**Name of Organization**

**Incident Response**

**Standard Operating Procedures**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

This (Name of Organization) Incident Response Standard Operating Procedure (SOP) is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction 5](#_Toc88584113)

[II. Incident Handling 5](#_Toc88584114)

[Initial Incident Handling Steps 6](#_Toc88584115)

[Generic Uncategorized Incidents - Handling Checklist 6](#_Toc88584116)

[Containment, Eradication, and Recovery Checklist 6](#_Toc88584117)

[III. Detailed SOP Instructions 8](#_Toc88584118)

[Root Access SOP 8](#_Toc88584119)

[Ransomware/Malware Outbreak SOP 11](#_Toc88584120)

[Elevation of Privileges SOP 14](#_Toc88584121)

[Unauthorized Access SOP 17](#_Toc88584122)

[Improper Computer Usage SOP 20](#_Toc88584123)

[Virus Outbreak SOP 23](#_Toc88584124)

[Phishing SOP 26](#_Toc88584125)

[Data Theft SOP 29](#_Toc88584126)

[DDoS SOP 32](#_Toc88584127)

# Introduction

This Standard Operating Procedure Document is intended to assist both newly formed and established incident response teams in managing key incidents to the correct approach. More precisely, this document covers the following key scenarios.

* Root Access - permissions to read, write to and administer systems and operating software
* Virus Outbreak - a virus, worm, Trojan horse, or other malicious entity comprised entirely of code that successfully infects a host
* Privilege escalations - users receive or manufacture privileges they are not entitled to
* Unauthorized Access - a person gains logical or physical access to a network, system, application, data, or other information technology resource without authorization
* Improper Computer Use - a person violates any network or computer policy governing acceptable use
* Ransomware/Malware Outbreak - malware that infected multiple assets and is spreading across networks and computers
* Phishing - sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software
* Data Theft - extraction or stealing of information
* Denial of Service (DoS) - an attack that prevents or impairs authorized use of networks, systems, or applications through resource exhaustion

For each incident there are several key steps to be performed. This document references the key major threats/risk that companies are experiencing and the exact process to follow, by whom, and in what order.

The Standard Operating Procedure (SOP) can be customized - if needed - based on the individual needs of departments and Organizational responsibilities.

# Incident Handling

The checklist below details the major steps that must be taken during the initial investigation of an incident. The items address only the detection and initial analysis of an incident; thereafter, incident handlers should refer to checklists tailored to the specific type of incident identified.

The actual steps taken will vary depending on the type of incident and the nature of the individual incidents. For instance, if the handler is certain what occurred based on an analysis of indications.

## Initial Incident Handling Steps

|  |  |  |
| --- | --- | --- |
| **Detection and Analysis** | | **Status** |
| Determine whether an incident has occurred |  | |
| Analyze the precursors and indications |  | |
| Look for correlating information |  | |
| Perform research (e.g., search engines, knowledge base) |  | |
| As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence. *(Use Incident Notification and Incident Management Log documents)* |  | |
|
| Classify the incident using the categories: malicious code; unauthorized access; inappropriate usage; multiple components. |  | |
| Follow the appropriate incident Standard Operating Processes outlines below |  | |

## Generic Uncategorized Incidents - Handling Checklist

|  |  |
| --- | --- |
| **Detection and Analysis** | **Status** |
| Prioritize handling the incident based on your business and operations impact (see Incident Categorization document and/or your Business Impact Analysis or Risk Management) |  |
| Identify which resources have been affected and forecast which resources will be affected |  |
| Estimate the current and potential technical and operational effect of the incident. If possible, assess cost of damage/remediation and if external help/support will be needed. |  |
| Report the incident to the appropriate internal personnel (e.g., Incident Commander, CIRT) and external organizations. |  |

## Containment, Eradication, and Recovery Checklist

|  |  |
| --- | --- |
| **Containment, Eradication, and Recovery** | **Status** |
| Acquire, preserve, secure, and document evidence obtained (logs, pictures, computers). *(Use Incident Response Toolkit, IR Forensic Intake and Chain of Custody Forms).* |  |
| Contain the incident (e.g., take compromised system offline, remove infected files) |  |
| Eradicate the incident |  |
| Identify and mitigate all vulnerabilities that were exploited |  |
| Remove malicious code, inappropriate materials, and other components |  |
| Recover from the incident (e.g., restore from safe backups, conduct lesson learned review). |  |
| Return affected systems to an operationally available state |  |

# Detailed SOP Instructions

## Root Access SOP

* Access which permits read and write to any files on the system, perform operations as any user including superuser, change system configuration, install and remove software, and upgrade the operating system and/or firmware.

There are several key Incident Response steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (e.g., Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Categorize Incident
* Define threat indicators (e.g., Alert from Anti-Virus, Extended Detection and Response [XDR], etc.)
* Discover new and unusual behavior on computer systems
* Discover addition of registry keys to automatically start processes at system boot-time
* Review antivirus detection notifications
* Ascertain if system is being used remotely to send spam or contribute to a DDoS attack
* Check network traffic for indications of unusual amounts or types of internal traffic, or changes in behaviors (if possible)

**Analyze**

* Review system and security logs on asset
* Collect logs and evidence on impacted assets
* Define timeline of suspicious behavior
* Investigate unexplained crashing of computer systems
* Investigate unauthorized and unexplained installation of software
* Investigate unexplained computer system performance issues
* Check with ISP and any other partners that have been contacted regarding this event
* Determine if customers are affected by this incident
* Determine if PII or other protected information at risk of being exposed
* Investigate products/goods/services that are affected by this attack
* Check for external/internal knowledge of this incident
* Start to determine worst-case business impact if unable to mitigate this attack

**Containment**

* Identify the systems that have been affected (e.g., Servers, Desktop, Laptop)
* Identify user credentials compromised or at risk (e.g., Lightweight Directory Access Protocol [LDAP], Virtual Machine [VM], Mobile)
* Identify IT services being impacted
* Identify additional system(s) that are at risk of being compromised
* Identify malicious code on any system(s) linked to fraudulent sites
* Identify business implications of the attack
* Identify any source attribution collected
* Identify how widespread the attack has spread (e.g., View Report, View Record Details, Select Records, Copy Record Details)
* Identify the tools used to detect the attack (e.g., Intrusion Detection System [IDS], Security Information and Event Management [SIEM], Firewall, Antivirus, Scanners)
* Identify

**Eradicate**

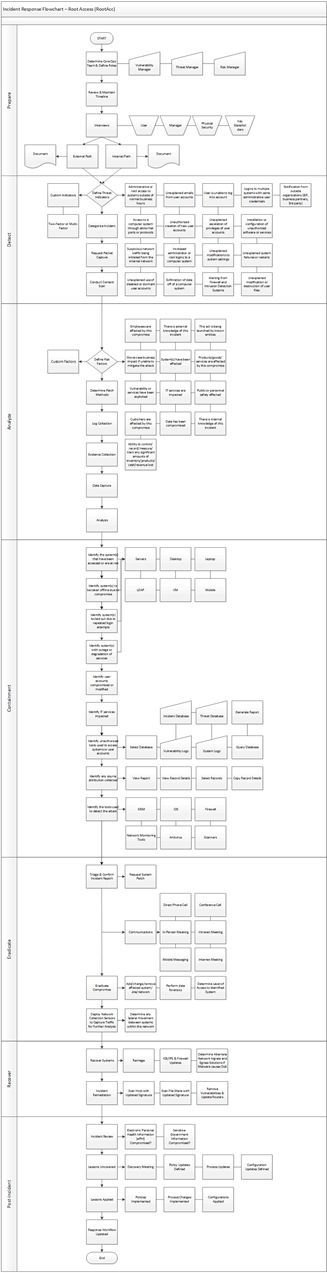
* Prevent Spread (e.g., Run in Sandbox, Analyze in Forensics, Block with Antivirus, Disable Services, Restrict Network)
* Apply SIEM Rules
* Adjust Firewall Rules
* Eradicate Malware (e.g., Clean with Antivirus, Quarantine with Antivirus, Malware Removal Tool, Manual Intervention)
* Deploy Network Collection Sensors and Traffic analysis tools

