INCIDENT HANDLING

THREE FUNCTIONS

- Incident Reporting
- Incident Analysis
- Incident Response

INCIDENT REPORTING

- Such functions enables a CERT (Computer Emergency Response Team) to serve as a central point of contact for reporting problems
- Allows all incidents reports and activity to be collected in one location
- Here, Information can be reviewed and correlated across the organization
- Information can then be used to determine patterns of intruders or activity

INCIDENT ANALYSIS FUNCTION

- Recommendation of corresponding preventative strategies can be given
- In-depth look at an incident report of the activity to determine the scope, priority and threat of the incident
- Researching possible response and mitigation strategies.

INCIDENT RESPONSE

- It can take many forms
- A CERT may send out recommendations for recovery, containment and prevention of systems
- Network administrators at sites then performs the response steps themselves
- CERT may also perform these steps themselves but only, when network administrators are unable to mitigate the problem
- Share information and lessons learned with other team members

SANS INSTITUTE RECOMMENDATIONS

- The SANS Institute is a private U.S. for-profit company founded in 1989.
- Specializes in information security, cybersecurity training and selling certificates.
- Topics available for training include cyber and network defenses, penetration testing, incident response, digital forensics, and audit.
- According to them, There are six steps to handle an incident most effectively

STEPS TO HANDLE AN INCIDENT

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Learning Lesson

PREPARATION

- The organization educates users and IT staff of the importance of updated security measures and trains them to respond to computer and network security incidents quickly and correctly.
- Any Incident Response methodologies will emphasize on preparation
- They should be able to prevent incidents by ensuring that systems, networks and applications are sufficiently secure

PREPARATION

- Incident Handler Communications and Facilities
  - Contact Information
  - On-call information
  - Incident reporting mechanisms
  - Issue tracking system
  - Smartphones
  - War Room
  - Secure Storage Facility

PREPARATION

- Incident Analysis Hardware and Software
  - Digital Forensic Workstations and/or Backup devices
  - Laptops
  - Spare workstations, servers, network equipment
  - Blank removable media
  - Portable Printers
  - Packet sniffers and protocol analyzers
  - Removable media with trusted tools
  - Evidence gathering accessories

PREPARATION

- **Digital forensic workstations21 and/or backup devices** to create disk images, preserve log files, and save other relevant incident data
- **Laptops** for activities such as analyzing data, sniffing packets, and writing reports
- **Spare workstations, servers, and networking equipment, or the virtualized equivalents**, which may be used for many purposes, such as restoring backups and trying out malware
- **Blank removable media**
- **Portable printer** to print copies of log files and other evidence from non-networked systems
- **Packet sniffers and protocol analyzers** to capture and analyze network traffic
- **Digital forensic software** to analyze disk images
- **Removable media** with trusted versions of programs to be used to gather evidence from systems
- **Evidence gathering accessories**, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

PREPARATION

- Incident Analysis Resources
  - Port lists
  - Documentations
  - Network diagrams and lists of critical assets
  - Current baselines
  - Cryptographic hashes of critical files
- Incident Mitigation Software
  - Access to images of clean OS and applications

PREPARATION

- **Port lists,** including commonly used ports and Trojan horse ports
- **Documentation** for OSs, applications, protocols, and intrusion detection and antivirus products
- **Network diagrams and lists of critical assets,** such as database servers
- **Current baselines** of expected network, system, and application activity
- **Cryptographic hashes** of critical files to speed incident analysis, verification, and eradication
- Incident Mitigation Software:
  - **Access to images** of clean OS and application installations for restoration and recovery purposes

PREPARATION

- Preventing Incidents
  - Risk Assessments
  - Host Security
  - Network Security
  - Malware Prevention
  - User Awareness and Training

PREPARATION

- **Risk Assessments.** Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organization-specific threats. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.
- **Host Security.** All hosts should be hardened appropriately using standard configurations. In addition to keeping each host properly patched, hosts should be configured to follow the principle of least privilege—granting users only the privileges necessary for performing their authorized tasks. Hosts should have auditing enabled and should log significant security-related events. The security of hosts and their configurations should be continuously monitored. Many organizations use Security Content Automation Protocol (SCAP) expressed operating system and application configuration checklists to assist in securing hosts consistently and effectively.
- **Network Security.** The network perimeter should be configured to deny all activity that is not expressly permitted. This includes securing all connection points, such as virtual private networks (VPNs) and dedicated connections to other organizations.
- **Malware Prevention.** Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., email server, web proxies), and the application client level (e.g., email clients, instant messaging clients).
- **User Awareness and Training.** Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications. Applicable lessons learned from previous incidents should also be shared with users so they can see how their actions could affect the organization. Improving user awareness regarding incidents should reduce the frequency of incidents. IT staff should be trained so that they can maintain their networks, systems, and applications in accordance with the organization's security standards.

