Intrusion and Incident Response Guidelines

Reference: NIST SP 800-61 Revision 2

Incident response for Federal agencies

- Organizations must create, provision, and operate a formal incident response capability.
- Federal law requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS).
- The Federal Information Security Management Act (FISMA) requires Federal agencies to establish incident response capabilities.

Capabilities of incident response

- Establishing an incident response capability should include the following actions:
  - Creating an incident response policy and plan
  - Developing procedures for performing incident handling and reporting
  - Setting guidelines for communicating with outside parties regarding incidents
  - Selecting a team structure and staffing model
  - Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
  - Determining what services the incident response team should provide
  - Staffing and training the incident response team

Six recommendations for every organization

1. Organizations should reduce the frequency of incidents by effectively securing networks, systems, and applications.
2. Organizations should document their guidelines for interactions with other organizations regarding incidents.
3. Organizations should emphasize the importance of incident detection and analysis throughout the organization.
4. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.
5. Organizations should create written guidelines for prioritizing incidents.
6. Organizations should use the lessons learned process to gain value from incidents

Recommendation 1:
Organizations should reduce the frequency of incidents by effectively securing networks, systems, and applications.

- Preventing problems is often less costly and more effective than reacting to them after they occur.
- Thus, incident prevention is an important complement to an incident response capability.
- If security controls are insufficient, high volumes of incidents may occur.
- This could overwhelm the resources and capacity for response, which would result in delayed or incomplete recovery and possibly more extensive damage and longer periods of service and data unavailability.
- Implement training, develop policies and procedures

Recommendation #2
Organizations should document their guidelines for interactions with other organizations regarding incidents.

- During incident handling, the organization will need to communicate with outside parties, such as other incident response teams, law enforcement, the media, vendors, and victim organizations.
- Because these communications often need to occur quickly, organizations should predetermine communication guidelines so that only the appropriate information is shared with the right parties.

Recommendation #3:
Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.

- Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident.
- Common attack vectors -
  - External/Removable Media: An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
  - Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
  - Web: An attack executed from a website or web-based application.
  - Email: An attack executed via an email message or attachment.
  - Improper Usage: Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
  - Loss or Theft of Equipment: The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
  - Other: An attack that does not fit into any of the other categories.

Recommendation #4:
Organizations should emphasize the importance of incident detection and analysis throughout the organization.

- In an organization, millions of possible signs of incidents may occur each day, recorded mainly by logging and computer security software.
- Automation is needed to perform an initial analysis of the data and select events of interest for human review.
- Event correlation software can be of great value in automating the analysis process.
- However, the effectiveness of the process depends on the quality of the data that goes into it.
- Organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.

Recommendation #5
Organizations should create written guidelines for prioritizing incidents.

- Incidents should be prioritized based on the relevant factors, such as
  - The functional impact of the incident (e.g., current and likely future negative impact to business functions),
  - The information impact of the incident (e.g., effect on the confidentiality, integrity, and availability of the organization's information), and
  - The recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident).

Recommendation #6:
Organizations should use the lessons learned process to gain value from incidents

- After a major incident has been handled, the organization should hold a lessons learned meeting to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices.
- Lessons learned meetings can also be held periodically for lesser incidents as time and resources permit.
- The information accumulated from all lessons learned meetings should be used to identify and correct systemic weaknesses and deficiencies in policies and procedures.
- Follow-up reports generated for each resolved incident can be important not only for evidentiary purposes but also for reference in handling future incidents and in training new team members

Terminology

- An event is any observable occurrence in a system or network.
- Adverse events are events with a negative consequence.
- A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Benefits of having an incident response capability

- It supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken.
- Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents.
- Provides the ability to use information gained during incident handling to better prepare for handling future incidents
- Provide stronger protection for systems and data.
- An incident response capability also helps with dealing properly with legal issues that may arise during incidents.
- Federal departments and agencies must comply with law, regulations, and policy directing a coordinated, effective defense against information security threats

Components of an Incident Response Policy

- 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 – including ability to confiscate equipment, escalation and handoff points
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms.

Components of Incident Response Plan

- 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

Components of Incident Response Procedure

- 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

Communication with outside parties

Figure 2-1. Communications with Outside Parties

Communicating with media

- Conduct training sessions on interacting with the media regarding incidents, which should include the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.

When talking to the media

- Maintain a statement of the current status of the incident so that communications with the media are consistent and up-to-date.
- Remind all staff of the general procedures for handling media inquiries.
- Hold mock interviews and press conferences during incident handling exercises.
- The following are examples of questions to ask the media contact:
  - Who attacked you? Why?
  - When did it happen? How did it happen? Did this happen because you have poor security practices?
  - How widespread is this incident? What steps are you taking to determine what happened and to prevent future occurrences?
  - What is the impact of this incident? Was any personally identifiable information (PII) exposed? What is the estimated cost of this incident?