**Recover**

* Recover Systems and Data
* Reimage
* Remove Vulnerabilities
* Determine alternate Network Ingress and Egress Solutions

**Post Incident Review**

* Perform Incident Review and lesson learned
* Check to see if Personally Identifiable Information (PII) is Compromised
* Check to see if Sensitive Government Information Compromised
* Update policies and procedures if needed
* Apply configuration changes
* Apply lesson learned and applied



## Ransomware/Malware Outbreak SOP

* With several hundred workstations within an organization accessing open file shares, a worm can quickly infect those several hundred workstations. An organization is typically notified via email by their antivirus vendor that a new worm is spreading rapidly across the Internet. In this case there are several Incident Response key steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (e.g., Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Define threat indicators (e.g., Alert from Anti-Virus, XDR, etc.)
* Discover new and unusual directories on computer systems
* Discover addition of registry keys to automatically start processes at system boot-time
* Discover unexplained encrypted data files on computer systems
* Check network traffic for indications of unusual amounts or types of internal traffic, or changes in behaviors (if possible)
* Investigate unauthorized and unexplained installation of software
* Investigate unexplained computer system performance issues

**Analyze**

* Define Risk Factors
* Custom Factors, Public or personnel safety affected
* Check with ISP and any other partners that have been contacted regarding this event
* Determine if customers are affected by this incident
* Determine if PII or other protected information at risk of being exposed
* Investigate products/goods/ services that are affected by this attack
* Determine ability to control/record/measure/track any significant amounts of inventory/product/cash/revenue lost – *Note: This incident could be exploited for criminal activity*
* Check for external/internal knowledge of this incident
* Start to determine worst-case business impact if unable to mitigate this attack

**Containment**

* Identify the systems that have been affected (e.g., Servers, Desktop, Laptop)
* Identify user credentials compromised or at risk (e.g., LDAP, VM, Mobile)
* Identify IT services being impacted
* Identify additional system(s) that are at risk of being compromised
* Identify malicious code on any system(s) linked to fraudulent sites
* Identify business implications of the attack
* Identify any source attribution collected
* Identify how widespread the attack has spread (e.g., View Report, View Record Details, Select Records, Copy Record Details)
* Identify the tools used to detect the attack (e.g., IDS, SIEM, Firewall, Antivirus, Scanners)

**Eradicate**

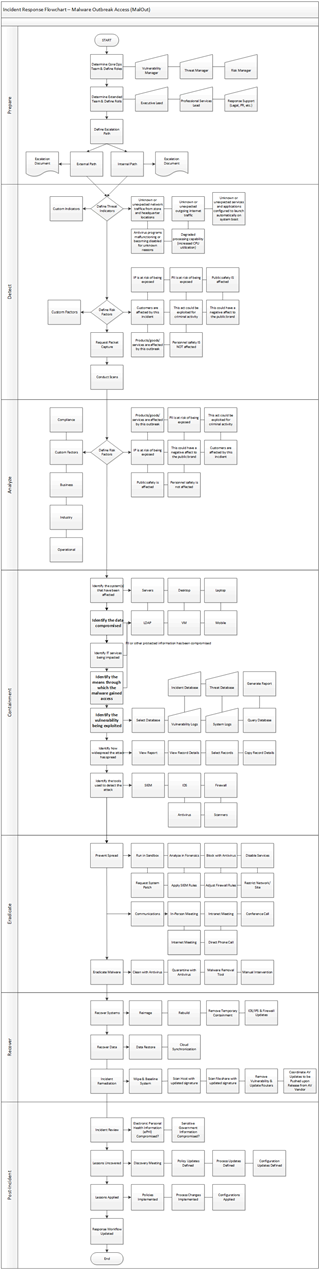
* Prevent Spread (Run in Sandbox, Analyze in Forensics, Block with Antivirus, Disable Services, Restrict Network)
* Apply SIEM Rules
* Adjust Firewall Rules
* Eradicate Malware (Clean with Antivirus, Quarantine with Antivirus, Malware Removal Tool, Manual Intervention)

**Recover**

* Recover Systems/Reimage/Rebuild
* Remove Temporary Containment
* Remove Vulnerabilities
* Update network devices with signatures and improved rules

