LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

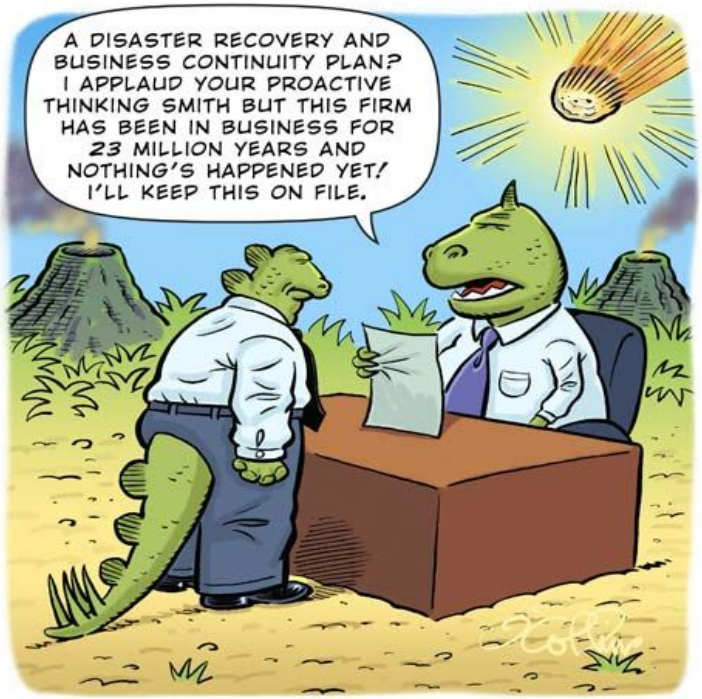
Incident Response

12/12/2019

Report #: 201912121000

Agenda

- Overview
- Event vs Incident
- Cybersecurity Kill Chain
- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post Incident Activities
- Incident Response: Small Organizations
- Questions



Slides Key:

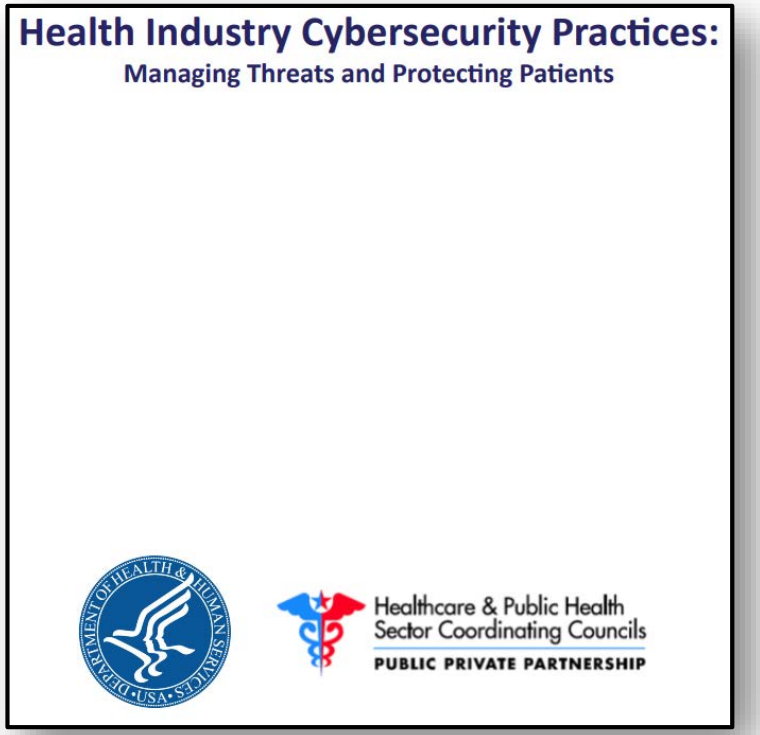
Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

8.M.B	*Incident Response*	NIST FRAMEWORK REF: PR. IP-9, RS.AN-1,RS.MI-1, RS.MI-2, RC

- Computer security incident response has become an important component of information technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive.
  - An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. (NIST SP 800-61)
- Performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks is essential.
  - Establishing clear procedures for prioritizing the handling of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data