Other outside parties

- Organization’s ISP
- Owners of attacking addresses
- Software vendors
- Other incident response teams
- Affected external parties

Incident Response Team Structure

- Possible structures for an incident response team include the following:
  - Central Incident Response Team. A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.
  - Distributed Incident Response Teams. The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization. This model is effective for large organizations.
  - Coordinating Team. An incident response team provides advice to other teams without having authority over those teams—for example, a departmentwide team may assist individual agencies' teams.

Staffing models for Incident Response Teams

- Employees: The organization performs all of its incident response work, with limited technical and administrative support from contractors.
- Partially outsourced: Outsources portions of its incident response work.
  - The most prevalent arrangement is for the organization to outsource 24/7 monitoring of intrusion detection sensors, firewalls, and other security devices to an offsite managed security services provider (MSSP).
- Fully outsourced: The organization completely outsources its incident response work, typically to an onsite contractor.
  - This model is most likely to be used when the organization needs a full-time, onsite incident response team but does not have enough available, qualified employees. It is assumed that the organization will have employees supervising and overseeing the outsourcer's work.

Factors in team model selection

- 1. The Need for 24/7 Availability.
  - Most organizations need incident response staff to be available 24/7.
  - This typically means that incident handlers can be contacted by phone, but it can also mean that an onsite presence is required.
  - Real-time availability is the best for incident response because the longer an incident lasts, the more potential there is for damage and loss.
  - Real-time contact is often needed when working with other organizations—for example, tracing an attack back to its source

Factors in team model selection

- Full-Time Versus Part-Time Team Members
  - Organizations with limited funding, staffing, or incident response needs may have only part-time incident response team members, serving as more of a virtual incident response team.
  - In this case, the incident response team can be thought of as a volunteer fire department.

Factors in team model selection

- 3. Employee Morale
  - Incident response work is very stressful, as are the on-call responsibilities of most team members.
  - This combination makes it easy for incident response team members to become overly stressed.
  - Many organizations will also struggle to find willing, available, experienced, and properly skilled people to participate, particularly in 24-hour support.

Factors in team model selection

- 4. Cost
  - Cost is a major factor, especially if employees are required to be onsite 24/7.
  - Organizations may fail to include incident response-specific costs in budgets, such as sufficient funding for training and maintaining skills.
  - Because the incident response team works with so many facets of IT, its members need much broader knowledge than most IT staff members.
  - They must also understand how to use the tools of incident response, such as digital forensics software.
  - Other costs that may be overlooked are physical security for the team's work areas and communications mechanisms.

Factors in team model selection

- 5. Staff Expertise
  - Incident handling requires specialized knowledge and experience in several technical areas; the breadth and depth of knowledge required varies based on the severity of the organization's risks.
  - Outsourcers may possess deeper knowledge of intrusion detection, forensics, vulnerabilities, exploits, and other aspects of security than employees of the organization.
  - Also, MSSPs may be able to correlate events among customers so that they can identify new threats more quickly than any individual customer could.
  - However, technical staff members within the organization usually have much better knowledge of the organization's environment than an outsourcer would, which can be beneficial in identifying false positives associated with organization-specific behavior and the criticality of targets

