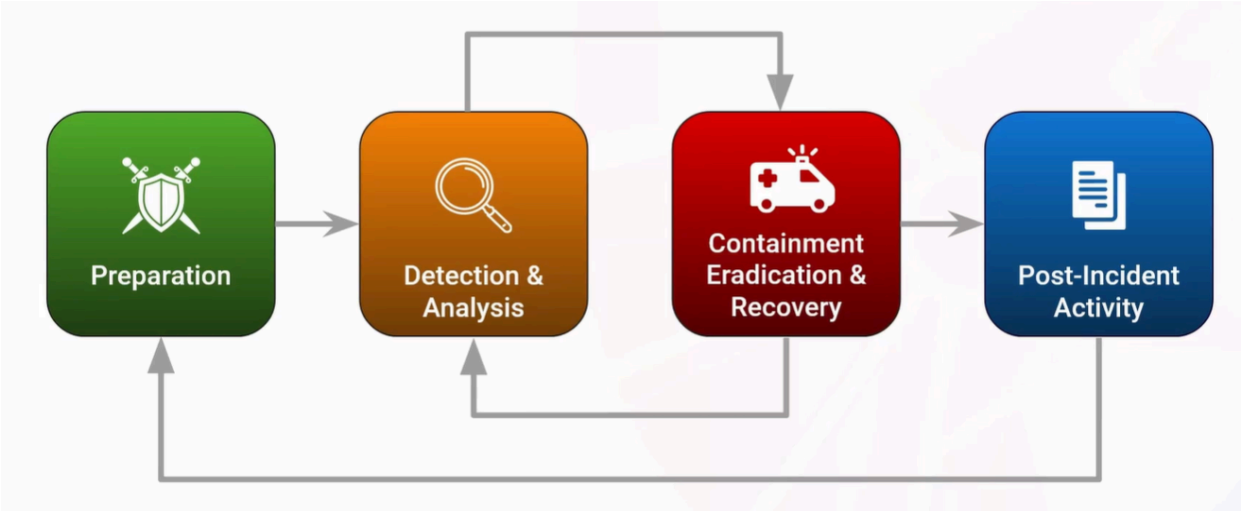
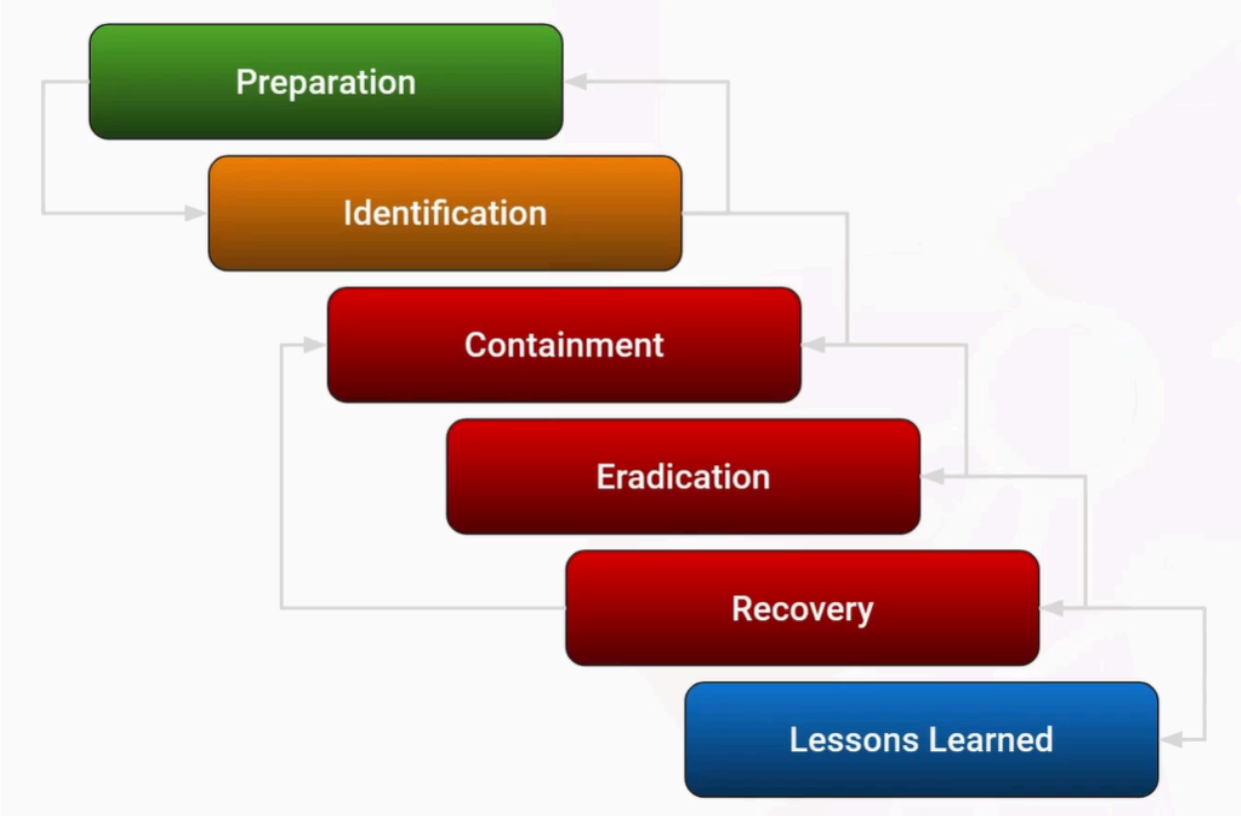
9. Incident Response