**Post Incident Review**

* Perform Incident Review and lesson learned
* Check to see if PII (Personal Identifiable Information) is Compromised
* Check to see if Sensitive Government Information Compromised
* Update policies and procedures if needed
* Apply configuration changes
* Apply lesson learned



## Elevation of Privileges SOP

* Privilege escalation is a common threat vector for adversaries, which allows them to enter organizations’ IT infrastructure and seek permissions to steal sensitive data, disrupt operations and create backdoors for future attacks.
* Privilege escalation happens when a malicious user gains access to the privileges of another user account in the target system
* act of exploiting a bug, a design flaw, or a configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

There are several Incident Response key steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (e.g., Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Discover increased user logins
* Discover addition and multiple user loggings from different locations
* Ascertain if system is being used remotely to send spam or contribute to a DDoS attack
* Check for unauthorized creation of new user accounts
* Check for unexplained modifications to system settings
* Investigate unexplained crashing of computer systems
* Investigate unauthorized and unexplained installation of software
* Investigate unexplained computer system performance issues

**Analyze**

* Investigate source of attack
* Ability to control/record/measure/track any significant amount of inventory
* Check for external/internal knowledge of this incident

**Containment**

* Identify the systems that have been affected (e.g., Servers, Desktop, Laptop)
* Identify user credentials compromised or at risk (e.g., LDAP, VM, Mobile)
* Identify IT services being impacted
* Identify additional system(s) that are at risk of being compromised
* Identify malicious code on any system(s) linked to fraudulent sites
* Identify business implications of the attack
* Identify any source attribution collected
* Identify how widespread the attack has spread (e.g., View Report, View Record Details, Select Records, Copy Record Details)

**Eradicate**

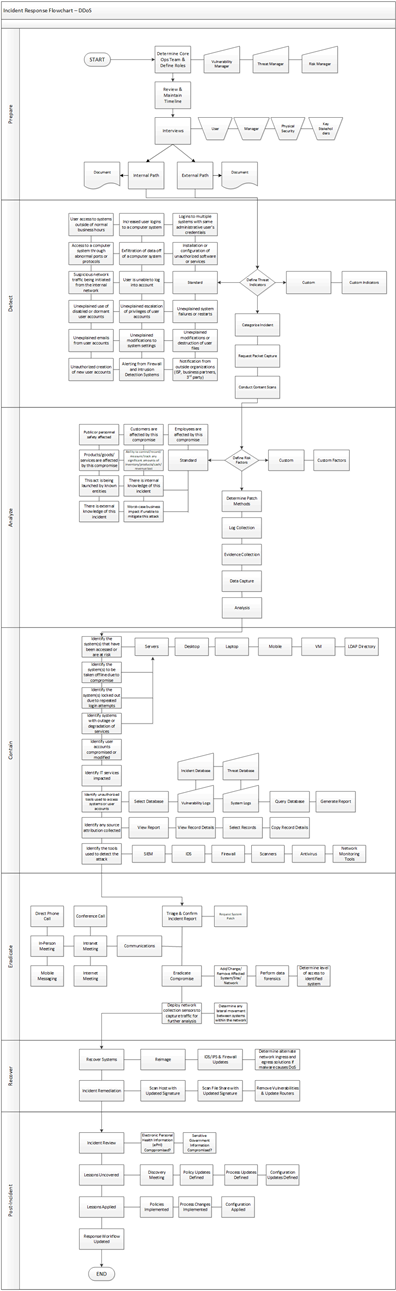
* Deploy network collection sensors to capture traffic
* Determine any lateral movement between systems
* Add/Change/Remove/Affected System/SIEM/Network
* Perform data forensics
* Adjust Firewall Rules
* Eradicate Malware (e.g., Clean with Antivirus, Quarantine with Antivirus, Malware Removal Tool, Manual Intervention)

**Recover**

* Recover Systems
* Scan Host with updated signature
* Remove Temporary containment
* Remove vulnerabilities and update routers

**Post Incident Review**

* Perform Incident Review and lesson learned
* Update policies and procedures if needed
* Apply configuration changes
* Apply lesson learned



## Unauthorized Access SOP

* A perpetrator gains unauthorized administrator access to a system and the sensitive data contained within, and then threatens the victim that the details of the break-in will be made public unless the organization pays a specified sum of money.