405(d) HICP

NIST SP 800-61

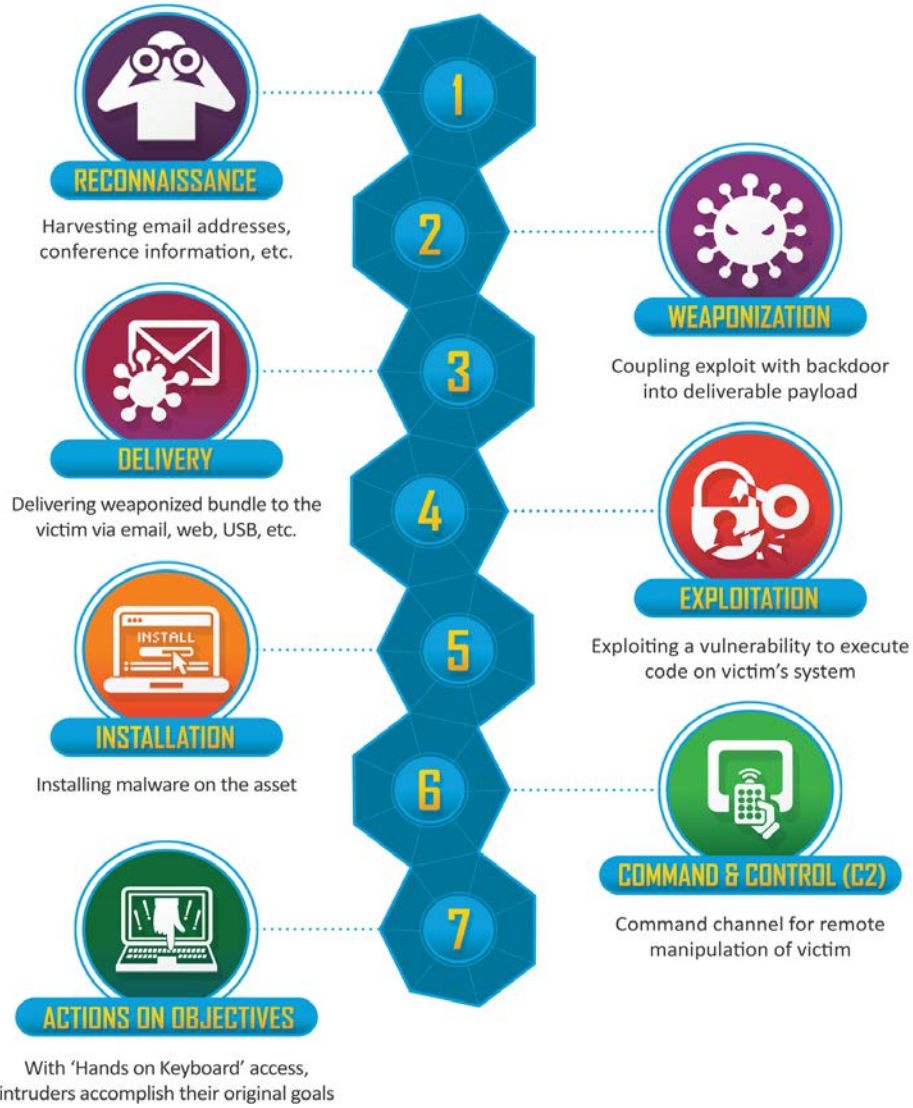
Event vs Incident

- NIST Special Publication 800-61 states, “A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.”
  - This definition assumes that adequate polices are in place to protect the intellectual property of the organization; the PII of employees, customers, and partners; and Protected Health Information (PHI) of patients.
  - Incidents are created when events are triggered that give an indication of an adverse action.
- An event is any observable occurrence in a system or network.
  - Events are things like IDS signature triggers, anti-virus detection, firewall detecting a host going to a known malicious domain, a phishing email is opened, or a firewall blocking a connection attempt. Even something like a “slow computer” is an event.

