Security Operational Center Task - 2

1. Alert Priority Levels

Core Concepts :-

- Priority Definitions.
- Assignment Criteria for Prioritization.
- Scoring Systems Used in SOC.
- Key Objectives.

Core Concepts Definitions

- Priority Definitions:- Priority definitions are used to classify security incidents and alerts based on their **severity, impact, and urgency**. This helps SOC analysts respond to the most dangerous threats first.

Critical
Description: Incidents causing immediate and severe damage to the organization.
Impact: Data breach, ransomware, full service outage, or loss of sensitive data.
Urgency: Active exploitation is occurring and requires immediate action.
Example: Ransomware actively encrypting systems or widespread malware infection.

High
Description: Serious security issues that can escalate quickly if not addressed.
Impact: Partial system compromise, privilege escalation, or unauthorized access.
Urgency: High risk but not yet fully destructive.
Example: Unauthorized administrative access detected on a production server.

Medium
Description: Suspicious activities with limited impact or partial exploitation.
Impact: Potential policy violation or early-stage attack.
Urgency: Requires investigation but not immediate emergency response.
Example: Multiple failed log in attempts from a single IP address.

Low
Description: Minor or informational security events.
Impact: Minimal or no immediate risk to systems or data.
Urgency: Can be reviewed during routine monitoring.
Example: Port scan detected on a test or non-production system.

- **Assignment Criteria for Prioritization**

  Security alerts should be prioritized using technical risk and business context to ensure effective incident handling.

  Asset Criticality
  - Evaluate whether the affected asset is critical to business operations.
  - Example: Production server alerts are higher priority than test or lab VM alerts.

  Exploit Likelihood
  - Determine how easily the vulnerability can be exploited.
  - Example: A known CVE with a publicly available exploit increases priority.

  Business Impact
  - Assess the potential damage to the organization.
  - Examples: Financial loss, service downtime, regulatory penalties, or reputation damage.

  Example Scenario
  - Log4Shell (CVE-2021-44228) with a CVSS score of 9.8 on an internet-facing production server is classified as Critical due to high exploitability and severe business impact.

- **Scoring Systems Used in SOC**

  Scoring systems help quantify risk and standardize alert prioritization across SOC teams.

  CVSS (Common Vulnerability Scoring System)
  - Provides a numerical score (0.0–10.0) based on exploitability and impact.
  - Usage:
    - 9.0–10.0 → Critical
    - 7.0–8.9 → High
    - 4.0–6.9 → Medium
    - 0.1–3.9 → Low
  - Widely used for vulnerability management and risk assessment.

  SOC Tool Risk Scoring (e.g. Splunk)
  - Combines multiple factors such as asset value, threat intelligence, and alert frequency.
  - Helps SOC analysts correlate events and focus on the highest-risk alerts.
  - Scoring systems in SOCs convert raw security data into measurable risk levels for consistent prioritization.
  - CVSS provides a standardized 0.0–10.0 score based on exploitability and impact factors.
  - These scores map vulnerabilities to severity levels such as Critical, High, Medium, and Low.

- **Key Objectives**
  The primary objective of this approach is to build strong alert assessment and prioritization skills required for efficient SOC operations.
  Objectives Include:
  - Applying standardized severity definitions consistently.
  - Using CVSS and risk scores to quantify technical risk.
  - Incorporating asset importance and business impact into decision-making.
  - Reducing alert fatigue by focusing on high-risk, high-impact incidents first.

- **Skill-Building Method :-**
- **Study CVSS Using FIRST's CVSS Guide**
  The Common Vulnerability Scoring System (CVSS), maintained by FIRST (Forum of Incident Response and Security Teams), is a standardized framework used to assess the severity of security vulnerabilities. CVSS helps security teams measure risk consistently by assigning numerical scores based on technical impact and exploitability.

  1. CVSS Base Metrics
  Base metrics represent the intrinsic characteristics of a vulnerability that do not change over time or across environments.
  Components of Base Metrics:
  - **Attack Vector** (AV): How the vulnerability is exploited (Network, Adjacent, Local, Physical).
  - **Attack Complexity** (AC): The difficulty of exploitation.
  - **Privileges Required** (PR): Level of access needed before exploitation.
  - **User Interaction** (UI): Whether user action is required.
  - **Scope** (S): Whether the exploit affects only the vulnerable component or other components.
  - **Impact Metrics**:
    - Confidentiality (C): Data exposure risk
    - Integrity (I): Data modification risk
    - Availability (A): Service disruption risk

  Purpose:
  Base metrics produce the initial CVSS score (0.0–10.0), which is widely used for vulnerability comparison and prioritization.

  2. CVSS Temporal Metrics
  Temporal metrics capture aspects of a vulnerability that change over time. These metrics help organizations assess how urgent a vulnerability is *right now*.
  Components of Temporal Metrics:
  - **Exploit Code Maturity** (E): Availability of exploit code (Proof-of-Concept, Functional, or High).

- **Remediation Level** (RL): Availability of fixes (Official Patch, Temporary Fix, or None).
- **Report Confidence** (RC): Credibility of vulnerability details.

Purpose:
Temporal metrics adjust the base score to reflect real-world exploitability and response readiness, helping SOC teams determine remediation urgency.

3. CVSS Environmental Metrics
Environmental metrics customize CVSS scoring based on the organization's specific environment.
Components of Environmental Metrics:

- **Security Requirements:**
  - Confidentiality Requirement (CR)
  - Integrity Requirement (IR)
  - Availability Requirement (AR)
- **Modified Base Metrics**:
  - Modified Attack Vector, Complexity, Privileges, and Impact scores

Purpose:
Environmental metrics allow organizations to align CVSS scoring with business impact, asset importance, and operational priorities.

4. Why Studying All Three Metrics Matters
Understanding Base, Temporal, and Environmental metrics together enables accurate risk assessment rather than relying only on raw CVSS numbers.

- Base metrics show technical severity
- Temporal metrics show current threat status
- Environmental metrics show business relevance

This layered approach ensures SOC analysts prioritize vulnerabilities that are both exploitable and impactful within their specific environment.

5. Learning Outcome
By studying CVSS using FIRST's official guide, analysts develop the ability to:

- Interpret CVSS scores correctly
- Adjust severity based on real-world conditions
- Align vulnerability management with business risk
- Improve alert prioritization and remediation decisions

- **Review of NIST SP 800-61: Incident Severity Classification and Prioritization Workflows**
  NIST Special Publication 800-61 (Computer Security Incident Handling Guide) is a widely adopted framework that provides structured guidance for identifying, classifying,

prioritizing, and responding to security incidents. It helps organizations establish a consistent and repeatable incident response (IR) process aligned with business and operational needs.

1. Purpose of Incident Severity Classification

Incident severity classification ensures that security incidents are handled according to their impact and urgency. Not all incidents require the same level of response, and NIST SP 800-61 emphasizes categorizing incidents so resources are used efficiently.

Key Goals:

- Ensure rapid response to high-impact incidents
- Reduce damage and recovery time
- Align technical response with business priorities
- Improve communication between SOC, IT, and management

2. Incident Categories in NIST SP 800-61

NIST SP 800-61 defines common incident categories to standardize classification across organizations.

Common Incident Categories Include:

- **Malware**: Viruses, ransomware, trojans, worms
- **Denial of Service** (DoS): Attacks that disrupt system availability
- **Unauthorized Access**: Insider misuse or external compromise
- **Inappropriate Usage**: Policy violations
- **Multiple Component Incidents**: Incidents involving more than one category

These categories help analysts quickly understand the nature of the incident before assigning severity.

3. Severity Levels and Impact Assessment

Severity levels in NIST SP 800-61 are determined by evaluating technical impact and business impact together.

Factors Used for Severity Classification:

- **Functional Impact**: Effect on system operations (e.g., service outage)
- **Information Impact**: Data confidentiality, integrity, or availability loss
- **Recoverability**: Time and effort required to restore systems
- **Scope**: Number of systems or users affected

Example:

- A malware infection on a single user system may be Medium severity
- Ransomware impacting multiple production servers may be Critical severity

4. Incident Prioritization Workflow

NIST SP 800-61 outlines a workflow that helps SOC teams decide which incidents to respond to first.

Step-by-Step Workflow:

1. **Detection and Reporting**: Incident identified via SIEM, EDR, or user report
2. **Initial Triage**: Validate whether the alert is a true incident
3. **Categorization**: Assign an incident category (malware, access, DoS, etc.)
4. **Severity Assignment**: Determine severity based on impact and urgency
5. **Prioritization**: Rank incidents to allocate response resources
6. **Escalation**: Notify appropriate teams and management if required

This workflow ensures consistent handling even during high alert volumes.

5. Incident Response Lifecycle Alignment

Severity classification directly influences actions in each phase of the NIST incident response lifecycle.

Lifecycle Phases:

- **Preparation**: Define severity criteria and response playbooks
- **Identification**: Classify and prioritize incidents accurately
- **Containment**: Apply controls based on severity level
- **Eradication**: Remove threats and vulnerabilities
- **Recovery**: Restore systems and monitor for recurrence
- **Lessons Learned**: Improve severity definitions and workflows

Higher-severity incidents trigger faster containment, deeper investigation, and executive involvement.

6. Role of Documentation and Communication

NIST SP 800-61 emphasizes clear documentation and communication during incident handling.

Best Practices:

- Maintain incident logs with severity and timestamps
- Use standardized severity definitions
- Communicate impact and status to stakeholders
- Preserve evidence for forensic and legal purposes

Proper documentation improves accountability and supports post-incident analysis.

7. Benefits of Using NIST SP 800-61 for SOC Operations

Adopting NIST SP 800-61 provides several operational advantages:

- Consistent incident classification across teams
- Improved prioritization and faster response times
- Better alignment with regulatory and compliance requirements
- Reduced confusion during high-pressure incidents
- Strong foundation for SOC maturity and audits

8. Learning Outcome

By reviewing and applying NIST SP 800-61, SOC analysts gain the ability to:

- Accurately classify incidents by severity
- Prioritize incidents based on business and technical impact
- Follow structured, repeatable response workflows
- Improve coordination and decision-making during incidents

- **Real-World Case Analysis: Log4Shell (CVE-2021-44228)**

Background of the Incident

Log4Shell is a critical remote code execution vulnerability discovered in Apache Log4j, a widely used Java logging library. Due to its presence in countless enterprise, cloud, and internet-facing applications, the vulnerability posed an unprecedented global risk. Attackers could exploit it remotely by sending a specially crafted request, resulting in full system compromise.

CVSS Scoring Breakdown

Log4Shell was assigned a CVSS v3.1 Base Score of 9.8 (Critical).

Key CVSS Factors:

- Attack Vector (AV): Network
- Attack Complexity (AC): Low
- Privileges Required (PR): None
- User Interaction (UI): None
- Scope (S): Changed
- Impact: High on Confidentiality, Integrity, and Availability

Interpretation:

This score indicated that Log4Shell was easy to exploit, required no authentication, and could result in complete system takeover, making it one of the most severe vulnerabilities ever recorded**.**

CVSS Score Range	Severity Level	Log4Shell Mapping
9.0 – 10.0	Critical	Log4Shell (9.8)
7.0 – 8.9	High	Not applicable
4.0 – 6.9	Medium	Not applicable
0.1 – 3.9	Low	Not applicable

CISA Alert-Based Prioritization

CISA escalated Log4Shell through emergency directives and alerts, emphasizing rapid mitigation due to:

- Active exploitation observed in the wild
- Publicly available exploit code
- Mass scanning and automated attacks
- High-value targets including government and critical infrastructure

Priority Determination Using CISA Criteria:

- Threat Activity: Active exploitation → Highest urgency
- Asset Exposure: Internet-facing systems → Critical
- Business Impact: Potential data breaches and outages → Severe
- Exploit Availability: Public PoCs and weaponized exploits → Immediate risk

SOC-Level Prioritization Workflow

A SOC would typically prioritize Log4Shell as follows:

1. Detection: Alerts from SIEM, WAF, IDS, or vulnerability scanners
2. Classification: Remote Code Execution vulnerability
3. Severity Assignment: CVSS 9.8 → Critical
4. Asset Context: Production, internet-facing applications
5. Priority Level: P1 / Critical Incident
6. Response Action: Immediate patching, mitigation, and monitoring

Factor	Assessment
CVSS Score	9.8 (Critical)
Exploit Maturity	Public, weaponized
Asset Type	Production servers
Exposure	Internet-facing
Business Impact	High financial and reputational risk
Final Priority	Critical (Immediate Response)

Even without environmental tuning, Log4Shell met **all high-risk criteria**:

- Maximum CVSS score range
- Zero authentication required
- Wide software dependency spread
- Rapid global exploitation

This made it a textbook example of how **CVSS scores, threat intelligence, and government alerts (CISA)** combine to drive **critical incident prioritization**.

