

**CISA Tabletop Exercise Package Electricity Subsector**

[Enter Organization Name]

<Exercise Date>

Updated July 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc164935928)

[Exercise Overview 5](#_Toc164935934)

[General Information 6](#_Toc164935935)

[Module 1 9](#_Toc164935936)

[Module 2 11](#_Toc164935937)

[Appendix A: Additional Discussion Questions 14](#_Toc164935938)

[Appendix B: Case Studies 18](#_Toc164935939)

[Appendix C: Malicious Activity 19](#_Toc164935940)

[Appendix D: Living Off the Land Best Practices 20](#_Toc164935941)

[Appendix E: Contacts and Resources 22](#_Toc164935942)

[Appendix F: Acronyms 23](#_Toc164935943)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world; there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):GREEN*”: Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

# 

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise Date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise Location | |
| Exercise Activities | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| 20 Minutes | Hotwash |
| Purpose | To explore, assess, and enhance plans, procedures, and overall enterprise resilience in response to a significant cyber incident impacting the Electricity Subsector. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Discuss organizational resilience and response to threats targeting the energy sector. 2. Examine plans, policies, and procedures in response to a cyber incident. 3. Assess internal/external communications processes. | |
| Threat or Hazard | Cyber Attack | |
| Scenario | A network compromise leads to impacts to information and communication systems, loss of control of power generation output, and customer outages. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact (POC) | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov)  **Energy Sector Risk Management Agency**  [EnergySRMA@hq.doe.gov](mailto:EnergySRMA@hq.doe.gov) | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s (NCEP) CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

The CTEP materials (<https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>), including this Situation Manual, are designed to support the planning and execution of a tabletop exercise. A tabletop exercise is a discussion-based exercise in response to a scenario intended to generate a dialogue of various issues, identify strengths and areas for improvement, and/or achieve changes in perceptions about plans, policies, or procedures.[[2]](#footnote-3) NCEP also offers facilitated CTEPs. If you are interested in NCEP assistance with the planning and execution of a facilitated CTEP, please contact [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov).

## Using this Situation Manual

This Situation Manual provides a scenario and accompanying discussion questions designed to identify strengths and areas for improvement, including understanding of plans, policies, and procedures. This Situation Manual is intended to be adaptable and editable.

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. The footnotes throughout the modules contain corresponding resources to guide your preparedness efforts, including the CISA Cross-Sector Cybersecurity Performance Goals (CPG). The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix C: An explanation of the malicious activity presented in this scenario.
* Appendix D: Best practices for mitigating Living Off the Land (LOTL) techniques.
* Appendix E: Additional cybersecurity preparedness and response resources.
* Appendix F: Reference section for acronyms used within this situation manual.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Players may include information technology (IT)/information security personnel, emergency management personnel, human resources personnel, legal personnel, and any other personnel with a role in incident response.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include senior-level leadership, IT/information security personnel, emergency management personnel, legal personnel, and any other personnel without a role in incident response.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

**Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces attempts by threat actors to gain access to your networks while simultaneously launching a Distributed Denial of Service (DDoS) attack against your organization and concludes with customers reporting difficulties using your website.
  + **Module 2:** This module continues the scenario with impacts to information and communication systems followed by a loss of control of power generation output and reports from customers of power outages.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The hotwash is a short meeting held immediately after the end of the exercise discussion/conduct. The facilitator will lead participants through a review of the exercise discussion, identifying strengths and areas for improvement. The hotwash is also an opportunity for evaluators to ask clarifying questions, as needed.[[3]](#footnote-4)

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA) and partner agencies release an alert detailing a confirmed compromise of IT and operational technology (OT) networks of a U.S. electric utility provider by a state-sponsored cyber actor.[[4]](#footnote-5) The threat actor used multiple techniques to gain access to IT/OT networks, including exploiting known vulnerabilities, obtaining valid administrator credentials through privilege escalation vulnerabilities and exfiltration of the Active Directory, and living off the land techniques to maintain persistence. CISA assesses with high confidence that state-sponsored actors intend to compromise additional IT/OT networks within the Electricity Subsector.

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What are the greatest cyber threats to your organization?
   1. What are the possible impacts of an intrusion into your systems?
2. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?[[5]](#footnote-6)
   1. What IT and OT systems or processes are the most critical to your organization?
   2. What improvements were implemented to enhance cyber resilience following recent risk assessments?
3. What cybersecurity threat information does your organization receive?
   1. What are your primary sources of information?
   2. How do you determine what information is relevant to your equipment and operations?
   3. What actions would your organization take in response to a report like the one presented in the scenario?

