CYBERSECURITY INCIDENT RESPONSE PLAN 1

Standards:

1. NIST Special Publication 800-61
2. NIST Cybersecurity Framework (CSF)

Compliance:

1. ISO 27001 – A.16
2. PCI DSS 3 – 10, 12.9

Regulation:

1. EU GDPR – Article 33, 34
2. CA CCPA - Standard of Reasonable Cybersecurity - Incident Response Plan

https://t.me/learningnets

DESCRIPTION

Cybersecurity

The words cybersecurity and security are synonymous and used interchangeably herein. Cybersecurity is the state of being protected against the violation of computer security policies, acceptable use policies, or standard security practices, or the measures taken to achieve this.

Asset

The words asset, information asset, information technology resource, and other processing activities are synonymous and used interchangeably herein.

Event

An event is an observable occurrence in a digital ecosystem or computer network. Event examples include a login, a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

Alert

The words alert and alarm are synonymous and used interchangeably herein.

An alert is an event having a security context usually generated from threat detection assets or treat hunting routines. Alerts may be the result of a negative consequence and generally require subsequent inspection. Examples of alerts include system crashes, unauthorized use of system privileges, unauthorized access to sensitive data, execution of malware, and destruction of data.

Incident

The word incident and the term event of critical interest are synonymous and used interchangeably herein.

An incident is an event or alert that signifies a security control failure, or a violation, or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that require critical triage and a more in-depth investigation known as **incident response**.

During disciplined cybersecurity operations, including investigating and analyzing alerts, it is common for information security professionals to label the resulting analysis in terms of risk of compromise. An incident, or event of critical interest, is an analysis that results in a declaration of **real or imminent danger and significant risk of asset compromise** or confirmation thereof.

https://t.me/learningnets

As an example, take two classes of typical cybersecurity events: *potentially unwanted program* and *ransomware*. The latter, ransomware, represents an event of critical interest because its progression through the environment represents real and imminent danger and could result in a significant risk of compromise to critical assets.

Another example may be an individual receiving a *phishing email* and realizing that it has attached malware, is in of itself NOT an incident (detective controls worked). However, an individual downloading that attached malware IS possibly an incident (preventative or corrective controls did not work) dependent on subsequent control failures (defense-in-depth failures) or **real or imminent danger and significant risk of asset compromise** or confirmation thereof.

An analogy in the natural world might be the comparison of a misdemeanor *vehicular moving violation* to a felony *armed robbery*. The latter, armed robbery, would be considered an incident.

Instruction

Implementers of this IRP use a **PICERL** model as guidance for organizing courses of action (COA):

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons / Opportunities For Improvement

Implementers of this IRP use an **OODA** loop as guidance for conducting COA:

1. Observe
2. Orient
3. Decide
4. Act

Preparation

Roles

1. ISO

https://t.me/learningnets

i. The Information Security Office or Officer(s) or designated representative(s) shall be responsible for ensuring the *strategic* effectiveness of this IRP.

2. CSIRT
    i. The Computer Security Incident Response Team or designated representative(s) shall be responsible for ensuring the *tactical* effectiveness of this IRP.

Risk Management

The ISO shall be responsible for establishing risk management strategies that meet or exceed a standard of reasonable cybersecurity practices. These activities protect information assets, controls, and processes against a violation of the organization's computer security policies or acceptable use policies. The ISO is responsible for establishing controls and processes aligned with the five (5) core functions of Cybersecurity Risk Management as defined by the NIST Cybersecurity Framework (CSF).

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Cybersecurity Technology Controls

The CSIRT shall routinely conduct inspections of the cybersecurity technology controls (cyber weapon assets) used to detect and or prevent incidents to ensure cyberweapon readiness. The CSIRT shall own the responsibility of remediating defects, disruptions, or degradation of cyber weaponry assets and security controls. The ISO shall routinely request from the CSIRT a report of the state of cyber weaponry assets and security controls readiness. The CSIRT shall promptly comply with an ISO request for a report of the state of cyber weaponry assets, and security controls readiness and maintain the provided report for no less than one (1) year.

Severity Ratings

This IRP uses the priority levels defined in the US National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Scoring System (CISS) as the model for rating the severity of an Information Security Incident.

https://t.me/learningnets

Severity rating levels shall be used to determine the necessary force and resource prioritization required to handle and respond to an incident. The CSIRT is responsible for declaring the initial severity rating. The ISO is responsible confirming and adjusting security ratings that meet or exceed a High rating.

Tactics, Techniques & Procedures

The CSIRT and ISO shall use qualified Information Security Personnel, and cyber weapons, and security controls capable of defending and preventing adversaries from using specific tactics, techniques, and procedures as described by the MITRE ATT&CK Framework.

Log Retention

The ISO shall be responsible for ensuring that log data transmitted by assets is properly preserved, protected, and maintained for a period of one (1) year.

Alert Response & Threat Hunting

The CSIRT shall respond to alerts generated by cyber weapons and security controls. The CSIRT shall routinely patrol (threat hunt) and audit log data and assets for indicators of compromise.