Learning Outcome

From this case, SOC analysts learn how to:

- Translate CVSS scores into real-world priority levels
- Incorporate threat intelligence and exploit activity
- Align vulnerability severity with incident response urgency
- Apply standardized prioritization during global security events

2. Incident Classification

Core Concepts

- Incident Categories
- Taxonomy
- Contextual Metadata

Core Concepts Definitions

- **Incident Categories:**
  Security incidents are classified into categories such as **malware, phishing, DDoS, insider threats, and data exfiltration** to help SOC teams quickly understand the type of threat and apply the correct response strategy.
- **Malware incidents** involve malicious software such as viruses, trojans, ransomware, or spyware that are designed to damage systems, steal information, or gain unauthorized control. *Example:* Ransomware encrypting files on a user's workstation and demanding payment for decryption.
- **Phishing incidents** use social engineering techniques to trick users into revealing credentials or sensitive information. *Example:* An employee clicking a fake email link that leads to a spoofed login page, resulting in account compromise.
- **DDoS incidents** target the availability of services by flooding servers or networks with excessive traffic. *Example:* A public-facing website becoming unavailable due to a coordinated traffic flood from a botnet.
- **Insider threat incidents** originate from trusted users such as employees or contractors who misuse their authorized access, either intentionally or accidentally. *Example:* An employee exporting confidential customer data to a personal USB drive without authorization.
- **Data exfiltration incidents** involve the unauthorized transfer of sensitive data outside the organization, often following a successful compromise. *Example:* An attacker stealing database records and sending them to an external command-and-control server.

- **Taxonomy**

  Taxonomy in cybersecurity refers to a **structured classification system** used to consistently label, organize, and describe security incidents and threats. It ensures that all analysts, tools, and teams use the **same terminology and categories**, reducing confusion and improving communication.

Purpose of Taxonomy

- Provides a common language for incident classification
- Enables consistent reporting across SOC teams and organizations
- Supports threat intelligence sharing and correlation
- Improves analysis, trend tracking, and metrics

Common Taxonomy Frameworks

- **MITRE ATT&CK:**
  Focuses on attacker behavior by mapping incidents to tactics and techniques.
  Example: Phishing emails are mapped to **T1566 – Phishing**, helping analysts understand how the attack was carried out.
- **ENISA Incident Taxonomy:**
  Used mainly in regulatory and national-level reporting to classify incidents by impact, root cause, and affected sector.
- **VERIS (Vocabulary for Event Recording and Incident Sharing):**
  Provides detailed categories for actors, actions, assets, and impacts, enabling deep analysis and standardized incident reporting.

Example Use Case

A credential theft incident can be classified as:

- **MITRE ATT&CK:** T1566 (Phishing) → T1078 (Valid Accounts)
- **VERIS Action:** Social Engineering
  This structured labeling allows SOC teams to compare incidents and identify recurring attack patterns.

- **Contextual Metadata**
  Contextual metadata refers to **additional supporting information** attached to a security incident that helps analysts understand the full scope, timeline, and impact of the event. It turns a basic alert into a meaningful incident record.
- **Purpose of Contextual Metadata**
  - Adds clarity and depth to incident analysis
  - Helps determine severity and priority
  - Supports faster investigation and response
  - Preserves evidence for forensics and compliance
- **Common Types of Contextual Metadata**
  Affected Systems: Hostnames, IP addresses, user accounts, or applications involved
  Timestamps: Event start time, detection time, and response time
  Network Details: Source and destination IPs, ports, and protocols
  Indicators of Compromise (IOCs): Malicious file hashes, URLs, domains, or IPs
  User Context: Account role, privilege level, and login history
  Example Use Case

  In a malware alert:
  Affected System: Finance-server-01
  Timestamp: 2025-01-10 14:32 IST
  Source IP: 203.0.113.45
  IOC: SHA-256 hash of malicious executable

This metadata helps analysts confirm the threat, assess impact, and take appropriate containment actions.

- **Why Taxonomy and Contextual Metadata Matter Together**
  When combined, taxonomy and contextual metadata enable **accurate classification, efficient triage, and effective response**. Taxonomy explains *what type of incident occurred*, while contextual metadata explains *how, where, and to what extent it occurred*.

- **Learning Outcome**
  - By understanding and applying taxonomy and contextual metadata, SOC analysts can:
  - Improve incident consistency and reporting quality
  - Accelerate investigation and response times
  - Enhance threat correlation and intelligence sharing
  - Support audits, compliance, and post-incident analysis

- **Key Objectives**
  - The primary objective of this process is to develop strong analytical and operational skills that enable SOC analysts to handle security incidents efficiently and consistently. By mastering categorization, labeling, and enrichment, analysts can transform raw alerts into well-defined incidents that are easier to investigate, prioritize, and resolve.

  - **Categorizing incidents** involves identifying the type of security event—such as malware, phishing, insider threat, or data exfiltration—based on observed behavior and evidence. Accurate categorization helps analysts quickly understand the nature of the threat and apply the correct investigation playbooks. For example, a phishing incident requires user credential analysis and email tracing, while a malware incident focuses on endpoint containment and file analysis.

  - **Labeling incidents** uses standardized taxonomies and frameworks such as MITRE ATT&CK, ENISA, or VERIS to describe attacker tactics, techniques, and actions in a consistent manner. Proper labeling ensures that incidents are documented uniformly across the SOC, enabling effective communication between analysts, teams, and management. It also allows historical incidents to be compared, helping identify recurring attack patterns and trends.

  - **Enriching incidents** adds contextual metadata such as affected systems, user accounts, timestamps, IP addresses, geolocation, and indicators of compromise (IOCs). Enrichment provides deeper visibility into the scope and impact of an incident, supporting accurate severity assessment and faster root-cause analysis. For instance, correlating multiple alerts tied to the same IP address or file hash can reveal a coordinated attack rather than isolated events.

  - Together, these practices streamline investigations by reducing ambiguity, minimizing manual analysis, and enabling faster decision-making. As proficiency improves, SOC teams experience reduced alert fatigue, improved response times, and higher-quality

incident documentation, ultimately strengthening the organization's overall security posture.

- **Skill-Building Method :-**

- **Exploring MITRE ATT&CK for Mapping Incidents**
  - MITRE ATT&CK is a globally recognized framework that documents **real-world adversary behaviors** based on observed attacks. It organizes attacker activity into **tactics** (the attacker's goal) and **techniques** (how the goal is achieved). By exploring MITRE ATT&CK, SOC analysts learn to map incidents to specific attacker behaviors, which improves investigation accuracy and threat understanding.
  - For example, a phishing email used to steal credentials can be mapped to **T1566 – Phishing** under the **Initial Access** tactic. If those credentials are later used to log in, the activity may also map to **T1078 – Valid Accounts** under the **Persistence or Privilege Escalation** tactic. This mapping helps analysts see the full attack chain rather than treating each alert in isolation. Using MITRE ATT&CK also enables better correlation of incidents, creation of detection rules, and alignment with threat intelligence reports.

- **Studying ENISA Incident Taxonomy and the VERIS Framework**
  - The **ENISA Incident Taxonomy** provides a structured way to classify incidents based on **type, root cause, impact, and affected sector**. It is commonly used in regulatory and national-level incident reporting, helping organizations meet compliance requirements and communicate incidents clearly to external stakeholders. Studying ENISA's taxonomy teaches analysts how to describe incidents in a way that is both technical and business-focused.
  - The **VERIS (Vocabulary for Event Recording and Incident Sharing)** framework offers a detailed classification model covering **actors, actions, assets, attributes, and impacts**. VERIS is especially useful for creating high-quality incident records and supporting data-driven analysis. By learning VERIS, analysts can break down incidents into structured components, making it easier to compare incidents over time and share information with other organizations.
  - Together, ENISA and VERIS provide strong classification standards that complement MITRE ATT&CK by focusing not only on attacker behavior, but also on impact, ownership, and reporting consistency.

- **Review case studies**

  Case studies, such as **phishing campaign reports from the SANS Reading Room**, provide real-world examples that help analysts practice applying theory to practical scenarios. By reviewing these case studies, analysts learn how attackers operate, what indicators are commonly observed, and how incidents unfold over time.

  While studying a phishing case, analysts can practice **adding contextual metadata**, such as:
  - Affected user accounts and email addresses
  - Phishing URLs, domains, and IP addresses

- Malicious file hashes from attachments
- Timestamps showing when emails were sent and clicked

This hands-on practice improves an analyst's ability to enrich incidents with meaningful context, which is critical for accurate severity assessment and efficient response. It also reinforces the importance of detailed documentation and evidence preservation.

Overall Learning Outcome

By exploring MITRE ATT&CK, studying ENISA and VERIS frameworks, and reviewing real-world case studies, SOC analysts develop the skills to:

- Map incidents accurately to attacker tactics and techniques
- Classify incidents using standardized and widely accepted frameworks
- Enrich incident records with actionable metadata
- Improve investigation quality, correlation, and reporting

3. Basic Incident Response

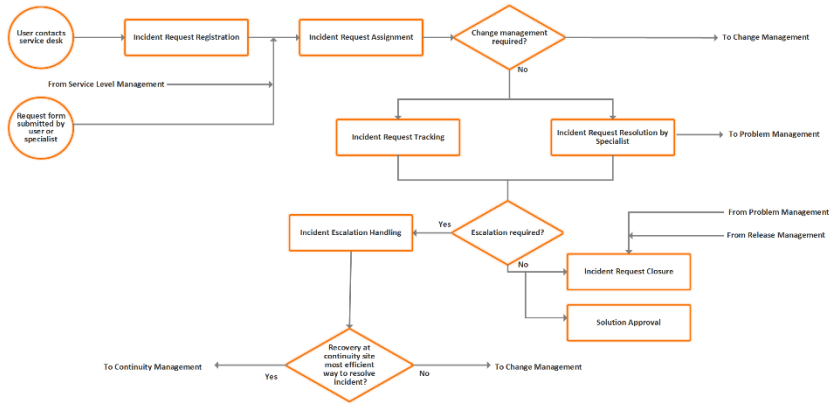
Incident Response (IR) is a structured approach used by organizations to manage and recover from cybersecurity incidents efficiently.It helps identify and analyze security events to reduce financial loss, protect sensitive data, and maintain business continuity. Incidents such as malware infections, phishing attacks, unauthorized access, and data breaches are detected through continuous monitoring using tools like SIEM and EDR. Security teams analyze logs and alerts to assess the severity of threats and take quick action to prevent further damage.Effective Incident Response requires coordination between people, processes, and technology to isolate affected systems and restore operations.After resolution, incidents are documented and reviewed to improve security controls and strengthen defenses against future attacks.

Core Concepts :-

- Incident Lifecycle
- Procedures

<u>Core Concepts Definitions</u>

- Incident Lifecycle :-
  1. The **Incident Lifecycle** defines a structured sequence of phases that organizations follow to effectively manage cybersecurity incidents. This lifecycle ensures incidents are handled consistently, damage is minimized, and security posture improves over time. Each phase has a specific purpose and set of activities that support rapid detection, response, and recovery.The Incident Lifecycle provides a structured framework for managing cybersecurity incidents effectively. It ensures incidents are handled in a consistent and organized manner across the organization. Each phase supports timely detection, response, and recovery from incidents. Overall, it helps organizations continuously improve their security posture over time.



- **Preparation**
  Preparation is the foundation of effective Incident Response. In this phase, organizations establish policies, procedures, and resources before any incident occurs. Incident Response playbooks are created for common scenarios such as phishing, malware, ransomware, or brute-force attacks. Teams define roles and responsibilities, escalation paths, and communication plans. Security tools such as SIEM, EDR, IDS/IPS, and log management systems are deployed and properly configured. Regular training, tabletop exercises, and simulations are conducted to ensure responders are familiar with procedures. Proper preparation reduces response time and limits the impact of real incidents.

- **Identification**
  The Identification phase focuses on detecting and confirming a security incident. Security teams continuously monitor alerts generated by SIEM, EDR, firewalls, and endpoint logs. During alert triage, analysts determine whether an alert represents a true incident or a false positive. Logs, network traffic, user behavior, and system events are analyzed to understand what happened. The scope, severity, and potential business impact of the incident are assessed. Accurate identification ensures the right level of response is applied without unnecessary disruption.

- **Containment**
  Containment aims to stop the incident from spreading and causing further damage. Once an incident is confirmed, immediate actions are taken to isolate affected systems, block malicious IP addresses, disable compromised user accounts, or disconnect infected machines from the network. Containment can be short-term, focusing on quick isolation, or long-term, involving temporary fixes while permanent solutions are prepared. Effective containment protects critical assets and limits attacker movement within the environment.