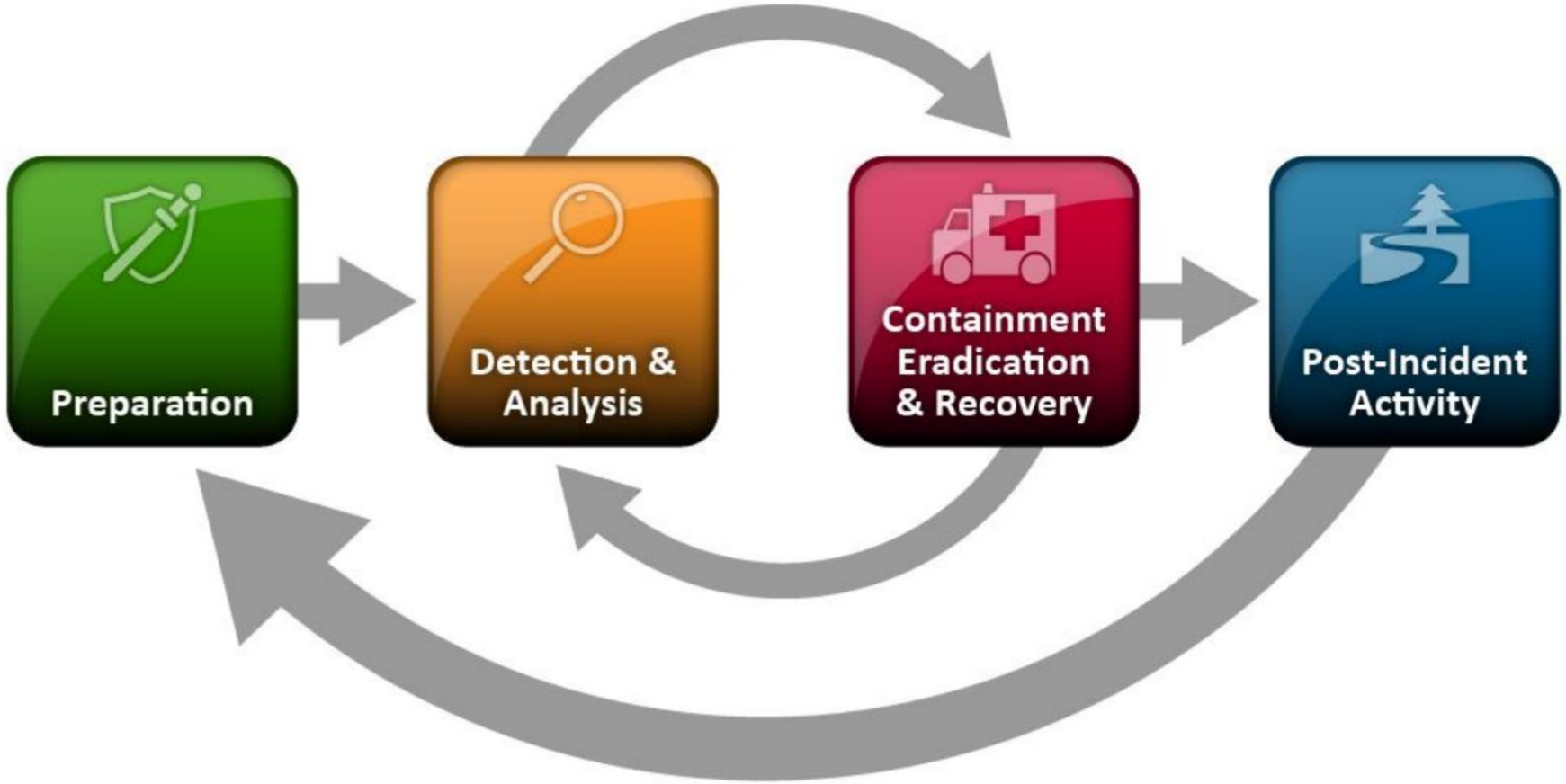
Dependencies within organizations

- It is important to identify other groups within the organization that may need to participate in incident handling so that their cooperation can be solicited before it is needed.
- Every incident response team relies on the expertise, judgment, and abilities of others, including:
  - Management
  - Information assurance
  - IT support
  - Legal
  - Public affairs
  - HR
  - Business continuity planning
  - Physical security and facilities management

Incident Response Team Services

- Intrusion Detection
- Advisory distribution
- Education and awareness
- Information sharing

Incident response life cycle



Incident Handler Communications and Facilities

- Contact information for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams
- On-call information for other teams within the organization, including escalation information
- Incident reporting mechanisms, such as phone numbers, email addresses, online forms, and secure instant messaging systems
- Issue tracking system for tracking incident information
- Smartphones
- Encryption software to be used for communications among team members, within the organization and with external parties; for Federal agencies, software must use a FIPS-validated encryption algorithm
- War room for central communication and coordination
- Secure storage facility for securing evidence and other sensitive materials

Incident analysis hardware and software

- Digital forensic workstations and/or backup devices
- Laptops
- Spare workstations, servers, and networking equipment, or the virtualized equivalents
- Blank removable media
- Portable printer
- Packet sniffers and protocol analyzers
- Digital forensic software
- Removable media
- 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

Incident analysis resources

- 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

Main recommended practices for securing networks, systems, and applications

- Risk Assessments
  - Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities.
- Host Security
  - All hosts should be hardened appropriately using standard configurations. 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
  - Awareness of policies and procedures regarding appropriate use of networks, systems, and applications.

Recommendations for making incident response effective and easier

- Profile networks and systems
- Understand normal behavior
- Create a log retention policy
- Perform event correlation
- Keep all host clocks synchronized
- Maintain and use a knowledge base of information
- Use Internet search engines for research
- Run packet sniffers to collect additional data
- Filter data
- Seek assistance from others

Incident documentation

- The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- 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 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
- Next steps to be taken (e.g., rebuild the host, upgrade an application)

Examples of functional impact categories

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

Examples of information impact categories

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

Examples of recoverability effort categories

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

Incident reporting

- Individuals who are typically notified are
- CIO
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- External incident response teams (if appropriate)
- System owner
- Human resources (for cases involving employees, such as harassment through email)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- US-CERT (required for Federal agencies and systems operated on behalf of the Federal government)
- Law enforcement (if appropriate)

Post incident activity

- Each incident response team should evolve to reflect new threats, improved technology, and lessons learned.
  - Exactly what happened, and at what times?
  - How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
  - What information was needed sooner?
  - Were any steps or actions taken that might have inhibited the recovery?
  - What would the staff and management do differently the next time a similar incident occurs?
  - How could information sharing with other organizations have been improved?
  - What corrective actions can prevent similar incidents in the future?
  - What precursors or indicators should be watched for in the future to detect similar incidents?
  - What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Metrics

- Possible metrics for incident-related data include:
- Number of incidents handled
- Time per incident
- Objective assessment of each incident
- Subjective assessment of each incident

Incident handling checklist

	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)	