Evidence Collection & Preservation

The CSIRT shall establish an electronic/virtual evidence locker to store and protect evidence collected during incident response. The CSIRT should maintain an electronic journal (manifest) of collection activities and their related evidence artifacts. The CSIRT shall maintain an electronic chain of custody ledger that includes the date, the evidence artifact, the transferrer, and the transferee for all activities involving the transfer of collected artifacts from the evidence locker to authorized recipients or electronic media. The ISO shall approve all transfers of evidence artifacts to authorized recipients or electronic media.

The ISO shall maintain and protect evidence locker artifacts collected during an Information Security Incident for one (1) year from the date of the initial detection. The ISO shall maintain and protect the Information Security Incident after-action incident report and any related communications for one (1) year from the date of the initial detection.

Restoring Operations

https://t.me/learningnets

The ISO shall certify that assets impacted by a successful compromise are eligible for being restored to their normal operational state only after remediation activities have prevented the assets from further risk of intrusion.

After-Action Report

The CSIRT shall produce an after-action report that provides the details of the incident. The CSIRT should produce content for the report iteratively during the response. The ISO shall approve all dissemination of the report.

Coordination, Sharing & Notifications

Internal

The ISO shall be responsible for coordinating and sharing details of an incident to internal authorized Personnel, without undue delay on a need to know basis, when the ISO deems that sharing is beneficial to response activities and per the organization's data classification policies.

Individuals, Customers & Data Subject Notifications (EU GDPR 34)

The ISO shall be responsible for coordinating and delivering notifications, without undue delay, to individuals, customers, and data subjects for the purposes of complying with statutes, regulations, or ordinances if the ISO determines the incident is likely to result in an infringement of, or high risk to, the rights and freedoms of those individuals, customers, and data subjects that have been impacted by the compromised assets.

Controller & Supervisory Authority Notifications (EU GDPR 33)

The ISO shall be responsible for coordinating and delivering notifications, within seventy two (72) hours of identifying an incident, to the supervisory authority (when organization is acting as a controller) or the controller (when organization is acting as a processor) for the purposes of compliance with the EU GDPR regulation if the ISO determines the incident is likely to result in an infringement of, or high risk to, the rights and freedoms of those individuals, customers, and data subjects that have been impacted by the compromised assets and/or information technology resources.

US State Authority Notifications

https://t.me/learningnets

The ISO shall be responsible for coordinating and delivering notifications, without undue delay, to various state authorities for the purposes of complying with statutes, regulation, or ordinances if the ISO determines the Information Security Incident is likely to result in an infringement of, or high risk to, the rights and freedoms of those individuals, customers, and data subjects that have been impacted by the compromised assets and/or information technology resources.

Law Enforcement

The ISO shall be responsible for notifying law enforcement to comply with statutes, regulation, or ordinances or threat actor prosecution if the ISO determines the incident meets the standard of a condition identified through discussions with law enforcement representatives provided such discussions have previously taken place. The ISO shall refrain from contacting multiple agencies when reporting an incident to avoid jurisdictional conflicts. The following is a list of law enforcement agencies:

1. Federal Bureau of Investigation
2. U.S. Secret Service
3. District Attorney
4. State Attorney General

Media

The ISO shall be responsible for coordinating and sharing the relevant details of an incident, without undue delay on a need to know basis, with the media when the ISO deems that sharing is beneficial to response activities and per the organization's data classification policies.

External Service Providers

The ISO shall be responsible for coordinating and sharing the relevant details of an incident, without undue delay on a need to know basis, with the organization's trusted 3rd party service providers when the ISO deems that sharing is beneficial to response activities and per the organization's data classification policies.

1. Cybersecurity-as-a-Service Providers
2. Incident Response Partners
3. Legal Counsel
4. Crisis Management Partners
5. Cybersecurity Insurance Broker

Response Practice

https://t.me/learningnets

1. Use real world IOC-Negative scenarios as if they were IOC-Positive to train response personnel and gauge response effectiveness
2. Become Familiar With Breach Notification Laws
    i. Security Breach Notification Laws

Identification

Assess & Rate

1. Breathe
2. Think "smooth is fast"
3. Inspect change logs to determine if activity is possibly the result of an authorized change
4. Review system baselines to determine if activity is possibly the result of expected behavior
5. Ask asset owners what they know in terms of Indicators Of Compromise (IOC) and record the results
    i. Top Indicators of Compromise (TOP-IOC) below for hints
    ii. MITRE ATT&CK Framework for hints
6. Ask asset owners **"Was there a loss of data?"** and record the results
7. Ask asset owners **"Was restricted data at risk?"** and record the results
8. Assign a severity rating
    i. NCCIC CISS Severity Rating Model

Memorialize & Share

IMPORTANT - When possible encrypt communication - threat actors may be listening to the channel

1. Make notes of actions you took during the assessment phase
    i. What you do, see, and hear will be used by investigators, after-action reporting, and maintained for posterity purposes
2. Record times
3. Communicate using 24HR/military time (e.g. 0900, 1330, 1845)
4. Record atomic attributes
5. Record behavioral attributes
6. Make factual assertions backed by evidence
7. Peer review observations and assertions with experienced personnel

https://t.me/learningnets

8. Mark email communication with "CONFIDENTIAL//ATTORNEY-CLIENT PRIVILEGE//TLP:AMBER" labels
9. Use encryption or an alternative band of communication if the material is extremely sensitive