- **Eradication**
  Eradication involves completely removing the root cause of the incident. This includes deleting malware, removing malicious files, closing exploited vulnerabilities, applying security patches, and correcting misconfigurations. Compromised credentials are reset, and unauthorized access points are eliminated. The goal of eradication is to ensure that the attacker no longer has access and that the environment is clean before systems are fully restored.

- **Recovery**
  Recovery focuses on restoring systems and services to normal operation in a secure manner. Clean backups are used to restore data and systems if necessary. Systems are tested and validated to ensure they function correctly and securely. Monitoring is increased during this phase to detect any signs of recurring or residual malicious activity. Recovery is performed gradually to reduce the risk of re-infection or re-compromise.

- **Lessons Learned**
  The Lessons Learned phase is critical for continuous improvement. After the incident is resolved, a post-mortem or review meeting is conducted to analyze what happened, how it was handled, and what could be improved. Documentation includes timelines, impact analysis, response actions, and effectiveness of controls. Incident Response playbooks, detection rules, and security policies are updated based on findings. This phase helps organizations strengthen defenses and improve readiness for future incidents.

- **Key Takeaway**
  The Incident Lifecycle provides a **systematic and repeatable approach** to managing cybersecurity incidents. By following these phases, organizations can respond quickly, minimize damage, restore operations efficiently, and continuously enhance their security posture.

- **Procedures**
  - Incident Response procedures define the practical actions security teams must take during a cybersecurity incident to control damage, preserve evidence, communicate effectively, and respond efficiently. These procedures ensure that responses are consistent, legally sound, and aligned with organizational and regulatory requirements. Key procedural areas include system isolation, evidence preservation, communication protocols, and the use of automation through SOAR tools.
  - **System isolation** is a critical procedure used to prevent an incident from spreading across the network. When a system is suspected to be compromised, it may be isolated from the network by disabling network interfaces, applying firewall blocks, or moving the system to a quarantine VLAN. Isolation is performed carefully to ensure business-critical services are not unintentionally disrupted. The goal is to stop attacker movement while maintaining the system in its current state for investigation.

- **Evidence preservation** ensures that digital evidence is collected and protected for forensic analysis and potential legal use. Procedures specify how to capture volatile data such as memory dumps, running processes, and network connections before a system is powered off. Non-volatile evidence, including log files, disk images, and configuration files, is also collected. Techniques such as file hashing (using SHA-256 or similar algorithms) are used to verify evidence integrity and demonstrate that data has not been altered during analysis. Proper chain-of-custody documentation is maintained throughout the process.
- **Communication protocols** define how information about an incident is shared internally and externally. Procedures establish who must be notified, how quickly, and through which channels. Internal communication may involve SOC analysts, IT teams, management, and legal departments, while external communication may include customers, regulators, or law enforcement. Clear communication protocols prevent misinformation, ensure timely decision-making, and help organizations meet compliance and reporting obligations.
- **SOAR (Security Orchestration, Automation, and Response) tools** play an important role in automating Incident Response procedures. Platforms such as Splunk Phantom enable workflow orchestration by automatically triaging alerts, enriching them with threat intelligence, and executing predefined response actions. For example, SOAR tools can automatically isolate endpoints, block IP addresses, open incident tickets, and notify stakeholders. Automation reduces response time, minimizes human error, and allows analysts to focus on complex investigations rather than repetitive tasks.

- **Key Objectives**
  - The primary objective of mastering the **Incident Response (IR) lifecycle and procedures** is to enable security professionals and organizations to respond to security events in a timely, structured, and effective manner. A deep understanding of the incident response lifecycle ensures that incidents are handled consistently, minimizing damage to systems, data, and business operations while maintaining compliance with security standards and regulations.
  - Mastering the incident response lifecycle allows responders to clearly understand **what actions to take at each phase of an incident**, from initial detection to final recovery and post-incident review. It helps security teams quickly identify genuine threats, assess their severity, and prioritize response actions based on risk and business impact. This structured approach reduces confusion during high-pressure situations and ensures that critical steps are not missed.
  - Understanding incident response procedures enhances the ability to **contain and mitigate threats efficiently**. Responders learn how to isolate affected systems, preserve forensic evidence, remove malicious artifacts, and restore services securely. Proper execution of these procedures prevents attackers from spreading further, protects sensitive data, and reduces downtime. It also ensures that evidence is handled correctly for forensic analysis, audits, or legal requirements.
  - Another important objective is improving **coordination and communication** during security incidents. Mastery of IR procedures ensures that security analysts, IT teams, management, and external stakeholders follow defined communication protocols. Clear communication enables faster decision-making, reduces operational disruption, and supports accurate reporting to regulatory bodies or customers when required.

- **Skill-Building Method :-**

NIST SP 800-61 – Incident Handling Guide

NIST SP 800-61, titled *Computer Security Incident Handling Guide*, is one of the most widely accepted standards for managing cybersecurity incidents. Published by the National Institute of Standards and Technology (NIST), this guide provides organizations with a comprehensive framework to prepare for, detect, analyze, contain, eradicate, and recover from security incidents, while continuously improving their incident response capabilities. The guide emphasizes that incident handling is not a single action but a lifecycle-driven process. It defines best practices, roles, tools, and methodologies that help organizations respond to incidents in a structured and repeatable manner. NIST SP 800-61 is commonly adopted by SOC teams, government agencies, and enterprises as a baseline for Incident Response programs.

Incident Response Lifecycle in NIST SP 800-61

NIST SP 800-61 defines six core phases of incident handling, ensuring a complete and effective response.

Preparation focuses on establishing the foundation for incident response. This includes developing incident response policies, defining roles and responsibilities, creating playbooks, deploying monitoring tools such as SIEM and EDR, and conducting regular training and tabletop exercises. Strong preparation reduces response time and minimizes errors during real incidents.

Containment aims to limit the damage caused by an incident. NIST recommends both short-term containment (immediate isolation of affected systems) and long-term containment (temporary fixes while preparing permanent solutions). The guide emphasizes balancing security actions with business continuity to avoid unnecessary disruption.

Eradication focuses on removing the root cause of the incident. This includes deleting malware, disabling attacker persistence mechanisms, closing vulnerabilities, and resetting compromised credentials. NIST highlights the importance of identifying how the attacker gained access to prevent reinfection.

Key Concepts Emphasized by NIST SP 800-61

NIST SP 800-61 strongly emphasizes documentation and evidence handling. Every incident should be properly recorded, including timelines, actions taken, indicators, and impact. Proper evidence preservation supports forensic investigations, audits, and legal requirements.

The guide also highlights the importance of communication and coordination. Clear internal and external communication channels ensure that management, legal teams, regulators, and affected stakeholders are informed appropriately and on time.

Another important aspect is incident prioritization and severity rating. NIST provides guidance on categorizing incidents based on functional impact, information impact, and recoverability, allowing organizations to allocate resources efficiently.

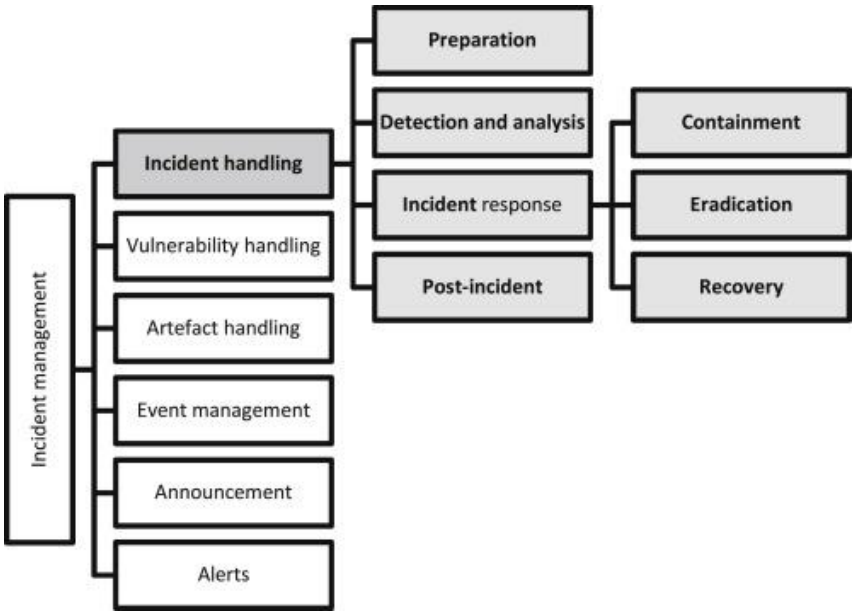
Importance of Studying NIST SP 800-61

Studying NIST SP 800-61 helps security professionals understand industry-standard best practices for incident handling. It provides a common language and structure for SOC operations, improves response consistency, and ensures alignment with compliance and regulatory expectations. Organizations that follow this guide are better prepared to respond to incidents quickly, minimize damage, and continuously strengthen their security posture.

- **SANS Incident Handler's Handbook**
- The SANS Incident Handler's Handbook is a practical, industry-respected resource designed to help security professionals respond to cybersecurity incidents in a structured, repeatable, and effective manner. It complements formal frameworks such as NIST SP 800-61 by providing hands-on response templates, checklists, and real-world best practices that are widely used by SOC analysts, incident responders, and digital forensics teams.
- A key strength of the SANS Incident Handler's Handbook is its focus on standardized response templates. These templates guide responders through each stage of an incident, ensuring critical steps are not overlooked during high-pressure situations. Templates typically include sections for incident description, date and time, systems affected, indicators of compromise (IOCs), actions taken, evidence collected, and current status. By using these templates, organizations ensure consistent documentation across incidents, which improves communication, reporting, and post-incident analysis.
- The handbook strongly emphasizes clear incident classification and prioritization. It provides guidance on categorizing incidents such as malware infections, unauthorized access, denial-of-service attacks, insider threats, and data breaches. Each category includes recommended response actions and escalation paths, helping teams determine the urgency of response and allocate resources effectively. This approach supports faster decision-making and reduces the risk of under- or over-reacting to incidents.
- Another important best practice highlighted in the SANS handbook is evidence handling and forensic readiness. It outlines procedures for preserving volatile and non-volatile evidence, including memory captures, log files, disk images, and network traffic. The handbook stresses maintaining chain of custody and using hashing to verify evidence

integrity. These practices ensure evidence remains reliable for forensic investigations, compliance audits, or legal proceedings.

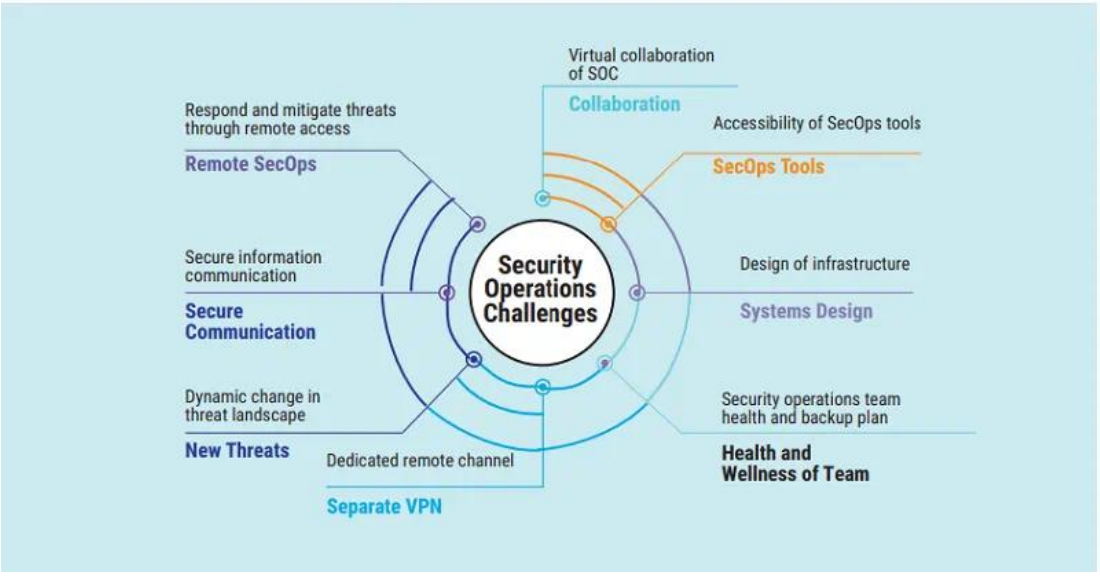
- The SANS Incident Handler's Handbook also provides guidance on containment, eradication, and recovery actions. It recommends isolating affected systems in a way that balances security and business continuity, removing malicious artifacts, closing vulnerabilities, and restoring systems from trusted backups. Best practices include validating restored systems, increasing monitoring during recovery, and ensuring attackers no longer have access to the environment.
- Communication and coordination are another major focus area. The handbook outlines best practices for internal and external communication, including when and how to notify management, legal teams, HR, customers, and law enforcement. It stresses the importance of controlled messaging to prevent misinformation, panic, or legal exposure. Proper communication templates help ensure accurate and timely information sharing throughout the incident lifecycle.
- Finally, the handbook highlights the importance of post-incident review and continuous improvement. After an incident is resolved, teams are encouraged to conduct lessons-learned sessions using structured review templates. These reviews identify gaps in detection, response, tools, and training, and feed improvements back into playbooks and procedures. Over time, this process helps organizations mature their incident response capabilities and improve resilience against future threats.



