their opposition to the increased fracking activity.

Table 6: Example 2—Threat Scenario

Element	Scenario Details
Threat scenario title and description	▪ **Title:** Denial-of-Service Attack on Customer Payment Website—Business Operations ▪ **Description:** A denial of service (DoS) attack on AG&E's IT infrastructure disrupts business operations. Impacts include cash flow interruptions due to customer inability to access accounts and submit bill payments.
Targeted organizational function and related assets	▪ **Function:** Business Operations ▪ **Assets:** IT networking assets, customer website, customer payment information
Potential impacts	▪ Customers use AG&E's network and website to access their account services. The AG&E website is currently hosted on-premises on web servers that are nearing end of life. ▪ A successful DoS attack would degrade internet communications and may overload webservers. Customers would be unable to access the bill payment functionality of the public website.

Element	Scenario Details
Resilience and cybersecurity priorities	▪ **Primary:** Availability of customer payment systems ▪ **Secondary:** Availability of other pages on the AG&E public website
Tactics, techniques, and procedures	▪ Threat intelligence suggests that, while these groups have not significantly impacted organizations in previous attacks, they are now leveraging more sophisticated methods, tools, and services. Recently, they have used Distributed Denial of Service-for-hire (DDoS-for-hire) services to draw attention to social media messages denouncing other energy-related organizations. ▪ Many DDoS-for-hire services use previously compromised Internet of Things (IoT) and other devices connected to the internet to flood victim networks with a sustained, high volume of User Datagram Protocol (UDP) packets (refer to MITRE ATT&CK T1498.001).
Vulnerabilities	▪ An existing secondary, lower-bandwidth connection with a second internet service provider (ISP) is available but would be sufficient to handle only a portion of typical network traffic. ▪ AG&E does not currently have DoS protection controls or similar services from a third-party provider.
Key controls	**Current controls** ▪ Secondary internet connection. **Planned controls** ▪ Implement DoS detection and prevention tools. ▪ Implement a more robust secondary internet connection. ▪ Investigate feasibility of migrating the company website to a cloud-based hosting service that has greater resilience, scalability, and DoS-mitigation protections.
Potential actors	▪ Various hacktivist groups
Potential motives	▪ Hacktivist groups are aware that AG&E sources all of its power from a large power utility that is increasingly reliant on natural gas. The reliance on natural gas to produce power has been associated with increased natural gas drilling and fracking activity, as well as increasing investor interest in the construction of additional natural gas pipelines. Hacktivist groups oppose this and have had little success in attacking AG&E's power supplier directly. They may shift their strategy and attack AG&E instead.

4.4 Example 3: Supply Chain Compromise Impacting Programmable Logic Controllers (PLCs)—Natural Gas Distribution

A report from an Information Sharing and Analysis Center (ISAC) with a detailed analysis of recent incidents indicates the targeting of third-party maintenance providers for a specific brand of programmable logic controllers (PLCs)—known as XYZ PLCs. The report states that the likely purpose of this campaign is to gain access to customers of the third-party providers. The report highlights an exemplary incident linked to this campaign that resulted in a compromise of a service provider. This compromise was used in an attempt to access systems owned by a utility customer who operates natural gas distribution assets. Fortunately, additional authentication controls stopped the threat actor from gaining access to utility systems.

AG&E owns a significant number of assets manufactured by XYZ PLCs and uses them throughout its natural gas distribution network. Additionally, AG&E relies on a third-party provider of maintenance services—similar to those being attacked—for its XYZ PLCs.

Table 7: Example 3—Threat Scenario

Element	Scenario Details
Threat scenario title and description	▪ **Title:** Supply Chain Compromise Impacting Gas Control PLCs—Natural Gas Distribution ▪ **Description:** An attacker accesses PLCs for distribution remotely by using credentials obtained during an attack on a third-party maintenance provider. Currently, AG&E uses single-factor credentials—not multifactor authentication—for the provider's access. Those credentials and access would enable the attacker to change the programming and functionality of PLCs.
Targeted organizational function and related assets	▪ **Function:** Natural gas distribution monitoring and control ▪ **Assets:** XYZ PLCs, remote access gateways, configuration files
Potential impacts	▪ Modification of PLC configurations or programming could cause unexpected system behavior, such as loss of visibility. ▪ Loss of visibility would degrade AG&E's ability to monitor the status of the natural gas distribution network, including commercial and residential service lines. ▪ In this event, service may be disrupted and shut down in certain areas until emergency manual monitoring measures can be put into place. ▪ AG&E may face legal and financial consequences due to service disruptions, remediation costs, fines, customer litigation, reputational impacts, or scrutiny from the state public utilities commission both for the immediate event and for future interactions.
Resilience and cybersecurity priorities	▪ **Primary:** Human life and safety. Delivery of gas residential and commercial gas service. ▪ **Secondary:** Availability and integrity of operational technology.

Element	Scenario Details
Tactics, techniques, and procedures	A threat actor has been observed targeting organizations that provide maintenance service for XYZ PLCs because such organizations may provide access to many potential victim companies. Specific TTPs that have been observed include: ▪ Targeted vendors receive phishing emails with links to malicious websites with modified versions of legitimate tools (refer to MITRE ATT&CK T1195.002). ▪ Injecting malware into running processes to evade detection (refer to MITRE ATT&CK T1055). The malware establishes a communication channel with the threat actor, enabling command and control (C2) through domain naming system (DNS) tunneling (refer to MITRE ATT&CK T1572). ▪ The malware deploys various payloads depending on the vendor operating environment. The payloads include tools to harvest credentials (refer to MITRE ATT&CK T1555) and enumerate running processes to determine what remote access tools are used to communicate with customer assets (refer to MITRE ATT&CK T1057). ▪ The threat actor uses valid credentials to impersonate the vendor and establish remote connections to customer assets. In past attacks, the threat actor has established a remote connection from outside the vendor environment. The AG&E cybersecurity policy does not require the investigation of remote connections from unexpected IP addresses. ▪ After establishing a remote connection, the threat actor was observed sniffing network traffic (refer to MITRE ATT&CK T0842) and performing host discovery (refer to MITRE ATT&CK T0846). ▪ If a threat actor gained access to the targeted PLCs, it is expected that they would attempt to modify configurations (refer to MITRE ATT&CK T0831) to cause operational impacts.
Vulnerabilities	▪ The third-party vendor managing XYZ PLCs previously failed to provide evidence of routine internal cybersecurity assessment. ▪ Vendor remote access does not use multifactor authentication. ▪ The vendor is suspected of potentially sharing credentials without the permission of AG&E. ▪ The third-party vendor contract does not require the vendor to perform periodic access reviews or revocation of access in a timely manner.

Element	Scenario Details
Key controls	**Current controls** ▪ Protection systems designed to fail-safe and prevent severe impacts, such as overpressure, from unexpected system behavior. ▪ Recently procured support for log monitoring from a Managed Security Service Provider (MSSP) to help identify potential cybersecurity incidents. ▪ Incident response and continuity plans include contact and escalation information for service vendors. **Planned controls:** ▪ Isolate OT technology from IT environments and the internet. ▪ Implement controls to enforce that remote access sessions must connect to a remote access server in the industrial Demilitarized Zone (DMZ). ▪ Switch remote access to a solution that allows for multifactor authentication. ▪ Enable additional logging for remote access connections. ▪ Further monitor remote access connections for anomalous behavior. ▪ Include service providers in incident response exercises. ▪ Include a clause in contracts that requires service providers to provide summary results of periodic cybersecurity control assessments. ▪ Issue unique credentials for service provider employees and enforce with multifactor authentication. ▪ Improve identity and access management processes and procedures for privileged credentials and assignment of privileges to third parties.
Potential actors	▪ State-sponsored threat actors ▪ Hacktivists
Potential motives	▪ Threat intelligence suggests that a state-sponsored actor is disrupting critical infrastructure to further the sponsoring state's strategic objectives by weakening public trust in the United States government. ▪ Hacktivists may wish to disrupt operations to raise awareness about their opposition to increased fracking activity in the region.

5. PLANNING FOR THREAT PROFILE DEVELOPMENT

Figure 4: Plan—Steps in the Threat Profile Development Process

Advanced planning improves the quality of a threat profile. Identify where planning can strengthen its viability and usability. Example areas include:

- Identifying and engaging with stakeholders
- Defining objectives for the profile
- Determining the right level of detail for the profile
- Determining whether to develop in-house or with support from a service provider
- Identifying threat information sources

Each example is discussed in detail in the following sections.