Collect

IMPORTANT - Keep a system POWERED ON prior to the collection of volatile media to preserve valuable evidence
(isolate the host by disconnecting its network connection or through the use of EDR)

1. Journal collection activities
2. Conduct log analysis
3. Conduct system forensics
    i. Use a DFIR checklist
    ii. Acquire volatile media
    iii. Acquire non-volatile media

Store

1. Follow a consistent evidence process that achieves the objective of provenance
2. Journal evidence activities
3. Establish an evidence locker
4. Preserve evidence

Contain

CONTAINMENT IS THE MOST IMPORTANT COA DURING INCIDENT RESPONSE

1. Create a list of COA based on the nature of the threat
2. Use the OODA loop method as guidance for COA
3. Organize the COA by using the mnemonic: **Inventory + 6-Ds**
    i. Inventory
    ii. Detect
    iii. Deny
    iv. Disrupt
    v. Degrade
    vi. Deceive
    vii. Destroy

https://t.me/learningnets

4. Force rank COA based on strategies that:
    i. Mitigate risk
    ii. Create an advantage for the responders
    iii. Preserve evidence
    iv. Consider collateral damage
    v. Align with policies
    vi. Respect the law
5. Use the properly maintained cyber weapons to fortify the **Inventory + 6-Ds**
6. Apply defensive and offensive force concentration tactics
    i. *NOTE: Force concentration does not guarantee relief from a flank of routine threat activity: **watch the wire!**
    ii. *NOTE: Force concentration is useless if containment assets are idle: **assign COA & put weapons to use**
7. Manage fatigue to avoid defective decision making and maintain consistent pressure on the adversary
8. Avoid decision avoidance, solve the problem, embrace the challenge, and be fast-acting
9. Get in the fight and regain control of the impacted assets!

Eradicate / Remediate

1. Inspect the asset to ensure the threat has been fully eradicated
2. Remediate all known vulnerabilities
3. Apply controls to prevent further intrusion

Recover / Restore

IMPORTANT - Restore only after remediation activities have prevented the assets from further risk of intrusion

1. Restore to a normal state
    i. Recovery point objective (RPO)
    ii. Recovery time objective (RTO)

Lessons / Opportunities For Improvement (OFI)

https://t.me/learningnets

1. Develop OFI as gaps are discovered during the response
2. Record the OFI in the after-action report

After-Action Report

1. Develop content for the report in an iterative manner as response activities are being conducted
2. Supply detailed and factual statements and artifacts
    i. Summary
    ii. Timelines (attack & response sequences)
    iii. Indicators of Compromise (IOC) (the nouns of the attack)
    iv. Intrusion Kill Chain (IKC) (threat actors activity - bad guy verbs)
    v. Courses of Action (COA) (reponders activity - good guy verbs)
    vi. Opportunities for Improvement (OFI) (lessons learned)
3. Disseminate the report

Notify External Entities

1. Individuals, Customers, & Data Subjects
2. Data Controllers
3. Supervisory Authorities
4. US State Authorities
5. Law Enforcement
6. Credit Reporting Agencies
7. The Media

Engage 3rd Party Service Providers

1. Cybersecurity-as-a-Service Providers
2. Incident Response Partners
3. Legal Counsel
4. Crisis Management Partners
5. Insurance Brokerage

EXAMPLES

TOP-IOC Annotation Statements

https://t.me/learningnets

```
# IOC NEGATIVE
## TOP-IOC: Attack surface DOES NOT exist
## TOP-IOC: Attack surface vulnerability DOES NOT exist
## TOP-IOC: Mitigating controls DO EXIST and ARE currently protecting the asset
## TOP-IOC: Subsequent attack activity DOES NOT exist
## TOP-IOC: Corroboration from other assets DOES NOT exist
## TOP-IOC: NOT CONSISTENT with unusual egress network traffic
## TOP-IOC: NOT CONSISTENT with unusual lateral movement
## TOP-IOC: NOT CONSISTENT with login anomalies
## TOP-IOC: NOT CONSISTENT with suspicious domain controller activity
## TOP-IOC: NOT CONSISTENT with suspicious byte counts

----

# IOC POSITIVE
## TOP-IOC: Attack surface DOES exist
## TOP-IOC: Attack surface vulnerability DOES exist
## TOP-IOC: Mitigating controls DO NOT EXIST or ARE NOT currently protecting the ass
## TOP-IOC: Subsequent attack activity DOES exist
## TOP-IOC: Corroboration from other assets DOES NOT exist
## TOP-IOC: CONSISTENT with unusual egress network traffic
## TOP-IOC: CONSISTENT with unusual lateral movement
## TOP-IOC: CONSISTENT with login anomalies
## TOP-IOC: CONSISTENT with suspicious domain controller activity
## TOP-IOC: CONSISTENT with suspicious byte counts
```