- **Exploring Let's Defend for Simulated Incident Response and SOAR Concepts**
  - Let's Defend is an interactive, hands-on cybersecurity training platform designed to help learners practice Incident Response (IR), SOC operations, and SOAR concepts in a realistic, simulated environment. It is especially useful for students, entry-level SOC analysts, and professionals who want practical experience handling security incidents without impacting real systems.

- One of the main strengths of Let's Defend is its simulated incident response scenarios. The platform presents users with real-world–style alerts such as phishing emails, brute-force login attempts, malware detections, suspicious network traffic, and endpoint compromise. Users are required to investigate these alerts by analyzing logs, user behavior, IP addresses, file hashes, and indicators of compromise. This helps learners understand how incidents are detected, analyzed, and validated in a real SOC environment.
- Let's Defend also helps users practice the incident response lifecycle in a hands-on manner. During simulations, learners perform alert triage, identify the root cause of incidents, decide containment actions, and document findings. This reinforces theoretical knowledge of frameworks like NIST SP 800-61 by applying them in practical scenarios. Users learn how to assess severity, prioritize incidents, and make response decisions under time pressure.
- A key learning outcome of Let's Defend is understanding SOAR (Security Orchestration, Automation, and Response) concepts. The platform introduces automation workflows such as automated alert enrichment, IP reputation checks, ticket creation, and response playbooks. Learners see how repetitive tasks can be automated to reduce response time and analyst workload, which is a core function of SOAR tools used in modern SOCs.
- Let's Defend also emphasizes documentation and communication, which are critical skills for incident responders. Users are required to create incident reports, record investigation steps, and recommend remediation actions. This builds the habit of clear documentation and structured reporting, aligning with best practices from SANS and NIST.
- Additionally, the platform improves decision-making and analytical thinking. Learners must choose appropriate response actions, such as blocking IPs, isolating hosts, or escalating incidents. Mistakes provide learning opportunities, helping users understand the consequences of incorrect decisions.

Figure 3—Challenges After a Pandemic

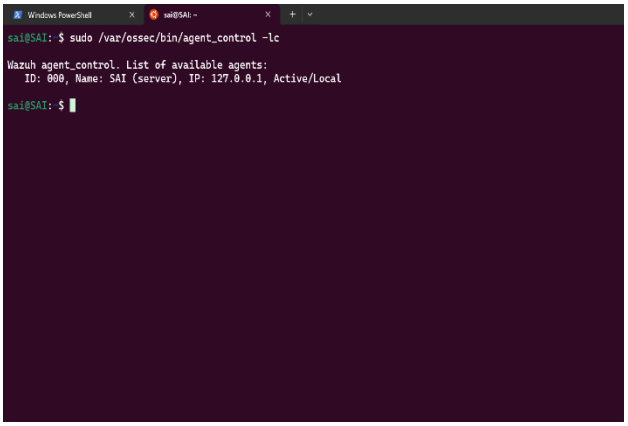


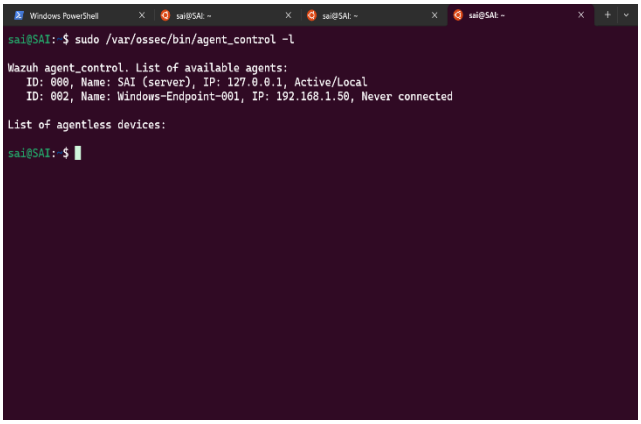
Practical Application

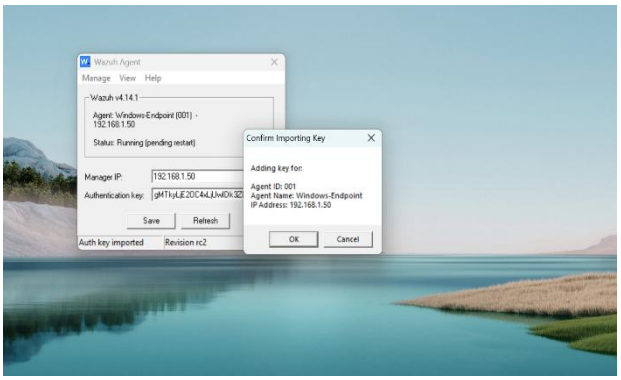
1. Alert Management Practice Activities:

Purpose

The alert classification system is designed to standardize how security alerts generated by Wazuh are analyzed, categorized, prioritized, and mapped to the MITRE ATT&CK framework before being handled as incidents in TheHive. This system ensures consistent triage, faster investigation, and effective escalation within a SOC environment.







Overview of the Classification Process

1. Alert Generation
   Wazuh continuously monitors endpoints, logs, and network activity. When suspicious behavior is detected (e.g., multiple failed logins, malware detection, PowerShell execution), Wazuh generates an alert with metadata such as rule ID, severity level, description, and MITRE ATT&CK mapping (if available).
2. Alert Review
   The SOC analyst reviews the alert details from the Wazuh dashboard or alerts log. Each alert is evaluated for its impact, scope, and relevance to security operations.

3. Classification Using Google Sheets
   A centralized Google Sheets alert classification table is used as a reference to map alerts to:
   - Alert category
   - Severity level
   - MITRE ATT&CK tactic and technique
   - Incident priority
   - Recommended response actions

This sheet acts as a decision-making guide for analysts during alert triage.

4. Incident Creation in TheHive
   Once classified and prioritized, relevant alerts are converted into incident tickets (cases) in TheHive, where investigation and response activities are tracked.
5. Escalation and Response
   Based on priority, alerts are escalated to appropriate teams (L1, L2, IR team, or SOC manager), following predefined response procedures.

Google Sheets – Alert Classification Table Description
The Google Sheets table contains the following fields:

- Alert Source
  Indicates the system generating the alert (e.g., Wazuh agent, Windows logs, Linux logs).
- Wazuh Rule ID
  The unique identifier of the Wazuh rule that triggered the alert.
- Alert Description
  A brief explanation of the detected activity (e.g., “Multiple failed SSH login attempts”).
- Alert Category
  Logical grouping of alerts such as:
  - Authentication attacks
  - Malware activity
  - Execution
  - Persistence
  - Privilege escalation
- Severity Level
  Technical severity assigned by Wazuh (Low, Medium, High, Critical).
- MITRE ATT&CK Tactic
  The high-level attacker objective, such as:
  - Initial Access
  - Execution
  - Credential Access
  - Persistence

    - Impact
- MITRE ATT&CK Technique
  The specific technique used by the attacker (e.g., T1110 – Brute Force, T1059 – Command and Scripting Interpreter).
- Incident Priority
  Business-oriented priority used by the SOC:
    - P0 – Critical
    - P1 – High
    - P2 – Medium
    - P3 – Low
- Recommended Response Action
  Initial actions analysts should take, such as:
    - Investigate logs
    - Isolate affected host
    - Block IP address
    - Reset user credentials
    - Escalate to incident response team

Example Classification Entries

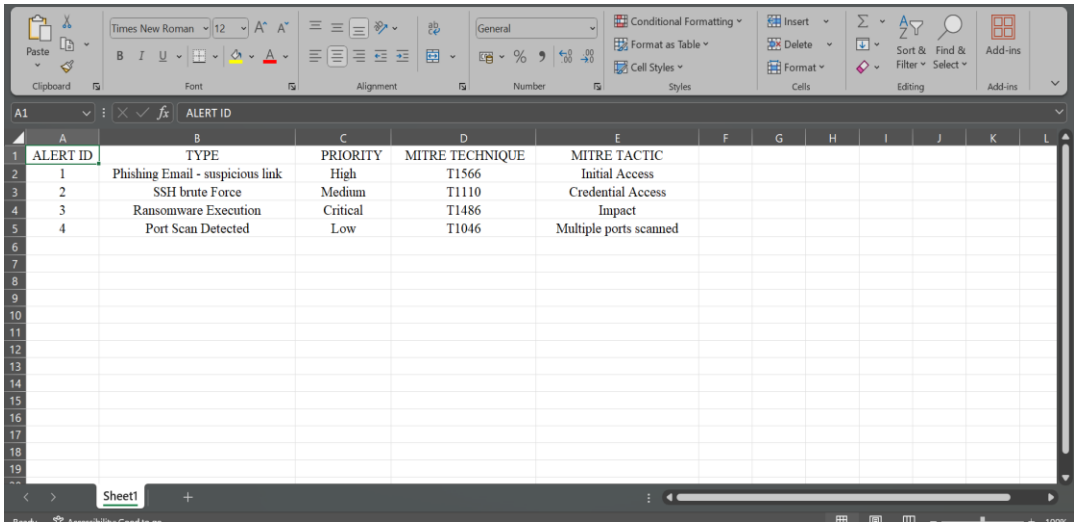
- SSH Brute Force Alert
  An alert triggered by multiple failed SSH login attempts is classified under *Credential Access*. It is mapped to the MITRE ATT&CK technique T1110 (Brute Force) and assigned a High severity and P1 priority, requiring immediate investigation and potential IP blocking.
- Suspicious PowerShell Execution
  A PowerShell execution alert is categorized as *Execution* and mapped to T1059.001 (PowerShell). Due to its high likelihood of malicious activity, it is marked as Critical severity and P0 priority, requiring rapid escalation to the incident response team.
- Malware Detection Alert
  Malware detection is classified under *Impact* and mapped to T1486 (Data Encrypted for Impact) or relevant malware techniques. This alert is assigned Critical severity, and an incident ticket is created immediately in TheHive.

Benefits of the Alert Classification System

- Ensures consistent and standardized alert handling
- Reduces analyst decision-making time during triage
- Aligns alerts with the MITRE ATT&CK framework for better threat understanding
- Improves coordination between Wazuh detection and TheHive incident management
- Supports auditing, reporting, and compliance requirements

Conclusion

The alert classification system acts as a bridge between detection and response. By using a structured Google Sheets table to map Wazuh alerts to MITRE ATT&CK techniques, SOC analysts can efficiently prioritize alerts, create accurate incident tickets in TheHive, follow documented response procedures, and escalate incidents appropriately. This approach reflects real-world SOC operations and best practices.

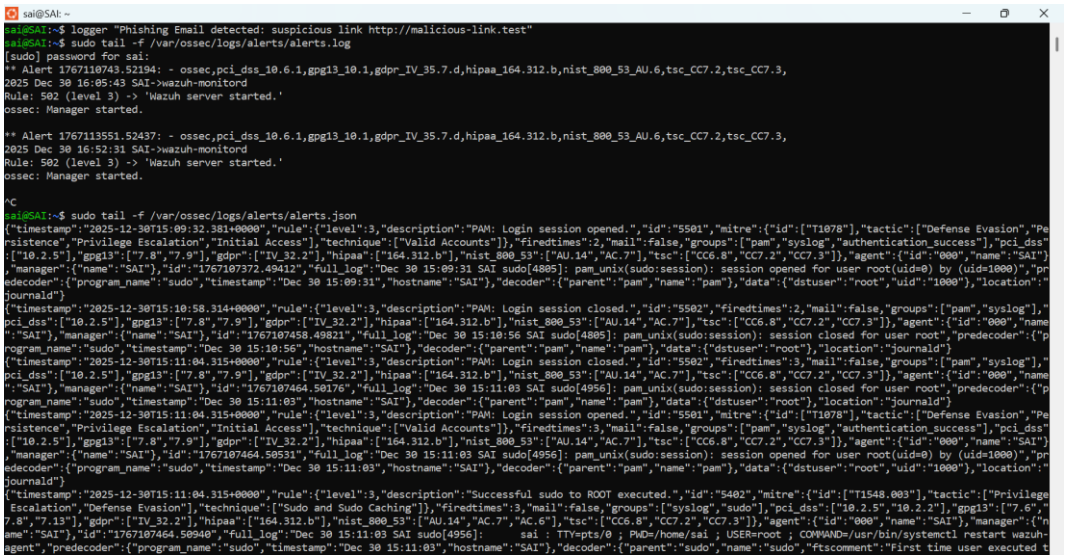


ALERT ID	TYPE	PRIORITY	MITRE TECHNIQUE	MITRE TACTIC
1	Phishing Email - suspicious link	High	T1566	Initial Access
2	SSH brute Force	Medium	T1110	Credential Access
3	Ransomware Execution	Critical	T1486	Impact
4	Port Scan Detected	Low	T1046	Multiple ports scanned

- **Test with a mock alert**
  - To validate the alert classification and incident response workflow, a mock phishing alert is used as a test scenario.
  - In this test, a simulated phishing email containing a suspicious hyperlink is introduced into the logging system monitored by Wazuh. The log message represents a common real-world phishing attempt where an attacker sends an email with a malicious or unknown URL intended to trick a user into clicking it.
  - Once the mock phishing event is generated, Wazuh detects the log entry through its log monitoring capability. The event is processed by Wazuh rules, which analyze the content of the message and identify it as suspicious activity related to phishing. As a result, Wazuh creates an alert containing details such as the alert description, severity level, timestamp, and the affected host or agent.
  - The alert is then visible in the Wazuh dashboard, where SOC analysts can review it as part of normal security monitoring activities. The alert is categorized under Initial Access, as phishing is commonly used by attackers as an entry point into an organization.
  - For threat context and standardization, the alert is mapped to the MITRE ATT&CK framework, specifically:
- Tactic: Initial Access
- Technique: T1566 – Phishing

- This mapping helps analysts understand the attacker's objective and aligns the alert with globally recognized threat intelligence standards.
- The mock phishing alert is assigned a medium severity and priority, reflecting that no confirmed compromise has occurred yet, but further investigation is required. Recommended response actions include analyzing the suspicious link, checking for similar emails across the environment, blocking the sender or domain if malicious, and notifying affected users if necessary.