5.1 Identifying and Engaging with Stakeholders

There are many individuals or groups who may provide useful input to or may be affected by a threat profile. These stakeholders may be internal or external to the organization. Consider when stakeholders should be engaged and what that engagement should entail.

Internal stakeholder collaboration provides opportunities to improve cybersecurity culture and build useful relationships between organizational units. The development effort not only brings diverse constituencies into the process but, by achieving consensus on the organization's exposures, it can inform immediate and impactful changes in operational practices, activities, and behaviors. Examples of internal stakeholders include:

- Cybersecurity
- Security Operations Center (SOC)
- Operations and Engineering
- Operational Technology
- Information Technology
- Cybersecurity Threat Intelligence
- Enterprise Risk Management
- Business Continuity and Disaster Response
- Legal
- Internal Audit
- Human Resources
- Facilities Management
- Physical Security
- Insurance

Senior leadership sponsorship is critical to the ongoing success of a threat profiling effort. Leaders and managers can provide valuable input to the process, especially with regard to strategic changes that might affect the organization in the future. Examples include upcoming organizational changes, potential merger and acquisition activities, business expansion plans, or impending legal challenges. This information may not be readily accessible to the threat profile development team. Senior leadership can provide this knowledge and help validate that the profile is adequate for the near future.

Enterprise risk management team members can serve as valuable partners for threat profile development and implementation. Cybersecurity threat is a component of cybersecurity risk, which itself is a component of enterprise risk. This creates a close link between cybersecurity and enterprise risk. Enterprise risk team members provide a broad perspective that includes both cyber and non-cyber risks. They can offer insight into organizational priorities and point out things that others might overlook such as secondary impacts or factors that could limit the impact of a cyber attack. These teams often maintain important inputs such as risk registers, enterprise risk assessments, and business impact analyses. They can also help increase visibility and leadership support for profile development and implementation efforts.

External stakeholders may offer valuable input to the threat profile. They may also be affected by the profile. Examples include vendors, peer organizations, ISACs and other threat intelligence-sharing organizations, external auditors, law enforcement, or regulatory authorities.

5.2 Defining Objectives for the Threat Profile

A threat profile is a tool to improve decision making. Prior to initiating development, in coordination with stakeholders, identify which decisions will leverage the threat profile. For each identified decision, briefly document a high-level process for using the threat profile and the objectives for using the profile as an input to that decision. When this is complete, record any additional requirements or objectives for development and use of the profile. Use this information to help communicate the profile's value and to focus profile development on achieving the highest-priority objectives for the profile.

5.3 Determining the Right Level of Detail

In this guide, the level of detail of a threat profile is categorized as basic, intermediate, and advanced. Before starting development, decide what level is appropriate for your organization and planned use. Additional factors to consider are resource capacity, the related experience and knowledge of the development team, budget, and time planned for development.

Profile Development Tip

If no profile exists, start with a basic profile. Refine and mature the profile as needed in subsequent versions.

5.3.1 Basic Profile

A basic profile is a simple articulation of high-priority threats and can create a useful resource to support many cybersecurity and risk management activities.

Development may consist of internal brainstorming activities to both gather stakeholder input and identify threats of concern and create a working list of potential threat scenarios. Development may be jump-started by use of a generic, off-the-shelf threat profile.

5.3.2 Intermediate Profile

An intermediate threat profile more detailed articulation of relevant threats. It requires added threat intelligence collection and closer analysis of the organization's operations and assets. It describes the threat environment in greater detail and further relates that detail to the organization's unique operational challenges.

5.3.3 Advanced Profile

An advanced profile incorporates an expansive array of threat information that is highly customized to the organization's operating environment and cybersecurity challenges.

At this level, the organization's threat intelligence gathering is sophisticated and aligned to managed detection and response (MDR) and endpoint detection and response (EDR) tools. An organization may integrate its profile into such processes as security information and event management (SIEM) or security orchestration, automation, and response (SOAR). In this case, the profile may include advanced threat models and is considered a foundational input throughout cybersecurity program activities, such as development of the cybersecurity architecture.

The threat profile update process may be operationally focused with daily or even hourly revisions, which result in timely changes to cybersecurity architectures and related practices. Table 8 summarizes the characteristics of each level of detail.

Table 8: Example—Levels of Detail for Threat Profiles

Level	Characteristics	Examples of Implementation
Basic	▪ Limited development cost and time ▪ Limited organizational engagement ▪ Focus on most critical threats and organizational assets ▪ Informs cybersecurity activities at a high-level ▪ Ad-hoc updates	▪ Review of logs and alerts ▪ Situational awareness and training ▪ Cybersecurity risk management ▪ High-level cybersecurity architecture considerations ▪ Informs basic cyber risk quantification efforts
Intermediate	▪ Moderate development cost and time ▪ Stakeholder engagement includes key operational and security personnel ▪ Expansion beyond critical threats ▪ Focused on critical and supporting assets ▪ Integrated within some cybersecurity capabilities ▪ Updated periodically	▪ Defined monitoring and analysis requirements ▪ Established indicators ▪ Established alerts and alarms ▪ Informative to third-party security operations requirements ▪ Supports intermediate cyber risk quantification efforts
Advanced	▪ Significant development costs ▪ Continuous development and updates ▪ Stakeholder engagement extends across the enterprise ▪ Threat environment is well-defined and understood ▪ Threat intelligence incorporates a wide range of sources including automated and classified sources ▪ Impact analysis considers all assets	▪ Full integration throughout the cybersecurity program ▪ Influences strategic planning and budgeting ▪ Informs threat hunting ▪ Full integration into third-party security operations activities ▪ Incorporated into monitoring and SOAR processes ▪ Informs advanced cyber risk quantification modeling

5.4 Developing In-House Versus Developing with a Service Provider

Several considerations may affect the decision to develop a threat profile in-house or with the support of a service provider, including the following:

- Cost of engaging a service provider
- Availability of internal resources to take on a new project
- Timeline for profile development (service providers may enable faster development)
- Experience of internal resources in threat intelligence
- Intended use of the profile
- Number of threat profiles to be developed
- Feasibility of sharing sensitive information (inputs or final profile) with vendors

5.4.1 Developing In-House

Typically, this approach involves a small team of cybersecurity staff supplemented by information technology personnel and other relevant stakeholders. When possible, engage stakeholders from throughout the organization to help develop a more complete profile that represents the concerns of all. Section 5.1 includes a list of stakeholder groups for consideration.

Profile Development Tip

A single individual with knowledge of an organization's threat environment, technology systems, and cybersecurity program can produce a useful profile.

Many service providers offer off-the-shelf threat profiles that can catalyze development efforts. Consider this as a basis for building a tailored threat profile. Tailoring incorporates organization-specific factors such as unique operating conditions, specific assets used by the organization, or specific threats of concern.

5.4.2 Developing with a Service Provider

Utilizing a service provider can offer several advantages. These entities can offer established development methodologies and experienced personnel, which may help expedite profile creation and reduce the potential burden on internal resources.

However, engaging a service provider may pose challenges. The selected provider may lack sufficient expertise in the organization's specific industry. Their services may be cost-prohibitive. And, though a service provider may relieve some of the development burden, internal staff will still need to review and validate the deliverables. Additionally, fully outsourcing the effort might decrease opportunities for internal collaboration and learning, which can be a meaningful benefit of profile development.

The range of service providers is vast. One or more of the following key considerations can help guide selection:

- The service provider has a current and comprehensive understanding of the cybersecurity threats relevant to the organization.
- The service provider currently supplies cybersecurity support services, such as staffing an organization's security operations center or providing managed detection and response capabilities. Such a service provider is more likely to have sufficient knowledge of the organization's threat environment which is necessary to quickly provide substantial input to the process.
- The service provider has verifiable expertise in creating and implementing threat profiles. This includes organizations that have access to or operate threat intelligence platforms that can provide inputs to development efforts.

5.5 Identifying Threat Information Sources

Creating a viable threat profile requires sufficient knowledge of the organization's priorities, operations, and threat environment. This information can come from many sources. Focus on sources of information most relevant to the organization's unique sector, industry, and operating constraints.

5.5.1 Internal Sources

Review internal documents to help identify threats that should inform the threat profile. Example documents to consider include:

- Enterprise risk assessments
- Business impact analyses
- Risk registers
- Risk analysis criteria
- Risk management policies and strategy
- Incident response and continuity plans
- After-action reports from incidents and exercises
- Cybersecurity assessment and penetration testing reports
- Audit reports
- Exceptions to cybersecurity policies
- Known vulnerabilities and unapplied patches
- Compliance documentation

Consult key personnel, such as enterprise risk personnel, that may have insight into potential threat exposures. Review available reports of previous incidents that document the activities of threat actors or tactics that have been previously observed within the organization. Additionally, many organizations have internal threat intelligence teams that aggregate threat information from many sources, both internal and external, that can act as valuable input.