O. Frameworks

NIST Incident Response Plan



SANS Incident Response Plan



I. Preparation

SANS Contact Form Templates: https://www.sans.org/media/security-training/mgt512/secinc_forms.pdf

- End Users
  - Security Awareness Training
  - Phishing Simulations
  - Incident Reporting
- Stakeholder Involvement
  - Information Technology
  - Legal Advisors
  - Public Relations (PR)
  - Data Owners
- Communication
  - Incident Reporting
  - Contact Information
  - On-call information

    - Escalation protocols
    - Out-of-band communication
- Physical Locations
    - War Room
    - Evidence Storage
        - Confidentiality
        - Integrity
        - Availability
- Incident Tracking
    - thehive-project.org
    - Existing ticketing system
    - Access control, version control
- Hardware and Software
    - Digital forensic workstations
    - Laptops
    - Removable media (USB, hard drives)
    - Evidence Documentation
    - Jumpkit
- Asset Management
    - OS, applications, hostnames, IPs
    - Protocols, services
    - Critical systems
    - Network diagrams
    - Baselines
    - Clean OS images
    - Cryptographic hashes
- Simulated Exercises
    - Tabletops
    - Prepare staff to handle incidents
    - Identify Weaknesses
    - NIS SP 800-84
    - play.backdoorsandbreaches.com
    - Identify log sources and event visibility
- Incident Response Plan
    - Playbooks
        - How to handle specific incidents
        - High-level perspective strategy
    - Runbooks

        - Technical procedures to execute tasks
        - Step-by-step
- Notification Policies
    - Engaging with law enforcement, legal, regulators
    - Cyber Insurance
    - Management
- Documentation
    - Documented Evidence
    - Slow Down

II. Identification

- Identification Sources
    - Network perimeter
    - Email perimeter
    - Host perimeter
    - Application-level detection
    - User Entity and Behavior Analytics (UEBA)
    - Human-level detection
    - User reports
- Alert Tuning
    - Alert Fatigue
    - Signal-to-noise ratio
- Incident Prioritization
    - Incident Triage
    - Incident Scope
    - Urgency, criticality, impact
- Documentation
    - Ticket, reports
    - Record of events
- Communication and Notification
    - Notify relevant parties
    - Situation Reports (Sitreps)
        - Key stakeholders
        - Clear summary
        - Severity
        - Status

        - Actions
        - Next Steps
    - Communication planning

III. Containment

- Short-term Containment
    - Quarantine
        - Limit before it gets worse
    - Isolate Networks
    - Take down systems
    - Network filtering and rules
        - Firewall
        - IPS/IDS
    - Killing Processes
        - `taskkill /pid <PID>`
    - Temporary Patches
- Business Impact
    - Plan containment measures carefully
    - Work with data owners and stakeholders
    - Mission critical systems
- Evidence Collection / System Backup
    - Creating forensic images
    - Capturing memory
    - Evidence documentation
- Long-term Containment
    - Stabilize the environment while rebuilding clean systems
    - Removing the attacker's access
        - Deleting user accounts
        - Resetting credentials
        - Disabling remote access
        - Removing backdoors
    - Traffic segmentation
    - Additional monitoring and detection
    - Patching and hardening

IV. Eradication

- Remove the attacker's system and network artifacts
- Restoring Systems
  - Known good backup
  - Original disk image
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
- Manually Removing Artifacts
  - Malware
    - Disk
    - Memory
  - Backdoors
  - Network Connections
  - Services
- Improving Defenses
  - Network Filters
  - Applying patches
  - Hardening Systems
  - CIS Benchmarks
- Vulnerability Management
  - Scanning the system and network
  - Vulnerability Scans
  - Threat Intelligence
  - Threat Hunting

V. Recovery

- Get affected systems back into production
  - Restore systems
  - Remove artifacts
- Confirm functionality
  - Testing
- Prevent future incidents
  - Hardening, scanning, monitoring
- Recovery decisions
  - Recovery time window
  - How to test and verify

    - Duration of monitoring
    - Tools for monitoring

VI. Lessons Learned

- Self reflect and improve incident response process
- Post-incident Reviews
    - Postmortem reports
    - Who, what, where, why, how
- Lessons Learned Meetings
    - When was the problem first detected
    - Who detected it
    - What was the scope of the incident
    - How was it contained, eradicated, recovered?
    - How were we effective?
    - What are the areas for improvement?
    - Questions, suggestions, discussions