[COMPANY LOGO]

INCIDENT RESPONSE PLAYBOOK

[COMPANY NAME]

Document Objectives:

This document follows the incident response phases as defined by NIST SP 800-61 Rev. 2, and a set of operational standards developed by CISA to provide the operational procedures to be followed in response to a cybersecurity incident impacting [COMPANY].

Document Properties:

Version:	[VERSION]
Last Revised Date:	[DATE]
Confidentiality Level:	[CONFIDENTIALITY]
Document Owner	[OWNER]
Publication Date:	[DATE]

Table of Contents:

1. Incident Criteria

This document follows NIST SP 800-61 Rev. 2 guidelines and classifies a cybersecurity incident as an occurrence that either:

- Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system
- Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

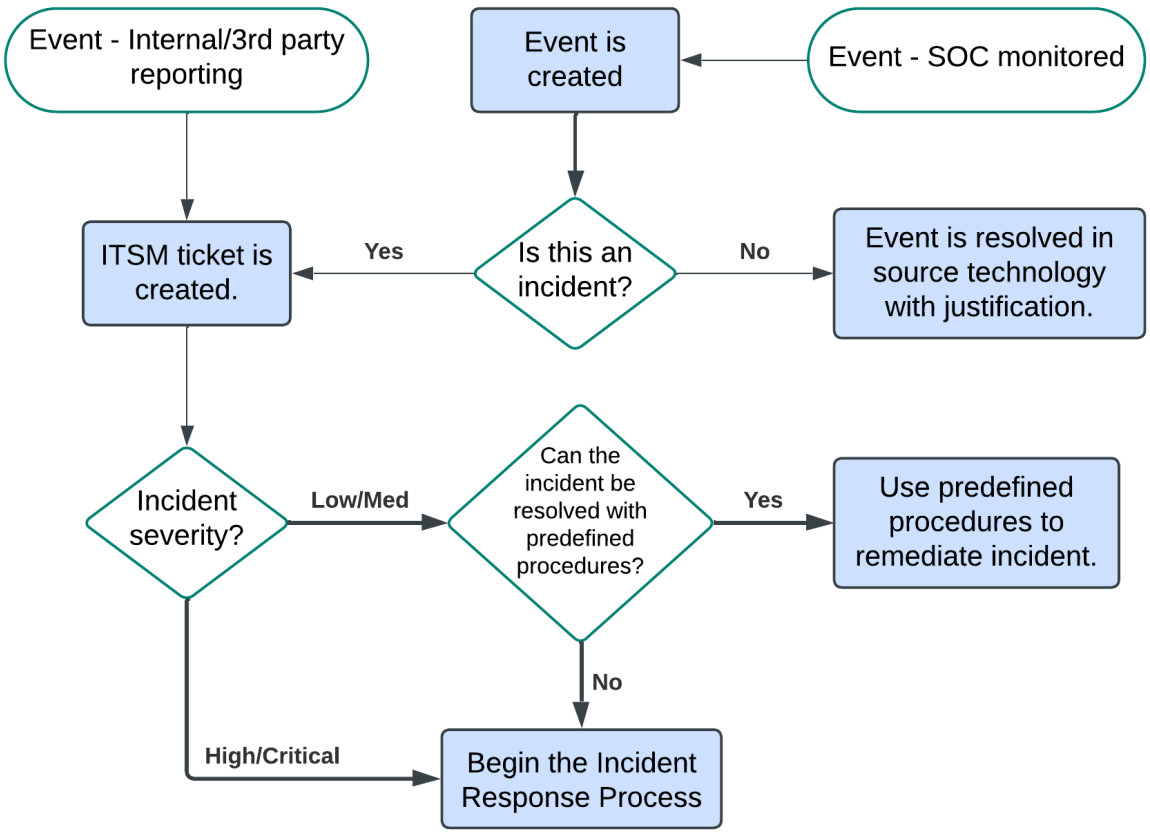
2. Incident Response Process

The incident response process begins with the identification of an incident. Many types of events can lead to the identification of an incident:

- Automated detection systems/alerting
- [COMPANY] employee report
- Partner/provider or other third-party reporting
- Proactive threat hunting or review of processes and/or systems

Once identified, an incident can be classified as:

- **Low:** [COMPANY] can still provide all critical services to all users but has lost efficiency.
- **Medium:** [COMPANY] has lost the ability to provide a critical service to a small number of users.
- **High:** [COMPANY] has lost the ability to provide a critical service to a large subset of system users.
- **Critical:** [COMPANY] is no longer able to provide some critical services to any users.