5.5.2 Threat Intelligence-Sharing Organizations

Participation in a threat intelligence-sharing organization may provide efficient access to threats of interest for a specific industry or another group. This includes, but is not limited to, highly structured organizations, such as sector-specific ISACs or less formal sources, such as peer groups. Information provided by sharing organizations may be enriched with additional considerations, such as the prevalence of attacks within a sector or observed TTPs.

5.5.3 Government and Community Resources

There are many no-cost government and community resources that provide substantial threat intelligence. Examples include:

- United States Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER) – information products for the energy sector, such as classified and unclassified threat briefings and reports
- United States Department of Homeland Security (DHS) CISA – guidance on security patches, analysis of emerging malware and threat actors, and the Known Exploited Vulnerabilities Catalog
- Federal Bureau of Investigation (FBI) – Internet Crime Complaint Center (IC3) and InfraGard Portal
- International cybersecurity information resources, such as United Kingdom National Cyber Security Centre reports and advisories, and European Union Agency for Cybersecurity (ENISA) Annual Threat Landscape reporting
- Vendor and community publications, such as security blogs, technical analysis bulletins, or annual threat reports

5.5.4 Threat Intelligence Subscription Services

Numerous threat intelligence service providers offer tailored intelligence services. Typically, the services are fee-based and can be integrated with the organization's cybersecurity architecture. Some data that these services provide is machine-readable for ingestion into automated detection and response tools. This type of information may not be immediately informative when constructing a threat profile.

5.5.5 Threat Frameworks

Threat frameworks classify and organize common TTPs. For example, the MITRE ATT&CK Framework is a "…globally accessible knowledge base of adversary tactics and techniques based on real-world observations" [MITRE 2023]. MITRE also catalogs groups defined as "activity clusters that are tracked by a common name in the security community" [MITRE 2024].

Frameworks provide a consistent foundation for creating, updating, and validating a threat profile, based on standard definitions and known TTPs. Frameworks also lend credibility that can help engage stakeholders.

6. DEVELOPING A THREAT PROFILE

Figure 5: Develop—Steps in the Threat Profile Development Process

The process for developing a threat profile varies significantly across organizations. The suggested approach in this document is an example starting point.

The high-level steps for developing a threat profile include:

- Step 1 – Identifying Organizational Functions and Potential Impacts
- Step 2 – Identifying, Describing, and Prioritizing Threat Scenarios
- Step 3 – Developing and Documenting Threat Scenarios
- Step 4 – Validating the Threat Profile

Profile Implementation Tip

Safeguard sensitive information throughout the threat profile development process.

Each step is discussed in detail in the following sections.

6.1 Step 1 – Identifying Organizational Functions and Potential Impacts

This step involves identifying the organizational functions to include in the profile and the potential impacts of highest concern for each function. Documenting this in table form helps facilitate brainstorming and establishes a map to guide the next step—identification of threat scenarios. This table is referred to in this document as a "threat scenario table". Table 9 is an example of a threat scenario table.

Table 9: Example—Threat Scenario Table

	Organizational Functions			
Potential Impacts	**Function 1**	**Function 2**	**Function 3**	**Function 4**
Potential Impact 1				
Potential Impact 2				
Potential Impact 3				

6.1.1 Identifying Organizational Functions

Functions are major operational processes or activities important to an organization. They include the business units, processes, and associated assets necessary to accomplish the mission of the organization. Functions may be defined by departmental boundaries, lines of business, product lines, facilities, systems, network security zones, groupings of assets, or processes—including those managed by a third party. Remember that organizational functions may cross many organizational boundaries.

To begin identifying functions, consider the core mission of the organization, then identify the functions critical to achieving that mission. For example, a business that sells goods on the internet may have an organizational function of "Collection and Processing of Customer Orders." Or a natural gas utility may have a core function of "Delivery of Natural Gas to End-User Consumers."

A natural starting point is defining functions at the organizational-unit level. For example, a natural gas company may start with three functions: production, transmission, and distribution. Consider whether organizational units require further decomposition to more accurately characterize important processes and their unique risks. For example, the cyber threats confronting a natural gas production organization may differ significantly from those confronting a natural gas transmission or midstream operation. If needed, develop separate threat scenario tables (and consequently, separate threat profiles) *for individual organizational units or functions*.

6.1.2 Identifying Potential Impacts

Potential impacts are the consequences of a cyber attack. This includes effects on an organization's mission, goals, functions, or assets. Examples include loss of human life, operational disruption, or destruction of hardware. Review Section 5.5 for examples of information sources, such as enterprise risk assessments, that may serve as inputs to jumpstart this process.

Begin by developing a list of potential impacts that could feasibly be caused by a cyber attack—even if the impact is unlikely. Think broadly. Consequential exposures may exist behind the scenes as part of third-party systems, interdependent systems, shared services, or other operational dependencies. Focus on the most significant impacts. Five-to-seven high-priority potential impacts is a reasonable initial target.

Profile Development Tip

Further considerations for identifying impacts can be found in the United States Department of Energy Cyber-Informed Engineering (CIE) Implementation Guide *[DOE 2023], specifically in "Principle 1 Consequence-Focused Design" (pages 13-22).*

6.1.3 Creating a Threat Scenario Table

In this activity, potential impacts and organizational functions are arranged in table format to facilitate threat scenario identification. Table 10 is an example of this.

Table 10: Example—Threat Scenario Table with Potential Impacts and Organizational Functions

	Organizational Functions		
Potential Impacts	**Electricity Distribution**	**Natural Gas Distribution**	**Business Operations**
Loss of Life, Safety, or Health			
Operational Disruption			
Loss of Operational Control or Visibility			
Disclosure of Sensitive Data			

6.2 Step 2 – Identifying, Describing, and Prioritizing Threat Scenarios

Three key activities are performed in this step:

- Identifying Candidate Threat Scenarios
- Describing Candidate Threat Scenarios
- Prioritizing and Selecting Threat Scenarios

Additional details for each activity are included in the following sections.

6.2.1 Identifying Candidate Threat Scenarios

To identify candidate threat scenarios, examine the intersection of each function and impact in the threat scenario table. Consider how a cyber attack could produce that impact. While performing this activity it is important to adopt an adversary's perspective rather than a defender's. Think creatively and explore how unconventional or indirect attack methods might lead to a potential impact. Seek out potential attack vectors that may go overlooked such as cloud assets, artificial intelligence (AI) systems, inter-dependencies between systems, and the supply chain.

Using one or two sentences, document the threat scenarios that might occur at the intersection of each potential impact and organizational function. Focus on the most impactful scenarios that could feasibly occur, even if unlikely. Include impacts affecting

other functions, such as downstream effects on functions that depend on the selected function.

As an example, consider the intersection of the potential impact "Disclosure of Sensitive Data" and the organizational function "Customer Payment Processing." A plausible scenario that describes this combination is "Exfiltration of customer credit card information via web attacks on customer payment processing to damage company reputation." Table 11 shows this.

Table 11: Example—Candidate Threat Scenario

	Organizational Function
Potential Impact	**Customer Payment Processing**
Disclosure of Sensitive Data	Exfiltration of customer credit card information via web attacks on customer payment processing to damage company reputation

Some threat scenarios may feasibly result in multiple impacts (such as, loss of human life, financial loss, or reputational damage). In this case, document that scenario in the space associated with the most significant impact. As an example, if a scenario may cause loss of human life but also may cause financial loss, note it in the "loss of human life" space for each function in which it may be feasible. The purpose of this exercise is to identify the scenarios of highest concern. It is acceptable to omit less-significant impacts to simplify the profile.

Consider using the list of common cyber attack types in Appendix D to help generate ideas and stimulate conversation.

Profile Development Tip

An advanced profiling effort may warrant the use of a framework, such as the MITRE ATT&CK Framework [MITRE 2023], to support scenario identification. Appendix E includes a description of how the MITRE ATT&CK Framework may be leveraged for threat profile development.

Table 12 presents a notional example of a completed threat scenario table. Some fields may contain more than one candidate scenario, and some may state that no feasible scenario exists. Once this table is constructed, perform a review to refine scenarios and uncover potential gaps. This review may result in new scenarios or changes to existing scenarios.