IDENTIFICATION

- Incidents can occur in countless ways
- Hence it is impossible to develop step-by-step instructions to handle every incident
- Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors

IDENTIFICATION

- Attack Vectors
  - External/Removable Media
  - Web
  - Email
  - Impersonation
  - Improper Usage
  - Loss or Theft of Equipment
  - Other

IDENTIFICATION

- Sources of Precursors and Indicators
  - Alerts
    - IDS & IPS
    - SIEMs (Security information and event management)
    - Antivirus
    - File integrity checking software
    - Third Party monitoring service

IDENTIFICATION

- Sources of Precursors and Indicators
  - Logs
    - OS logs
    - Service Logs
    - Application Logs
    - Network Logs

IDENTIFICATION

- Sources of Precursors and Indicators
  - Publicly Available Information
    - Information on new Vulnerabilities
  - People
    - People from within the organization
    - People from other organizations

INCIDENT ANALYSIS

- Incident detection and analysis is generally easy if all precursor or indicator are guaranteed to be accurate; however, that may not be the case sometimes.
- User provided indicators such as a complain a server being unavailable can be incorrect.
- IDS may produce false positive
- Each indicators ideally should be evaluated to determine if it is a legitimate or not. But, depending on an organization, number of indicators may be thousands or millions a day.
- Such scenarios makes incident analysis a difficult task

INCIDENT ANALYSIS

- Recommendations for performing initial analysis
  - Profile networks and systems
  - Understand normal behaviors
  - Create a log retention policy
  - Perform event correlation
  - Keep all host clocks synchronized

INCIDENT ANALYSIS

- **Profile Networks and Systems.** *Profiling* is measuring the characteristics of expected activity so that changes to it can be more easily identified. Examples of profiling are running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. In practice, it is difficult to detect incidents accurately using most profiling techniques; organizations should use profiling as one of several detection and analysis techniques.
- **Understand Normal Behaviors.** Incident response team members should study networks, systems, and applications to understand what their normal behavior is so that abnormal behavior can be recognized more easily. No incident handler will have a comprehensive knowledge of all behavior throughout the environment, but handlers should know which experts could fill in the gaps. One way to gain this knowledge is through reviewing log entries and security alerts. This may be tedious if filtering is not used to condense the logs to a reasonable size. As handlers become more familiar with the logs and alerts, they should be able to focus on unexplained entries, which are usually more important to investigate. Conducting frequent log reviews should keep the knowledge fresh, and the analyst should be able to notice trends and changes over time. The reviews also give the analyst an indication of the reliability of each source.
- **Create a Log Retention Policy.** Information regarding an incident may be recorded in several places, such as firewall, IDPS, and application logs. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks. Another reason for retaining logs is that incidents may not be discovered until days, weeks, or even months later. The length of time to maintain log data is dependent on several factors, including the organization's data retention policies and the volume of data.
- **Perform Event Correlation.** Evidence of an incident may be captured in several logs that each contain different types of data—a firewall log may have the source IP address that was used, whereas an application log may contain a username. A network IDPS may detect that an attack was launched against a particular host, but it may not know if the attack was successful. The analyst may need to examine the host's logs to determine that information. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.
- **Keep All Host Clocks Synchronized.** Protocols such as the Network Time Protocol (NTP) synchronize clocks among hosts. Event correlation will be more complicated if the devices reporting events have inconsistent clock settings. From an evidentiary standpoint, it is preferable to have consistent timestamps in logs—for example, to have three logs that show an attack occurred at 12:07:01 a.m., rather than logs that list the attack as occurring at 12:07:01, 12:10:35, and 11:07:06.