NOTES

TOP Indicators Of Compromise (TOP-IOC)

Threat Analysis Model

1. Analysts shall use a TAM similar to the TOP-IOC
2. Analysts shall annotate cases using one or more TOP-IOC annotation statements
3. All ticket annotation shall start with IOC-NEGATIVE -or- IOC-POSITIVE
4. Evidence that intelligence assets were searched and analyzed is required
5. Annotations should indicate the COA related to the specific activities conducted

General TOP-IOC

1. Attack Surface Vulnerability Exists
2. Corroboration From Multiple Intelligence Assets

https://t.me/learningnets

3. Unusual Egress Network Traffic
4. Unusual Ingress Network Traffic
5. Anomalies In Privileged User Account Activity
6. Geographical Irregularities
7. Log-In Anomalies
8. Volume Increase For Database Reads
9. HTTP Response Size Anomalies
10. Large Numbers Of Requests For The Same File
11. Mismatched Port-Application Traffic
12. Suspicious Registry Or System File Changes
13. DNS Request Anomalies
14. Unexpected Patching Of Systems
15. Mobile Device Profile Changes
16. Data In The Wrong Places
17. Unusual Lateral Movement
18. Velocity Increase For Share / Mount Activity
19. Time Based Anomalies
20. Suspicious Byte Counts
21. Suspicious Domain Controller Activity
22. Subsequent Activity By Attacker Address / GEO
23. HTTP Response Code Success

Insider Threat TOP-IOC

1. Logons To New Or Unusual Systems
2. New Or Unusual Logon Session Types
3. Unusual Time Of Day Activity
4. Unusual GEO
5. Unlikely Velocity
6. Shared Account Usage
7. Privileged Account Usage
8. Unusual Program Execution
9. New Program Execution
10. High Volume File Access
11. Unusual File Access Patterns
12. Cloud-based File Sharing Uploads

https://t.me/learningnets

13. New IP Address Association
14. Bad Reputation Address Association
15. Unusual DNS Queries
16. Bandwidth Usage
17. Unusual Or Suspicious Application Usage
18. Dark Outbound Network Connections
19. Known Command And Control Connections
20. Building Entry And Exits
21. High Volume Printing Activity
22. Unusual Time Period Printing
23. Endpoint Indicators Of Compromise
24. Sensitive Table Access
25. Sensitive Data Movement Combined With Other Risk Indicators

Network and Packet Analysis Observation TOP-IOC

1. Known Signatures
2. Reputation
3. IP Addresses
4. Domains
5. DNS Queries
6. DLP Indicators
7. Anomalous Traffic Patterns
8. Protocols
9. Inconsistent Protocols
10. Malformed Protocols
11. Masquerading Protocols
12. Prohibited Protocols

Suspicious Domain TOP-IOC

1. Domain registered date is recent
2. Domain registrant is anonymous or non-reputable
3. Domain shares similar characteristics with prior known bad
4. Domain has a suspicious email infrastructure
5. Domain has a suspicious website infrastructure
6. Domain has a disreputable history

https://t.me/learningnets

7. Domain has suspicious IP addresses / DNS data

Azure & Office 365 TOP-IOC

1. Privileged account logon from foreign address
2. Creation of accounts in Azure AD
3. Traffic restrictions loosened on Virtual Network
4. Storage account accessed via stolen key from foreign address
5. Subscription Administrator added
6. Windows level intrusion of VM
7. High priority target's mailbox is accessed

Tactics, Techniques & Procedures

Protecting Against Ransomware

1. Prioritize software updates for internet facing systems and systems having access to the internet
2. Practice least privilege principles including role based access controls and access limitations
3. Implement end point detection / host based intrusion technologies
4. Maintain backups of mission critical data
5. Educate the user community
6. Create a response / MISSION plan and assign a strike force to execute that plan when it becomes necessary

Protecting Against Phishing

1. Conduct security awareness training
2. Conduct phishing simulation tests
3. Deploy Application Whitelisting (AWL)
4. Deploy Endpoint Detection and Response (EDR) technology
5. Inspect outbound URLs
6. Ensure user accounts do not execute with elevated (admin) privileges
7. Use inbound email sandboxing
8. Deploy packet capture inspection technology with decryption capability
9. Deploy HTTPS inspection technology that validates certificate chains

https://t.me/learningnets

CYBERSECURITY INCIDENT RESPONSE PLAN 2

https://t.me/learningnets

Response Procedures

The actions required to deal with cyber security incidents are detailed below for each relevant stakeholder, in each of the seven phases (preparation, detection, analysis, containment, eradication, recovery, and lessons learned).

Phase 1 - Preparation

During the Preparation Phase teams begin to put in place what they will need to help them respond to an incident in the best way possible. Proper policies, procedures, and tools need to be put into place.