Some scenarios raised during discussion may not be cyber in nature, such as physical threats, but may still warrant consideration or further action by the organization. Preserve all scenario concepts at this stage. Scenarios that may be of use to other groups, such as physical security teams or business continuity and disaster response planning teams, should be shared accordingly. Lower-priority cybersecurity scenarios may be useful for future iterations of the threat profile.

Table 12: Example—Threat Scenario Table with Candidate Threat Scenarios

Potential Impacts	Organizational Functions: Electricity Distribution	Natural Gas Distribution	Business Operations
Loss of Life, Safety, or Health	Nation-state threat actor targeting AG&E	Nation-state threat actor targeting AG&E	(1) Physical damage to communications and safety assets critical to facility building management systems (2) Ransomware attack affecting internal financial systems leading to an unexpected gap in insurance premium payment and temporary loss of employee health insurance coverage
Operational Disruption	(1) Ransomware attack affecting OT systems (may include attacks on IT systems that affect OT systems) (2) Supply chain compromise of control system PLCs	(1) Ransomware attack affecting OT systems (may include attacks on IT systems that affect OT systems) (2) Supply chain compromise of control system PLCs	(1) Ransomware attack affecting IT systems, such as email, telephone, network connectivity (2) Supply chain compromise affecting IT software with high-level access privileges (3) Denial-of-Service attack on customer payment website
Loss of Operational Control or Visibility	(1) Malware compromise of jump hosts in industrial DMZ (2) Interference with long-range wireless communication (3) Widespread physical damage to communications assets that OT systems use	(1) Malware compromise of jump hosts in industrial DMZ (2) Interference with long-range wireless communication (3) Widespread physical damage to communications assets that OT systems use	Malware compromise affecting critical support functions such as telephone, network, or email
Disclosure of Sensitive Data	Ransomware attack that results in the release of customer information	No scenario	Ransomware attack that results in the release of customer information

6.2.2 Describing Candidate Threat Scenarios

In this part of Step 2, prepare for prioritization of the candidate threat scenarios in the threat scenario table. For each scenario add a title, brief description, and list of potential impacts. Do not provide additional details until prioritization is complete.

Table 13 shows an example list of candidate threat scenario titles, descriptions, and potential impacts.

Table 13: Example—List of Candidate Threat Scenarios

Threat Scenario Title	Description	Potential Impacts
Supply Chain Compromise Impacting Gas Control PLCs—Natural Gas Distribution	A threat actor gains access to vendor systems and leverages that access to remotely modify the configuration of natural gas distribution control PLCs.	Loss of life, safety, and health if customer supply of natural gas is disrupted, especially during heating season.
Malware Compromise of Jump Hosts in Industrial DMZ—Electricity Distribution	A threat actor compromises jump hosts in the industrial DMZ via malware. As a result, engineers are unable to remotely access OT assets from the enterprise network.	Loss of operational visibility or control.
Ransomware Attack—Business Operations	Ransomware delivered via a phishing email encrypts data and renders business operations workstations inoperable.	Inability to perform critical business operations such as making and receiving payments. Potential ransom payment to threat actor in exchange for a decryption key.

6.2.3 Prioritizing and Selecting Threat Scenarios

The objective of this activity is to select the highest-priority scenarios to include in the threat profile. The threat profile may guide many cyber and non-cyber activities within the organization. Thus, effective prioritization is important to ensure that resources are dedicated to the most important threats.

Ideally, the final list contains a small number of scenarios: between 10 and 12. Keep in mind that the *development* of each threat scenario is time-intensive, so larger lists may require a substantial resource investment.

Start with a review of internal documents, such as those listed in Section 6.1.2, to ensure the prioritization process and criteria align with organizational priorities. Then, engage appropriate stakeholders, such as enterprise risk management, operations, or legal team members.

Selecting the right decision-making method can streamline prioritization and improve results. A practical approach is to host a workshop where participants vote to assign priorities. Voting may consist of participants selecting their top three scenarios or using a balanced scorecard [Harvard 1996] to rate multiple factors, such as asset criticality and degree of impact, for each scenario. The weighting value *balances* the final score toward the most important factors. Example factors include:

- Criticality of impacted assets
- Degree of impact on resilience and cybersecurity priorities, such as safety or operational priorities
- Cost to mitigate
- Cost and time to recover
- Knowledge that a potential threat actor may target your organization
- Susceptibility of the organization to the scenario, that is, threat scenarios more likely to be successful may take higher priority
- Likelihood that a threat actor will execute the cyber attack

Likelihood is noted above as a potential factor for prioritization and may arise as part of the discussion. Several techniques exist to estimate likelihood; many estimation techniques require extensive effort. Consider a simple approach, such as a group exercise where participants rank scenarios from most to least likely.

Table 14 shows an example of voting results from a process in which six subject matter experts (SMEs) each cast three votes. In this example, SMEs cast votes for the scenarios they believe have the greatest potential impact on the organization. The list is then sorted by the number of votes received. Participants then select the final list of scenarios that move forward in the threat profile development process. For brevity, not all scenarios are included in Table 14. In practice, include all scenarios.

Table 14: Example—Threat Scenario Prioritization Results

Threat Scenario Title	Votes
Nation-State Threat Actor Targeting AG&E—Electricity Distribution	4
Ransomware Impacting Operational Technology Assets—Natural Gas Distribution	3
Supply Chain Compromise Impacting Gas Control PLCs—Natural Gas Distribution	2
Physical Damage to Communications Assets Critical to Facility Building Management Systems—Business Operations	2
Malware Compromise of Jump Hosts in Industrial DMZ—Natural Gas Distribution	2
Interference with Long-Range Wireless Communication—Electricity Distribution	2
Ransomware Attack Affecting Internal Financial Systems Leading to Unexpected Gap in Insurance Premium Payment and Temporary Loss of Employee Health Insurance Coverage—Business Operations	1
Widespread Physical Damage to Communications Assets That OT Systems Use—Natural Gas Transmission	1
Ransomware Attack that Results in Release of Customer Information—Electricity Distribution	1
Denial-of-Service Attack on Customer Payment Website—Business Operations	0
Malware Compromise Affecting Critical Support Functions, Such as Telephone, Network, and Email—Business Operations	0

6.3 Step 3 – Developing and Documenting Threat Scenarios

After selecting threat scenarios to be included in the profile, populate each data element in them. Table 15 includes an objective, relevant considerations, and examples for each data element. This is an iterative process, so it is likely that, during detailed development, some scenarios may be altered or eliminated and new scenarios added.

Table 15: Example—Objectives and Considerations for Each Threat Scenario Data Element

Element	Objectives and Considerations	Examples
Threat scenario title and description	**Objective:** Establish a brief title and description for the threat scenario. Use a consistent structure when developing titles and descriptions. ▪ What title best describes the threat scenario? ▪ What are the key pieces of information that clearly identify this scenario? ▪ What potential impacts might occur if the scenario were realized?	**Examples of Titles and Descriptions** ▪ Command and Control Attack – Supervisory Control and Data Acquisition (SCADA) System ▪ Denial-of-Service Attack – Customer Website ▪ Ransomware Attack – SCADA System ▪ Physical Damage – Electricity Distribution

Element	Objectives and Considerations	Examples
Targeted organizational function and related assets	**Objective:** Document the organizational function and related assets that might be affected by the attack. Consider how the disruption of the functions or assets would affect the organization's ability to meet its mission. ▪ Which functions and assets are most important to the organization's mission? ▪ Which functions and assets might this actor target directly? **Note:** This scenario element relates directly to the "organizational function" in the threat scenario table. Assets supporting the function may be added as needed to further develop sections and make the profile relevant.	**Examples of Functions and Assets** ▪ **Function:** Natural Gas Distribution ▪ **Assets:** OT network, email application, SCADA system, configuration files ▪ **Function:** Electronic medical records system ▪ **Assets:** Cloud-hosted databases, staff workstations, health records ▪ **Function:** Specialty chemical production ▪ **Assets:** Programmable logic controllers (PLCs), industrial tanks and mixers, configuration files
Potential impacts	**Objective:** Document the potential negative or unwanted impacts that could result from a cyber attack. Consider areas of impact such as life, safety, and health; operational disruption; reputational damage; economic loss; or legal penalties. Consider interdependent functions and other downstream impacts to other functions if the scenario were realized. ▪ What direct and indirect impacts could occur if the attack were successful? ▪ How would processes be impacted? ▪ How would assets be impacted? ▪ What long-term impacts to the organization's mission (regulatory, financial, reputational) may occur if the scenario were realized? **Note:** Quantitative estimates are not necessary but will help the organization establish a reference point for decision making, such as evaluating investments in cybersecurity controls.	**Examples of Impacts** ▪ Destruction of equipment would lead to five days of downtime. ▪ Loss of control would require a shutdown of natural gas transmission. ▪ Theft of component designs would lead to reduced revenue and impact market position. **Examples of Impacts Estimated Using Quantitative Measures** ▪ Reputation and lack of customer confidence results in a potential revenue loss of $250,000. ▪ Potential fines of approximately $500,000.