### Day 6

An IT employee notices a remote desktop protocol window open on their device without any user input. The window closes shortly after it opens, and the employee attributes the issue to a recent update completing its install and takes no further action.[[6]](#footnote-7)

### Day 7

One of your third-party vendors releases a patch for a known exploited vulnerability in their devices. They provide edge devices (e.g., firewalls, routers) for your organization.[[7]](#footnote-8) IT is working to implement the patch on the appropriate devices and estimates the patch will be applied to all impacted devices in the next 48 hours.[[8]](#footnote-9)

1. Describe your organization’s cybersecurity training program for employees.
   1. How often are employees required to complete this training?
   2. What additional training is required for employees who have system administrator-level privileges?
   3. What additional training is required for employees who have access to OT systems?
   4. What type of training methods or approaches have you found most beneficial?
2. How do employees report and log anomalous IT/OT activity?
3. What tools (e.g., threat hunting, security audits) do you leverage as part of a proactive cybersecurity strategy?
   1. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?[[9]](#footnote-10)
4. Describe your organization’s patch management and vulnerability management plans.
   1. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
   2. Describe your policies on remote access to your organization’s network.
   3. What security protocols, such as Multi-Factor Authentication (MFA) and encryption, exist on your hardware?
5. What is the role of cybersecurity in the review and selection of third-party vendor support?
   1. What cybersecurity language (e.g., cybersecurity training and cyber incident notification requirements) is included within third-party vendor contracts?
   2. How do you evaluate the cybersecurity posture of your vendors?
   3. How often are contracts reviewed?

### Day 11

IT observes multiple attempts to gain access to your organization’s networks. Threat actors are attempting a variety of attacks based upon legacy edge devices present within your network. The malicious actors are also repeatedly executing distributed denial-of-service (DDoS) attacks against your organization.

1. Describe your organization’s approach to managing the lifecycle of critical equipment.
   1. How do you obtain new or replacement equipment?
   2. How do you continue to provide services to your customers while waiting for new/replacement equipment?
   3. Does your organization have any memorandums of understanding or mutual aid agreements with sector partners to maintain services if your equipment fails or is damaged?
2. How does your organization baseline network activity on IT and OT networks?
   1. How do you distinguish between normal and abnormal traffic?
   2. What are your next steps when abnormal activity is detected/reported?
   3. What Indicator of Compromise (IOC) feeds does your organization use?
3. Describe your organization’s network configuration and your approach to network segmentation of IT and OT systems.
   1. How is physical security integrated into IT and OT security?
4. What are your response priorities?
   1. What actions do you take in response to multiple unauthorized attempts to access your networks and systems?
   2. How would you address the DDoS attacks?
   3. What other protective actions are needed to safeguard your organization?

# Module 2

### Day 33

Internal functions within your organization are inaccessible. Employees are unable to access information databases, and internal communication methods such as instant messaging and phone lines are not functioning. Dispatching service personnel for maintenance tasks using the normal methods becomes all but impossible. Devices such as electronic locks and thermostats are also no longer functioning throughout your organization.

## Discussion Questions

1. Discuss your organization’s procedures for declaring a cyber incident.
   1. What escalation criteria are defined in your cyber incident response plan (CIRP)?
2. What alternate communication methods does your organization have if primary systems are unavailable?
   1. How are personnel dispatched to maintenance locations using alternate methods?
   2. How often are alternate communication methods tested and verified?
3. What manual methods for monitoring physical security and safety can you employ if devices such as electronic locks and thermostats are no longer functioning?

### Day 35 – Morning

Power generation output at your organization is no longer fully controlled. Sensors are showing fluctuating outputs. Digital industrial control systems are not responsive to operator commands. Turbines are spinning down and back up without input. The power distribution network also shows signs of distress. Transformers and substations are receiving inadequate or, in some cases, too much power. Your organization receives numerous reports of catastrophic failures of transformers and emergency shutdowns, resulting in widespread power outages.[[10]](#footnote-11)

1. How do IT and OT security teams coordinate incident response efforts?
2. What alternate systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
   1. Who can authorize the use of alternate systems or procedures?
   2. How long can you operate using manual processes or alternate systems when your primary critical systems fail?
   3. What additional staffing requirements are necessary for alternate systems or procedures, if any?
3. How do you respond to widespread power outages?
   1. How do cascading impacts to essential services, critical infrastructure, and other sectors impact your restoration priorities?
   2. How will you continue to provide services to your customers while responding to these incidents?