Homeland Preparedness News

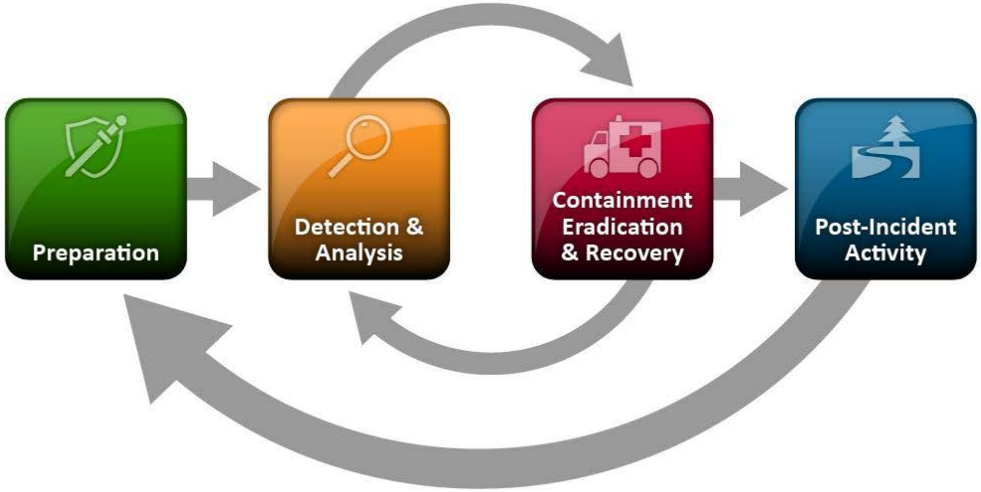
NIST SP 800-61

Cybersecurity Kill Chain



Lockheed Martin

Incident Response: Preparation



Preparation

- Preparation Incident response methodologies typically emphasize 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.
  - Keeping the number of incidents reasonably low is very important to protect the business processes of the organization. If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team. This can lead to slow and incomplete responses, which translate to a larger negative business impact

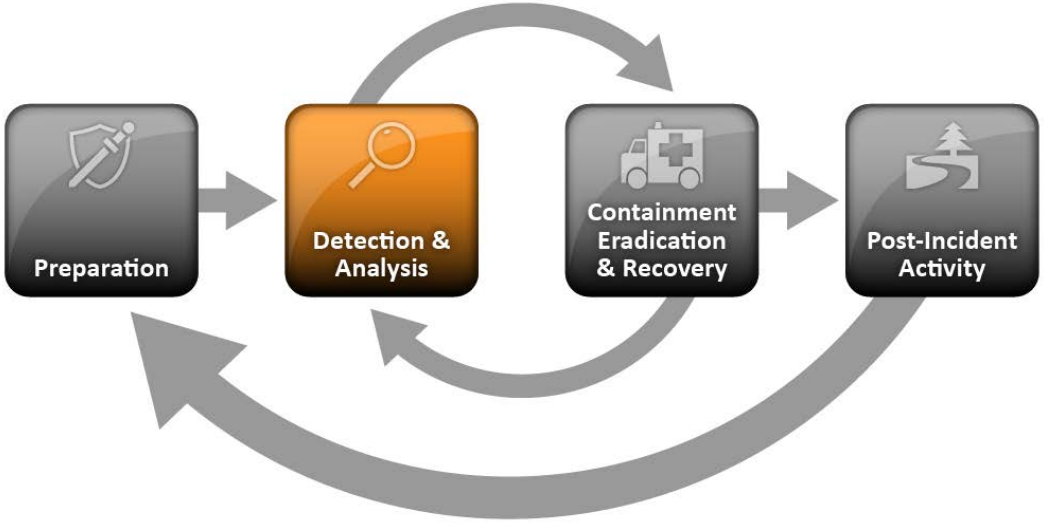
NIST SP 800-61

Incident Response: Preparation

- **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. 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.
- **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, the application server level, and the application client level.
- **User Awareness and Training.** Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications.