Technologies involved in this phase include:

- Firewalls
- IDS/IPS
- Web proxy
- Antivirus
- Anti-malware
- Email gateway
- SIEM

Preparation Phase			
Team	**Description**	**Questions**	**Action**
Preparation: End User	No incident response responsibilities.		
Preparation: Help Desk	During the preparation phase, help desk staff will make sure they are ready to respond to incidents.	• Am I aware of my responsibilities as they relate to incident response? • Do I need any additional training?	☐ Review and understand incident response roles and responsibilities. ☐ Take training courses and participate in available webinars
Preparation: IT Operations	During the preparation phase, cybersecurity staff configure firewall, IDS/IPS, web proxy, antivirus, anti-malware, email gateway, SIEM, DLP, and other systems to enable them to better detect potential issues	• Have we kept up to date with patches to our systems? • Have we researched new technologies to increase our cybersecurity posture? • Are we taking advantage of new features and functionality? • Do we need any additional training?	☐ Review new technologies on a regular basis. ☐ Update firewalls, IDS/IPS, DLP, web proxy connections, antivirus, anti-malware, and other systems. ☐ Take training courses and participate in available webinars
Preparation: Technical Lead	During the preparation phase the TECHNICAL LEAD will ensure that the CSIRP is up to date and tested and that the organization is ready to respond to an incident.	• Has the IR plan been updated and tested? • Have employees received up to date, relevant cyber security training? • Do employees know how to report a potential incident? • Are the members of the	☐ Plan and execute a tabletop exercise. ☐ Ensure all employees are trained to help avoid and report potential cybersecurity incidents. ☐ Hold meetings with the CSIRT on a regular basis.

https://t.me/learningnets

		CSIRT aware of their roles and responsibilities?	
Preparation: Legal, Compliance, HR, PR, Communications	During the preparation phase these areas will try to identify changes to laws, policies, etc. that could require changes to the IR plan or response procedures. These areas will work together to create appropriate communications templates.	• Are there any new laws or policies that needs to comply with? • Do we have any additional reporting requirements?	☐ Take training courses and participate in available webinars.
Preparation: Senior Management	No incident response responsibilities.		

https://t.me/learningnets

Phase 2 - Detection

During the Detection Phase, teams evaluate a potential cyber security incident. Once an incident has been detected, a help desk ticket or incident record/ticket is opened to initiate the detection phase.

Incident triggers can include:

1. End users reporting to help desk.
2. Technology trigger (FW, IDS/IPS, etc.)
3. Pen tests (vulnerability management)
4. Hunt function (threat intel)

Technologies involved in this phase include:

- Firewalls
- IDS/IPS
- Web proxy
- Antivirus
- Anti-malware
- Email gateway
- SIEM

Detection Phase			
Team	**Description**	**Questions**	**Action**
Detection: End User	During the detection phase, the end user may report suspicious behaviors or issues and system/service disruptions.	• Did I receive a suspicious email? • How do I resolve the issue with my endpoint? • Why is a system or service not available or behaving abnormally? • Is my device possibly lost or stolen? • Why can't I access my data or account?	☐ Report a suspected incident or issue to help desk. Examples include: o Data is missing/altered. o Passwords aren't working. o Experiencing significant number of pop-up ads. o Computer keeps crashing. o Account/network cannot be accessed.
Detection: Help Desk	During the detection phase, help desk staff will monitor calls and submitted tickets.	• Are any end users experiencing potential security incidents?	☐ Open a help desk ticket. (see Appendix for examples of information to be included in a help desk ticket.) ☐ Determine if incident needs to be escalated to other stakeholders. ☐ Assign help desk ticket to appropriate team and/or begin the Analysis phase.
Detection: IT Operations	During the detection phase, cybersecurity staff monitor firewall, IDS/IPS, web proxy, antivirus, anti-malware, email gateway, SIEM, DLP, and other events, and escalate to incidents as needed.	• Are assets or services being impacted by a security incident? • Has data been exposed or exfiltrated? • Has an executive been targeted or affected by a security incident? • Are security technologies identifying one or a series of events?	☐ Identify suspicious behavior of assets or services. ☐ Review events from sources such as a firewall, IDS/IPS, DLP, web proxy connections, antivirus, anti-malware, email gateway, SIEM logs, or other security. ☐ Determine if incident needs to be escalated to initiate the incident management process.

https://t.me/learningnets

Detection: Technical Lead	No incident response responsibilities.		
Detection: Legal, Compliance, HR, PR, Communications	No incident response responsibilities.		
Detection: Senior Management	No incident response responsibilities.		

https://t.me/learningnets

Phase 3 - Analysis

During the Analysis Phase, teams will investigate the incident to determine the impact and scope of the threat. Depending on the impact and scope, a threat escalation tier level will be assigned, indicating the number of teams that will be involved in the remediation of the incident, and the notification of the threat will be escalated as appropriate. A third party may be involved if deep forensic analysis is needed.

Technologies involved in this phase include:

- Firewalls
- IDS/IPS
- Web proxy
- Email gateway
- SIEM or another log correlator
- Digital forensics tools, including:
  - File viewing and analysis tools
  - OS analysis tools
  - Network analysis tools
  - Database analysis tools
- Threat intelligence

Analysis Phase			
Team	**Description**	**Questions**	**Action**
Analysis: End User	During the analysis phase, end users will provide information related to the incident as required.	• What are the events that led up to this suspected incident? • What did I do as a result?	☐ Provide information related to the incident to the help desk.