### Day 35 – Afternoon

Customers are posting on social media that they have lost power to their homes. A few posts include videos of what appears to be a transformer exploding. News media reports on the outages and contacts your organization for comments.[[11]](#footnote-12)

1. What information are you sharing internally (e.g., with employees, leadership)?
2. What information are you sharing externally (e.g., with customers, partners)?
   1. How do you respond to the media inquiries?
   2. How would you work to regain public trust and the trust of your customers following this incident?
3. What legal and regulatory notifications are required based on the scenario?
   1. When are notifications made?
   2. Who is responsible for making the notifications?

### Day 40

Your organization is conducting rolling blackouts as staff work to ensure systems are fully operational following the incident. The source of the initial intrusion appears to be an unpatched legacy edge device. Malicious cyber actors exploited a known vulnerability and then used DDoS attacks to evade detection and mask their activity. The threat actors then moved laterally through your system into the OT network to disrupt power generation and distribution.

1. When would your organization transition to the recovery and post-incident phases?
   1. How is the decision to transition to the recovery phase made?
   2. How does your organization conduct post-incident review?
   3. How are lessons learned/areas for improvement incorporated into process improvement planning (e.g., incident response plans, training)?
2. How do you verify the integrity of your critical systems following a cyber incident?
   1. What actions do you take to mitigate future vulnerabilities?
3. What supply chain challenges would you anticipate when restoring damaged/destroyed equipment?
4. Based on discussion and lessons learned, what changes will you implement to increase the resilience of your organization?

# 

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Questions are aligned with the NIST functional areas and organizational roles and responsibilities. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. ***This instructional paragraph, as well as undesired discussion questions, should be deleted.***

## Cyber Resilience

1. Discuss how cyber preparedness is integrated with your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
3. Discuss your risk management strategy.
4. How is it developed/maintained?
5. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data)?
6. Describe your organization’s review process for your CIRP.
7. How is your CIRP integrated with other incident or emergency response/management plans?
8. How often is the CIRP reviewed?
9. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
10. How are updates to the plan communicated to department or agency employees?
11. Do your vendor risk management processes include ensuring suppliers and partners adhere to strict security standards?
12. Are any foreign ownership, control, or influence (FOCI) relationships clearly identified and managed?
13. Does your organization use secure by design principles to help inform vendor selection?
14. What cybersecurity language is included within third-party vendor contracts?
15. How do you evaluate the cybersecurity posture of your vendors?
16. How often are contracts reviewed?
17. How do your service level agreements address cyber incident notification?
18. Are vendor patching plans included in contract language?
19. Discuss your supply chain concerns related to your IT/OT infrastructure.
20. What is your method for tracking and identifying firmware vulnerabilities in your network?
21. How is the integrity of your critical data protected and validated?
22. What external entities have access to your data?
23. How would those entities report a breach of their systems to your office?
24. What essential functions are impacted by the incidents described in the scenario?
25. If primary communications are compromised, how do you provide information to internal and external entities?
26. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. What are your organization’s policies or procedures for IT account management?
2. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?
3. Describe your organization’s bring your own device (BYOD) policy.
4. Describe your organization’s employee off-boarding process.
5. Is this process coordinated with IT and Human Resources (HR)?
6. What additional actions are taken if the employee’s termination is contentious?
7. How does your organization retrieve all information system-related property during the employment termination process (e.g., authentication token, system administrator’s handbook/manual, keys, identification cards)?

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by regulation, state law, and/or organization policy?
3. What training do employees receive regarding reporting requirements and your cyber incident response plan?
4. What cybersecurity incident escalation criteria are defined in your cyber incident response plan?
5. Who is responsible and what actions would they take based on the scenario?
6. Who should be notified internally and externally according to the plan?
7. When would leadership be notified?
8. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
10. How often is your organization’s data reviewed?
11. How would you determine whether unauthorized manipulation of data occurred?

## Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
2. At what point in the scenario would you contact law enforcement?
   1. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
3. Is contact information for IT/OT system owners documented in your response plans to ensure the correct personnel can be reached during a cyber event or incident?
4. What are the processes for contacting critical personnel outside of core hours?
5. How do you proceed if critical personnel are unreachable or unavailable?
6. How would a breach of vendor(s) affect your organization if they have access to your information?
7. What are vendor notification requirements to your organization?

