Module 13 Incident Response

Events and Incidents –

An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

1. An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
2. Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
3. An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
4. A user provides or exposes sensitive information to others through peer-to-peer file sharing services

Need for Incident Response –

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur.

Besides the business reasons to establish an incident response capability, Federal departments and agencies must comply with law, regulations, and policy directing a coordinated, effective defense against information security threats. Chief among these are the following:

1. OMB's Circular No. A-130, Appendix III, released in 2000, which directs Federal agencies to "ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations … and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.
2. FISMA (from 2002), which requires agencies to have "procedures for detecting, reporting, and responding to security incidents" and establishes a centralized Federal information security incident center, in part to: –

- “Provide timely technical assistance to operators of agency information systems … including guidance on detecting and handling information security incidents …
- Compile and analyze information about incidents that threaten information security …
- Inform operators of agency information systems about current and potential information security threats, and vulnerabilities

3. Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006, which specifies minimum security requirements for Federal information and information systems, including incident response. The specific requirements are defined in NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.
4. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information , May 2007, which provides guidance on reporting security incidents that involve PII.

Incident Response Policy, Plan, and Procedure Creation

1. Policy Element –

   Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements:

   - Statement of management commitment
   - Purpose and objectives of the policy
   - Scope of the policy (to whom and what it applies and under what circumstances)
   - Definition of computer security incidents and related terms
   - Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process
   - Prioritization or severity ratings of incidents
   - Performance measures
   - Reporting and contact forms.

2. Plan Elements –

   Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements, which relates to the organization’s mission, size, structure, and functions. The plan should lay out the necessary resources and management support. The incident response plan should include the following elements:

   - Mission

- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations.
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

Once an organization develops a plan and gains management approval, the organization should implement the plan and review it at least annually to ensure the organization is following the roadmap for maturing the capability and fulfilling their goals for incident response.

3. Procedure Elements –
   Procedures should be based on the incident response policy and plan. Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations. In addition, following standardized responses should minimize errors, particularly those that might be caused by stressful incident handling situations. SOPs should be tested to validate their accuracy and usefulness, then distributed to all team members. Training should be provided for SOP users; the SOP documents can be used as an instructional tool.

Incident Response Team Services –

The main focus of an incident response team is performing incident response, but it is fairly rare for a team to perform incident response only. The following are examples of other services a team might offer:

1. Intrusion detection –
   The first tier of an incident response team often assumes responsibility for intrusion detection the team generally benefits because it should be poised to analyze incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies.
2. Advisory Distribution –
   A team may issue advisories within the organization regarding new vulnerabilities and threats Automated methods should be used whenever appropriate to disseminate information; for example, the National Vulnerability Database (NVD) provides information via XML and RSS feeds when new vulnerabilities are added to it Advisories are often most necessary when new threats are emerging, such as a high-profile social or political event (e.g., celebrity wedding) that attackers are

likely to leverage in their social engineering. Only one group within the organization should distribute computer security advisories to avoid duplicated effort and conflicting information.