If the determination is made that the incident has a “Low” or “Medium” level of severity, then the internal Standard Operating Procedures can be followed to remediate the incident without activation of the Incident Response team.

If the severity has been determined to be “High” or “Critical” the incident response team must be activated as quickly as possible.

Standing Up Cybersecurity Incident Response Team (CSIRT)

Following the initial detection and confirmation a severe incident. The CSIRT must be activated as quickly as possible. If the detection occurs during business hours, this can be accomplished through [COMMUNICATION SOFTWARE]. Outside of business hours, each member of the IR team will need to be contacted directly.

Incident response roles:

- **Incident manager:** Drives and coordinates all incident response team activity, and keeps the team focused on minimizing damage, and recovering quickly.
- **Lead investigator:** Collects and analyzes all evidence, determines root cause, directs the other security analysts, and implements rapid system and service recovery.
- **Incident responders:** Team of security analysts that work directly with the affected network/systems to research the time, location, and details of an incident. They will also work to recover key artifacts and maintain integrity of evidence to ensure a forensically sound investigation.
- **Legal liaison:** An attorney able to provide advice regarding liability issues when an incident affects customers, vendors, and/or the general public.
- **General communications manager:** The communications manager is the person familiar with public communications. They are responsible for writing and sending internal and external communications about the incident. This is usually also the person who updates the status page (when applicable).
- **Response communications manager:** The response communications manager is responsible for facilitating communications between the parties directly involved in the incident response efforts. They will also provide periodic status updates to the communications manager so they can distribute the information as needed.
- **Incident scribe:** A scribe is responsible for recording key information about the incident and its response effort.
- **Subject matter experts:** A technical responder familiar with the system or service experiencing an incident. Often responsible for suggesting and implementing fixes.

Role designations:

- **Incident manager:** [INSERT PERSON(S)]
- **Lead investigator:** [INSERT PERSON(S)]
- **Incident responders:** [INSERT PERSON(S)]
- **Legal liaison:** [INSERT PERSON(S)]
- **Incident scribe:** [INSERT PERSON(S)]
- **General communications manager:** [INSERT PERSON(S)]

- **Response communications manager:** [INSERT PERSON(S)]
- **Subject matter experts:**
  - Cloud infrastructure: [INSERT PERSON(S)]
  - Network infrastructure/management: [INSERT PERSON(S)]
  - Windows servers: [INSERT PERSON(S)]
  - Linux servers: [INSERT PERSON(S)]
  - Workstations: [INSERT PERSON(S)]
  - Active directory: [INSERT PERSON(S)]
  - Account management: [INSERT PERSON(S)]

Engage IR Retainer, as Necessary

An IR Retainer is available through a third party: [IR COMPANY NAME] to provide outside expertise, if needed.

Hotline: [PHONE]

[Contact #1]: [PHONE] ext. 123 - [EMAIL]

[Contact #3]: [PHONE] ext. 123 - [EMAIL]

The incident response process can be separated into 5 phases:

2.1 Preparation

The primary objective for the Corporate Security Team (CST) is to prepare for major incidents before they occur to mitigate the possible impact to [COMPANY]. These preparations include:

2.1.1 Documenting and understanding policies and procedures

The CST has created and is maintaining a knowledge base [LINK NEEDED] to store and centrally access policies, standard operating procedures, and specific incident playbooks.

2.1.2 Utilize security tooling and cyber threat intelligence (CTI) to automate the detection of suspicious and malicious activity and response processes.

[SIEM] is being utilized as the Security Incident and Event Management platform. It performs centralized log ingestion, normalization, and correlation.

[EDR] is deployed to all Windows, Mac, and Linux machines in the environment for detection and response capabilities. The [MSSP/MDR] team is providing ongoing monitoring and response for detections. The [COMPANY] interaction with this team is outlined in the “Coordination” section. The specific playbooks the [MSSP/MDR] team follows are detailed in separate playbooks within the CST knowledge base. [EDR] CTI is being utilized directly by the [EDR] tooling and [SIEM].

The intrusion/detection and network firewall systems are being managed by a 3rd party, [MSSP/MDR]. [FIREWALL] firewall logs are being ingested into the [SIEM] platform. The [COMPANY] team interaction with the [MSSP/MDR] team is detailed in the "Coordination" section. [MSSP/MDR]-specific processes are detailed in separate playbooks in the CST knowledge base.

Email monitoring and DLP is being monitored and provided by [EMAIL SECURITY GATEWAY]. This system can proactively block email threats identified by CTI being ingested from [EMAIL SECURITY GATEWAY] and [EDR].

2.1.3 Defining baseline systems and networks

A baseline has been established for the event activity in [SIEM] and [EDR]. A network-wide mapping and baselining is a work in progress to more easily detect deviations. These baselines are available in [INFRASTRUCTURE MONITORING SOLUTION] and [SIEM].

2.1.4 Training Response Personnel

Ongoing training for Cybersecurity staff is available through the [LEARNING PLATFORM]. The [MSSP/MDR] team is available to assist in the incident response process in the event of an incident. An annual tabletop exercise is performed to test incident response/recovery activities and the [COMPANY] continuity of operations plan.

2.1.5 Communications and Logistics

Currently primary communications through [COMMUNICATION SOFTWARE], Email, and [BACKUP COMMUNICATION SOFTWARE].

2.1.6 Educate users on cyber threats and notification procedures

User security awareness training is performed [TIME INTERVAL], and ongoing simulated phishing emails are sent out to reinforce email safety. These are managed with the [SECURITY AWARENESS PLATFORM] platform. An email report button has been implemented into [EMAIL APPLICATION] to give users an easy way to report suspicious emails directly to the platform for analysis.

2.2 Detection and Analysis

The CST works to implement appropriate technology and processes to form a sufficient baseline to monitor, detect, and alert on anomalous or suspicious activity. All available information must be utilized to assess the observed activity to identify possible threats to the organization.

2.2.1 Methods of detection

The initial identification of an incident is often dependent on well-established methods of detection:

Automated detection systems: [EDR], [SIEM], [EMAIL SECURITY GATEWAY], and [FIREWALL].

Findings during threat hunting: [EDR], [SIEM], and [FIREWALL].

Managed security service providers: [MSSP/MDR] and [EDR].

Reporting: User, partner, provider, or third-party.

The CST places an emphasis in reviewing and testing detection fidelity for the automated systems and implementing improvements and extending coverage where needed as an ongoing process.

2.2.2 Collecting and preserving data

Endpoint data is collected by the [EDR] sensor deployed to Windows, Linux, and Mac OS machines. This data is ingested into the [EDR] cloud and stored for [RETENTION PERIOD].

[SIEM] collectors are being utilized for log collection from:

- Servers
- Workstations
- [CLOUD PLATFORM(S)]
- [WAF]
- [GIT PLATFORM]
- [FIREWALL]
- [AUTHENTICATION SOLUTION]
- [HR SOLUTION(S)]
- [OTHER PLATFORMS]

[SIEM] data is stored in the [SIEM] platform for [RETENTION PERIOD].

2.2.3 Technical analysis

The analysis process begins with the examination of all available data sources in the environment to discover and correlate activity indicative of threats to [COMPANY]. The ultimate goals are to determine the root cause and extent of the activity, classify the behavior according to the MITRE ATT&CK framework, and determine which stage in the Cyber Kill Chain® the adversary has reached to better inform the containment and eradication efforts.