## Recovery

* 1. When does your organization determine a cyber incident is resolved?

1. Who makes this decision?
2. What post-incident activities would your organization conduct?
   1. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
3. What is the risk associated with reactivating critical business processes and systems?
4. Describe the process to completely rebuild these systems.
5. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. What additional training and/or exercise requirements do you require for your incident response staff?
3. How often does your organization exercise its CIRP?
4. Who is involved in the exercises?
5. What external agencies are involved in the exercises?
6. How do your organization’s training and exercise efforts address both physical and cyber risks?
7. How often do senior staff/leadership participate in cybersecurity exercises?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
2. How do these goals align with organizational objectives?
3. Are there ways leadership can better support a secure by design-oriented organization?
4. Describe your organization’s cybersecurity culture.
5. What cybersecurity training is required for senior leadership?
6. At what point would you activate your organization’s Security Operations Center/Emergency Operations Center?
7. What is your role during a cyber incident?
8. What information do you need to support your decision-making process?
9. What are the gaps in your cybersecurity workforce?
10. How does your organization recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. What training do employees receive on reporting contact with the media?
      2. How do you build and maintain trust with the public?

## Legal

1. Describe the role your legal office/department plays in responding to a cyber incident.
   1. How does your legal team contribute to the incident management and recovery process?
2. Does your legal office/department create or maintain documents to assist with responding to a cyber incident?
   1. What documents might your legal office anticipate preparing or reviewing during such incidents?

# Appendix B: Case Studies

## Network Devices Exploited in Attacks Against U.S. Critical Infrastructure

In August 2023, the advanced persistent threat group Volt Typhoon, sponsored by the People’s Republic of China (PRC), repeatedly attacked part of the U.S. electrical grid. The group attempted entry into the electrical grid networks by exploiting Internet connectivity, however, a network breach was prevented.[[12]](#footnote-13) Volt Typhoon operates by exploiting network edge devices such as routers and Virtual Private Networks, particularly those past end-of-life but still in service. The malware used by Volt Typhoon persists secretively by living off the land, meaning they leverage existing capabilities within the system instead of creating new files. Living off the land techniques can allow for deep infiltration without detection.

In addition to attacking the electricity subsector, Volt Typhoon compromised the IT environments of critical infrastructure organizations in the communications, transportation, and water and wastewater sectors across the U.S. Attackers appear to be pre-positioning themselves on IT networks to enable lateral movement to OT assets.[[13]](#footnote-14) None of the confirmed intrusions resulted in a disruption to critical infrastructure operations in the U.S.[[14]](#footnote-15)

## Vulnerabilities in Firewalls Used in Attacks Against Danish Energy Operators

In May 2023, threat actors launched cyberattacks against numerous Danish energy operators, successfully compromising 11 of the 16 targeted operators during the first set of attacks. The attackers exploited a recently published vulnerability in firewalls used by all of the targeted energy operators. The vulnerability allowed attackers to gain control of the firewalls by sending network packets to the firewalls to steal the firewall configuration and current usernames. The 11 compromised organizations addressed the vulnerable firewalls and no further access to systems, including OT networks, was observed at the time. The second wave of attacks began over a week later. Shortly after the new attacks began, the same firewall company announced two additional vulnerabilities that were exploited by unknown attackers. The second wave of attacks consisted of commandeering additional firewalls of Danish infrastructure operators that were subsequently used in DDoS attacks against targets in the U.S. and Hong Kong.[[15]](#footnote-16)

Contributing factors to the success of both rounds of attacks included a lack of proper firewall patching practices and poor network segmentation leading to easy traversal through the organizations’ systems. The attacks also highlighted the lack of understanding of the connection between IT and OT systems amongst Danish critical infrastructure owners and operators.[[16]](#footnote-17)

# Appendix C: Malicious Activity

## Living Off the Land

LOTL is a set of techniques that allow sophisticated cyber threat actors to compromise and subsequently maintain persistent access to networks by camouflaging their activity with typical system and network behavior. Cyber threat actors use native tools and processes on systems to reduce the risk of detection, as the tools and processes are already deployed and trusted in the IT environment. LOTL techniques can be used in multiple IT environments, including on-premises, cloud, hybrid, Windows, Linux, and macOS environments. Third-party tools with built-in functionality and high privileges are opportunity-rich targets for exploitation by cyber threat actors.