3. Education and Awareness –

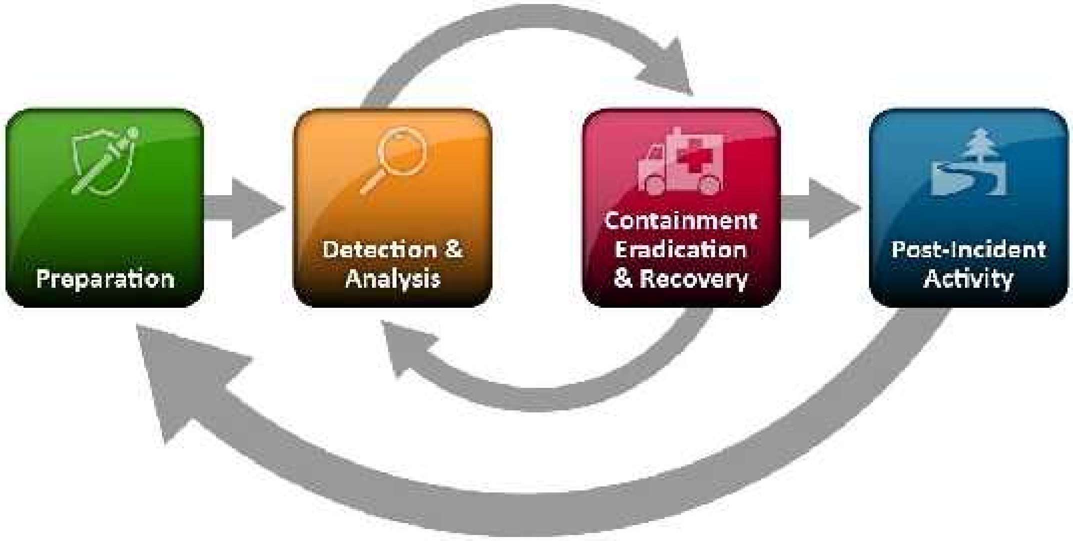
   Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there. Should be on the incident response team. This information can be communicated through many means: workshops, websites, newsletters, posters, and even stickers on monitors and laptops.

4. Information Sharing –

   Incident response teams often participate in information sharing groups. Accordingly, incident response teams often manage the organization's incident information sharing efforts, such as aggregating information related to incidents and effectively sharing that information with other organizations, as well as ensuring that pertinent information is shared within the enterprise.

Incident Handling –

The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources.



Preparation –

Incident response methodologies typically emphasize preparation not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs. This section provides basic advice on preparing to handle incidents and on preventing incidents.

Detection and Analysis –

1. Detection Attack Vectors -

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling 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. Different types of incidents merit different response strategies. The attack vectors listed below are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, which can be used as a basis for defining more specific handling procedures.

- External/Removable Media: An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
- Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
- Web: An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
- Email: An attack executed via an email message or attachment for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.
- Impersonation: An attack involving replacement of something benign with something malicious. For example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
- Improper Usage: Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
- Loss or Theft of Equipment: The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token
- Other: An attack that does not fit into any of the other categories.

2. Incident Analysis –

   Incident detection and analysis would be easy if every precursor or indicator were guaranteed to be accurate; unfortunately, this is not the case. For example, user-provided indicators such as a complaint of a server being unavailable are often incorrect. Intrusion detection systems may produce false positives—incorrect indicators. These examples demonstrate what makes incident detection and analysis so difficult: each indicator ideally should be evaluated to determine if it is legitimate. Making matters worse, the total number of indicators may be thousands or millions a day. Finding the real security incidents that occurred out of all the indicators can be a daunting task.

Containment, Eradication, and Recovery

1. Choosing a Containment Strategy

   Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, and disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly. Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making.

Criteria for determining the appropriate strategy include:

1. Potential damage to and theft of resources
2. Need for evidence preservation
3. Service availability (e.g., network connectivity, services provided to external parties)
4. Time and resources needed to implement the strategy
5. Effectiveness of the strategy (e.g., partial containment, full containment)
6. Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Eradication and Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery. In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.

Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rule sets, boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

Eradication and recovery should be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible

Post-Incident Activity

One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:

1. Exactly what happened, and at what times?
2. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
3. What information was needed sooner?
4. Were any steps or actions taken that might have inhibited the recovery?
5. What would the staff and management do differently the next time a similar incident occurs?
6. How could information sharing with other organizations have been improved?
7. What corrective actions can prevent similar incidents in the future?
8. What precursors or indicators should be watched for in the future to detect similar incidents?

Incident Handling Checklist –

The checklist in the below table provides the major steps to be performed in the handling of an incident. Note that the actual steps performed may vary based on the type of incident and the nature of individual incidents.

Sr.no	Action	Completed
Detection and Analysis		
1	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4	Acquire, preserve, secure, and document evidence	
5	Contain the incident	
6	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8	Create a follow-up report	
9	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	