- This test confirms that the alert classification system functions correctly by:
  - Detecting simulated phishing activity
  - Generating a meaningful alert in Wazuh
  - Supporting MITRE ATT&CK mapping
  - Enabling consistent triage and response decisions
- Overall, the mock phishing alert serves as a controlled test case to demonstrate how Wazuh detects threats and how SOC analysts classify and respond to them before escalating or creating incident tickets in TheHive.



- **Prioritize Alerts:**
  In this scenario, a simulated alert represents the detection of a **Log4Shell (Log4j) remote code execution exploit** affecting a vulnerable server. Log4Shell allows attackers to execute arbitrary code remotely without authentication, making it one of the most severe vulnerabilities.
  The alert is evaluated using CVSS criteria such as:
  - Network-based exploitation
  - No authentication required
  - High impact on confidentiality, integrity, and availability

  Based on these factors, the alert is assigned a **CVSS score of 9.8**, which falls into the **Critical severity** range. In the Google Sheets prioritization table, this alert is marked as

Critical (P0), indicating that it requires immediate attention and escalation to the incident response team.
This classification reflects the high risk of system compromise and potential widespread impact on the organization.

2. Low Alert: *Port Scan Detected*
In contrast, a simulated **port scan alert** represents reconnaissance activity where an external system probes open ports on a network device or server. While port scanning may indicate attacker interest, it does not necessarily confirm exploitation or compromise.
When assessed using CVSS:

- The impact on systems is minimal
- No direct exploitation occurs
- Confidentiality, integrity, and availability are not immediately affected

As a result, the alert is assigned a **low CVSS score (for example, 3.5)**. In the Google Sheets table, this corresponds to a **Low severity** and **P3 priority**, meaning the alert should be monitored and documented but does not require immediate escalation.

CVSS-Based Prioritization Logic
The following logic is applied in the Google Sheets document to convert CVSS scores into SOC priorities:

- **CVSS 9.0 – 10.0:** Critical (P0)
- **CVSS 7.0 – 8.9:** High (P1)
- **CVSS 4.0 – 6.9:** Medium (P2)
- **CVSS 0.1 – 3.9:** Low (P3)

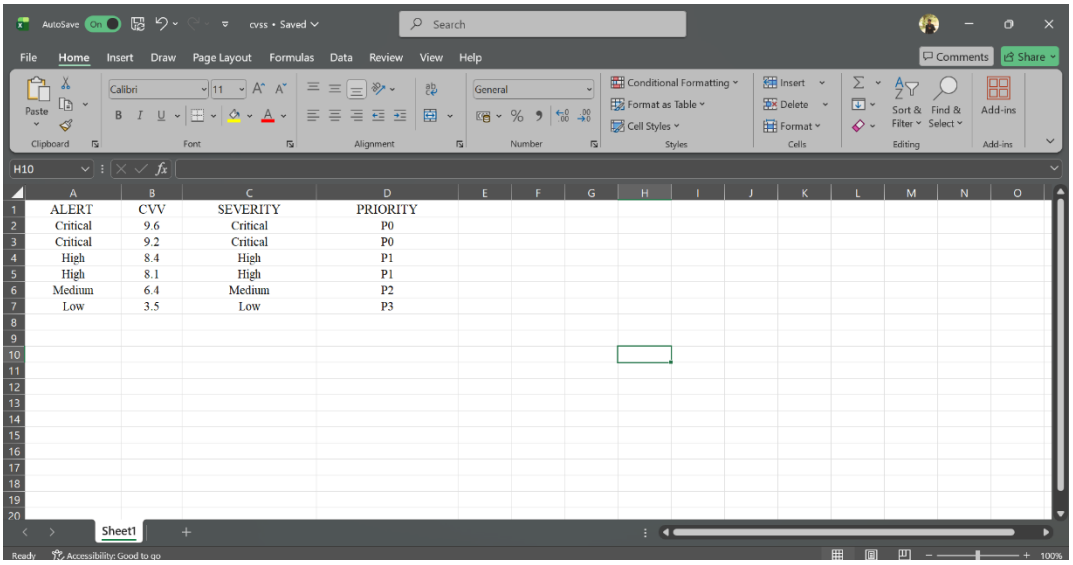
This mapping ensures that technical vulnerability severity is consistently translated into operational response priorities.

Outcome of the Prioritization Process
By simulating alerts such as **Log4Shell exploitation** and **port scanning**, the SOC team can demonstrate how different threat types receive different priorities based on CVSS scoring. High-risk vulnerabilities are escalated immediately, while low-risk activities are monitored without disrupting operations.
This prioritization process helps SOC analysts:

- Focus on the most dangerous threats first
- Reduce alert fatigue
- Align technical severity with business impact
- Support structured and documented incident response decisions

Conclusion
Using CVSS scoring within Google Sheets provides a clear and standardized method for prioritizing alerts. By comparing high-impact alerts like **Log4Shell (CVSS 9.8 –**

Critical) with low-impact alerts such as **port scans**, the SOC can effectively manage risks and respond appropriately to security events.



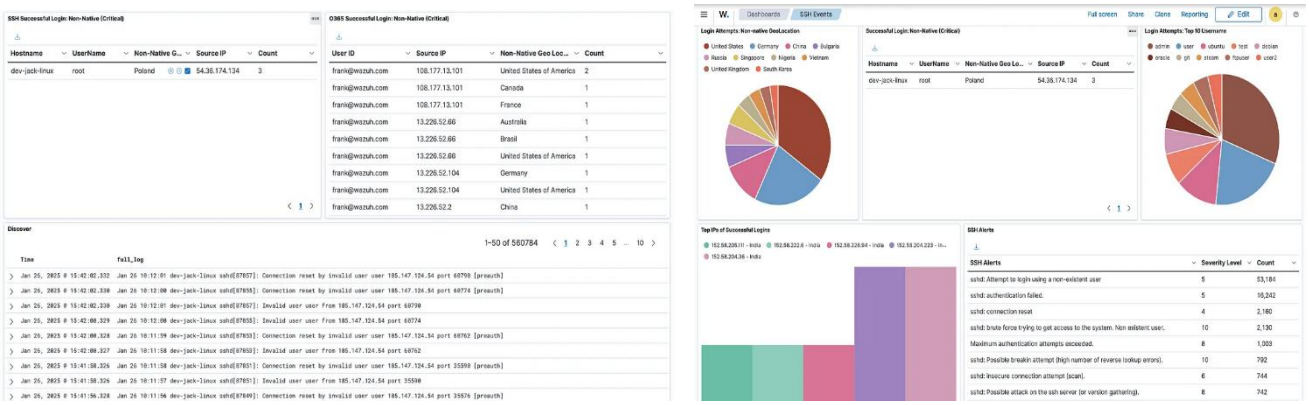
ALERT	CVV	SEVERITY	PRIORITY
Critical	9.6	Critical	P0
Critical	9.2	Critical	P0
High	8.4	High	P1
High	8.1	High	P1
Medium	6.4	Medium	P2
Low	3.5	Low	P3

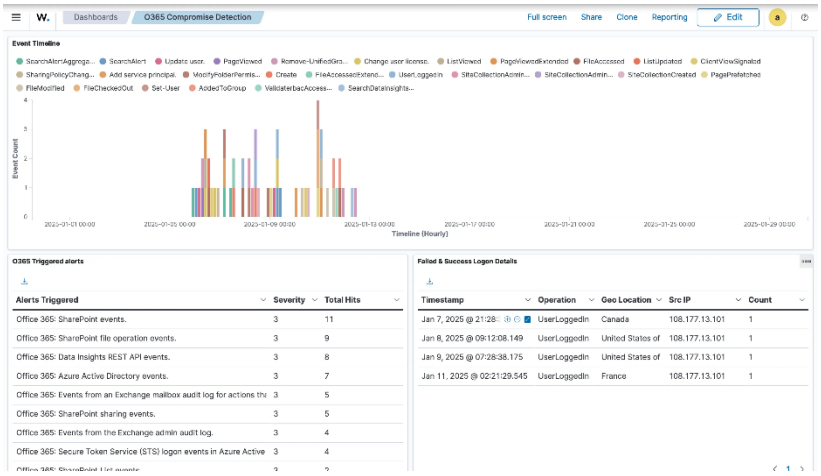
Dashboard Creation

- A security monitoring dashboard in Wazuh is designed to provide a centralized and real-time view of security events occurring across the monitored infrastructure. The dashboard consolidates alerts collected by the Wazuh manager and presents them visually to help SOC analysts quickly understand the security posture, identify threats, and prioritize incident response.
- In this dashboard, alert data indexed in **wazuh-alerts-*** is used as the primary data source. The dashboard focuses on alert severity, which is determined by the **rule.level** field generated by Wazuh rules. Severity levels are mapped to operational priorities, where higher rule levels represent more critical security incidents such as malware activity, privilege escalation, or ransomware behavior.
- A **pie chart visualization** is used to represent alert priorities. This chart divides alerts into segments such as **Critical** and **High**, allowing analysts to immediately assess the proportion of severe threats compared to less critical alerts. Critical alerts typically correspond to rule levels between 12 and 15, while high-severity alerts fall between levels 8 and 11. This visualization helps SOC teams quickly determine whether immediate response actions are required.
- To complement severity analysis, the dashboard also includes a **time-based visualization** that displays alerts over time. This allows analysts to detect spikes in malicious activity, identify ongoing attacks, and correlate alerts with specific time periods. Sudden increases in alerts may indicate active threats such as brute-force attacks or ransomware execution.
- Another important component of the dashboard is the visualization of **top affected agents**. This view highlights the systems that generate the highest number of alerts, enabling SOC

analysts to identify compromised or high-risk endpoints. By correlating alert severity with affected agents, analysts can prioritize investigations and containment efforts more effectively.

- Overall, the Wazuh dashboard serves as a decision-support tool for security operations. By presenting complex security data through intuitive visualizations, it enhances situational awareness, reduces investigation time, and supports faster and more accurate incident response. This dashboard is particularly useful in SOC environments for continuous monitoring, threat detection, and compliance reporting.





- **Incident Ticket:**
  - A critical ransomware incident has been detected on **Server-X** based on security alerts generated by the Wazuh SIEM. The observed activity indicates potential ransomware execution with characteristics consistent with file encryption behavior.
  - Key indicators of compromise (IOCs) include the presence of a suspicious executable file identified as **crypto_locker.exe** and an outbound network connection to the IP address **192.168.1.50**, which is suspected to be associated with malicious command-and-control activity.
- The alert has been mapped to the **MITRE ATT&CK technique T1486 (Data Encrypted for Impact)**, suggesting a high risk of data loss and possible lateral movement within the

environment. Immediate investigation and containment actions are required to prevent further impact.