Analysis: Help Desk	During the analysis phase, help desk staff directly interact with the end user, ask incident-related questions, take actions, and document findings in the help desk ticket.	• What may have caused the incident?
		  o Did the end user click a hyperlink or open a file attachment?
		  o Did the end user visit a suspicious website?
		  o Did the end user download software recently?
		  o Did the end user plug in a flash drive?
		• What type of user is affected – i.e., what privileges does the user have?
		• Are any locally stored suspicious file extensions identified?
		• Has the end user been denied access when accessing data or a server?
		• If a device was misplaced, where was it last seen?
		• What types of data or
			☐ Open a help desk ticket, if not opened.
			☐ Gather answers to incident-related questions and document findings in the ticket.
			☐ Identify incident-related keywords *(malware, ransomware, distributed denial of service [DDoS], compromised credentials)*.
			☐ Search ticketing platform to identify other impacted end users. If multiple end users are impacted, create a parent/child ticket.
			☐ Determine the impact and scope of the incident.
			☐ Assign help desk ticket to cybersecurity team, as appropriate.
			☐ Facilitate end-user notifications.
			☐ If the incident was a false positive, update the ticket and close the incident record.

https://t.me/learningnets

		equipment were involved?	
Analysis: IT Operations	During the analysis phase, cybersecurity staff will analyze appropriate logs, conduct open-source intelligence research, provide technical support, provide incident coordination support, interact with the end user directly, ask incident-related questions, take actions, and document findings in the incident record.	• What may have caused the incident? o Did the end user click a hyperlink or open a file attachment? o Did the end user visit a suspicious website? o Did the end user download software recently? o Did the end user plug in a flash drive? • Are any other IoCs identified within the organization? • What type of user is affected; i.e. what privileges does the user have? • Are any locally stored suspicious file extensions identified? • Has the end user been denied access when accessing data or a server? • If a device was misplaced, where was it last seen? What types of data or equipment were involved?	☐ Gather answers to incident-related questions. ☐ Conduct open-source threat intelligence analysis to identify comparative IoCs. ☐ Perform IoC search in firewall, IDS, IPS, email gateway, and system and server logs. ☐ Determine the scope of the incident, such as how much of the network was impacted, how many endpoints, or how many files were compromised. ☐ Determine the scope and impact of the incident, and the resulting TEP tier level. ☐ Determine if any end-user device or devices were compromised. ☐ Assess if any servers were impacted and decide if any server infections are to be assigned to the infrastructure team. ☐ Based on the scope and impact, determine the TEP tier level. Inform necessary parties, as required. ☐ If there are any indications that a crime was committed, immediately escalate to the TECHNICAL LEAD. ☐ If the incident was a false positive, update the ticket and close the incident record. ☐ Investigate and respond to security events.
Analysis: Technical Lead	During the analysis phase, TECHNICAL LEAD will notify and coordinate with the relevant stakeholders and senior management.	• Has a crime been committed? • Has data been lost or stolen? • Are any business applications impacted? • Does a disaster recovery plan need to be enacted?	☐ Publish corporate-wide situational awareness alerts to inform end users of any system outages. ☐ Coordinate and inform senior management of any incident updates. ☐ Approve disaster recovery plan enactment, if necessary. ☐ Report any external criminal activities to senior management. ☐ Engage Legal, HR, and PR to address the incident, as appropriate. ☐ Determine if any incident information should be shared with external parties.
Analysis: Legal, Compliance, HR, PR,	During the analysis phase, legal, HR, and PR staff will analyze any insider	• Are there potential legal repercussions to the incident? • Was there any insider	Legal: ☐ Determine if any regulatory, legal, or compliance mandates have been violated or impacted.

https://t.me/learningnets

Communications	activity, legal requirements, and brand/ reputational damage.	activity or other misuse of assets? • Was there any brand or reputational damage?	☐ Determine if any breach notifications are required. ☐ Begin process to notify required parties. Human Resources: ☐ Determine if any employee acceptable-use or security policies have been violated. ☐ Determine if any preliminary employee disciplinary actions are required immediately. Public Relations: ☐ Determine if any public reputational or brand damage has occurred. If so, begin process/campaign to address it.
Analysis: Senior Management	During the incident response analysis phase, senior management staff will notify and coordinate with the relevant stakeholders.	• Was there any insider activity or other misuse of assets? • Have any core business functions been affected? • Was there any brand or reputational damage? • Has a crime been committed? • Has data been lost, and does a disaster recovery plan need to be enacted?	☐ Provide an incident summary and updates to the board of directors/ stakeholders. ☐ Approve reporting crime to law enforcement, if necessary. ☐ Analyze and approve emergency budget, resource, or control requests, as appropriate. ☐ Approve communication of incident information with external parties.

https://t.me/learningnets

Phase 4 - Containment

During the Containment Phase, teams will isolate and contain the incident to limit its ability to spread to the rest of the organization.