There are several Incident Response key steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (e.g., Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Define threat indicators (e.g., Alert from logs etc.)
* Increased logins to a computer system
* Discover addition of registry keys to automatically start processes at system boot-time
* Unexplained escalation of privileges
* Unexplained modifications or destruction or user files
* Discover unexplained encrypted data files on computer systems
* Discovery new and unusual registry keys on computer systems
* Investigate access to systems outside of business hours

**Analyze**

* Define Risk Factors
* Determine if customers are affected by this incident
* Determine if PII or other protected information at risk of being exposed
* Investigate products/goods/ services that are affected by this attack
* Check for external/internal knowledge of this incident
* Start to determine worst-case business impact if unable to mitigate this attack
* Identify additional business risk

**Containment**

* Identify the systems that have been affected (e.g., Servers, Desktop, Laptop)
* Identify user credentials compromised or at risk (e.g., LDAP, VM, Mobile)
* Identify additional system(s) that are at risk of being compromised
* Identify malicious code on any system(s) linked to fraudulent sites
* Identify business implications of the attack
* Identify any source attribution collected
* Identify how widespread the attack has spread (e.g., View Report, View Record Details, Select Records, Copy Record Details)

**Eradicate**

* Prevent Spread (e.g., Run in Sandbox, Analyze in Forensics, Block with Antivirus, Disable Services, Restrict Network)
* Apply SIEM Rules
* Adjust Firewall Rules
* Eradicate Malware (e.g., Clean with Antivirus, Quarantine with Antivirus, Malware Removal Tool, Manual Intervention)
* Deploy Network Collection Sensor to Capture Traffic

**Recover**

* Recover Systems
* Reimage/Rebuild
* Remove Temporary Containment
* Update access control system policies

**Post Incident Review**

* Perform Incident Review and lesson learned
* Update policies and procedures if needed
* Apply lesson learned

A sheet of music

Description automatically generated with low confidence

## Improper Computer Usage SOP

* Through peer-to-peer file sharing services, a user distributes illegal copies of software to others.
* A person sends an email threatening another person (e.g., cyberbullying)
* Use of a computer to carry out improper or illegal activities
* Violation of an organization's acceptable-use policies by an authorized user

There are several Incident Response key steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (e.g., Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Review excessive amount of web browsing traffic or downloads
* Review indication of large emails being sent received
* Check for unexplained malware, spyware or virus infections
* Use of unauthorized communication methods or network protocols

**Analyze**

* Check with ISP and any other partners that have been contacted regarding this event
* Determine if customers are affected by this incident
* Determine if PII or other protected information at risk of being exposed
* Investigate products/goods/ services that are affected by this attack
* Determine ability to control/record/measure/track any significant amounts of inventory/product/cash/revenue lost – *(This incident could be exploited for criminal activity)*
* Check for external/internal knowledge of this incident
* Vulnerabilities or services that have been exploited

**Containment**

* Identify the systems that have been affected (e.g., Servers, Desktop, Laptop)
* Identify user credentials compromised or at risk (e.g., LDAP, VM, Mobile)
* Identify IT services being impacted
* Identify additional system(s) that are at risk of being compromised
* Identify malicious code on any system(s) linked to fraudulent sites
* Identify business implications of the attack
* Identify any source attribution collected
* Identify how widespread the attack has spread (e.g., View Report, View Record Details, Select Records, Copy Record Details)