Title:[Critical] Ransomware Detected on Server-X
Description: Indicators [File:crypto_locker.exe], [IP:192.168.1.50]
Priority: Critical
Assignee: SOC Analyst

- **Malware Infection**
  Title: [High] Malware Infection Detected on Workstation-12
  Description: [File:**trojan_dropper.exe]**
  Priority: High
  Assignee: SOC Analyst

- **Phishing Attack**
  Title: [High] Phishing Email Detected – User Account Compromised
  Description: A phishing email containing a malicious link was reported by the user. The link redirected to a fake login page, potentially leading to credential compromise.
  Priority: High
  Assignee: SOC Analyst

- **Brute Force Attack**
  Title: [Medium] Multiple Failed Login Attempts Detected
  Description: Multiple failed authentication attempts were detected against the SSH service on Server-Y. The activity suggests a possible brute-force attack attempt.
  Priority: Medium
  Assignee: SOC Analyst

- **Unauthorized Access**
  Title: [High] Unauthorized Privileged Access Detected
  Description: An unauthorized privilege escalation attempt was detected on Server-Z. A non-administrative user attempted to gain root-level access.
  Priority: High
  Assignee: SOC Analyst

- **Suspicious Network Activity**
  Title: [Medium] Suspicious Outbound Network Connection Detected
  Description: The system initiated outbound communication to an untrusted external IP address **45.67.89.10**, indicating possible command-and-control activity.
  Priority: Medium
  Assignee: SOC Analyst

- **Escalation Role-Play:**

  Subject : [Critical] Ransomware Activity Detected on Server-X – Immediate Action Required

  Dear Tier 2 SOC Team,

  A **Critical ransomware incident** has been detected on **Server-X**, triggered by multiple Wazuh SIEM alerts. The observed activity indicates **potential file encryption behavior** consistent with active ransomware execution.

  Key Indicators of Compromise (IOCs):
  - Malicious file: crypto_locker.exe
  - Suspicious outbound connection: 192.168.1.50
  - MITRE ATT&CK mapping: **T1486 – Data Encrypted for Impact**

  Initial Tier 1 triage confirms a **high risk of data loss**, with potential indicators of lateral movement within the environment.

  Recommended immediate actions:

  - Isolate the affected host from the network
  - Initiate containment procedures
  - Perform deeper forensic analysis (memory, disk, and network artifacts)

  Kindly advise on further remediation steps and investigation priorities.

  Regards,
  SAI
  SOC Tier 1 Analyst

2. Response Documentation :-

1. Executive Summary

On the morning of **[date]**, the Security Operations Center (SOC) identified a phishing incident targeting an internal employee through a deceptive email impersonating a trusted business service. The email contained a malicious hyperlink designed to harvest user credentials. The incident was detected through a combination of user reporting and email security monitoring. Immediate response actions were initiated to prevent account compromise and limit potential exposure. The incident was contained successfully with no confirmed data loss or system

compromise. This report documents the incident response activities following the SANS Incident Handling framework.

2. Timeline

The phishing email was delivered to the user's inbox during regular business hours. Shortly after receiving the email, the user clicked the embedded link, which redirected to a fraudulent login page. Within minutes, the user recognized suspicious behavior and reported the email to the SOC. Upon receiving the report, SOC analysts validated the phishing indicators, classified the event as a confirmed security incident, and escalated it according to incident response procedures. Containment actions, including account password resets and blocking of malicious indicators, were completed promptly. The incident was fully contained within a short timeframe, followed by post-incident review activities.

3. Impact Analysis

The phishing incident affected a single user account, with no evidence of malware execution, lateral movement, or data exfiltration. Although credentials may have been exposed, rapid response actions prevented unauthorized access to internal systems. Business operations were not disrupted, and no critical systems were impacted. The overall impact was assessed as **low to moderate**, with potential risk mitigated through swift detection and containment. The incident highlighted the ongoing risk posed by social engineering attacks rather than technical vulnerabilities.

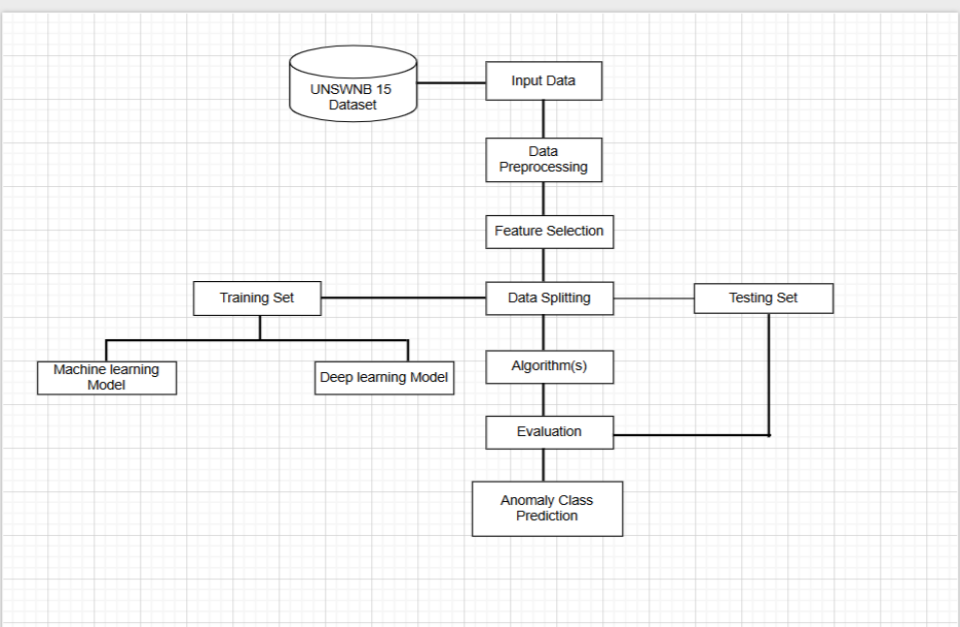
4. Remediation Steps

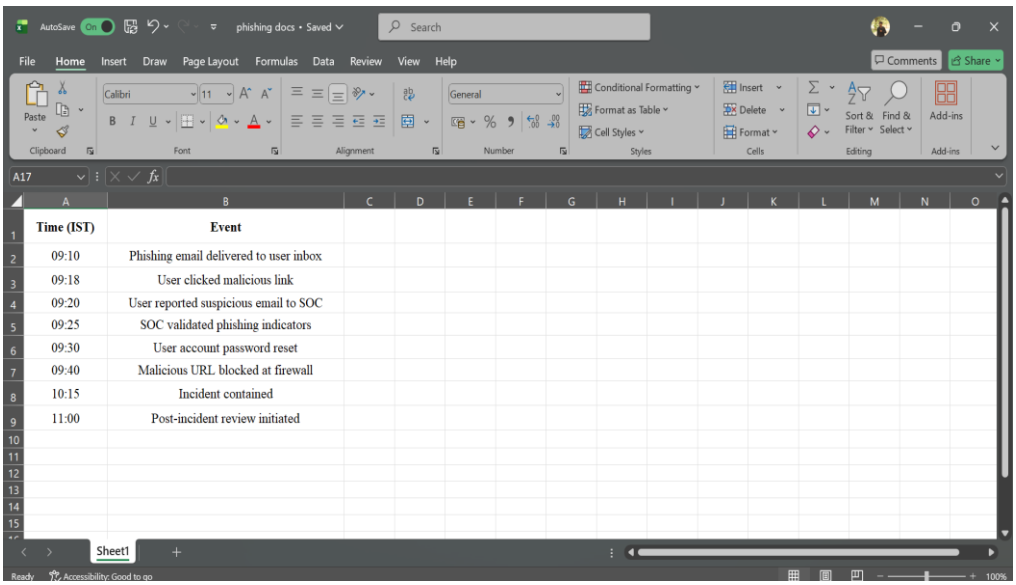
Immediate remediation steps included forcing a password reset for the affected user, revoking active authentication sessions, and blocking the malicious URL and sender domain at the email gateway and firewall. Additional actions were taken to review email security rules to prevent similar phishing attempts in the future. The affected user was informed of the incident and advised to change passwords on any external services where the same credentials may have been used. The SOC also conducted a targeted review of logs to ensure no further suspicious activity occurred after containment

5. Lessons Learned

The incident demonstrated the effectiveness of user awareness and rapid SOC response in minimizing impact. However, it also revealed gaps in email filtering controls and user susceptibility to phishing techniques. Improvements were identified, including enhancing email detection rules, increasing phishing awareness training, and enforcing multi-factor authentication (MFA) for all users. Regular phishing simulations and continuous monitoring were recommended to strengthen the organization's resilience against future social engineering attacks.

Flowchat



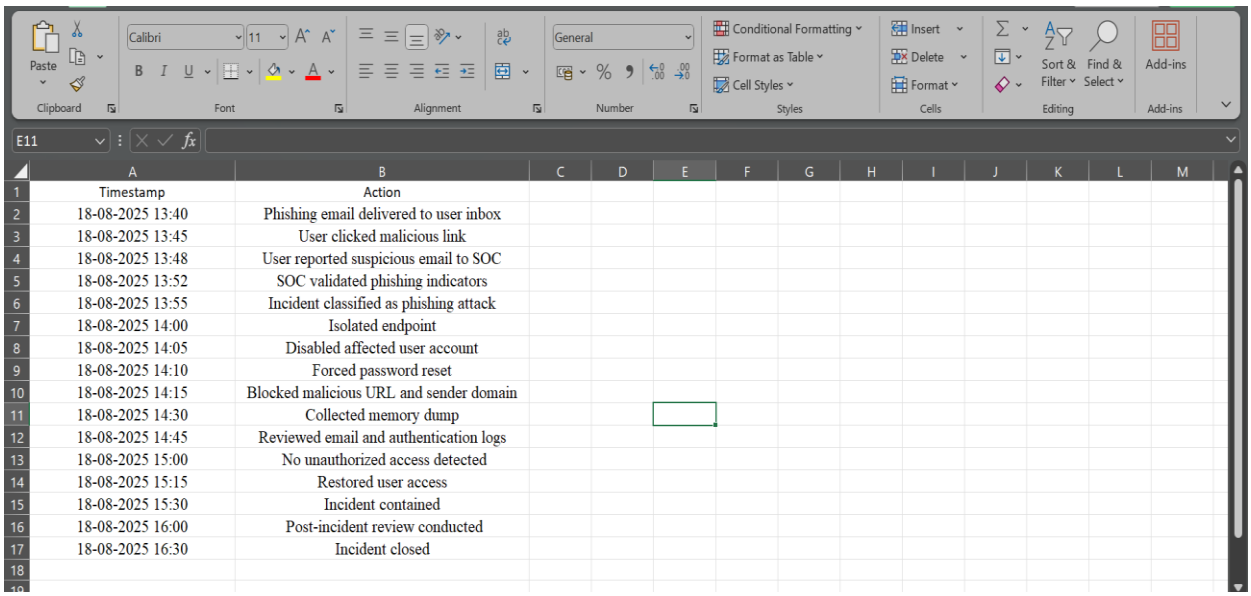


Time (IST)	Event
09:10	Phishing email delivered to user inbox
09:18	User clicked malicious link
09:20	User reported suspicious email to SOC
09:25	SOC validated phishing indicators
09:30	User account password reset
09:40	Malicious URL blocked at firewall
10:15	Incident contained
11:00	Post-incident review initiated

- **Investigation Steps**
- The investigation begins once the phishing alert is received from either the user or the email security system. The SOC analyst first reviews the reported email to identify phishing indicators such as suspicious sender addresses, unexpected attachments, shortened URLs, spelling errors, or impersonation of trusted brands. Email headers are analyzed to verify the sender's origin and detect spoofing or domain anomalies.
- Next, the analyst determines whether the user interacted with the email. This includes confirming whether the malicious link was clicked or if any attachments were opened. If a

link was clicked, the analyst examines the URL using threat intelligence sources to identify known malicious infrastructure and determine whether it hosts a credential-harvesting page.

- If there is a possibility that credentials were submitted, the affected user account is immediately reviewed for abnormal login activity. Authentication logs are checked for unusual login locations, failed login attempts, or access outside normal business hours. Any active sessions associated with the account are identified and reviewed to confirm whether unauthorized access occurred.
- The investigation then expands to ensure no lateral movement or additional compromise has taken place. Email logs are reviewed to identify whether similar phishing messages were delivered to other users. Network and SIEM logs are analyzed to detect suspicious outbound connections, data exfiltration attempts, or abnormal system behavior linked to the incident.
- Once evidence collection is complete, all findings are documented, including indicators of compromise, user actions, impacted assets, and confirmed outcomes. The incident is then classified based on severity and impact, and investigation results are shared with the incident response team to support containment, remediation, and post-incident review activities.

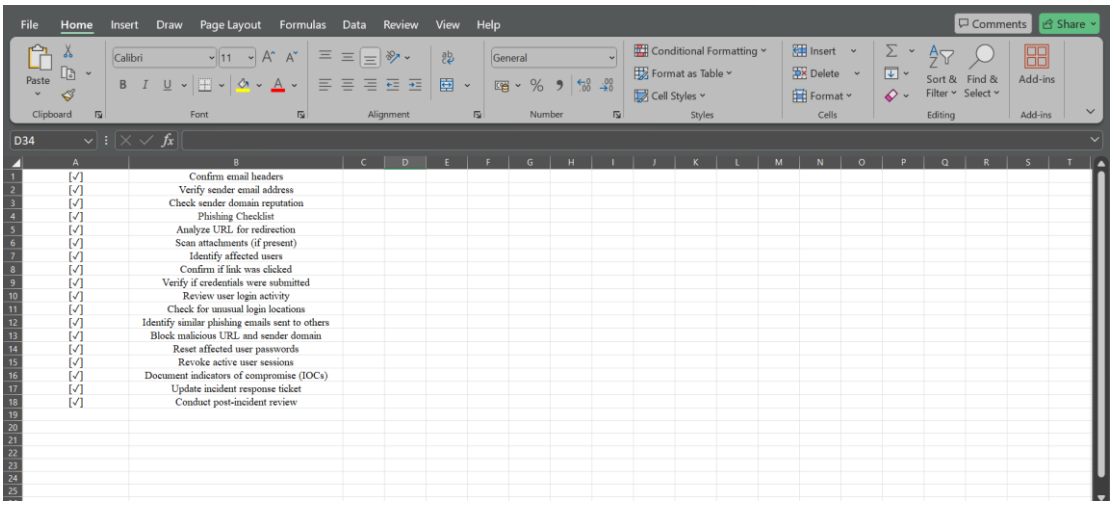


	A	B
1	Timestamp	Action
2	18-08-2025 13:40	Phishing email delivered to user inbox
3	18-08-2025 13:45	User clicked malicious link
4	18-08-2025 13:48	User reported suspicious email to SOC
5	18-08-2025 13:52	SOC validated phishing indicators
6	18-08-2025 13:55	Incident classified as phishing attack
7	18-08-2025 14:00	Isolated endpoint
8	18-08-2025 14:05	Disabled affected user account
9	18-08-2025 14:10	Forced password reset
10	18-08-2025 14:15	Blocked malicious URL and sender domain
11	18-08-2025 14:30	Collected memory dump
12	18-08-2025 14:45	Reviewed email and authentication logs
13	18-08-2025 15:00	No unauthorized access detected
14	18-08-2025 15:15	Restored user access
15	18-08-2025 15:30	Incident contained
16	18-08-2025 16:00	Post-incident review conducted
17	18-08-2025 16:30	Incident closed

- The phishing incident was successfully detected, investigated, and contained through timely user reporting and effective SOC response procedures. Although the user interacted with a malicious link, rapid containment actions—including account isolation, credential resets, and blocking of malicious indicators—prevented unauthorized access and data compromise. No evidence of lateral movement or system exploitation was identified during the investigation. This incident highlights the importance of continuous user awareness, strong email security controls, and well-defined incident response processes. Implementing the recommended improvements will further strengthen the organization's ability to detect and respond to phishing threats in the future.

- **Phishing Checklist:**

- The phishing incident response checklist is designed to ensure a structured and consistent approach when investigating suspected phishing emails. The first step involves confirming the email headers to validate the sender's authenticity. Analysts review fields such as "From," "Return-Path," and "Received" headers, along with SPF, DKIM, and DMARC results, to detect spoofing or unauthorized email sources. This helps determine whether the email originated from a legitimate or malicious domain.
- The next step is to verify the sender's email address and assess the reputation of the sender domain. Threat intelligence platforms and internal blocklists are used to check whether the domain or IP address has been previously associated with phishing campaigns. Analysts then examine embedded links within the email and check their reputation using services such as VirusTotal. URL analysis includes inspecting redirections, domain age, and whether the link leads to a credential-harvesting or malware-hosting site.
- If attachments are present, they are scanned in a secure environment to identify any malicious payloads. Analysts also confirm whether the user interacted with the email by clicking links or opening attachments. Identifying affected users is critical, as it helps determine the scope of the incident and whether similar emails were delivered to multiple recipients across the organization.
- Once user interaction is confirmed, authentication and access logs are reviewed to detect abnormal login attempts, unusual geolocations, or unauthorized access following the phishing attempt. If credentials may have been compromised, immediate containment actions such as password resets, session revocation, and account lockdown are performed. Malicious URLs, sender domains, and related indicators of compromise are blocked at email gateways, firewalls, and SIEM platforms to prevent further exposure.
- The final steps of the checklist focus on documentation and continuous improvement. All findings, actions taken, and indicators of compromise are documented in the incident response ticket. A post-incident review is conducted to identify gaps in detection or user awareness and to recommend improvements such as enhanced email filtering, phishing awareness training, and enforcement of multi-factor authentication. This checklist ensures that phishing incidents are handled efficiently while reducing the likelihood of recurrence.



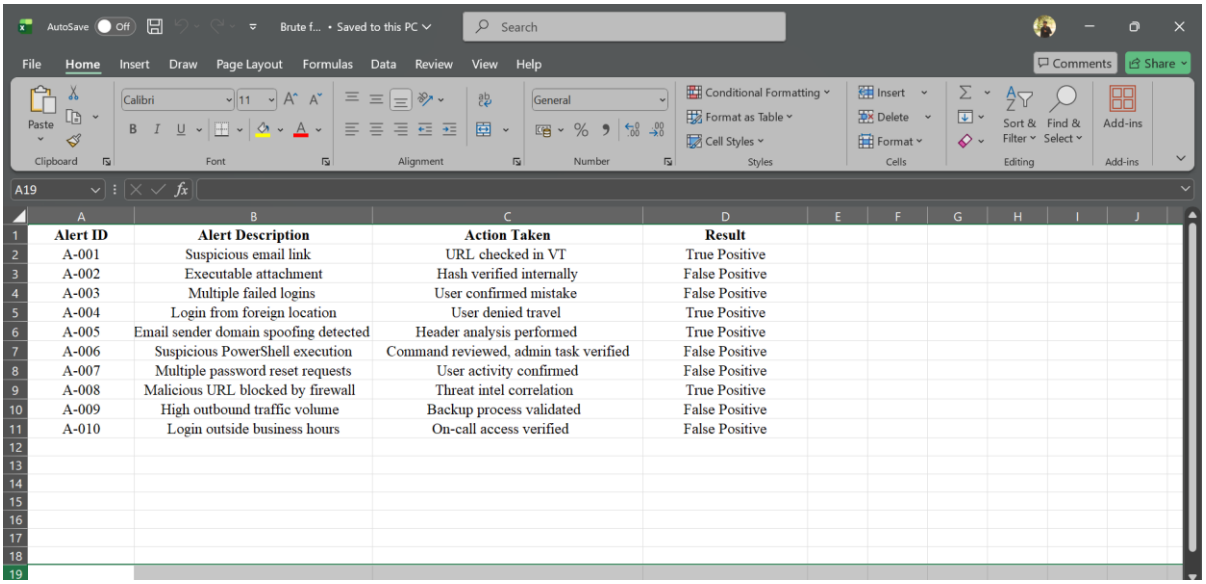
- **Post-Mortem**

  The simulated breach highlighted the need for faster detection, clearer escalation paths, and stronger preventive controls. Improving email filtering, enforcing multi-factor authentication, and enhancing user awareness training will reduce risk. Regular incident response drills and better documentation will strengthen coordination, speed containment, and improve overall SOC effectiveness.

3. **Alert Triage Practice**

Activities:

- The simulated triage program begins by collecting sample security alerts generated from monitoring tools such as a SIEM, email security gateway, or authentication logs. These alerts represent common security events including suspicious email links, abnormal login behavior, or potentially malicious file attachments. Each alert is assigned a unique alert ID, severity level, and brief description to standardize analysis.
- Once alerts are collected, the triage process is initiated by reviewing each alert individually. The analyst examines the alert source, timestamp, and triggered rule to understand why the alert was generated. Initial context is gathered to determine whether the alert aligns with known attack patterns or routine user activity. This step helps prioritize alerts that require immediate attention.
- The next stage focuses on indicator validation. For phishing-related alerts, email headers, sender domains, and embedded URLs are analyzed. URLs and file hashes are checked using threat intelligence platforms such as VirusTotal. For login-related alerts, authentication logs are reviewed to identify unusual login locations, failed attempts, or abnormal access times. This validation step is critical for distinguishing genuine threats from benign activity.
- After validating indicators, the analyst correlates additional contextual information. User confirmation is obtained when possible to verify whether the activity was expected or accidental. Business context, such as scheduled maintenance, VPN usage, or legitimate administrative tasks, is also considered. Many false positives are identified during this phase due to normal operational behavior.
- Based on the collected evidence, each alert is classified as either a True Positive or False Positive. True positives are escalated for containment and response actions, while false positives are documented and closed with justification. All findings, actions taken, and decisions are recorded in the incident tracking system to maintain auditability and improve future detection accuracy.
- The program concludes with a review of triage outcomes to identify patterns in false positives. Detection rules are fine-tuned, and response procedures are updated to reduce alert noise and improve SOC efficiency. This simulated triage execution demonstrates the practical application of alert analysis, validation, and decision-making in a controlled environment.



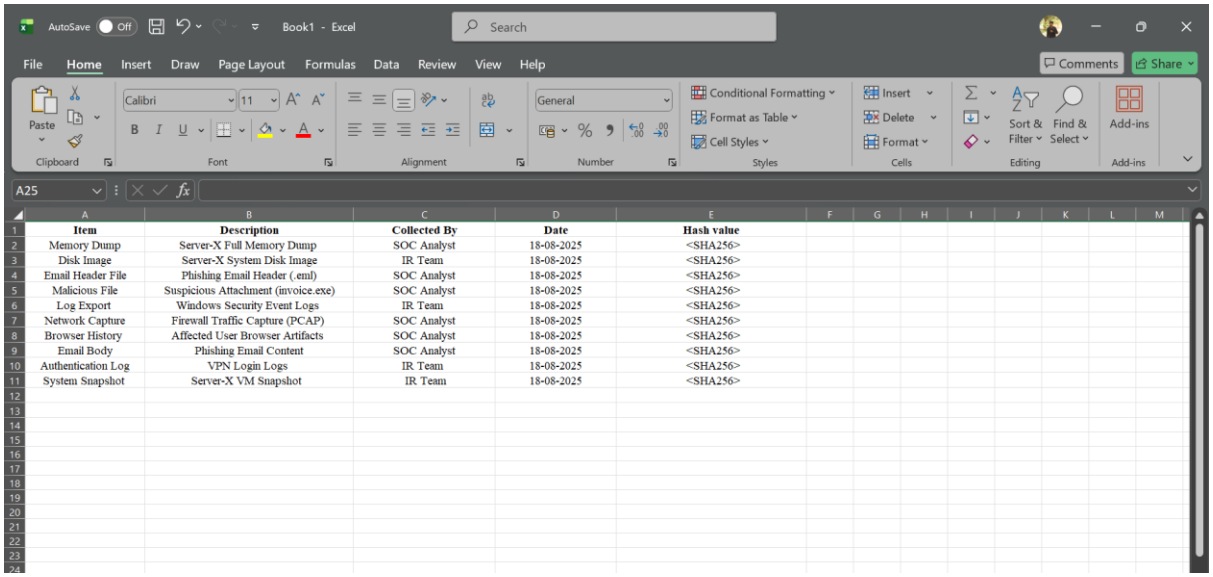
Alert ID	Alert Description	Action Taken	Result
A-001	Suspicious email link	URL checked in VT	True Positive
A-002	Executable attachment	Hash verified internally	False Positive
A-003	Multiple failed logins	User confirmed mistake	False Positive
A-004	Login from foreign location	User denied travel	True Positive
A-005	Email sender domain spoofing detected	Header analysis performed	True Positive
A-006	Suspicious PowerShell execution	Command reviewed, admin task verified	False Positive
A-007	Multiple password reset requests	User activity confirmed	False Positive
A-008	Malicious URL blocked by firewall	Threat intel correlation	True Positive
A-009	High outbound traffic volume	Backup process validated	False Positive
A-010	Login outside business hours	On-call access verified	False Positive

Threat Intelligence Validation:

The alert's IP address and file hash were cross-referenced with AlienVault OTX. The indicators matched known malicious activity associated with phishing and credential-harvesting campaigns. Multiple pulses confirmed prior abuse reports, increasing confidence in classification as a true positive and supporting escalation and containment actions.

4. Evidence Preservation :

- Evidence preservation and chain-of-custody are critical steps in incident response to ensure investigation accuracy and legal validity.
- Evidence preservation involves collecting and securing digital artifacts (logs, malware files, memory, network data) without altering them.
- Analysts must follow the order of volatility, capturing volatile data like memory and running processes first.
- Hashing (e.g., SHA-256) is used to verify evidence integrity and detect any changes.
- Chain-of-custody documents who collected the evidence, when, where, and how it was handled.
- Each transfer or access to evidence must be logged and authorized. Proper storage in secure, restricted locations prevents tampering or loss.
- Together, these practices ensure evidence remains trustworthy for forensic analysis and legal proceedings.