Element	Objectives and Considerations	Examples
Resilience and cybersecurity priorities	**Objective:** Detail the impact on requirements for resilience and cybersecurity as a result of the attack. ▪ How are the resilience requirements for safety, reliability, and performance affected by the attack? ▪ How are the cybersecurity requirements for confidentiality, integrity, and availability affected by the attack? ▪ What is the priority of each requirement?	**Examples of Requirements** ▪ **Primary:** Reliability of electricity transmission if SCADA communication is lost. ▪ **Secondary:** Availability of SCADA system.
Tactics, techniques, and procedures	**Objective:** Document the ways in which the cyber attack may be executed. Include only necessary details for the planned purpose of the profile. Consider using the common attacks provided in Appendix D – Common Cyber Attack Types or an attack framework, such as the MITRE ATT&CK Framework. ▪ What cyber attack method could be used? ▪ How would the attack initially be delivered?	**Examples of Tactics, Techniques, and Procedures** ▪ **Malware containing a rootkit:** A phishing email delivers a malware package that contains a rootkit to a third-party vendor with access to the organization's email system. The third-party vendor is logged on to the OT network and opens the email, exposing the network to the malware. The rootkit opens a backdoor to the SCADA system, which gives the threat actors the ability to control the system remotely.
Vulnerabilities	**Objective:** Document the known or perceived technical, procedural, or situational weaknesses that could enable a cyber attack to occur. ▪ What are some of the key weaknesses or vulnerabilities that might make the organization more susceptible to this type of attack? ▪ Is the attack more likely to succeed during specific times or operating states, such as non-business hours, system maintenance periods, holidays, or times of stress?	**Examples of Vulnerabilities** ▪ Uncontrolled or unmonitored vendor access to the OT network. ▪ The ability to use the IT-based email application while logged into the OT network. ▪ The OT network being able to communicate directly with the internet and other external applications. ▪ Failure to properly segment IT and OT networks. ▪ No training for employees and vendors on how to recognize and respond to phishing attacks.

Element	Objectives and Considerations	Examples
Key controls	**Objective:** Document the mitigations important to avoid or limit the effect of the scenario or TTPs. ▪ What *existing* controls are most important for this type of cyber attack? ▪ What controls should be *added in the future*? ▪ What controls address *common* TTPs for this type of cyber attack? ▪ What controls are critical for *preventing* this scenario? ▪ What controls are critical for *responding to* this scenario?	**Examples of Controls** ▪ Multi-factor authentication. ▪ Segmentation. ▪ Training and awareness campaigns focus on identification and reporting of phishing emails. ▪ Internet scans to look for identifiable patterns, such as certificates in use. ▪ Monitoring for anomalous changes to domain registrant information that may indicate compromise of a domain.
Potential actors	**Objective:** The types of actors that might execute the attack. Consider the example list of threat actors included in Table 3. ▪ What actors would have sufficient and reasonable motivation to attack our organization's key operational processes and assets?	**Examples of Actors** ▪ State-sponsored threat actor groups. ▪ Cybercrime gangs ▪ Hacktivists
Potential motives	**Objective:** Document the reasons why a potential actor might want to attack the organization. If needed, consider the example motivations included in Table 4. ▪ Do some threat actors have particularly strong motivations? ▪ Why would the actor execute the attack? ▪ Does the actor have more than one motivation?	**Examples of Motives** ▪ A state-sponsored threat actor group that is known to be testing their capabilities for gaining access to OT systems. ▪ Cybercrime gangs have been increasingly targeting critical infrastructure due to a perception of an increased likelihood of ransomware payments. ▪ A hacktivist group has persistently opposed the construction of a new pipeline. They have published online manifestos naming the organization as a target.

6.4 Step 4 – Validating a Threat Profile

Validation of the threat profile is important because it may drive many cybersecurity priorities, requirements, and actions. When determining what activities are needed to validate the profile, consider how it will be used and the impact it will have on the organization. A threat profile influencing many processes warrants more validation than a threat profile influencing few processes. Examples of processes that may be influenced by a threat profile can be found in Section 7.1.

Validating a profile may include many different types of activities. The following list includes a few examples.

- *Comparison to other sources of information* involves reviewing the profile against internal and external sources of threat information such as risk registers and threat advisories to confirm that the profile is complete and accurate. See Section 5.5 for examples of potential threat information sources.
- *Independent expert review* is evaluation by knowledgeable individuals who may or may not have been directly involved in profile development. This may include internal experts, such as team members from enterprise risk management, operations, or IT. This may also include external experts, such as vendors or peers from other organizations.
- *User walkthroughs* involve step-by-step performance of operational processes with users of the profile to verify that it works as intended. An example is walking through preparation of a quarterly risk report with enterprise risk management.
- *Simulated use* is testing the threat profile in a safe environment that mimics real-world use. Examples of this may include using historical data to test new monitoring alert rules or incorporating a threat scenario into an incident response exercise.

Validation may result in revisions to the profile. When these are complete the profile is ready for use.

7. USING A THREAT PROFILE

Figure 6: Use—Steps in the Threat Profile Development Process

A threat profile identifies and prioritizes the threats of highest concern to an organization. Thus, it is important to not only create a profile but to "institutionalize" it operationally within the organization, including existing cybersecurity and risk management activities. This means that the profile should be implemented and supported throughout the organization in such a way that it becomes part of the underlying fabric of the cybersecurity program and a guiding document for decision making.

A threat profile may contain sensitive information that requires restricted access. Consider how the profile should be protected. Also consider whether a separate version—without sensitive information—may be useful for broader distribution.

7.1 Using a Threat Profile to Inform Cybersecurity and Operations

Stakeholders from across the organization may find the profile useful for informing a broad range of activities, such as:

- Developing the cybersecurity program strategy
- Identifying, analyzing, and selecting responses to cyber risks
- Informing future cybersecurity investments
- Designing, configuring, and implementing a cybersecurity architecture
- Analyzing the security impact of changes within the organization
- Designing and engineering new projects [DOE 2024]
- Establishing requirements for vendors and managed service providers
- Developing and exercising incident response and business continuity plans
- Guiding cybersecurity training and awareness priorities
- Influencing other key cybersecurity activities, such as asset management, vulnerability management, patching, logging, or monitoring
- Guiding the agenda of cybersecurity committees, such as risk, change, or architecture review boards
- Supporting cybersecurity insurance acquisition and optimization
- Informing those outside of the cybersecurity team (such as leadership, risk management, operations, or legal) about the evolving threat environment
- Framing cybersecurity program accomplishments when communicating to board members and senior management

7.2 Protecting a Threat Profile

A profile may contain sensitive information because it establishes key threats, vulnerabilities, and the actions planned to mitigate cyber attacks. If disclosed, it may reveal weaknesses previously unknown to a threat actor or aid a threat actor in selecting tactics that would circumvent controls or response actions. Limit distribution of sensitive information from the profile to those with a need to know.

Many internal and external stakeholders may benefit from the information contained in the threat profile, such as high-priority threats or recommendations about key cybersecurity controls. Consider creating a summary version for broader sharing with internal and external stakeholders. This will facilitate distribution of useful information contained in the profile without sharing sensitive data further than necessary.

The organization's data classification, information protection, and other relevant policies should guide how to classify and protect the profile throughout its lifecycle; if not, this should be documented. An individual should be assigned accountability for stewardship and ongoing maintenance of the profile. Typically, the individual in this role has a position of authority with cybersecurity or risk management responsibilities such as the Chief Security Officer or the Chief Risk Officer. It may be practical to share this responsibility, especially in organizations with substantial IT and OT operations.

8. MAINTAINING A THREAT PROFILE

Figure 7: Maintain—Steps in the Threat Profile Development Process

8.1 Planning and Managing the Update Process

To be effective, a threat profile should be supported by a continuous development process. An organization's technology footprint—and thus, its attack surface—evolves over time. Additionally, the capabilities of threat actor groups are changing constantly and increasing in sophistication. Establish a periodic review cycle to ensure that the profile reflects the current state of assets and threat exposures. Involve relevant stakeholders who may have information that would necessitate changes to the profile.