Technologies involved in this phase include:

- Network isolation
- Endpoint isolation
- Endpoint containerization

Containment Phase			
Team	**Description**	**Questions**	**Action**
Containment: End User	No containment responsibilities beyond ongoing cooperation with incident responders.		
Containment: Help Desk	During the containment phase, the help desk will maintain communications with any impacted end users.	• Do any end users need to be notified?	☐ Maintain communications with any impacted end users. o Inform users if any critical systems or data will be unavailable or affected during the response process.
Containment: Cybersecurity	During the containment phase, the cybersecurity team will provide support to isolate the incident and remove compromised assets/users, if necessary.	• How can the issue be isolated with minimal disruption (sandboxing, quarantining, revoking user access, etc.)? • Was a server infected? Can it be quarantined? • What stakeholders need to be notified?	☐ Provide incident coordination support. ☐ Isolate or disconnect any infected endpoints from the network, shut down organizational Internet access, if necessary. ☐ Disable compromised user accounts, change passwords, or remove privileges, if necessary. ☐ Determine if other actions are necessary to contain the spread of the incident. ☐ Notify affected users and stakeholders. ☐ Create an OS-level image of any endpoint, servers, or storage arrays to prevent future data loss. ☐ Isolate or disconnect any servers and/or infected endpoints. ☐ Disable compromised accounts or change passwords. Change the password to the affected system.
Containment: Technical Lead	During the containment phase, the TECHNICAL LEAD will evaluate any control weaknesses and make recommendations for	• Are the current security controls sufficient?	☐ Provide senior management with incident updates. ☐ Approved additional resourcing of controls or processes, as necessary for the containment of the incident.

https://t.me/learningnets

	remediation.		
Containment: Legal, Compliance, HR, PR, Communications	During the containment phase, PR may address the public and other stakeholders to inform them of the status of the incident and contain possible rumors, speculation, and reputational damages. Legal and HR will continue ongoing efforts that began in the Analysis phase.	• What types of communication are required? • Are there any Legal and HR processes that need to be continued?	Legal: ☐ Continue legal actions as necessary, informing affected parties as required by regulations. PR: ☐ If necessary, address the affected stakeholders (including the public), informing them of the steps that have been taken to contain the incident and future steps to fully remediate the incident. HR: ☐ Continue HR actions, as necessary, particularly containing any further employee misuse or violations.
Containment: Senior Management	During the containment phase, senior management will determine if any core business function is impacted and will provide final approval for drastic measures.	• Do any business-critical services, systems, or data need to be taken offline for effective containment of the incident?	☐ Determine if any additional stakeholders need to be notified. Provide the notification. ☐ Provide final approval for taking business-critical systems offline or other major containment decisions.

https://t.me/learningnets

Phase 5 - Eradication

During the Eradication Phase, teams will eliminate components of the incident, such as deleting malware and removing unauthorized user access, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

Technologies involved in this phase include:

- Network isolation
- Endpoint isolation
- Endpoint containerization

Eradication Phase			
Team	**Description**	**Questions**	**Action**
Eradication: End User	No eradication responsibilities beyond ongoing cooperation with incident responders.		
Eradication: Help Desk	During the eradication phase, the help desk will maintain communications with impacted end users and reissue devices, if necessary.	• Does the end user need to be notified of any updates? • Do any users need new/updated devices issued?	☐ Seize, prepare replacement, and reissue endpoint, if necessary. ☐ Maintain communications with any impacted end users.
Eradication: IT Operations	During the eradication phase, IT Operations will ensure possible sources of compromise are eliminated. IT Operations will install patches and eliminate other possible sources of the incident.	• Are there any infected endpoints still on the network? • Are there any compromised user accounts still on the network? • Have systems been adequately patched? • What data needs to be restored? • Are there any control gaps that allowed this incident to occur?	☐ Eliminate the root cause of the incident (e.g. remove malware/virus, block all unauthorized users, de-escalate elevated privileges). ☐ Backup affected systems for later investigation and forensics. ☐ Install system/security patches to resolve malware/network/other vulnerabilities. ☐ Build replacement server. ☐ Disable breached user accounts. ☐ Inform the TECHNICAL LEAD of any organizational security control gaps, if necessary.
Eradication: Technical Lead	During the eradication phase, the TECHNICAL LEAD will approve new or updated controls.	• Do any new controls need to be implemented? • Do any controls need to be updated? • Are there any control gaps that allowed this incident to occur?	☐ Approve new controls and the updating of existing ones.
Eradication: Legal,	During the eradication phase,	• Are there any changes to Legal, HR, or PR	☐ Reassess if any new findings have changed the required

https://t.me/learningnets

Compliance, HR, PR, Communications	Legal, HR, and PR staff will evaluate if any new findings have led to new actions, otherwise they will continue any ongoing processes.	requirements?	Legal, HR, or PR actions. If so, address those requirements. ☐ Otherwise continue Legal, HR, and PR efforts already begun.
Eradication: Senior Management	No specific eradication responsibilities beyond ongoing support and approval, as necessary.		

https://t.me/learningnets

Phase 6 - Recovery

During the Recovery Phase, teams will enact processes and procedures for recovery and full restoration of any systems, devices, or accounts during the incident. In recovery, responders will restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.

Recovery may involve actions such as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, re-issuing devices, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists).

Technologies involved in this phase include:

- System backup tools
- Patches
- Vulnerability scanners

Recovery Phase			
Team	**Description**	**Questions**	**Action**
Recovery: End User	No recovery responsibilities beyond ongoing cooperation with incident responders.		
Recovery: Help Desk	During the recovery phase, the help desk will maintain communications and coordinate recovery with affected end users.	• Does the end user need to be notified? What do they need to know? • Is the ticket up to date?	☐ Maintain communications with any impacted end users. Inform users: o When operations are back to normal. o Of any required changes (e.g. updates to systems, passwords). o Of updated training and awareness material regarding the incident. ☐ Re-issue end-user devices and credentials, if necessary. ☐ Ensure help desk ticket is updated with all relevant information.
Recovery: IT Operations	During the recovery phase, IT Operations will recover and restore systems back to regular operations.	• Do any other servers or systems need to be restored? • Is the incident report comprehensive? • Has the incident been successfully remediated?	☐ Rectify any component that was compromised; restore systems and data, as necessary. ☐ Once restored, perform system/ network/device validation and testing to verify that the system functions the way it was intended/had functioned in the past. Coordinate with the business units as needed. ☐ Perform vulnerability assessment, antivirus, and anti-malware scans

https://t.me/learningnets

			on any endpoints or servers to ensure that operations are back to normal. ☐ Ensure incident record/ticket is updated with relevant information. ☐ Advise the TECHNICAL LEAD of any controls, processes, or policies that need to be updated.
Recovery: Technical Lead	During the recovery phase, the TECHNICAL LEAD will evaluate any weaknesses in security controls or policies as appropriate.	• Do any controls or policies need to be updated?	☐ Review any security policies or controls, as appropriate. ☐ Inform senior management that operations have been restored.
Recovery: Legal, Compliance, HR, PR, Communications	During the recovery phase, Legal, HR, and PR staff will complete their respective processes, and ensure all actions are documented.	• Do any employees need disciplinary action? • What message needs to be communicated to stakeholders/the public? • What legal or regulatory next steps are required?	☐ Legal: Follow-up with any legal implications and requirements. ☐ HR: Ensure employee records are updated with any infractions (e.g., misuse of corporate resources causing an incident) and subsequent disciplinary actions. If disciplinary actions have not been issued yet, begin process in coordination with the employee's manager. ☐ PR: Communicate with stakeholders/public that the incident has been resolved, including next steps.
Recovery: Senior Management	No incident response responsibilities.		

Phase 7 – Lessons Learned

During the Lessons Learned Phase, teams will perform root-cause analysis and lessons learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement, and all related active tickets should be updated and closed.

This phase involves performing a post-mortem, root-cause analysis, and lessons learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement, and all related active tickets should be updated and closed.

Lessons Learned Phase			
Team	**Description**	**Questions**	**Action**
Lessons Learned:	During the lessons learned phase,	• What happened? • What was learned?	☐ If necessary, a primary affected user may answer questions

https://t.me/learningnets

End User	affected users may provide additional details for post-incident meetings/reports and may participate in additional awareness and training.	• What has changed?	regarding the source of the incident. ☐ General end users may participate in updated awareness and training as a result of the incident.
Lessons Learned: Help Desk	During the lessons learned phase, the help desk may participate in post-incident meetings, as necessary.	• What happened? • How did we respond? • What should we do next time?	☐ Participate in lessons learned (post-mortem) meetings, as necessary.
Lessons Learned: IT Operations	During the lessons learned phase, IT Operations will support any post-incident activities, as appropriate.	• What happened? • How did we respond? • What should we do next time? • Are there any IT operations processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ Update and close incident ticket
Lessons Learned: Technical Lead	During the lessons learned phase, the TECHNICAL LEAD will facilitate any post-incident activities.	• How can the incident response process be improved?	☐ Determine if a full-fledged post-mortem/lesson learned meeting is necessary. ☐ Determine who should participate (e.g. end users, Legal, Compliance, HR, PR, Communications). ☐ Facilitate post-incident meetings (or assign the responsibility to another individual). Ensure a record is maintained.
Lessons Learned: Legal, Compliance, HR, PR, Communications	During the lessons learned phase, Legal, HR, and PR staff will support any post-incident activities, as appropriate.	• Are there any Legal, HR, or PR processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ If new findings become known as a result of post-incident activities, follow-up with any new or ongoing Legal, HR, and PR duties that have not already been addressed. ☐ Legal: Follow up with any legal actions, if required. ☐ HR: Follow up with any employee disciplinary action, if required. ☐ PR: Follow up on public and internal communications to address the resolution of the incident and steps being taken to prevent reoccurrences.
Lessons Learned: Senior Management	During the lessons learned phase, senior management will	• Are there any senior management processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ Address stakeholders/board of directors, if necessary.

https://t.me/learningnets

	support any post-incident activities, as appropriate.		☐ Approve future investments to help prevent reoccurrences.

https://t.me/learningnets