INCIDENT ANALYSIS

- Recommendations for performing initial analysis
  - Maintain and Use a Knowledge base of information
  - Use Internet search engines for research
  - Run Packet sniffers to collect additional data
  - Filter the data
  - Seek assistance from others

INCIDENT ANALYSIS

- Recommendations for performing initial analysis
- **Maintain and Use a Knowledge Base of Information.** The knowledge base should include information that handlers need for referencing quickly during incident analysis. Although it is possible to build a knowledge base with a complex structure, a simple approach can be effective. Text documents, spreadsheets, and relatively simple databases provide effective, flexible, and searchable mechanisms for sharing data among team members. The knowledge base should also contain a variety of information, including explanations of the significance and validity of precursors and indicators, such as IDPS alerts, operating system log entries, and application error codes.
- **Use Internet Search Engines for Research.** Internet search engines can help analysts find information on unusual activity. For example, an analyst may see some unusual connection attempts targeting TCP port 22912. Performing a search on the terms "TCP," "port," and "22912" may return some hits that contain logs of similar activity or even an explanation of the significance of the port number. Note that separate workstations should be used for research to minimize the risk to the organization from conducting these searches.
- **Run Packet Sniffers to Collect Additional Data.** Sometimes the indicators do not record enough detail to permit the handler to understand what is occurring. If an incident is occurring over a network, the fastest way to collect the necessary data may be to have a packet sniffer capture network traffic. Configuring the sniffer to record traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other information. Because of privacy concerns, some organizations may require incident handlers to request and receive permission before using packet sniffers.
- **Filter the Data.** There is simply not enough time to review and analyze all the indicators; at minimum the most suspicious activity should be investigated. One effective strategy is to filter out categories of indicators that tend to be insignificant. Another filtering strategy is to show only the categories of indicators that are of the highest significance; however, this approach carries substantial risk because new malicious activity may not fall into one of the chosen indicator categories.
- **Seek Assistance from Others.** Occasionally, the team will be unable to determine the full cause and nature of an incident. If the team lacks sufficient information to contain and eradicate the incident, then it should consult with internal resources (e.g., information security staff) and external resources (e.g., US-CERT, other CSIRTs, contractors with incident response expertise). It is important to accurately determine the cause of each incident so that it can be fully contained and the exploited vulnerabilities can be mitigated to prevent similar incidents from occurring.

INCIDENT DOCUMENTATION

- An IR team that suspects that an incident has occurred should immediately start recording all facts regarding the incident
- A logbook is an effective and simple medium for this, but laptops, audio recorders and digital cameras can also serve this purpose.
- It leads to more efficient, more systematic and less error-prone handling of the problem.
- Every step taken from the time the incident was detected to its final resolution should be documented and timestamped and signed by the incident handlers.

INCIDENT DOCUMENTATION

- The issue tracking system should contain information on the following:
  - The current status of the incident
  - A summary of the incident
  - Indicators related to the incident
  - Other incidents related to this incident
  - Actions taken by all incident handlers on this incident
  - Chain of custody, [if applicable]

INCIDENT DOCUMENTATION

- The issue tracking system should contain information on the following:
  - Impact assessments related to the incident
  - Contact information for other involved parties (e.g. system owners, system administrators)
  - A list of evidence gathered during the incident investigation
  - Comments from incident handlers on each evidence
  - Next steps to be taken

INCIDENT PRIORITIZATION

- It can be considered as the most critical decision point in the incident handling process
- Incidents should NEVER be handled on first-come first-served basis
- Incident should always be prioritized on the relevant factors

INCIDENT PRIORITIZATION

- The relevant factors are as follow:
  - Functional Impact of the Incident
  - Information Impact of the Incident
  - Recoverability from the Incident

FUNCTIONAL IMPACT OF THE INCIDENT

- Incidents targeting IT systems typically impact the business functionality that those system provide
- It can leave negative impact to the users of those systems
- Handlers should consider how the incident will impact the existing functionality of the affected systems.

FUNCTIONAL IMPACT OF THE INCIDENT

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

INFORMATION IMPACT OF INCIDENT

- Incidents may affect the confidentiality, integrity and availability of the organization's information.
- For example, A malicious agent may exfiltrate sensitive information.
- Incident handlers should consider how this information exfiltration will impact the organization's overall mission.

INFORMATION IMPACT OF INCIDENT

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

RECOVERABILITY FROM THE INCIDENT

- The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.
- In fact, In some instances it is never possible to recover from an incident

RECOVERABILITY FROM THE INCIDENT

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation