Compounding Threat Trends on National Critical Infrastructure (v1)

Date: December 6, 2024
Final Paper

Sandia National Laboratories
Lead:
Cyrus-Jian Bonyadi (cbonyad@sandia.gov)

Problem Mentors:
Ruby Booth (rbooth@sandia.gov)
Jason Reinhardt (jcreinh@sandia.gov)
Danielle Jacobs (djacob@sandia.gov)

Mercy University
Advisor:
Zhixiong Chen (zchen@mercy.edu)

Students:
Ruth Kolo (rkolo@mercy.edu)
Bhusan Ulak (bulak@mercy.edu)
Wensael Jean Marie (wjeanmarie@mercy.edu)
Jahmari Moodie (jmoodie4@mercy.edu)
Kripesh Acharya (kacharya@mercy.edu)
Jason Culpepper (jculpepper@mercy.edu)

MERCY UNIVERSITY

Abstract 1

Introduction 4

Purpose 5

Problem statement 5

Methodology Assumption 6

By default, assume no risk 6

Threats are not isolated 6

Threats are context specific 6

Threats amplify with intent 6

Some NCFs are at increased threat from some actors 7

Low risk threats can escalate into higher risks 7

Use cases 7

Use Case 1: Austin Energy's Substation Infrastructure – Seaholm Substation 8

Step 1: For Each Asset 8

Step 2: For Each Threat 8

Step 3: Location Overlap Analysis 9

Use Case 2: New York Metropolitan Transportation Authority (MTA) Subway System 9

Step 1: For Each Asset 9

Step 2: For Each Threat 10

Step 3: Location Overlap Analysis 10

Methodology Input 11

Threat 11

Asset 11

Methodology Background Data 11

Category 12

Known Threat Actor Repositories 12

Intent 14

CISA Infrastructure Data Taxonomy 15

CISA Regions 15

National Critical Functions Set (NCFs) 16
Risk Levels 16
Incidents 17
CVE 18
Known exploited vulnerabilities 18
Methodology 19
Visual 19
Overview 19
Methodology Output 21
Likelihood 22
Conclusion 22
Next steps 23
Future considerations and Refinement 23
References 24

MERCY UNIVERSITY

Abstract

In this report, we present a comprehensive framework designed to assess and prioritize threats to national critical infrastructure. The framework integrates various threat types digital, physical, and human by evaluating factors such as asset characteristics, threat relevance, geographic alignment, and historical occurrences. The primary objective is to provide a systematic methodology for identifying and addressing the compounded effects of threats, ensuring a more resilient infrastructure.

This framework was developed using foundational data sources, including historical threat patterns, regional contexts, and asset criticality, with key assumptions focusing on the geographic and functional relevance of threats. We will first outline the assumptions that underpin the methodology, followed by a discussion of the use cases that helped shape its design. Finally, we demonstrate the application of this framework through detailed steps for asset and threat analysis, including the likelihood-based prioritization of identified risks. The report concludes with a discussion on the practical implications of using this framework to enhance risk management and guide mitigation efforts in critical infrastructure sectors.

Introduction

In the rapidly evolving landscape of cybersecurity, organizations face an increasingly diverse array of threats that span across digital, physical, and human domains. These threats, driven by varied actors and intents, present complex challenges that necessitate a structured approach to identifying, categorizing, and mitigating risks to critical assets. As organizations strive to safeguard their operations, the ability to accurately map relevant threats to specific assets becomes paramount, particularly in the context of ensuring efficient resource allocation and robust risk management strategies.

The proposed methodology addresses the critical need for a structured approach to evaluating and linking threats to assets by introducing a framework that categorizes and prioritizes threats based on their relevance and severity. This methodology systematically classifies threats into low, medium, or high categories before ranking them to identify the most critical threats to a given asset. By leveraging key attributes—such as the type of threat, the actor behind it, its intent, and its geographical or functional context—the framework ensures a detailed and targeted threat assessment. This approach allows for a nuanced understanding of vulnerabilities and operational priorities, providing a robust foundation for protecting critical assets.

MERCY UNIVERSITY

Purpose

This project identifies connections among human, digital, and physical threats to national critical infrastructures, focusing on how these threats can interact and amplify the overall risk landscape. By investigating interconnected threats, this methodology seeks to address current shortcomings in the threat portion of risk assessment approaches, providing organizations with improved methods to identify and manage a variety of potential risks. The goal is to develop a holistic framework that combines these threat factors, strengthening the resilience of critical infrastructures against complex and compounded threats.

Problem statement

The variety of threat assessment frameworks is robust, and their uses depend on the area of risk management and security, the industry, and the type of risk we need to address. Some of the most common frameworks are but not limited to Factor Analysis of Information Risk (FAIR), Information Systems Audit and Control Association (COBIT), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Risk Management Guide for Information Technology Systems from the National Institute of Standards and Technology (NIST) and Threat Agent Risk Assessment (TARA). These frameworks have been widely adopted and have helped organizations improve their security posture by offering clear steps to identify and manage risks.

Despite their utility, these frameworks **often treat digital, physical, and human risks as separate entities**. They do not always account for the complex interactions between these domains, particularly how threats can be coupled and amplified across them. Additionally, these frameworks are generally broad and may lack the granularity needed to address specific scenarios of threat coupling.

The real-world scenarios often involve multiple, interconnected threats. For example, hackers are more active during natural disasters. Durings hurricanes Sandy, hackers were more active on phishing and creating fake ads about benefits and insurance. Rather than treating risks as isolated incidents, our project aims to assess how threats from different domains (digital, physical, human) can interact and amplify one another. Unlike existing frameworks that often treat risks in isolation, our project focuses on assessing how threats across digital, physical, and human domains interact and amplify one another. By addressing these overlooked connections, we aim to fill a critical gap in current risk assessment methodologies, providing a comprehensive approach that better reflects the complexities of real-world threat landscapes.

MERCY UNIVERSITY

Methodology Assumption

There are several assumptions which guide the structure and influence the design of this methodology, ensuring the project remains focused on identifying and quantifying compounded threats across human, digital, and physical domains as they relate to critical infrastructure.

By default, assume no risk

By assuming null, we enable prioritization even at a baseline version of our analysis which simply decides “yes” or “no.” This may appear contradictory to the aims of this methodology, but this makes the proof of the methodology to identify when to turn no risk into a risk.

Threats are not isolated

We assume threats across different domains—human, digital, and physical—interact with one another, and this interaction can create compounded risks that are greater than the sum of individual risks. For instance, a digital malware attack that disables a security system may pave the way for a physical breach, while human error or malicious insiders can exacerbate both digital and physical vulnerabilities. The project assumes that understanding these connections is crucial to developing more accurate risk assessments.

Threats are context specific

Different organizations, sectors, and geographies experience unique threat landscapes. We assume risk assessments must be adaptable and context specific. A threat that is highly relevant in one sector, such as an advanced persistent threat (APT) in the financial industry, may have very different implications in the transportation or healthcare sectors. Another example can be that a hurricane is a high impact threat in CISA Region 4 than in CISA Region 8. The methodology assumes that threat interactions and risk amplification will vary based on factors like industry, geographical location, and asset type, requiring customized assessments.

Threats amplify with intent

Human threats can vary greatly in intent—ranging from deliberate sabotage by insiders to accidental errors made by staff. The methodology will differentiate between malicious and non-malicious threats, as this distinction is critical in assessing the severity, likelihood,

and amplification potential of threats across domains. For example, an ethical hacker may be a threat, but their likelihood to act may be influenced by a malicious intent.

Some NCFs are at increased threat from some actors

The National Critical Functions (NCF) framework provided by the Cybersecurity and Infrastructure Security Agency (CISA) can be used to map assets to the functions they perform. The NCF framework organizes critical infrastructures into functional groups, which allows this methodology to assess threats in a structured manner across different sectors. This will aid in developing threat coupling scenarios that are aligned with national security interests. If an asset serves one of the NCFs, we assume there is a greater risk.

Threats have historical patterns which may indicate future events

Historical data provides valuable insights into how threats evolve and intensify over time. By studying previous incidents, we can identify recurring patterns and trends in the behaviors of threat actors, the vulnerabilities they exploit, and the industries they target. For instance, a cyberattack technique that was initially isolated may become more widespread as attackers refine and reuse it. Similarly, certain natural disasters, like hurricanes or wildfires, may become more frequent or severe in specific regions due to environmental changes.

Low risk threats can escalate into higher risks

Several low-risk factors can converge and escalate into a high-risk scenario, particularly when compounded over time or performed in a sequence. In 2021, hackers exploited four separate zero-day vulnerabilities in Microsoft Exchange servers' Outlook Web Access (OWA), gaining unauthorized access to entire servers and networks, including emails and calendar data. Similarly, seemingly isolated incidents, such as minor human errors or small-scale cyber intrusions, may accumulate and cause a cascading effect, amplifying the overall risk. This assumption highlights the importance of not overlooking low-level risks, as their collective impact can significantly elevate the threat landscape.

Use cases

This section illustrates the application of the proposed methodology using two real-world scenarios to evaluate its effectiveness in categorizing and prioritizing threats to critical assets. The methodology has been tailored to determine threat relevance and severity, ultimately ranking threats to identify the most critical to specific assets. The selected use

cases represent diverse sectors, demonstrating the adaptability of the methodology across various operational and functional contexts.

Use Case 1: Austin Energy's Substation Infrastructure – Seaholm Substation

The Seaholm Substation, part of Austin Energy's infrastructure, is a critical energy distribution hub located in Austin, Texas, ensuring reliable energy delivery to residential, commercial, and industrial areas while integrating into Texas's broader energy network. This use case was chosen to evaluate the threats associated with energy infrastructure, as substations are frequently targeted by cyberattacks (e.g., SCADA vulnerabilities) and face physical threats like extreme weather events. Seaholm's localized significance and far-reaching implications for energy security and grid stability make it an ideal candidate for analyzing asset-threat relevance.

Step 1: For Each Asset

1.1 Identify Asset Location

- **Location**: Seaholm Substation is in Austin, Texas, Travis County.
- **CISA Region**: Region 6 (Southwest).

1.2 Check NCF Alignment

- **Taxonomy Check**: Cross-referenced with the Infrastructure Data Taxonomy.
- Seaholm Substation enacts critical energy transmission functions.
- **Result**: Relevant.

1.3 Check Known Exploited Vulnerabilities (CVE)

- **Known Exploited Vulnerabilities Database (CVE)**: Substations often rely on SCADA systems, which have known vulnerabilities. Check confirms SCADA software used by Seaholm Substation is in the CVE database.
- **Result**: Relevant.

Step 2: For Each Threat

2.1 Identify Threat Location

- **Threat Example**: Physical attack or cyber intrusion.
- **FEMA Index Check**: Public EM-DAT shows a history of natural disasters (e.g., hurricanes) impacting Texas, making physical threats relevant.
- **Result**: Relevant.

2.2 Determine Historical Use

- **Threat Actor Usage**: Cyber intrusions targeting substations (e.g., ransomware or ICS attacks) are well-documented globally, including in Texas.
- **Result**: Relevant.

2.3 Map Threat to CISA Region

- **Region**: Threat incidents in Texas are categorized under CISA Region 6.
- **Result**: Region 6 assigned.

Step 3: Location Overlap Analysis

3.1 Compare Asset and Threat Regions

- **Asset CISA Region**: Region 6.
- **Threat CISA Region**: Region 6.
- **Result**: Relevant.

3.2 Historical Analysis

- **Historical Threat Incidents in Region**: Natural disasters and cyberattacks have historically occurred in Texas (Region 6).
- **Result**: Relevant.

Overall Result for Seaholm Substation: **Relevant**.

Use Case 2: New York Metropolitan Transportation Authority (MTA) Subway System

The MTA Subway System in New York City is one of the largest public transportation systems in the world, consisting of 472 stations and over 6,000 subway cars, serving millions of commuters daily and acting as a lifeline for the city's economy and emergency response capabilities. This use case was chosen to analyze threats to large-scale public infrastructure, as urban transit systems are high-value targets for terrorism, cyberattacks, and natural disasters like flooding and storms. The MTA subway system's significance, combined with its exposure to diverse threats, makes it an ideal candidate for understanding and mapping threat scenarios for critical public transportation assets.

Step 1: For Each Asset

1.1 Identify Asset Location

- **Location**: MTA subway system operates in New York City, New York County.
- **CISA Region**: Region 2 (Northeast).

1.2 Check NCF Alignment

- **Taxonomy Check**: Cross-referenced with the Infrastructure Data Taxonomy.
- The subway system enacts critical public transportation functions.
- **Result**: Relevant.

1.3 Check Known Exploited Vulnerabilities (CVE)

- **Known Exploited Vulnerabilities Database (CVE)**: Transit systems may use software or communication networks vulnerable to cyberattacks. Confirmed vulnerabilities in transit control software.
- **Result**: Relevant.

Step 2: For Each Threat

2.1 Identify Threat Location

- **Threat Example**: Terrorism or natural disasters (e.g., flooding, storms).
- **FEMA Index Check**: Historical records in Public EM-DAT confirm flooding and severe storms impacting New York.
- **Result**: Relevant.

2.2 Determine Historical Use

- **Threat Actor Usage**: Terrorism targeting public transportation systems (e.g., subway bombings in 2005 London and Madrid) is well-documented.
- **Result**: Relevant.

2.3 Map Threat to CISA Region

- **Region**: Threat incidents in New York are categorized under CISA Region 2.
- **Result**: Region 2 assigned.

Step 3: Location Overlap Analysis

3.1 Compare Asset and Threat Regions

- **Asset CISA Region**: Region 2.
- **Threat CISA Region**: Region 2.
- **Result**: Relevant.

3.2 Historical Analysis

- **Historical Threat Incidents in Region**: Natural disasters and terrorism have historically occurred in New York (Region 2).
- **Result**: Relevant.

MERCY UNIVERSITY

Overall Result for MTA Subway System: Relevant.

Methodology Input

Before developing this methodology, we gathered some foundational input. These inputs are essential for understanding the fundamental data and the interactions between different threat domains.

Threat

Any activity or event that compromises the confidentiality, integrity, or availability of an organization's assets. It may be intentional, being carried out by threat actors such as hackers, or unintentional caused by natural disasters, system failures, or human error. Threat actions are designed or occur because of exploiting vulnerabilities, disrupting operations, natural occurrences, stealing data, or causing harm to an organization or individual.

Asset

A resource(s) considered valuable to an organization that requires protection. When conducting a risk assessment, the asset plays a vital role in determining the risk and impact.

Schema:

```
"properties": {
        "ID": "integer",
        "Name": "string",
        "Type": "string",
        "Value": "string",
        "Location": "string",
        "Protection Level": "string"
    }
```

Methodology Background Data

Background data are foundational elements that aid in evaluating the likelihood of threats. These inputs, such as historical threat patterns, asset criticality, intent, and regional factors, provide crucial context for the assessment process. They enhance the quality and accuracy of the risk analysis by offering insights into how threats interact, escalate, and compound across digital, physical, and human domains.

MERCY UNIVERSITY

Category

Category defines a domain. A classification of threat and a threat actor. It is important to classify a threat because the threat becomes **much higher risk when they interact** with a threat another classification.

Schema:

```
"properties": {
  "Id": {"type": "string"},
  "Name": {"type": "string"},
  "Description": {"type": "string"}
 }
```

Example:

ID	Name	Description
1	Digital	Software related
2	Physical	Natural disasters, Fire, Infrastructure damage, physical security
3	Human	People

Known Threat Actor Repositories

Microsoft categorizes threat actors into five key groups:

Nation-state actors: cyber operators acting on behalf of or directed by a nation/state-aligned program, irrespective of whether for espionage, financial gain, or retribution. Microsoft observed that most nation state actors continue to focus operations and attacks on government agencies, intergovernmental organizations, nongovernmental organizations, and think tanks for traditional espionage or surveillance objectives.

Financially motivated actors: cyber campaigns/groups directed by a criminal organization/person with motivations of financial gain and are not associated with high confidence to a known non-nation state or commercial entity. This category includes ransomware operators, business email compromise, phishing, and other groups with purely financial or extortion motivations.

Private sector offensive actors (PSOAs): cyber activity led by commercial actors that are known/legitimate legal entities, that create and sell cyberweapons to customers who then select targets and operate the cyberweapons. These tools were observed targeting and surveilling dissidents, human rights defenders, journalists, civil society advocates, and other private citizens, threatening many global human rights efforts.

Influence operations: information campaigns communicated online or offline in a manipulative fashion to shift perceptions, behaviors, or decisions by target audiences to further a group or a nation's interests and objectives.

Groups in development: a temporary designation given to an unknown, emerging, or developing threat activity. This designation allows Microsoft to track a group as a discrete set of information until we can reach high confidence about the origin or identity of the actor behind the operation. Once criteria are met, a group in development is converted to a named actor or merged into existing names.

We have curated a list of known human threat actors based on a list curated by Microsoft Defender Threat Intelligence.

Some other categories of threat actors are listed below:

Threat Actor	Targeted Assets	Motivations
Cybercriminals	Financial data, PII, intellectual property, corporate systems	Financial gain
Script Kiddies	Web applications, public-facing servers, IoT devices	Fame, curiosity, challenge
Hacktivists	Corporate websites, social media accounts, government systems, sensitive data	Promote political, social, or environmental ideologies
State-Sponsored Actors	Intellectual property, critical infrastructure, sensitive government data, supply chain systems	Espionage, political/economic advantage, destabilization of adversaries
Insider Threats	Company secrets, customer databases, IT infrastructure	Financial gain, revenge, ideological alignment
Advanced Persistent Threats (APTs)	National security systems, long-term network access, intellectual property	Long-term strategic advantages (political, military, economic)
Cyberterrorists	Critical infrastructure, government systems, public-facing systems	Spread fear, disrupt societal norms, advance extremist ideologies

Competitors	Intellectual property, customer data, financial data	Gain competitive advantage
Organized Crime Groups	Financial institutions, sensitive personal data, ransomable data	Financial gain through coordinated attacks
Lone Wolf Hackers	Specific systems or networks, high-profile targets	Personal challenge, fame
Thrill Seekers	Randomly selected targets, IoT devices	Adrenaline rush, curiosity, fun
Third-Party Vendors or Supply Chain Threats	Supply chain systems, credentials, access information	Varies (compromise or collusion)
Cyber Espionage Actors	Trade secrets, communication channels, critical industry insights	Intelligence for strategic advantage (economic or political)
Ideological Extremists	Public websites, media channels	Spread extremist beliefs, disrupt perceived adversaries

Intent

Intent is defined by two key properties: Malicious and Non-Malicious. Malicious intent involves actions aimed at causing harm, while non-malicious intent refers to actions that result in damage without harmful intentions. Recognizing these distinctions is crucial, as intent significantly influences the assessment and mitigation of risks within risk management strategies.

Schema:

```
"properties": {

    "ID": "integer",
    "Type": "string",
    "Description": "string"
}
```

Example:

ID	Type	Description
1	Malicious	Intentional damage

2	Non malicious	Nonintentional damage

CISA Infrastructure Data Taxonomy

The IDT Table of Contents serves as a quick reference of the taxonomy, in which infrastructure assets are categorized up to five levels. The first level is determined by broad infrastructure categories, which are then detailed further by increasingly granular differentiators as needed. The five levels of differentiation found within the IDT are the sector, sub-sector, segment, sub-segment, and asset type.

CISA Regions

We also integrate CISA region data to identify geographic areas in the United States where certain threats are more likely to occur. This regional context allows us to explore how threats may compound across interconnected systems within or across regions, helping us analyze potential compounding impacts. For example, a natural disaster in one region could weaken physical infrastructure and open vulnerabilities for digital or human-based threats, such as cyberattacks or social engineering. Identifying these interdependencies is critical for developing proactive risk management strategies.

Schema:

```
"properties": {
        "Region": "integer",
        "Locales": "string"
    }
```

Example:

Region	Locales
1	Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont
2	New Jersey, New York, Puerto Rico, U.S. Virgin Islands
3	Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia
4	Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee
5	Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin
6	Arkansas, Louisiana, New Mexico, Oklahoma, Texas
7	Iowa, Kansas, Missouri, Nebraska
8	Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming
9	Arizona, California, Hawaii, Nevada, Guam, American Samoa, Commonwealth of the Northern Mariana Islands
10	Alaska, Idaho, Oregon, Washington

MERCY UNIVERSITY

National Critical Functions Set (NCFs)

The National Critical Functions (NCFs) framework is designed to identify key properties of infrastructure categories and functions that are most at risk. These properties include Category, which classifies the type of function, and Functions, which specify the activities or services provided within each category. In our methodology, we intend to leverage this framework to systematically assess vulnerabilities, prioritize risk management efforts, and develop targeted mitigation strategies for critical infrastructure.

CONNECT	Connections by technologies that enable critical communications and capabilities to send and receive data (e.g., internet connectivity and satellite access)
DISTRIBUTE	Distribution methods that allow the movement of goods, people, and utilities inside and outside the United States (e.g., electricity distribution and cargo transportation)
MANAGE	Management processes that ensure our national security and public health and safety (e.g., managing hazardous material, conducting elections, and national emergencies)
SUPPLY	Supplies of materials, goods, and services that secure our economy (e.g., water and housing)

Schema:

```
"properties": {
        "Category": "string",
        "Functions": "string"
    }
```

Example:

Category	Functions
CONNECT	Operate Core Network
CONNECT	Provide Cable Access Network Services
DISTRIBUTE	Distribute Electricity
SUPPLY	Transport Cargo and Passengers by Road
MANAGE	Conduct Election

Risk Levels

Risk levels define the different levels of analytical sophistication in the treatment of uncertainties in risk analysis, and the possibility of transfer of experience across fields of application. It was published by M. Elisabeth Pate-Cornell at Department of Industrial Engineering and Engineering Management at Standford University, Stanford, CA, USA.

Since threats and risks are uncertain and each risk assessment differs on a case-to-case basis, we use the risk levels to develop risk assessments.

Schema:

```
"properties": {
        "LevelId": "integer",
        "Name": "string",
        "Description": "string",
        "Likelihood": "string",
        “Impact”: “string”
}
```

Example:

LevelId	Name	Description	Likelihood (Probability) Values	Impact Values
0	**Level 0**	Hazard Detection and Failure Modes Identification	Irrelevant, Relevant	Impact, No-impact
1	**Level 1**	Worst-Case Approach	None, Very High	No-impact, High-impact
2	**Level 2**	Quasi-Worst Cases and Plausible Upper Bounds	None, Very Low, Low, High, Very High	None, Minimal, Moderate, Significant, Severe
3	**Level 3**	Best Estimate	??	??
4	**Level 4**	Probabilistic Risk Assessment (Single Risk Curve)	??	??
5	**Level 5**	Probabilistic Risk Analysis (Multiple Risk Curves)	??	??