NIST SP 800-61

Incident Response: Detection & Analysis

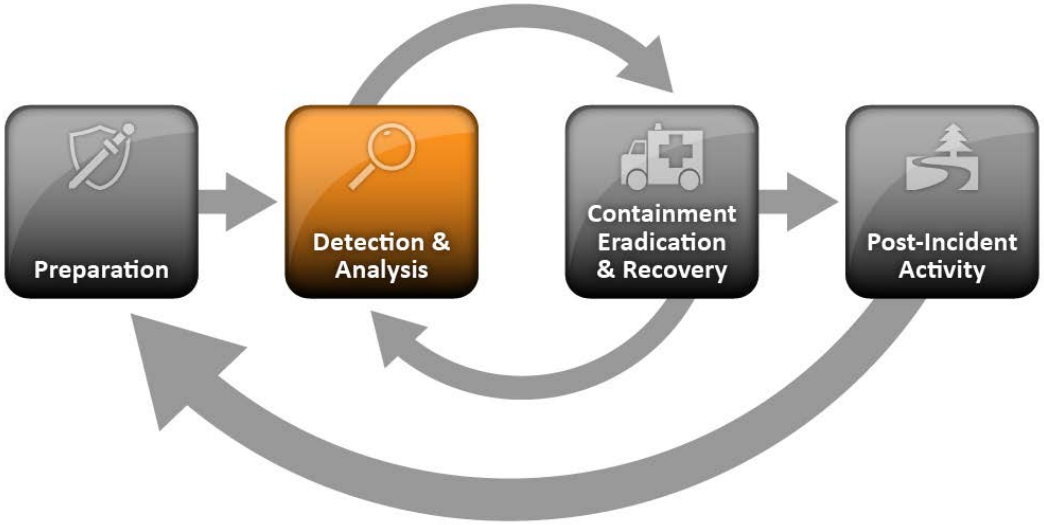


Detection

- Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users.
  - The volume of potential signs of incidents is typically high—for example, it is not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day.
  - Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.

NIST SP 800-61

Incident Response: Detection & Analysis



Analysis

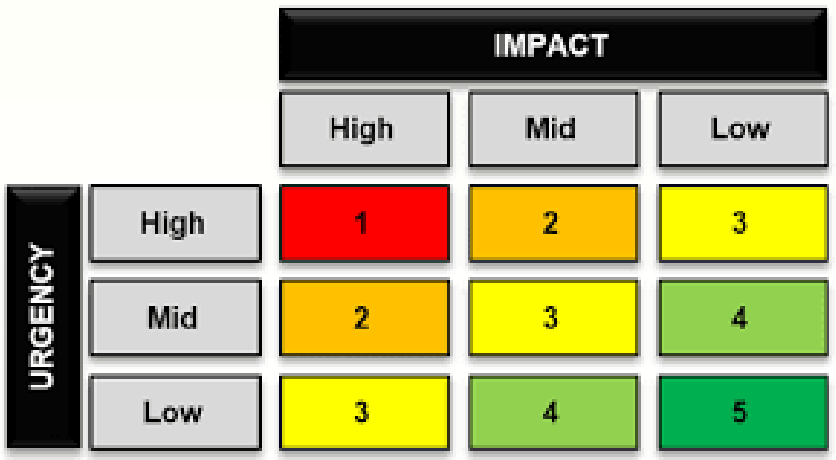
- The incident response team should work quickly to analyze and validate each incident, following a pre-defined process and documenting each step taken.
  - When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring.
- The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

NIST SP 800-61

Incident Response: Detection & Analysis

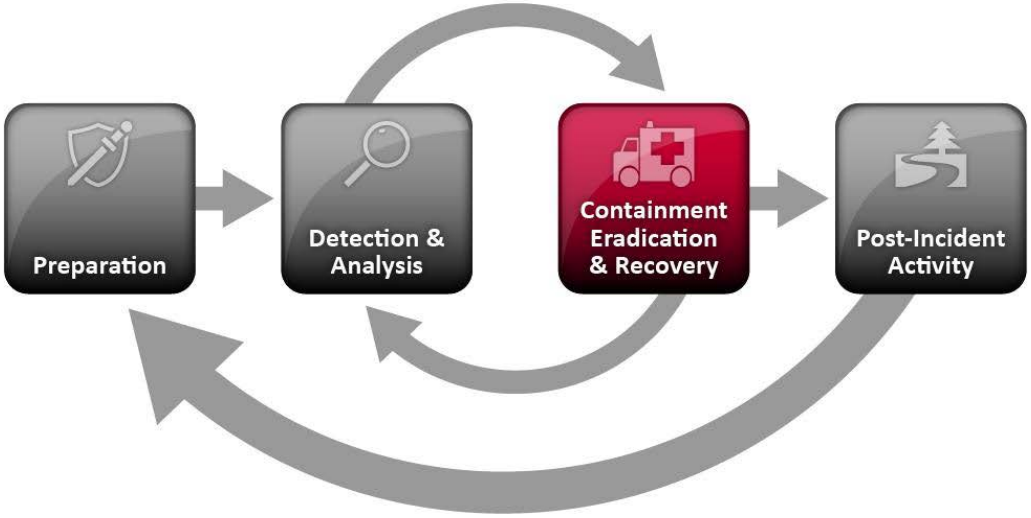
Incident Prioritization

- **Functional Impact of the Incident.** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems.
- **Information Impact of the Incident.** Incidents may affect the confidentiality, integrity, and availability of the organization's information.
- **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.