Consider how the profile is being used and whether its content is appropriate to meet the demands of its users. Questions you may ask during this process include the following:

- How are users implementing the threat profile? Have they provided feedback?
- Does each scenario include enough information to adequately inform the processes for which it is being used? Is it actionable?
- Is there information in the profile that is no longer relevant or not being actively used?
- Is the profile manageable? For example, are there too many scenarios, or is there too much detail in any data elements?

In addition to a periodic review, identify the events that should trigger updates to the profile. These events vary by organization, but may include changes in organizational strategy, changes to organizational structure, changes to assets, updated threat intelligence, or internal cybersecurity incidents. As part of each update, revalidate the profile to ensure that it is still complete, accurate, and suitable for its intended use.

Consider how new versions should be distributed to users, and what information is needed to aid in implementing updated versions. Different users may require different information to understand the changes and identify actions that should follow from the update, such as updating cybersecurity monitoring alerts, updating vendor evaluation criteria, or changing cybersecurity awareness training material.

APPENDIX A – REFERENCES

[CISA 2024]
Cybersecurity and Infrastructure Security Agency (CISA). *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* February 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[CMU 2007]
Caralli, Richard; Stevens, James; Young, Lisa; and Wilson, William. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* CMU/SEI-2007-TR-012. Software Engineering Institute. 2007. https://doi.org/10.1184/R1/6574790.v1

[CMU 2016]
Caralli, Richard; Allen, Julia; White, David; Young, Lisa; Mehravari, Nader; and Curtis, Pamela. *CERT Resilience Management Model (CERT-RMM), Version 1.2*. Software Engineering Institute. 2016. https://insights.sei.cmu.edu/library/cert-resilience-management-model-cert-rmm-version-12/

[DOE 2022]
Adams, Joseph; Anjous, Shola; Batallones, Amy; Batz, Dave; Biddle, Howard; Bilak, Shawn; Brain, Steve; Bransky, Jonathan; Brausieck, Jeff; et al. *Cybersecurity Capability Maturity Model (C2M2) Version 2.1*. United States Department of Energy. Office of Cybersecurity, Energy Security, and Emergency Response (CESER). June 2022. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[DOE 2023]
Anderson, Robert; Atkins, Victor; Ayala, Marco; Baker, KatherineAnne; Barnes, Lance; Castillo, Krystel; Chanoski, Samuel; Cox, Joel; Edsall, Robert; et al. *Cyber-Informed Engineering Implementation Guide*. United States Department of Energy. Office of Cybersecurity, Energy Security, and Emergency Response (CESER). September 2023. https://www.osti.gov/servlets/purl/1995796

[Harvard 1996]
Kaplan, Robert S., and David P. Norton. *The Balanced Scorecard: Translating Strategy into Action*. Boston: Harvard Business School Press, 1996. ISBN 978-0-87584-651-4. https://www.hbs.edu/faculty/Pages/item.aspx?num=8831

[MITRE 2020]
Alexander, Otis; Mi-Hye Belisle; & Steele, Jacob. *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy*. The MITRE Corporation. 2020. https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf

[MITRE 2023]
The MITRE Corporation. *The MITRE ATT&CK Framework*. 2023. https://attack.mitre.org/

[MITRE 2024]
The MITRE Corporation. *The MITRE ATT&CK Groups*. 2024. https://attack.mitre.org/groups/

[NIST 2018]
National Institute of Standards and Technology (NIST). *Glossary.* "threat" definition. https://csrc.nist.gov/glossary/term/threat

[NIST 2024]
National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF) 2.0.* February 2024. https://doi.org/10.6028/NIST.CSWP.29

[Splunk 2023]
Bianco, David; Fetterman, Ryan; Marrone, Sydney. *The PEAK Threat Hunting Framework*. Splunk. 2023. https://www.splunk.com/en_us/blog/security/peak-threat-hunting-framework.html

APPENDIX B – GLOSSARY

The following table defines terms used in this document.

Term	Definition	Source
asset	Something of value to the organization, typically, people, information, technology, and facilities that enable organizations to carry out their mission.	CERT-RMM v1.2
cyber attack	An unauthorized attempt by a threat actor conducted via cyber means to access, change, disrupt, or use the assets of an individual or an organization.	DOE Cybersecurity Threat Profile Development Guide
cybersecurity controls	Actions that an organization may take to help prevent or reduce the impact of cybersecurity incidents.	DOE Cybersecurity Threat Profile Development Guide
cybersecurity threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial-of-service. Common cyber threats include ransomware, malware, social engineering, denial-of-service, or the actions of insiders.	Adapted from NIST Computer Security Resource Center Glossary
function	Functions are major operational processes or activities important to an organization. They are the business units, processes, and associated assets necessary to accomplish the mission of the organization. They might include departments, lines of business, distinct facilities, network security zones, groupings of assets, or processes, including those that may be managed by a third party. For C2M2 users, “function” is synonymous with the C2M2 model definition.	DOE Cybersecurity Threat Profile Development Guide
information assets	Information of value to the organization, such as intellectual property, customer information, contracts, security logs, metadata, set points, or operational data. Information assets may be in digital or non-digital form.	Adapted from CERT-RMM

Term	Definition	Source
information technology (IT)	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. This includes interconnected or interdependent business and technology systems and the environment in which they operate.	DOE RMP
key controls	Important actions to help prevent or reduce the impact of the scenario. This may include current and planned controls.	DOE Cybersecurity Threat Profile Development Guide
MIL	A measure of the cybersecurity maturity of an organization in a given domain of the model. The model currently defines four maturity indicator levels (MILs). Each of the four defined levels is designated by a number (0 through 3) and a name, for example, "MIL3: managed." A MIL is a measure of the progression within a domain from individual and team initiative, as a basis for carrying out cybersecurity practices, to organizational policies and procedures that institutionalize those practices, making them repeatable with a consistently high level of quality. As an organization progresses from one MIL to the next, the organization will have more complete or more advanced implementations of the activities in the domain.	C2M2
operational technology (OT)	OT assets refer to assets that are on the OT segment of the organization's network and are necessary for service delivery or production activities. Examples include industrial control systems, building management systems, fire control systems, process control systems, safety instrumented systems, IoT devices, or physical access control mechanisms. Most modern control systems include assets traditionally referred to as IT, such as workstations that use standard operating systems, database servers, or domain controllers.	C2M2
potential actors	Individuals or groups that may execute a cyber attack described in a threat scenario.	DOE Cybersecurity Threat Profile Development Guide
potential impacts	The consequences of a cyber attack. This includes effects on an organization's mission, goals, functions, and assets. Examples include loss of human life, operational disruption, or destruction of hardware. For C2M2 users, potential impacts are synonymous with threat objectives.	DOE Cybersecurity Threat Profile Development Guide
potential motives	The reasons potential actors may have for attempting the actions described in a threat scenario.	DOE Cybersecurity Threat Profile Development Guide

Term	Definition	Source
resilience and cybersecurity priorities	The fundamental requirements necessary to achieve the mission and maintain the operating state of an organization.	DOE Cybersecurity Threat Profile Development Guide
tactics, techniques, and procedures	The actions that may be executed by a threat actor in the pursuit of a cyber attack.	Adapted from NIST SP 800-150
threat	See *cybersecurity threat*.	
threat actor	An individual or a group posing a threat.	NIST SP 800-150
threat environment	An understanding of an organization's operating environment and the threats that could potentially impact the organization. Threats may range from general attack trends to threat actor campaigns targeting a specific sector.	DOE Cybersecurity Threat Profile Development Guide
threat hunting	Proactively searching for cybersecurity incidents that other detection methods may have missed.	The PEAK Threat Hunting Framework—adapted from [Splunk 2023]
threat objective	The potential impacts of threat actor activities that are of concern because they would have negative impacts on the organization. For C2M2 users, threat objectives are synonymous with potential impacts.	C2M2 V2.1
threat profile	A characterization of the likely intent, capability, and targets for threats to the function. It is the result of: ▪ One or more threat assessments throughout the range of feasible threats to the IT, OT, and information assets of an organization and to the organization itself ▪ Identifying feasible threats ▪ Describing the nature of the threats ▪ Evaluating their severity ▪ Determining their priority A threat profile is composed of one or more threat scenarios.	C2M2 V2.1
threat scenario	A description of a situation in which a threat is realized. A threat scenario details important characteristics of a threat, such as vulnerabilities, potential impacts, potential actors, potential motives, or tactics, techniques, or procedures.	DOE Cybersecurity Threat Profile Development Guide

Term	Definition	Source
threat scenario table	A grid that includes the potential impacts (in the left-most column), organizational functions (in the first row), and threat scenarios of concern (intersections of rows and columns). A threat scenario table is one of many tools that may be used to facilitate brainstorming, documentation, and selection of threat scenarios for inclusion in the threat profile.	DOE Cybersecurity Threat Profile Development Guide

APPENDIX C – ACRONYMS

Term	Definition
APT	advanced persistent threat
C2	command and control
C2M2	Cybersecurity Capability Maturity Model
CESER	The Office of Cybersecurity, Energy Security, and Emergency Response
CIE	Cyber-Informed Engineering
CISA	Cybersecurity and Infrastructure Security Agency
CSF	Cybersecurity Framework
CVE	common vulnerabilities and exposures
DDoS	distributed denial-of-service
DHS	Department of Homeland Security
DMZ	demilitarized zone
DOE	Department of Energy
DoS	denial of service
DNS	domain name system
DoS	denial-of-service
EDR	endpoint detection and response
ENISA	European Union Agency for Cybersecurity
FBI	Federal Bureau of Investigation
IC3	Internet Crime Complaint Center
ICS	Industrial control system
iOS	iPhone Operating System
IoT	internet of things
ISAC	Information Sharing and Analysis Center
ISP	internet service provider
IT	information technology
MDR	managed detection and response
MIL	maturity indicator level
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques and Common Knowledge

Term	Definition
MSSP	managed security service provider
NIST	National Institute of Standards and Technology
OSTI	Office of Scientific and Technical Information
OT	operational technology
PLC	programmable logic controller
SCADA	supervisory control and data acquisition system
SIEM	security information and event management
SME	subject matter expert
SMS	Short Message Service
SOAR	security orchestration, automation, and response
SOC	security operations center
SQL	Structured Query Language
TTP	tactics, techniques, and procedures
UDP	user datagram protocol
XSS	cross-site scripting

APPENDIX D – COMMON CYBER ATTACK TYPES

Cybersecurity vendors often publish lists of common cyber attacks based on research data from real-world customer experiences. Table 16 lists common types of cyber attacks that may serve as a starting point for creating a threat profile.

Table 16: Common Cyber Attacks and Associated Methods

Attack Name	Description	Common Attack Methods
Denial-of-Service 	Consuming network bandwidth or system resources to the extent that a network or system is unresponsive.	Denial-of-Service (DoS) Attack, Distributed Denial-of-Service (DDoS) Attack
Identity and Password Attacks 	Gaining unauthorized access to resources with previously compromised credentials, automated password guessing techniques, password cracking tools or other identity- and credential-based techniques.	Kerberoasting, machine-in-the-middle attack, pass-the-hash attack, credential stuffing, password spraying, brute force, dictionary attack
Insider Threats 	Intentional or unintentional actions performed by trusted parties, such as employees, former employees, or contractors.	Misuse of privileged accounts, collusion, exposure of confidential information, accidental misuse or misconfiguration
Malware 	Computer code that performs an action that aids a threat actor in the pursuit of a cyber attack.	Spyware, adware, trojans, worms, rootkits, keyloggers
Ransomware 	Locking a system or encrypting data with malware to coerce payment from victims. These attacks are often combined with threats of data disclosure.	Crypto ransomware, locker ransomware, ransomware-based extortion
Social Engineering and Spoofing 	Using false information to mislead victims into revealing information or performing an action that would—unknowingly to them—aid in a cyber attack.	Phishing, spear phishing, whaling, smishing, vishing, pretexting Domain Name System (DNS) spoofing, website spoofing, email spoofing, business email compromise, message redirection and data interception

Attack Name	Description	Common Attack Methods
Supply Chain Attacks 	Compromise of vendors or other third parties that aids a threat actor in the pursuit of a cyber attack. Examples include inserting malicious code in third-party applications, compromised hardware, or targeting vendor access methods to enable a cyber attack.	Software-based supply chain attacks, hardware-based supply chain attacks
Cloud-Based Attacks 	Exploiting cloud services, storage, or applications to steal data, disrupt systems, gain unauthorized access, or spread malware across cloud environments.	Exploiting misconfigured resources or insecure Application Programming Interfaces (APIs), identity-based attacks, DoS or DDoS
Artificial Intelligence 	Using Artificial Intelligence (AI) tools or targeting AI systems to steal data, bypass security controls, generate convincing scams, accelerate vulnerability discovery and exploit development, or automate cyberattacks at greater speed and scale.	**Attacks using AI:** Automating attacks, accelerating vulnerability discovery, exploit chaining, deepfake impersonation, AI-assisted phishing **Attacks on AI systems:** Prompt injection, data poisoning, model evasion
Web Attacks 	Using malicious code to extract information from websites or inserting malicious code into a website.	SQL Injection, Cross-Site Scripting (XSS), Malvertising, Session Hijacking

APPENDIX E – APPLYING THE MITRE ATT&CK FRAMEWORK

E.1 Introduction

Appendix E provides guidance on using the MITRE ATT&CK Framework for threat profile development. This appendix presents a simplified example approach and may be useful for organizations that have not implemented MITRE ATT&CK and want to do so as part of threat profile creation. It presents a process that is modular, easy to follow, and pulls together several MITRE ATT&CK capabilities and tools.

E.2 Background

To implement the MITRE ATT&CK Framework, it is important to understand what it is, why use it, and which of the three ATT&CK frameworks should be used.

E.2.1 What Is the MITRE ATT&CK Framework?

The MITRE Corporation defines the framework as

> *…a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.* [MITRE 2023]

In threat profile development, the MITRE ATT&CK can help provide structure for analysis of many different elements of threat scenarios.

E.2.2 Why Use MITRE ATT&CK?

The MITRE ATT&CK Framework presents a standardized taxonomy for analyzing and communicating threat actors behaviors. This provides three primary benefits:

- *Process Maturity* Applying an established, standardized taxonomy facilitates maturation and standardization of processes. This can help enable more consistent and reliable outcomes and decision making.
- *Accuracy and Completeness* MITRE ATT&CK includes an industry-vetted inventory of TTPs. This can help ensure consideration of the full landscape of threat actor behaviors. Additionally, the taxonomy included within ATT&CK can facilitate in-depth analysis—such as frequency analysis—by providing a classification system for commonly observed behaviors.
- *Interoperability* MITRE ATT&CK is widely used and integrated into many tools. This can help translate threat profile outputs further into more processes and across internal and external stakeholder groups.

E.2.3 Selecting the Right MITRE ATT&CK Framework

MITRE ATT&CK offers three frameworks: Enterprise, Mobile, and ICS.

- *Enterprise* focuses on IT systems using Windows, Linux, and Mac operating systems.
- *Mobile* focuses on Android and iOS devices.
- *ICS* stands for Industrial Control Systems and focuses on targets and activities that may be part of operational technology. An example of ICS is the "Industroyer" software which "has the capability to issue Unauthorized Command Messages (T0855) to change the state of electrical substation switches and circuit breakers directly."

Select the appropriate framework according to the types of assets in-scope for threat profile development.

MITRE ATT&CK for Industrial Control Systems: Design and Philosophy describes the originating concept for the framework and provides additional details about its development [MITRE 2020].

E.3 Organization of This Appendix

This appendix follows the same process described in the body of the Cybersecurity Threat Profile Development Guide, and suggests modifications to incorporate MITRE ATT&CK. Although all processes may be affected, discussed here is a sample of processes that may benefit most from integration of the MITRE ATT&CK Framework. They are highlighted in bold in Figure 8 and included in the following list.