**Eradicate**

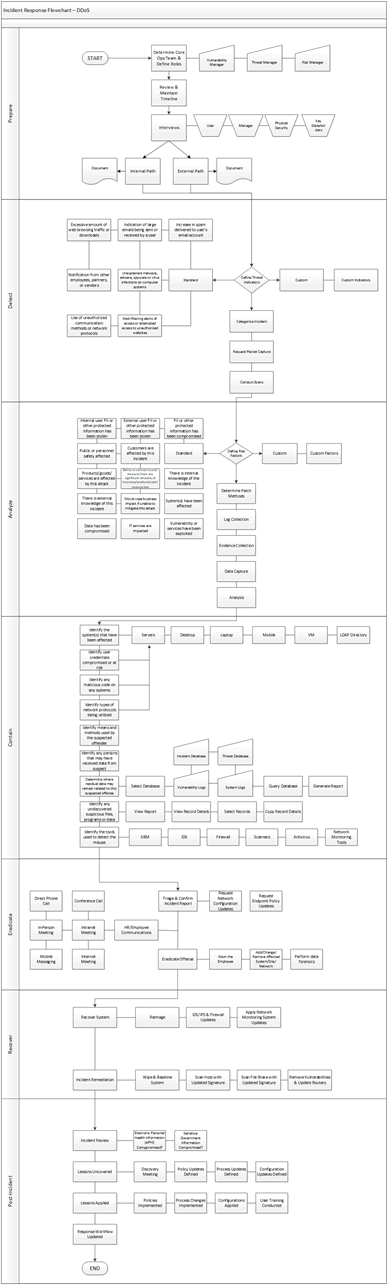
* Request Network Configuration Updates
* Eradicate Malware (e.g., Clean with Antivirus, Quarantine with Antivirus, Malware Removal Tool, Manual Intervention)

**Recover**

* Recover and restore Systems and/or Data
* Reimage or rebuild
* Remove Temporary Containment
* Apply network monitoring System Updates

**Post Incident Review**

* Perform Incident Review and lesson learned
* Update policies and procedures if needed
* Apply configuration changes
* Apply lesson learned



## Virus Outbreak SOP

* Computer viruses are a subcategory of malware that got their name from the way they spread by "infecting" other files on a disk or computer. Viruses then spread to other disk drives and machines via downloads from websites, email attachments, shared drives, or physical media such as USB flash drives or—in the early days—floppy disks.

There are several Incident Response key steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Define threat indicators (e.g., Virus alerts, user notification, service degradation, spam emails)
* Discover new and unusual directories on computer systems
* Discover addition of registry keys to automatically start processes at system boot-time
* Review antivirus detection notifications
* Discovery new and unusual registry keys on computer systems
* Ascertain if system is being used remotely to send spam or contribute to a DDoS attack
* Search remote systems for keyword strings
* Investigate unexplained crashing of computer systems
* Investigate unauthorized and unexplained installation of software
* Investigate unexplained computer system performance issues

**Analyze**

* Custom Factors, Public or personnel safety affected
* Check with ISP and any other partners that have been contacted regarding this event
* Determine if customers are affected by this incident
* Determine if PII or other protected information at risk of being exposed
* Investigate products/goods/ services that are affected by this attack
* Determine ability to control/record/measure/track any significant amounts of inventory/product/cash/revenue lost – *(This incident could be exploited for criminal activity)*
* Check for external/internal knowledge of this incident
* Start to determine worst-case business impact if unable to mitigate this attack

**Containment**

* Identify the systems that have been affected (e.g., Servers, Desktop, Laptop)
* Identify user credentials compromised or at risk (e.g., LDAP, VM, Mobile)
* Identify IT services being impacted
* Identify additional system(s) that are at risk of being compromised
* Identify malicious code on any system(s) linked to fraudulent sites
* Identify business implications of the attack
* Identify any source attribution collected
* Identify how widespread the attack has spread (e.g., View Report, View Record Details, Select Records, Copy Record Details)

**Eradicate**

* Prevent Spread (e.g., Run in Sandbox, Analyze in Forensics, Block with Antivirus, Disable Services, Restrict Network)
* Run in sandbox/reverse engineer malware
* Eradicate Malware (e.g., Clean with Antivirus, Quarantine with Antivirus, Malware Removal Tool, Manual Intervention)

**Recover**

* Recover Systems
* Remove Temporary Containment
* Recover Data
* Data Restore

**Post Incident Review**

* Lessons Uncovered
* Policy and Process Updates Defined
* Configuration Updates Defined
* Policies Implemented
* Process Changes Implemented
* Configurations Applied
* Response Workflow Updated

Diagram, schematic

Description automatically generated

## Phishing SOP

* An attempt by cybercriminals posing as legitimate institutions, usually via email, to obtain sensitive information from targeted individuals.
* The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