NIST SP 800-61

Incident Response: Containment, Eradication & Recovery

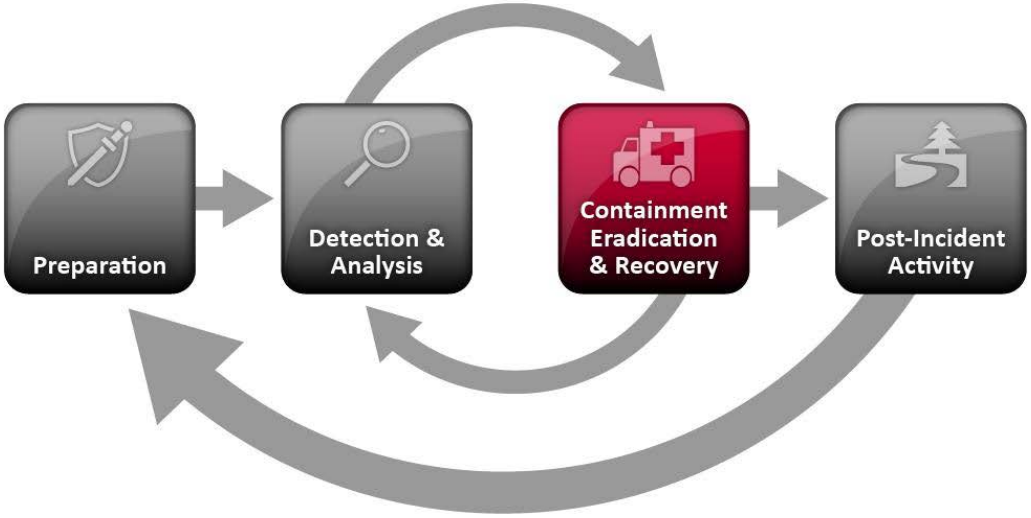


Containment

- 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, disable certain functions).
  - Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident.

NIST SP 800-61

Incident Response: Containment, Eradication & Recovery

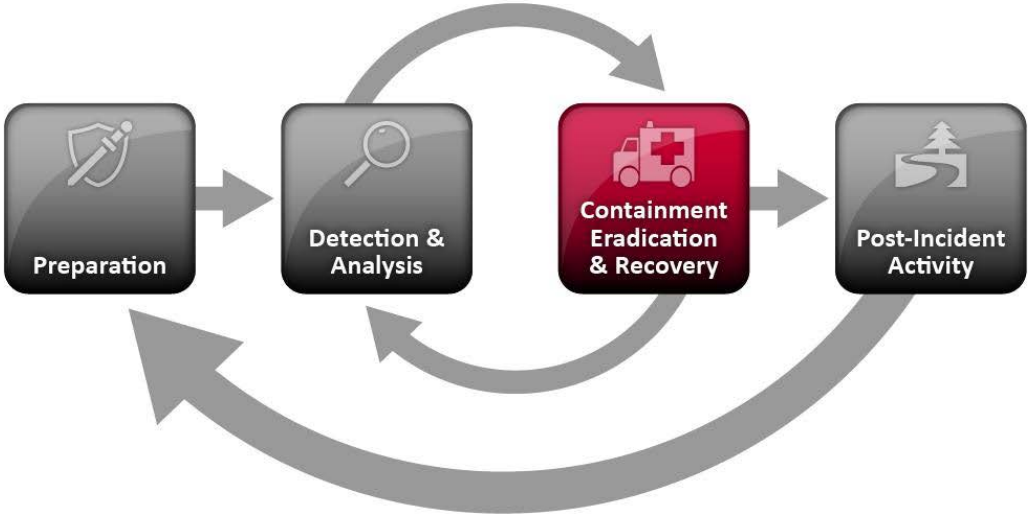


Eradication

- 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.