- *Develop*
  - Identifying, Describing, and Prioritizing Threat Scenarios
  - Developing and Documenting Threat Scenarios
  - Validating a Threat Profile
- *Use*
  - Using a Threat Profile to Inform Cybersecurity and Operations

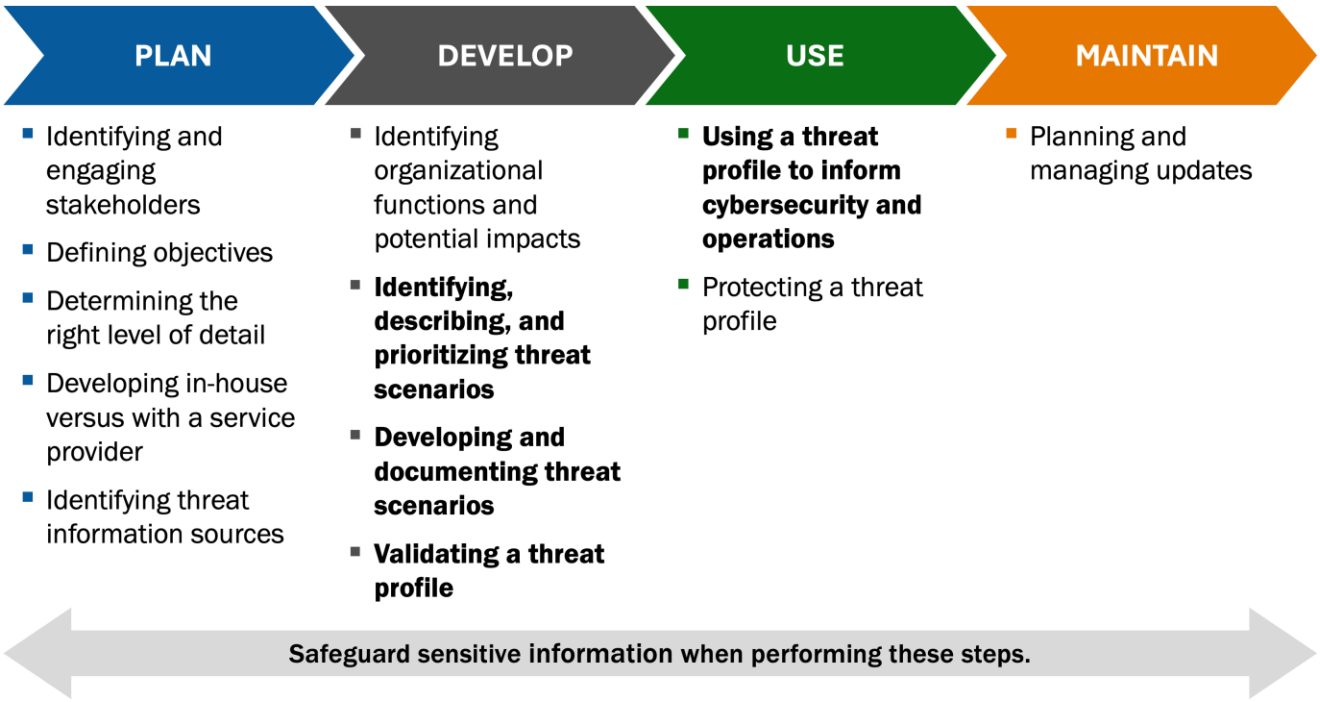

Figure 8: Threat Profile Development Processes Discussed in This Appendix

E.4 Identifying, Describing, and Prioritizing Threat Scenarios

The threat profile subprocess *Identifying, Describing, and Prioritizing Threat Scenarios* is part of the *Develop* process and includes the three additional subprocesses shown in Figure 9.

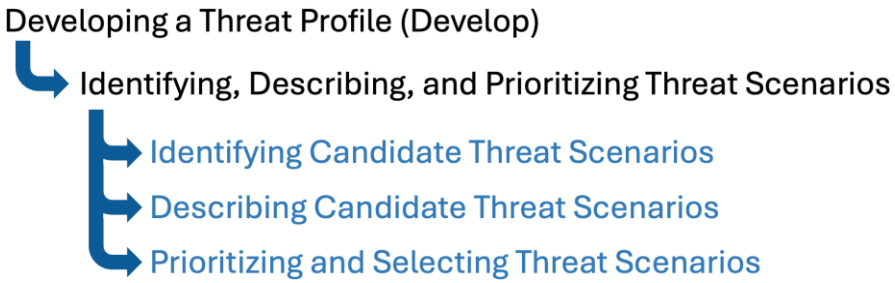

Figure 9: Subprocesses of *Identifying, Describing, and Prioritizing Threat Scenarios*

Integration of MITRE ATT&CK with each of the three aforementioned subprocesses is discussed in detail in the following sections.

E.4.1 Identifying Candidate Threat Scenarios

At this point in the threat profile development process an organization has identified the functions and impacts of highest concern and captured this information in table format, referred to as a threat scenario table. Table 17 shows an example threat scenario table.

Table 17: Example—Threat Scenario Table with Potential Impacts and Organizational Functions

	Organizational Functions		
Potential Impacts	**Electricity Distribution**	**Natural Gas Distribution**	**Business Operations**
Loss of Life, Safety, or Health			
Operational Disruption			
Loss of Operational Control or Visibility			
Disclosure of Sensitive Data			

To integrate MITRE ATT&CK in this process, use the MITRE ATT&CK Framework as a brainstorming aid to help populate the threat scenario table. Along with others participating in the identification process, review the Framework *Tactics* and *Techniques* to help stimulate discussions about how hackers may achieve potential impacts. Start with *Tactics*, then move to *Techniques* of interest.

Because the framework includes approximately 200 *Techniques*, it may be useful to incorporate strategies to simplify the process. Consider prioritizing or preselecting *Tactics* and *Techniques* in advance by reviewing threat advisories, potential vulnerabilities of concern within the organization, or reports that aggregate observed threat actor behaviors (such as "top 10" reports).

E.4.2 Describing Candidate Threat Scenarios

The purpose of this step is to prepare candidate threat scenarios for prioritization. This is accomplished by adding enough descriptive information to enable those participating to understand each scenario and its potential impacts. *Techniques* in the MITRE ATT&CK Framework include procedure examples as well as references to reports and advisories that summarize the situations and impacts related to prominent historical cyber attacks. If, during scenario brainstorming, discussion about impacts begins to stall, these resources may help to rekindle the conversation with real-life examples. Note that to find this information on the MITRE ATT&CK, select a *Technique* and scroll down to the *Procedure Examples* and *References* sections.

E.4.3 Prioritizing and Selecting Threat Scenarios

This step is focused on selecting the highest priority threat scenarios to include in the profile. The MITRE ATT&CK Framework is a knowledge base that can help answer questions that arise during this discussion. Review *Techniques*, *Procedure Examples*, and *References* for additional information about how a cyber attack may occur and impact an organization. Consider reviewing *Mitigations* and *Detection* to identify controls not in place (or not fully in place) that may make some scenarios a higher priority than others with stronger controls. Additionally, consider reviewing reports that aggregate observed threat actor behaviors (such as "top 10" reports) to identify prevalent techniques that may increase the priority of some scenarios.

E.5 Developing and Documenting Threat Scenarios

The focus of this subprocess is to document relevant information for each threat scenario data element, such as Key Controls, Vulnerabilities, or Potential Impacts. Information in MITRE ATT&CK Framework *Techniques* may be useful for the development of the following data elements:

- *Key Controls* Information about potential controls can be found in *Mitigations* and in *Detection*.
- *Vulnerabilities* MITRE ATT&CK *Techniques* include descriptions, *Procedure Examples*, and *References* that explain how adversaries carried out prominent historical attacks. This may be of use in identifying and prioritizing vulnerabilities related to each threat scenario.
- *Potential Actors* *Procedure Examples* and *References* identify threat actor groups that have been observed using each technique. This information may be useful when defining the "Potential Threat Actors" data element for each scenario.
- *Potential Impacts* The *References* section provides information about the impacts of previous real-world cyber attacks.

E.6 Validating a Threat Profile

The purpose of threat profile validation is to make sure the profile is relevant, accurate, and complete. Similar to using the MITRE ATT&CK Framework for developing threat scenarios, MITRE ATT&CK can be used to validate a threat profile. This may include gaps or inaccuracies in specific data elements (such as key controls) or entire threat scenarios that may be missing. Start by reviewing the MITRE ATT&CK *Tactics* and *Techniques*—as a whole—to help identify missing scenarios that may be caused or enabled by tactics or techniques that were not already considered. Then, as needed, review individual scenario data elements against corresponding MITRE ATT&CK elements. For example, review key controls against MITRE ATT&CK *Mitigations*.

E.7 Using a Threat Profile to Inform Cybersecurity and Operations

There are several ways that the MITRE ATT&CK Framework can support use of a profile within day-to-day cybersecurity activities and operations. Examples include:

- *Cybersecurity tool integration* Many popular cybersecurity tools support the MITRE ATT&CK taxonomy, which can speed implementation and bring focus to TTPs of concern captured in the profile.
- *Threat advisories* Many threat advisories incorporate ATT&CK technique identification numbers, which you can compare with techniques included in the threat profile.
- *Mitigations and detection activities* MITRE ATT&CK *Techniques* include potential cybersecurity controls in *Mitigations* and *Detection* sections. This information, combined with a threat profile, may aid in identifying and prioritizing potential mitigation and detection controls.
- *Communication* The community support and consensus among subject matter experts on the content in the MITRE ATT&CK Framework can add validity to the parts of your program that are aligned to MITRE ATT&CK. This, along with the real-world examples included in *Techniques*, can help bring to life discussions about cybersecurity threats and aid in making the case for strong cybersecurity protections.