There are several Incident Response key steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (e.g., Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Identification of spoofed system
* Check peaked amount of inbound data
* Detection of unknown or unidentified packets from unknown senders
* Notification from outside organizations (e.g., ISP, business partners, 3rd party)
* Define Threat Indicators
* Request Packet Capture

**Analyze**

* Products/goods/ services are affected by this attack
* Define Risk Factors
* Check for external/internal knowledge of this incident
* Determine worst-case business impact if unable to mitigate this attack
* Determine Patch Methods
* Review network or asset logs for suspicious events
* Conduct additional evidence Collection

**Contain**

* Capture Relevant Data
* Identify the system(s) that have been targeted (e.g., Servers, Desktop, Laptop, Mobile, VM, LDAP)
* Identify the system(s) that have suffered outage or degradation of services
* Identify critical systems that are at risk
* Identify the system(s) that have suffered outage or degradation of services
* Identify the IT services being impacted
* Identify critical choke points or bottlenecks on network that could increase the effect
* Establish best plan to contain this event (e.g., taking assets offline, disabling services).

**Eradicate**

* Identify the source and if their network can be blacklisted
* Identify additional traffic rerouting or egress filtering to block more traffic
* View Report, View Record Details, Select Records, Copy Record Details
* Identify the tools used to detect the attack (e.g., SIEM, IDS, Firewall, Scanners, Antivirus, Network Monitoring Tools)

**Recover**

* Triage & Confirm Incident Report
* Request System Patch
* Add/Change/Remove Affected System/Site/ Network
* Identify any alternate course for business operations
* Create whitelist of Source IPs & services that must be allowed into network
* IDS/Intrusion Protection System (IPS) & Firewall Updates
* Determine alternate network ingress and egress solutions

**Post Incident Review**

* Perform Incident Review and lesson learned
* Update policies and procedures if needed
* Apply configuration changes
* Apply lesson learned

A sheet of music

Description automatically generated with low confidence

## Data Theft SOP

* Data Theft is an attack that results in the extraction and exfiltration of data from the organization.
* An incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner.

There are several Incident Response key steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (e.g., Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Define Threat Indicators
* Define Escalation Path
* Categorize Incident
* Check for emails returned as undeliverable due to size limitations
* Check for identification or publication of proprietary information outside the organization
* Check for notification of extortion to recover stolen data
* Check for local disk or network shares that are near full capacity
* Check for work performed outside of normal business hours
* Check for any reporting of large emails being sent by a single user
* Check for reports of removable and/or mobile devices being used to copy data
* Check for large data dumps of databases, network shares or other computer systems
* Conduct Packet Capture to identify suspicious activities

**Analyze**

* Define Risk Factors
* Is public or personnel safety affected
* Is stolen data damaging to business operations or brand of the organization
* Have PII or other protected information been compromised/stolen
* Have Compliance regulations been violated?
* Any customers affected by this incident
* Products/goods/services affected
* Is there indication of who performed the data theft
* Is there is internal knowledge of this incident
* Identify worst-case business impact if unable to mitigate this attack
* identify Business implications of the Data Theft
* Identify business operations that may be affected and identify any alternate courses

**Containment**

* Identify the system(s) that have been affected (e.g., Servers, Desktops, Laptops)
* Identify user credentials compromised or at risk, Mobile, VM, LDAP
* Identify method used to steal data
* Identify system(s) used to steal data
* Identify any source attribution collected (e.g., Select Database, Vulnerability Logs, System Logs, Query Database, Incident Database, Threat Database, Generate Report)
* Identify lateral movement of compromised users throughout enterprise
* View Report, View Record Details, Select Records, Copy Record Details
* Identify the tools used to detect the attack, (e.g., SIEM, IDS, Firewall, Scanners, Antivirus, Network Monitoring Tools)