Incidents

Incidents that have occurred in the past provide valuable insights into historical threat trends, frequency, and impact, making them an essential component of our project. By reviewing where, when, and how threats have occurred in the past, we aim to identify patterns and recurring vulnerabilities across different infrastructures and regions.

Schema:

```
"properties": {
        "ID": "integer",
        "Name": "string",
        "Year": "integer",
        "CVEs": [“Id”: “string” ]
        "NCF": "string",
        "ThreatActor": "string",
    }
```

Example:

MERCY UNIVERSITY

ID	Name	Year	CVEs	NCF	Threat actor
1	Stuxnet	2009	CVE-2010-2772		Nation-State
2	Colonial Pipeline Attack	2021	CVE-2019-5544		Nation-State
3	Target data breach	2013	null		
4	Ukraine Power Grid	2015	null		
5	Cisco breach	2022	null		
6	CrowdStrike	2024	null		Insider
7	Exagrid ransomware attack	2021	null		
8	WannaCry	2017	CVE-2017-0147		
9	Code Red Worm	2001	CAN-2001-0500		

CVE

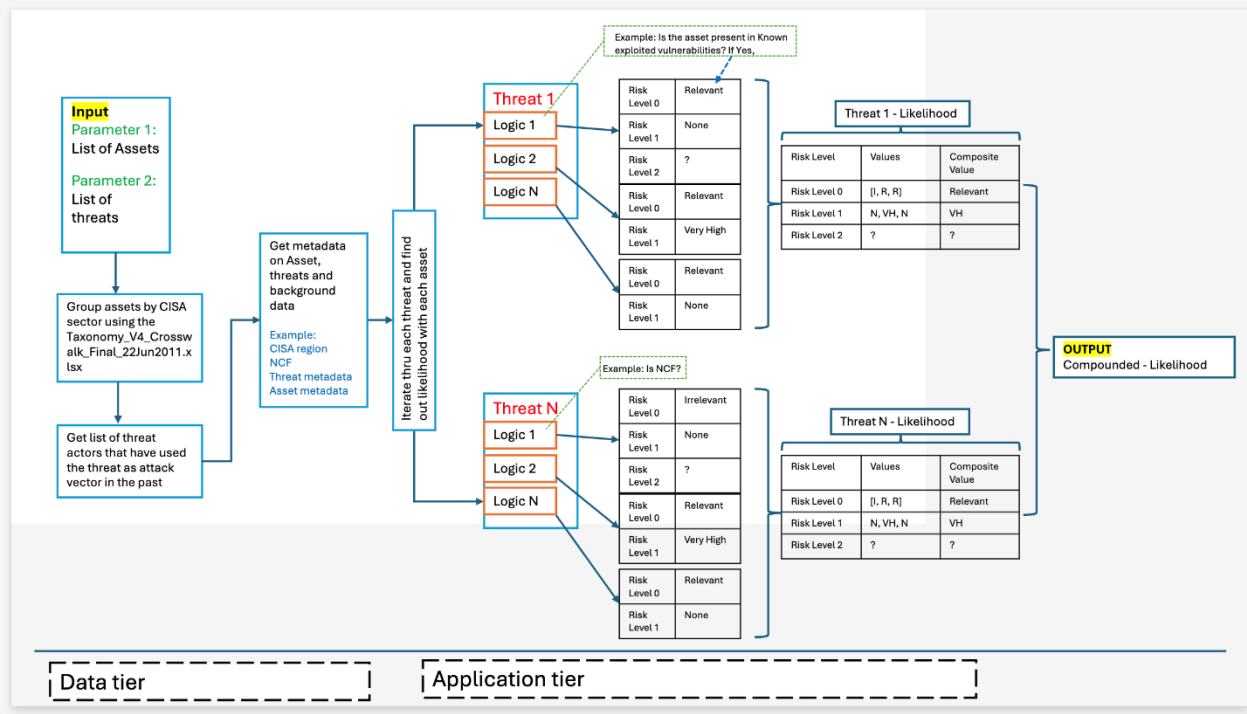
CVE helps to identify and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered, then assigned and published by organizations from around the world that have partnered with the CVE Program. CVE provides us insights on whether some assets are more vulnerable than others. You can download CVE in a single spreadsheet from CVE - Download CVE List.

Known exploited vulnerabilities

“Known exploited vulnerabilities” (KEV) is a catalog curated by CVE and helps us identity if some sectors are targeted more than others. It also helps us understand what attack vectors were used. It can be found at Known Exploited Vulnerabilities Catalog | CISA. The KEV catalog sends a clear message to all organizations to prioritize remediation efforts on the subset of vulnerabilities that are causing immediate harm based on adversary activity

Methodology

Visual



Overview

Once we create relationships between each of the inputs, we use likelihood assessment logics to calculate a threat likelihood value. These logics consist of structured hypotheses or formulas that guide the evaluation of threats at each level of analysis. The primary purpose of this process is to evaluate threats systematically, allowing them to be scoped and prioritized effectively.