Correlate events and document timeline:

Events are ingested and stored in [SIEM], [EDR], and the [MSSP/MDR] platforms respectively. Utilizing data from all three to determine the timeframe over which the suspicious activity occurred will narrow the investigation to the necessary timeline. Findings should be documented by the Incident scribe in the Incident Response Tracker (FREE TRACKER IS AVAILABLE HERE).

Identify anomalous activity:

Not all adversarial activity is inherently malicious. Observing deviations from established baselines is a critical component for identifying malicious activity and can often give indications to the stage of the Cyber Kill Chain® that the adversary has reached.

Identify root cause:

If possible, identify the root cause during the initial investigation as it can be used to inform the direction of the investigation and subsequent response process.

Gather incident indicators:

Identifying and documenting indicators of compromise will assist in correlating additional activities and determining the scope of the incident. They can also be utilized in containment and eradication efforts.

Analyze activities for common adversary tactics, techniques, and procedures (TTPs):

Observed TTPs can be compared to common adversary TTPs in the ATT&CK framework and fit into the steps of the Cyber Kill Chain® and be used to help understand the adversary's "why," "what," and "how." This information can serve defenders as reference points to better predict the adversary's next course of action.

Validate and refine the investigation scope:

As new activities are observed and more information is collected, it is critical that the investigation scope be validated and refined where needed. New information can uncover previously unknown adversarial activities and adjustments to the scope will be needed.

2.2.4 Key questions to answer during the investigative process

- How did the adversary gain initial access to the network?
- How is the adversary accessing the environment?
- Is the adversary exploiting vulnerabilities to achieve access or privilege?
- How is the adversary maintaining command and control?
- Does the actor have persistence on the network or device?
    - What is the method of persistence?
- What accounts have been compromised and what privilege level has been attained?
- What method was/is being used for reconnaissance?
- Is lateral movement suspected or known?
    - How is lateral movement conducted?
- Has data been exfiltrated and, if so, what kind and via what mechanism?

2.2.4 Third-Party analysis

Ongoing analysis is provided by the CST and [MSSP/MDR] teams as the technologies they employ detect suspicious activity. If the above key questions are not able to be answered to a satisfactory level, additional third-party analysis may be needed.

2.3 Containment

Containment of a cybersecurity containment in one of the highest priority items in the incident response process. While the strategy for containment will be dependent on the type of incident, the main objectives are to mitigate the impact of the incident to [COMPANY] and remove adversarial access.

2.3.1 Considerations

Containment actions are critical to the incident response process but can also have impacts on business functions. The following should be considered before performing containment actions:

- Additional adverse impacts to [COMPANY] operations
    - Network connectivity
    - Service availability
- Duration of the containment process, resources needed, and effectiveness.
- Impact on the collection, preservation, and documentation of evidence.

2.3.2 Containment activities

Short-term mitigations are implemented to isolate adversarial activity and prevent malicious activity from spreading to additional systems:

- Leverage [EDR] to contain a host. This prevents the host from communicating with anything other than the [EDR] cloud.
- Network segmentation can be performed by the network infrastructure/management SMEs.
- Legally valid forensic capture process. Detailed in: [TECHNOLOGY-SPECIFIC PLAYBOOKS].
- Temporary firewall rule changes/filtering can be performed by the Network infrastructure/management SMEs and [MSSP/MDR].
- Changing system admin passwords or rotating private keys and/or account secrets to revoke privileged access. These activities can be performed by the Active Directory, Account Management, and Server Administrator SMEs.

The containment scope must encompass all incident and adversarial activity. If new signs of compromise are identified following containment, the incident must be re-scoped to include the newly observed activity.

2.4 Eradication and Recovery

The primary objective for this phase is to facilitate the return to normal business operations by eliminating the malicious artifacts of the incident and mitigating the conditions that were initially exploited. This phase can begin once all the means of persistence have been accounted for, the adversary is sufficiently contained, and all needed evidence has been collected.

2.4.1 Eradication activities

The actions taken during the eradication portion of this phase are to eliminate all evidence of compromise and prevent the adversary from maintaining a presence in the environment.

- Confirm the scope of infected systems and environments that was identified in the investigation phase.
- Reimaging or rebuilding affected systems.
- Rebuilding hardware if required.
- Replacing compromised files with validated clean versions.
- Resetting passwords for compromised accounts.
- Patching systems and/or removing conditions which allowed initial compromise.
- Allow adequate time to ensure all systems are clear of persistence mechanisms.

2.4.2 Recovery actions

The main objective of this portion of the phase is to restore systems to normal operations and confirm they are functioning properly.

- Reconnecting rebuilt/new systems to networks.
- Increase security controls and rulesets.
- Thoroughly test systems, including newly implemented security controls.
- Monitor operations for abnormal behaviors.

2.5 Post Incident Activity

The objectives for this phase are to thoroughly document the incident, inform leadership, harden the environment, and apply lessons-learned to improve future incident response processes.

2.5.1 Adjust sensors, alerting, and log collection

Identify and address blind spots which did not have a [EDR] agent or adequate logging to the [SIEM] platform to detect early indicators of attack.

2.5.2 Finalize reports

Provide post incident updates to management and key stakeholders.

2.5.3 Lessons-learned

Conduct a lessons-learned analysis to review the effectiveness and efficiency of the incident handling. Document what improvements could be implemented in future incidents. Conduct final analysis to verify:

- Ensure root-cause has been eliminated or adequately mitigated.
- Identify organizational problems and/or procedures that may have created the conditions which lead to the initial compromise.
- Identify technical or operational training needs.
- Identify needed improvements to tools (or usage of tools) or threat intelligence to better perform prevention, detection, analysis, and response actions.

3. Coordination

Coordination between internal teams within [COMPANY] and external vendor/managed provider teams is a critical component of the incident response process.

3.1 Internal Coordination

The teams engaged in the incident response process can vary depending on observed activities in the incident. [COMMUNICATION SOFTWARE] will be used as a centralized coordination channel is needed for internal communications.

3.1.1 Corporate Security Team (Security Operations Center)

The CST is the primary team responsible for cybersecurity incident management and will be involved in all incident response efforts. The CST utilizes [COMMUNICATION SOFTWARE] and email to coordinate between its members and the members of other internal teams.

3.1.2 Network Operations Center (NOC)

The NOC is primarily responsible for monitoring network reliability and resource availability. Coordination between the CST and NOC will be necessary in identifying threats to the availability of [COMPANY] resources as well as performing network segmentations to contain adversarial activity. Additionally, cooperation with the CST and other technical service teams will be needed during the eradication and recovery process.

3.1.3 Technical services team

The technical services team includes desktop, laptop, and server system administrators. The CST will most commonly work with these teams in the containment phase, where [EDR] is not available and to better understand the operational impacts that containment activities may have. These teams will also work together during the eradication and recovery phase for the reimaging and rebuilding of affected systems and implementations of strengthened security controls.

3.1.4 DevOps team

The CST work with the DevOps team will be in areas similar to the technical services team. The DevOps team can aid and insight during the containment phase and perform eradication, rebuilding, and the strengthening of security controls.

3.2 External Coordination

[COMPANY] has relationships with several vendors and managed service providers and may require communication and coordination with their associated teams during the incident response process.

3.2.1 [MSSP/MDR]

The [MSSP/MDR] team is a managed service that provides 24/7 analysis and response to the systems that report to the [MSSP/MDR] platform. A separate playbook with their processes is available in the CST knowledgebase. This team will work with the CST in the detection, analysis, containment, and response/eradication activities. Communications with these teams are mostly through the [MSSP/MDR] platform, the support portal, and via email to: [EMAIL].

3.2.2 [MANAGED FIREWALL VENDOR]

[MSSP/MDR] provides 24/7 managed network and security services for the [FIREWALL] firewalls. The CST will work with their teams during planning, detection, analysis, and eradication activities. Communications are available for the two managed teams via email and phone.

[MANAGED SECURITY TEAM]:

Phone: [PHONE]

Email: [EMAIL]