**Eradicate**

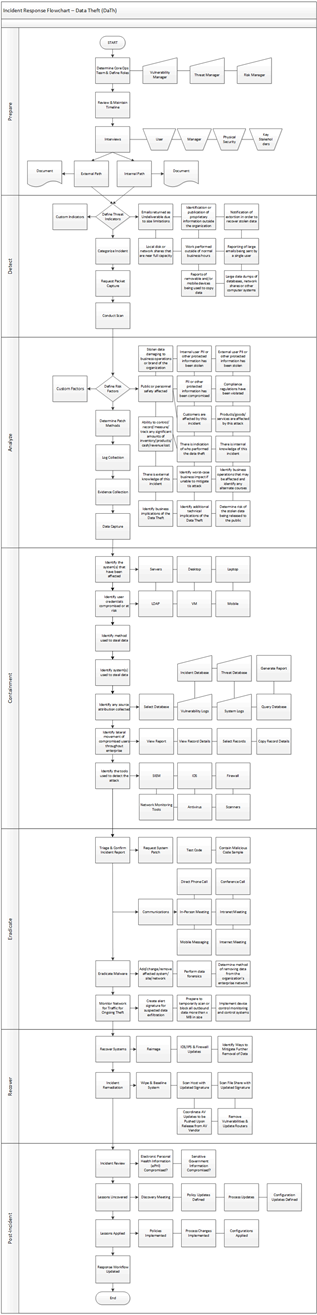
* Triage & Confirm Incident Report
* Request System Patch
* Add/change/remove affected system/ site/network
* Determine method of removing data from the organization’s enterprise network
* Monitor Network for Traffic for Ongoing Theft
* Create alert signature for suspected data exfiltration
* Prepare to temporarily scan or block all outbound data more than x MB in size
* Implement device control monitoring and control systems

**Recover**

* Recover Systems
* Reimage
* IDS/IPS & Firewall Updates
* Identify Ways to Mitigate Further Removal of Data
* Wipe & Baseline System
* Scan Host with Updated Signature
* Scan File Share with Updated Signature
* Coordinate AV Updates to be Pushed Upon Release from AV Vendor
* Remove Vulnerabilities & Update Routers

**Post Incident Review**

* Perform Incident Review and lesson learned
* Update policies and procedures if needed
* Apply configuration changes
* Apply lesson learned



## DDoS SOP

* A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
* An attack that prevents or impairs authorized use of networks, systems, or applications through resource exhaustion.

There are several Incident Response key steps to be performed as follows:

**Prepare**

* Determine Core Ops Team & Define Roles (e.g., IT Team, CIRT)
* Determine Extended Team (e.g., Exec Lead, Pro Service Lead, Legal, PR, etc.)
* Review Timeline
* Perform interviews (e.g., User, IT Manager, Key Stakeholders)
* Document Incident - *use “Incident Notification Form”*

**Detect**

* Unknown or unexpected incoming Internet traffic
* Peaked amount of inbound data
* Detection of unknown or unidentified packets from unknown senders
* Alerting from Firewall and Intrusion Detection Systems
* Notification from outside organizations (e.g., ISP, business partners, 3rd party)
* Categorize Incident
* Request Packet Capture

**Analyze**

* Public or personnel safety affected
* Products/goods/ services are affected by this attack
* Ability to control/record/measure/track any significant amounts of inventory/products/cash/revenue lost
* This act is being launched by known entities
* There is internal/external knowledge of this incident
* Worst-case business impact if unable to mitigate this attack
* Collect logs and review

**Containment**

* Identify the system(s) that have been targeted (e.g., Servers, Desktop, Laptop, Mobile, VM, LDAP)
* Identify the system(s) that have suffered outage or degradation of services
* Identify the IT services being impacted
* Identify critical systems that are at risk from DoS/DDoS
* Identify the system(s) that have suffered outage or degradation of services
* Identify critical systems that are at risk from DoS/DDoS
* Identify type of packets being utilized
* Identify critical choke points or bottlenecks on network that could increase the effect

**Eradicate**

* Identify the source and if their network can be Blackholed
* Request network segment or other configuration change
* Identify additional traffic rerouting or egress filtering to block more traffic
* Create whitelist of source IPs and services that must be allowed

**Recover**

* Reimage
* IDS/IPS & Firewall Updates
* Determine alternate network ingress and egress solutions if malware causes DoS
* Incident Remediation

**Post Incident Review**

* Perform Incident Review and lesson learned
* Update policies and procedures if needed
* Apply configuration changes
* Apply lesson learned