Item	Description	Collected By	Date	Hash value
Memory Dump	Server-X Full Memory Dump	SOC Analyst	18-08-2025	<SHA256>
Disk Image	Server-X System Disk Image	IR Team	18-08-2025	<SHA256>
Email Header File	Phishing Email Header (.eml)	SOC Analyst	18-08-2025	<SHA256>
Malicious File	Suspicious Attachment (invoice.exe)	SOC Analyst	18-08-2025	<SHA256>
Log Export	Windows Security Event Logs	IR Team	18-08-2025	<SHA256>
Network Capture	Firewall Traffic Capture (PCAP)	SOC Analyst	18-08-2025	<SHA256>
Browser History	Affected User Browser Artifacts	SOC Analyst	18-08-2025	<SHA256>
Email Body	Phishing Email Content	SOC Analyst	18-08-2025	<SHA256>
Authentication Log	VPN Login Logs	IR Team	18-08-2025	<SHA256>
System Snapshot	Server-X VM Snapshot	IR Team	18-08-2025	<SHA256>

All relevant digital evidence was successfully identified, collected, and preserved following proper incident response and forensic procedures. Hash values were generated to maintain data integrity and ensure chain of custody. The collected artifacts provide sufficient information to support investigation, validation of indicators of compromise, and potential legal or compliance requirements.

5. Capstone Project

- **Simulate the Attack**

A mock phishing attack is simulated by sending a crafted email containing a malicious link that impersonates a trusted service. The link redirects users to a fake login page designed to capture credentials. The objective of the simulation is to test detection capabilities, analyst triage, and incident response procedures without causing real harm.

- **Detect the Incident**

The attack is detected through a combination of user reporting and security monitoring tools. The email security gateway flags the message as suspicious, and the SIEM generates an alert for a potentially malicious external link. This alert is logged and forwarded to the SOC for analysis.

- **Triage the Alert**

SOC analysts review the alert details, including severity, source, and indicators. Email headers and embedded URLs are analyzed, and the link reputation is checked using threat intelligence

platforms. User activity is verified to confirm whether the link was clicked. Based on evidence, the alert is classified as either a true positive or a false positive.

- **Respond to the Incident**

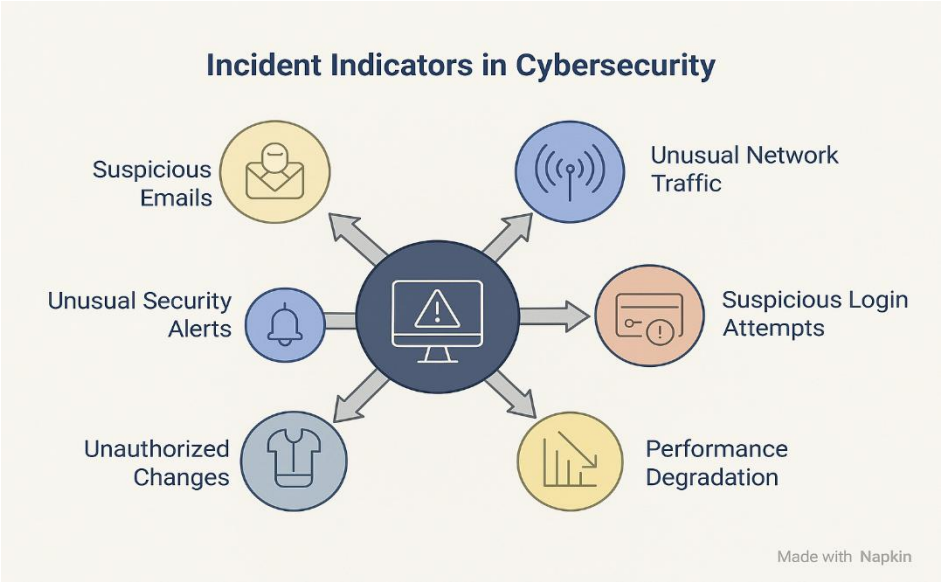
Upon confirming a true positive, containment actions are initiated. The affected user account is temporarily disabled, passwords are reset, and active sessions are revoked. Malicious URLs and sender domains are blocked at the email gateway and firewall. Additional monitoring is enabled to ensure no further malicious activity occurs.

- **Document the Incident**

All actions taken during detection, triage, and response are documented in the incident response report. This includes timelines, indicators of compromise, evidence collected, and final outcomes. A post-incident review is conducted to identify gaps and recommend improvements in controls and processes.

- **Final Outcome**

The simulated incident is successfully detected, contained, and resolved with no data loss. The exercise validates SOC readiness and highlights areas for improving detection accuracy, response speed, and documentation practices.



The simulated incident successfully demonstrated the complete security incident lifecycle, from attack execution to detection, triage, response, and documentation. The exercise confirmed the effectiveness of monitoring tools, analyst decision-making, and response procedures while highlighting opportunities to improve detection accuracy, response speed, and documentation consistency.

- **Detection and Triage**
  - **Detection and triage** is the initial phase of incident response where security teams identify a potential security event and quickly assess its severity, scope, and impact.
  - Detection occurs through security tools such as **Wazuh SIEM**, IDS/IPS, EDR, antivirus, firewall logs, or user reports. Alerts are generated based on predefined rules, anomaly detection, or threat intelligence indicators.
  - During triage, analysts validate whether the alert is a **true positive or false positive**, identify affected systems (e.g., Server-X), and determine the attack type (such as ransomware).
  - Key activities include reviewing alert details, correlating logs, identifying **IOCs** (malicious files, IPs, hashes), and mapping the activity to **MITRE ATT&CK techniques**.
  - The incident is then **classified and prioritized** (Low, Medium, High, Critical) based on business impact and risk.
  - Proper detection and triage ensure rapid escalation, informed decision-making, and effective containment actions.
  - **Detection**
  - Detection begins when a security control identifies abnormal or malicious activity. This can occur through automated tools or human reporting.

- **Common detection sources:**

  SIEM (Wazuh): Correlates logs and triggers alerts based on rules
  Endpoint Security / EDR: Detects malicious processes or file behavior
  IDS/IPS: Identifies suspicious network traffic
  Firewall & Proxy Logs: Reveal malicious connections
  User Reports: Suspicious emails, system slowdowns, file encryption
  Example:
  Wazuh generates a Critical alert for ransomware behavior due to detection of a known malicious file and suspicious outbound traffic.

- **Alert Validation**

  Once an alert is triggered, analysts must determine if it is a **true positive** or **false positive**.
  Validation steps:
  Review alert severity and rule ID
  Analyze correlated logs from multiple sources
  Check file names, hashes, and IP reputation
  Compare activity against baseline behavior
  Outcome:
  The alert is confirmed as malicious ransomware activity rather than a benign event.

- **Triage**

  Triage is the process of **quickly assessing impact, scope, and urgency**.
  Key triage questions:

What systems are affected? (Server-X only or more?)
Is the threat active or contained?
Is sensitive data at risk?
Is lateral movement occurring?
Triage data analyzed:
Running processes
Network connections
User sessions
Recent system changes

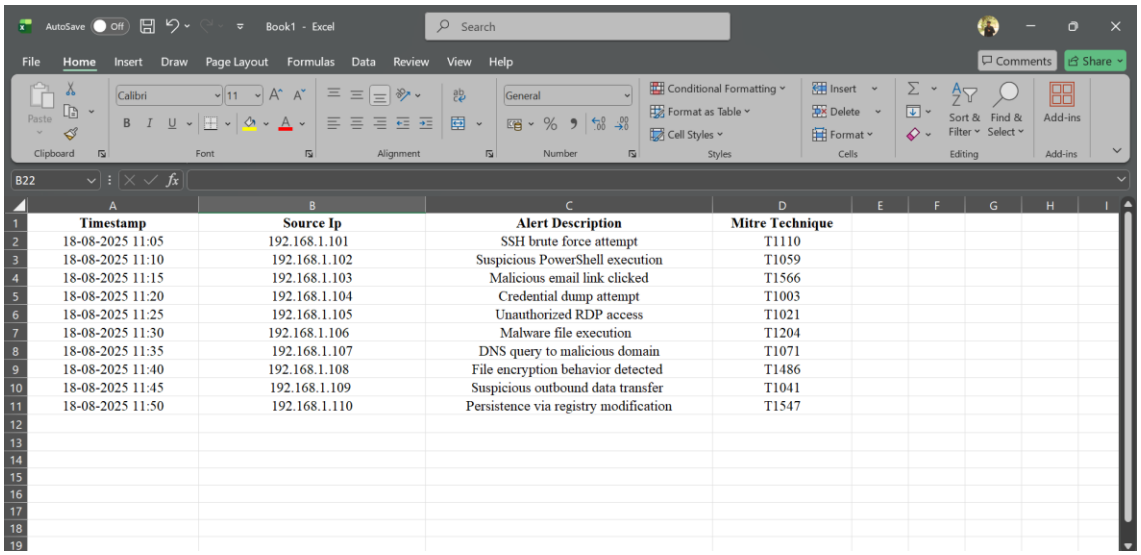
- **Incident Classification**
  After triage, the event is categorized based on type and threat level.
  Examples:
  Malware → Ransomware
  Network → Command-and-Control
  Endpoint → Unauthorized encryption
  Mapped to **MITRE ATT&CK**:
  T1486 – Data Encrypted for Impact

- **Prioritization**
  Incidents are prioritized to ensure high-impact threats are handled first.
  Factors considered:
  Severity of threat
  Business impact
  Asset criticality
  Likelihood of spread
  Example:
  Priority: **Critical**
  Escalation: Tier-2 SOC

- **Documentation & Escalation**
  All findings are documented in an **incident ticket (TheHive)**, including:
  Alert details
  IOCs
  Affected assets
  Initial response actions
  If critical, the incident is escalated with a summary to higher tiers.

- **Importance of Detection & Triage**
  Reduces **mean time to detect (MTTD)**
  Prevents unnecessary escalations

Ensures consistent response
Improves SOC efficiency
Supports compliance (NIST SP 800-61)



	A	B	C	D
1	**Timestamp**	**Source Ip**	**Alert Description**	**Mitre Technique**
2	18-08-2025 11:05	192.168.1.101	SSH brute force attempt	T1110
3	18-08-2025 11:10	192.168.1.102	Suspicious PowerShell execution	T1059
4	18-08-2025 11:15	192.168.1.103	Malicious email link clicked	T1566
5	18-08-2025 11:20	192.168.1.104	Credential dump attempt	T1003
6	18-08-2025 11:25	192.168.1.105	Unauthorized RDP access	T1021
7	18-08-2025 11:30	192.168.1.106	Malware file execution	T1204
8	18-08-2025 11:35	192.168.1.107	DNS query to malicious domain	T1071
9	18-08-2025 11:40	192.168.1.108	File encryption behavior detected	T1486
10	18-08-2025 11:45	192.168.1.109	Suspicious outbound data transfer	T1041
11	18-08-2025 11:50	192.168.1.110	Persistence via registry modification	T1547

- **Incident Response Report**

- On 18 August 2025, the Security Operations Center (SOC) identified a simulated phishing incident targeting an internal user. The attack involved a malicious email containing a deceptive external link designed to harvest user credentials. The incident was detected through a combination of user reporting and SIEM alerts. Prompt triage and response actions prevented unauthorized access, lateral movement, and data loss. The incident was successfully contained within a short timeframe, demonstrating effective SOC monitoring and response capabilities.

- **Incident Timeline**

  At 11:00 AM, the phishing email was delivered to the user's inbox. The user interacted with the email and clicked the embedded link shortly afterward. By 11:10 AM, the user reported suspicious activity to the SOC. Analysts validated the alert, confirmed phishing indicators, and classified the event as a true positive. Containment actions, including account isolation, password reset, and blocking of malicious URLs and sender domains, were completed by 11:30 AM. A post-incident review followed.

- **Recommendations**

  To reduce the risk of similar incidents, it is recommended to enhance email filtering rules, enforce multi-factor authentication for all users, and conduct regular phishing awareness

training. Additionally, periodic incident response drills should be performed to further improve detection speed and response coordination.

- **Stakeholder Briefing:**

  A simulated phishing incident was identified involving an employee receiving a deceptive email that appeared legitimate. The employee interacted with the message and promptly reported it, allowing the Security Operations Team to respond quickly. Our team investigated the alert, confirmed the email was malicious, and immediately secured the affected account by resetting credentials and blocking the malicious link and sender. No unauthorized access, data loss, or business disruption occurred. The incident was fully contained within a short time. As a preventive measure, we are strengthening email filtering controls, reinforcing multi-factor authentication, and continuing employee awareness training to reduce the likelihood of similar incidents in the future.