Distinguishing malicious LOTL activity from legitimate behavior can be difficult for network defenders, as there is not one consistent set of IOCs. Common network defense strategies such as relying on untuned endpoint detection and response systems and maintaining default logging configurations create an environment that allows LOTL activity to remain undetected. Additionally, software defects or unsecure default configurations often allow cyber threat actors to carry out malicious activity using LOTL techniques. See the following Appendix D: Best Practices for Mitigating LOTL Techniques.

### Additional Resources

* CISA Identifying and Mitigating Living Off the Land Techniques (<https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques>)
* CISA PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders (<https://www.cisa.gov/resources-tools/resources/prc-state-sponsored-cyber-activity-actions-critical-infrastructure-leaders>)

## Software Supply Chain Attacks

A software supply chain attack occurs when a threat actor infiltrates a software vendor’s network and employs malicious code to compromise the software. The vendor unknowingly sends the compromised software to its customers, which compromises their customer’s data and/or system. Newly acquired software may be compromised from the outset, or a compromise may occur through other means like a patch or hotfix. In these cases, the compromise still occurs prior to the patch or hotfix entering the customer’s network. These types of attacks affect all users of the compromised software and can have widespread consequences. To increase resilience against supply chain attacks an organization should implement an enterprise-wide cybersecurity supply chain risk management approach. This approach includes managing critical components and suppliers, understanding the supply chain, collaborating with key suppliers, and including suppliers in resilience and improvement activities. For more information on supply chain risk management, see the resources listed below.

### Additional Resources

* CISA Defending Against Software Supply Chain Attacks (<https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks>)
* CISA Information and Communications Technology (ICT) Supply Chain Resource Library (<https://www.cisa.gov/ict-supply-chain-resource-library>)
* NIST Cybersecurity Supply Chain Risk Management Practices for Systems (<https://csrc.nist.gov/pubs/sp/800/161/r1/final>)

# Appendix D: Best Practices to Mitigate Living Off the Land Techniques

Introduction

CISA and partner agencies strongly urge critical infrastructure organizations to apply the following best practices from the joint guidance [Identifying and Mitigating Living Off the Land Techniques](https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques) to hunt for potential LOTL activity. There is no foolproof solution to fully prevent or detect LOTL activity, however by applying these best practices organizations can better position themselves against LOTL techniques.

Detection

* Implement comprehensive and verbose/detailed logging and aggregate logs in an out-of-band, centralized location where adversaries cannot tamper with them. Comprehensive and aggregate logs enable behavior analytics, anomaly detection, and proactive hunting.
* Establish and continuously maintain a baseline of installed tools and software, account behavior, and network traffic.
* Use automation to continually review all logs and increase the efficiency of hunting activities. Set up regular audits for use of system files. For cloud services, audit for unusual application programming interfaces (API) calls, especially as it relates to account permissions and sensitive data.
* Reduce alert noise by tuning monitoring tools. Pay careful attention to remote access tools and administrative logons.
* Leverage user and entity behavior analytics to focus on users and programs that are acting significantly outside of their normal routines.

Hardening

* Apply hardening guidance. Use software and hardware configurations based on vendor-provided or industry-standard recommendations. Default configurations are generally insecure. Hardening measures that are universally applicable aid in compliance throughout the organization, so that incompatible devices do not become attack vectors. Two additional hardening methods include securing critical assets by limiting their access and avoiding cached credentialing.
* Implement application allowlisting. This means limiting the users who can access data and applications to only those who require it. This also limits what applications can be run on the machine.
* Enhance network segmentation and monitoring to limit lateral movement possibilities. Analysis tools should track internet traffic. Strategically place sensors and parsers to capture the communication between different segmented systems. The goal is zero trust architectures.
* Implement authentication controls that prevent mistaken access to files and applications. MFA should be mandatory for all users on all networked systems. Expand your controls to include a Privileged Access Management system, allowing access only when necessary for job functions and only as necessary for a user and group to complete work.

Remediation

* After a compromise is discovered, investigate to determine the highest privilege level account that the malicious actor could have accessed. If the actor controls an administrative account, reset credentials of privileged and non-privileged accounts within the trust boundary of each compromised account, force password resets, and revoke and issue new certificates for all accounts/devices. Otherwise, reset the relevant account(s) credentials or access keys, and monitor related accounts closely.
* Audit all network appliance and edge device configurations with indicators of malicious activity for signs of unauthorized or malicious configuration changes. Organizations should ensure they audit the current network device running configuration and any local configurations that could be loaded at boot time. If configuration changes are identified, change all credentials used to manage network devices, and update all firmware and software.

### Additional Resources

* CISA Identifying and Mitigating Living Off the Land Techniques (<https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques>)
* CISA PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders (<https://www.cisa.gov/resources-tools/resources/prc-state-sponsored-cyber-activity-actions-critical-infrastructure-leaders>)
* CISA Logging Made Easy (<https://github.com/cisagov/LME>)
* CISA Zero Trust Maturity Model (<https://www.cisa.gov/zero-trust-maturity-model>)
* CISA Phishing Resistant Multi-Factor Authentication (<https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>)

# Appendix E: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact: <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)
* Federal Bureau of Investigation (FBI)
* Field Offices (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)
* Department of Energy (DOE)
* Energy Response Center ([energyresponsecenter@hq.doe.gov](mailto:energyresponsecenter@hq.doe.gov))

Energy Sector Resources

* Department of Energy Cybersecurity (<https://www.energy.gov/ceser/cybersecurity>)
* Exercises and Training (<https://www.energy.gov/ceser/exercises-and-training>)
* Electricity Information Sharing and Analysis Center (<https://www.eisac.com/s/>)
* Electricity Subsector Coordinating Council (<https://www.electricitysubsector.org/>)
* CISA Industrial Control Systems (<https://www.cisa.gov/topics/industrial-control-systems>)
* CISA Energy Sector (<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector>)

Preparedness Resources

* Cyber Security Evaluation Tool (CSET) (<https://www.cisa.gov/downloading-and-installing-cset>)
* CISA Find Help Locally (<https://www.cisa.gov/audiences/find-help-locally>)
* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>)
* NIST Cybersecurity Framework Tools ([<https://www.nist.gov/cyberframework>](https://www.nist.gov/cyberframework))

State Level Resources

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* DHS Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)

Additional Resources

* InfraGard (<https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>)
* Internet Security Alliance (<https://isalliance.org/>)
* Information Sharing and Analysis Organizations (<https://www.isao.org/information-sharing-groups/>)
* Information Sharing and Analysis Centers ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

# Appendix F: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| API | Application Programming Interfaces |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| DDOS | Distributed Denial of Service |
| DOE | Department of Energy |
| FBI | Federal Bureau of Investigation |
| FOCI | Foreign Ownership, Control, or Influence |
| HR | Human Resources |
| IOC | Indicators of Compromise |
| IT | Information Technology |
| LOTL | Living Off the Land |
| MFA | Multi Factor Authentication |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| POC | Point of Contact |
| PRC | People’s Republic of China |
| TLP | Traffic Light Protocol |
| ZTA | Zero Trust Architecture |

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. “Homeland Security Exercise and Evaluation Program,” FEMA, February 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-3)
3. FEMA, “Homeland Security Exercise and Evaluation Program,” January 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-4)
4. CISA Cybersecurity Alerts & Advisories, <https://www.cisa.gov/news-events/cybersecurity-advisories>. [↑](#footnote-ref-5)
5. NIST CPRT – CSF2.0, “ID.RA – Risk Assessment,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA>. [↑](#footnote-ref-6)
6. NIST CPRT – CSF2.0, “PR.PS-05, Installation and execution of unauthorized software are prevented,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-05>. [↑](#footnote-ref-7)
7. NIST CPRT – CSF2.0, “GV.SC-09, Supply chain security practices,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC-09>. [↑](#footnote-ref-8)
8. NIST CPRT – CSF2.0, “PR.PS-02, Software is maintained, replaced, and removed commensurate with risk,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-02>. [↑](#footnote-ref-9)
9. CISA Known Exploited Vulnerabilities Catalogue, <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>. [↑](#footnote-ref-10)
10. NIST CPRT – CSF2.0, “Respond,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS>. [↑](#footnote-ref-11)
11. NIST CSRC – CSF2.0, “RS.CO,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.CO>. [↑](#footnote-ref-12)
12. Ellen Nakashima and Joseph Menn, “China’s cyber army is invading critical U.S. services,” *The Washington Post*, December 11, 2023, <https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/>. [↑](#footnote-ref-13)
13. CISA, “Cybersecurity Alert: PRC State Sponsored Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,“ February 7, 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>. [↑](#footnote-ref-14)
14. Nakashima and Menn, ibid. [↑](#footnote-ref-15)
15. SektorCERT, “The Attack Against Danish Critical Infrastructure,” November 2023, <https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf>. [↑](#footnote-ref-16)
16. Ibid. [↑](#footnote-ref-17)