One of the foundational principles of the methodology is that threats are evaluated for their relevance based on specific criteria, including geographic and functional alignment. Threats are assessed in terms of how they may relate to an asset's characteristics, historical occurrences, or more. For instance, a threat with a history of occurrence in the same CISA region as an asset is considered relevant (and could be high likelihood). This structured analysis ensures that each threat is scoped for its likelihood to impact national critical infrastructure.

The methodology is designed to evaluate the relevance of threats to specific assets systematically. By establishing relationships between inputs and applying structured

assessment logics, the process calculates the likelihood of a threat impacting an asset. These logics rely on hypotheses or formulas that guide the evaluation at multiple levels. These initializing logics ensure threats can be prioritized effectively based on their relevance to critical infrastructure.

The likelihood score is determined by analyzing specific criteria such as geographic alignment, historical occurrences, and functional importance. For example, a threat that has previously occurred in the same CISA region as an asset or has been historically used by threat actors can be considered relevant. The process combines historical data with regional and functional considerations to provide a structured analysis that scopes threats for prioritizations by initializing the likelihood of effect on an asset.

The process begins by mapping assets and threats to their respective CISA regions to identify alignment. Historical data is then reviewed to determine if threats have previously occurred in relevant regions, sectors, or asset types. Regional context further compresses the analysis, accounting for geographically specific threats, such as natural disasters in certain areas or possibly cyberattacks in regions with known vulnerability exposure. This approach ensures that the relevance of threats reflects both historical trends and regional conditions.

Threat prioritization relies primarily on evaluating the likelihood of occurrence. High-likelihood threats would be given priority for mitigation planning and resource allocation, as they are the most probable. This enables organizations to focus their efforts on addressing the most significant threats while deprioritizing those less likely to occur.

Steps

1. Asset Analysis:

1.1 Identify Asset Location:

- What is the county/state of the asset?
    - Assign asset to CISA region.

1.2 Check NCF Alignment:

- Is the asset listed in the Infrastructure Data Taxonomy?
    - Yes: Relevant (1)
    - No: Irrelevant (0)

1.3 Check Known Exploited Vulnerabilities (KEV):

- Does the asset use any product listed in the KEV database?
    - Yes: Relevant (1)

    - No: Irrelevant (0)

2. Threat Analysis:

2.1 Map Threat to CISA Region:

- What CISA region(s) are associated with this threat?
    - Is it listed in FEMA Index for physical threats?
        - Yes: Relevant (1)
        - No: Irrelevant (0)

2.2 Identify Threat Location(s):

- Where is the threat located?
    - Assign threat to CISA Region

2.3 Determine Historical Occurrence:

- Has the threat been exercised by threat actors as an attack vector before?
    - Yes: Relevant (1)
    - No: Irrelevant (0)

3. Overlap Analysis:

3.1 Compare Asset and Threat Regions:

- Do the CISA regions of the asset and the threat overlap?
    - Yes: Relevant (1)
    - No: Irrelevant (0)

3.2 Historical Analysis:

- Has the threat historically occurred in the region where the asset is located?
    - Yes: Relevant (1)
    - No: Irrelevant (0)

Methodology Output

The output of this evaluation determines whether a specific threat is relevant or not relevant to a particular asset. The decision is based on several criteria, and if more than 50% of those criteria are deemed relevant, the threat is considered relevant to the asset. This result helps decide whether the threat needs to be prioritized for further analysis/action.

If the output is "Relevant," it means that the threat has enough connection to the asset to warrant attention. This connection could include the threat and the asset being in the same CISA region, the threat having been used in the past, or the asset being part of a National Critical Function. It could also mean that the asset uses a product listed in the Known Exploited Vulnerabilities (KEV) database, making it a potential target. A "Relevant"

result suggests that the threat is significant enough to require further evaluation or preparation to address it.

If the output is "Not Relevant," it means that fewer than half of the criteria were met, so the threat does not have a strong enough connection to the asset. This might be because the threat has not historically occurred in the same region as the asset, has not been used in similar situations before, or does not target the functions or systems the asset supports. A "Not Relevant" result means that the threat is unlikely to be a direct or immediate risk to the asset and may not need to be prioritized at this time.

The output includes a simple determination: either "Relevant" or "Not Relevant." It also provides a relevance percentage, showing how many criteria were deemed relevant out of the total.

Likelihood Score = Total Relevant Logics / Total Logics * 100

If the Likelihood Score is => 50%, then the threat is Relevant.
Otherwise, the threat is considered irrelevant.

Likelihood

Likelihood is a cornerstone of the methodology's output, serving as a critical factor in determining the relevance and priority of identified threats. It serves as an indicator of the probability of a threat affecting a given asset through clearly defined criteria, such as historical occurrences, geographic alignment, and contextual factors. By systematically analyzing these elements, the methodology establishes a structured framework for determining which threats are most likely to affect critical assets.

Building on this likelihood assessment, the methodology will advance to ranking threats by their proclivity to affect a specific asset or a group of assets. By considering the likelihood of each threat, we can prioritize threats. Furthermore, qualitative and quantitative evaluations and impact modeling will allow for a deeper understanding of which threats pose the greatest concern. This ranking process helps ensure that resources are allocated strategically, focusing on mitigating the most significant threats while strengthening the resilience of critical assets.

Conclusion

In this report, we have developed a methodology to systematically assess and prioritize threats to national critical infrastructure by analyzing their likelihood and relevance to

specific assets. The methodology uses a step-by-step process to combine essential inputs such as asset characteristics, threat locations, historical occurrences, and regional alignment. By evaluating these factors, we can identify connections between threats and assets, ensuring that the most relevant threats are addressed.

The use of structured assessment logic and a threshold-based output simplifies the process, allowing us to determine whether a threat is relevant or not. This approach ensures that critical threats are prioritized while minimizing the focus on those with lower likelihood or impact. The transition from qualitative to quantitative likelihood assessments further strengthens the methodology, providing a clear framework for ranking threats based on their potential impact.

Overall, this methodology provides a practical way to analyze and prioritize risks in a complex and interconnected environment. By focusing on threats that pose the greatest risk to critical infrastructure, it supports better resource allocation and proactive risk management, ultimately helping to protect vital national assets.

Next steps

Future considerations and Refinement

Compounded Value of threats

In the future, the direction would be to identify and create a compounded value based on the relevance of the threat, which would then be used to determine the likelihood of that threat affecting the relevant asset.

Get more input data

Future consideration should be made to get more input data to assist in determining both relevance and likelihood.

Extend the logics

Having more input data, logic could be extended to determine likelihood. One additional logic could be like whether or not the location of the asset itself is secure.

Consider impact given likelihood

While impact was not the focus in this stage, it is acknowledged as a factor that will play a larger role in future iterations. So future refinements will integrate impact assessments to

account for the broader consequences of threats, enabling a more balanced prioritization that considers both likelihood and severity.

Use additional data to determine the next risk level

We are currently at level 0, but the conclusions made from level 0 and level 1 as well as additional data would be used to come up with conclusion in level 2.

Build AI and Automation framework

The future of this framework is for all these logics and conclusions to be automated aside from the input data. Right now, everything has to be done by hand.

References

1. Critical Infrastructure Sectors: CISA, Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (accessed October 17, 2024).

2. Grant, et al. “Publications Search.” Research, www.sandia.gov/research/publications/search/ . Accessed 17 Oct. 2024.

3. “Channel File 291 Incident RCA Is Available.” CrowdStrike, www.crowdstrike.com/blog/channel-file-291-rca-available/ . Accessed 17 Oct. 2024.

4. M.Elisabeth Paté-Cornell, “Uncertainties in Risk Analysis: Six Levels of Treatment.” Reliability Engineering & System Safety, Elsevier, 12 May 1999, www.sciencedirect.com/science/article/pii/S0951832096000671.

5. Griffith, Kevin, et al. Credit Rating Processes Applied to Critical Infrastructure Cyber Risk Assessment. 2022,

6. *Osti.gov*, 2022, www.osti.gov/servlets/purl/2006265. Accessed 5 Dec. 2024.

7. “National Critical Functions Resources | CISA.” *Www.cisa.gov*, 17 Dec. 2020, www.cisa.gov/resources-tools/resources/national-critical-functions-resources.

8. “Matrix | MITRE ATT&CK®.” *Attack.mitre.org*, attack.mitre.org/matrices/ics/.

https://attack.mitre.org/matrices/ics/

9. *Nationalacademies.org*, 2020, www.nationalacademies.org/.

10. Vpattnaik. “How Microsoft Names Threat Actors - Microsoft Defender XDR.” *Microsoft Defender XDR | Microsoft Learn*, learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming. Accessed 1 Nov. 2024.

11. FBI. “Welcome to FBI.gov | Federal Bureau of Investigation.” *Federal Bureau of Investigation*, 2019, www.fbi.gov/.

12. “Disasters.” *Tdem.texas.gov*, tdem.texas.gov/disasters.https://tdem.texas.gov/disasters

13. NOAA. “National Oceanic and Atmospheric Administration.” *Noaa.gov*, 2022, www.noaa.gov/.