NIST SP 800-61

Incident Response: Containment, Eradication & Recovery

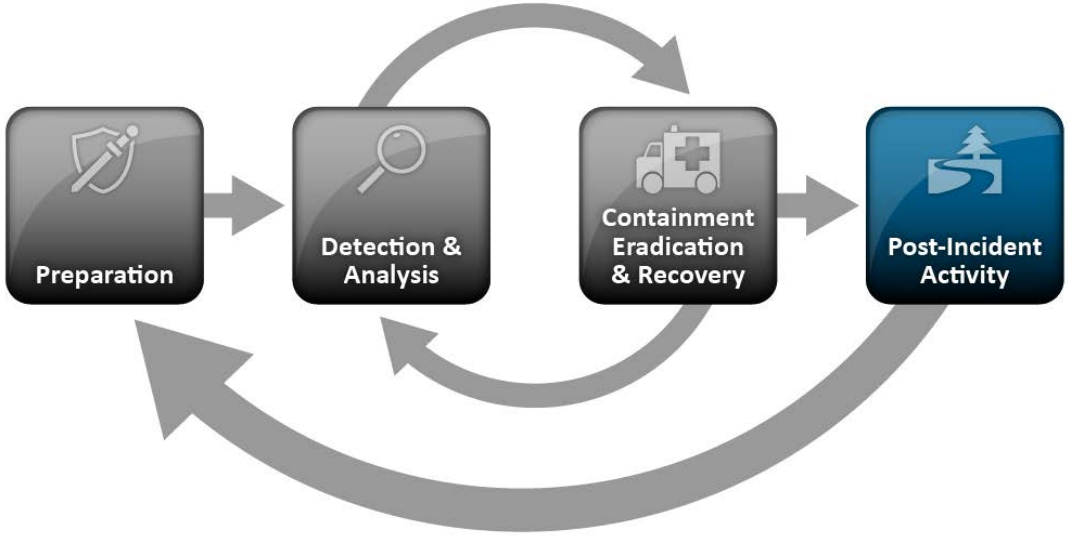


Recovery

- 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 rulesets, boundary router access control lists).

NIST SP 800-61

Incident Response: Post-Incident Activity



Lessons Learned

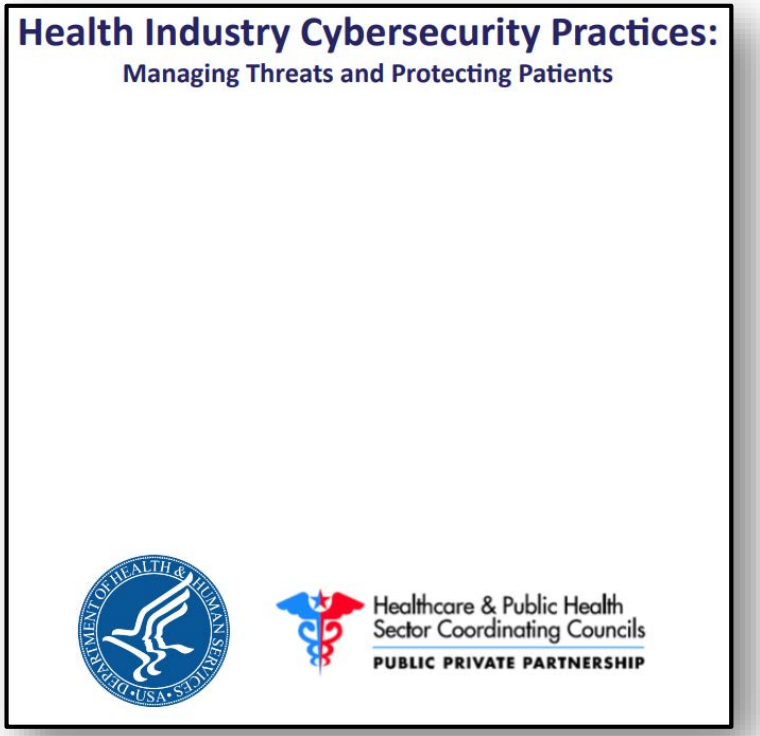
- Lessons learned activities should produce a set of objective and subjective data regarding each incident.
  - The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team.
  - A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends.
  - This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls.

NIST SP 800-61

Slide 1 title

8.S.A	Incident Response	NIST FRAMEWORK REF: PR. IP-9

- Small organizations are often challenged by incident response management, in part because incident response procedures may not be established.
- Before an incident occurs, make sure you understand who will lead your incident investigation.
  - At minimum, you should identify the top security expert who will provide direction to the supporting personnel.
  - Decide whether Incident Response procedures will be conducted in-house or with a 3rd Party vendor.



405(d) HICP

NIST SP 800-61

Reference Materials

References

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
  - https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
- Computer Security Incident Handling Guide
  - https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- Cyber Kill Chain
  - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Questions

Questions

Upcoming Briefs

- Emotet Update
- Trickbot

Previous HC3 briefs

- Cyber Kill Chain

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV