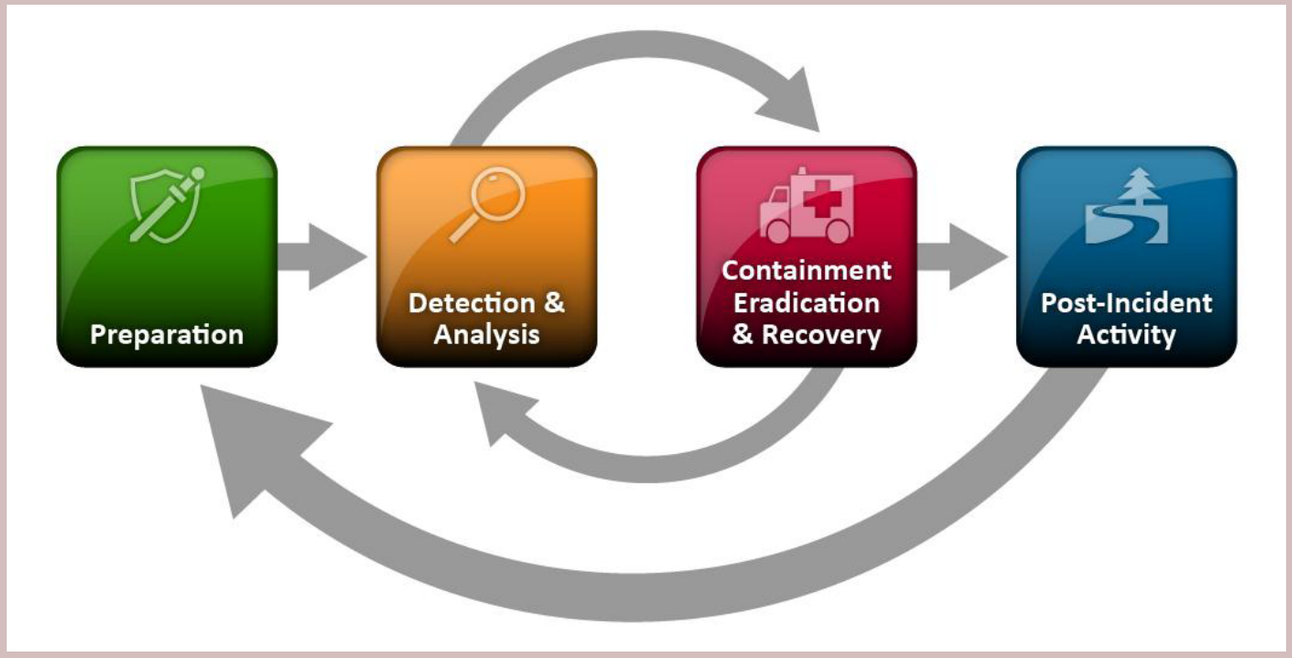
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Incident Response Phases

CYBER INCIDENT RESPONSE

Incident Response Phases



This process is not linear…it is cyclical

NIST SP 800-61
(Computer Security Incident Handling Guide)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Preparation

- Takes preparation to build a well-prepared CSIRT
- Requires proper policy foundation within the organization
- Preparation includes building proper cyber defenses in the organization
- Also, includes identifying/training personnel and building response kits

Preparation: Toolkits

- Digital forensic workstations
- Forensic software
- Packet capture devices
- Spare servers/network gear
- Backup devices
- Blank removable media
- Collection, analysis, & reporting laptops
- Portable printers
- Office supplies
- Evidence collection materials

Detection and Analysis

- Hardest to standardize
- Tools help in detection, but it takes a trained analyst to understand all the details during analysis
- When detection occurs, analysts shift to validation mode, then into analysis
- Primarily passive activities designed to uncover and analyze incident

Detection and Analysis: Event Indicators

- Alerts
  - IDS/IPS, SIEM, Anti-virus, or other software alerts
- Logs
  - From operating systems, services, applications, network devices, and network flows
- Publically Available Information
  - News, media, and other open-source information
- People
  - Suspicious activity reported by users or admins

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Detection and Analysis: Best Practices for Analysis

- Profile networks/systems
- Understand the baseline
- Create good logging policies
- Conduct event correlation
- Synchronize network & system clocks
- Maintain organization knowledge base
- Capture network traffic ASAP in incident
- Filter information to reduce confusion
- Know when to bring in outside help

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Containment, Eradication, and Recovery

- Focuses on stopping the spread of the incident, remove it from the network, and recovering from it

- Phase focuses on active detection and removal of the incident

Containment, Eradication, and Recovery (5 Steps)

1. Pick containment strategy
2. Use strategy to limit the damage incident causes
3. Gather evidence needed for potential future legal actions
4. Identify attacking system or attacker
5. Remove effects of incident and recover normal business operations

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Post-Incident Activities

- CSIRT isn't done once the incident is contained and eradicated, they still need to conduct:
  - Event reconstruction
  - Lessons learned
  - Evidence retention

Post-Incident Activities: Event Reconstruction

- Recreate a timeline of the incident
- Identify the root cause of the intrusion and/or incident
- Conduct consultations with system administrators and management

Post-Incident Activities: Lessons Learned

- Utilizes the timeline to aid improvement of procedures and tools used by CSIRT
- Group discussion to determine how the incident was handled, and how it could have been handled better.
- Lessons learned must be fed into the ITSM processes in order to follow-on actions to be taken

Post-Incident Activities: Lessons Learned

- What happened and when?
- How did staff perform?
- Were procedures followed?
- Were procedures adequate?
- What should have been done differently?
- Was information shared effectively?
- How could we detect incident sooner?
- What new tools or resources does the organization need?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Post-Incident Activities: Evidence Retention

- Large quantities of evidence have been collected
- What do we do with it all?
- CSIRT must identify internal/external retention requirements

If legal actions will be conducted, consult an attorney before deleting anything!

Post-Incident Activities: Evidence Retention Timelines

- US Government Agencies must retain all incident handling items for **3 years** due to legal requirements

- Most organizations maintain records for **2 years**, unless otherwise required by regulatory requirements

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE