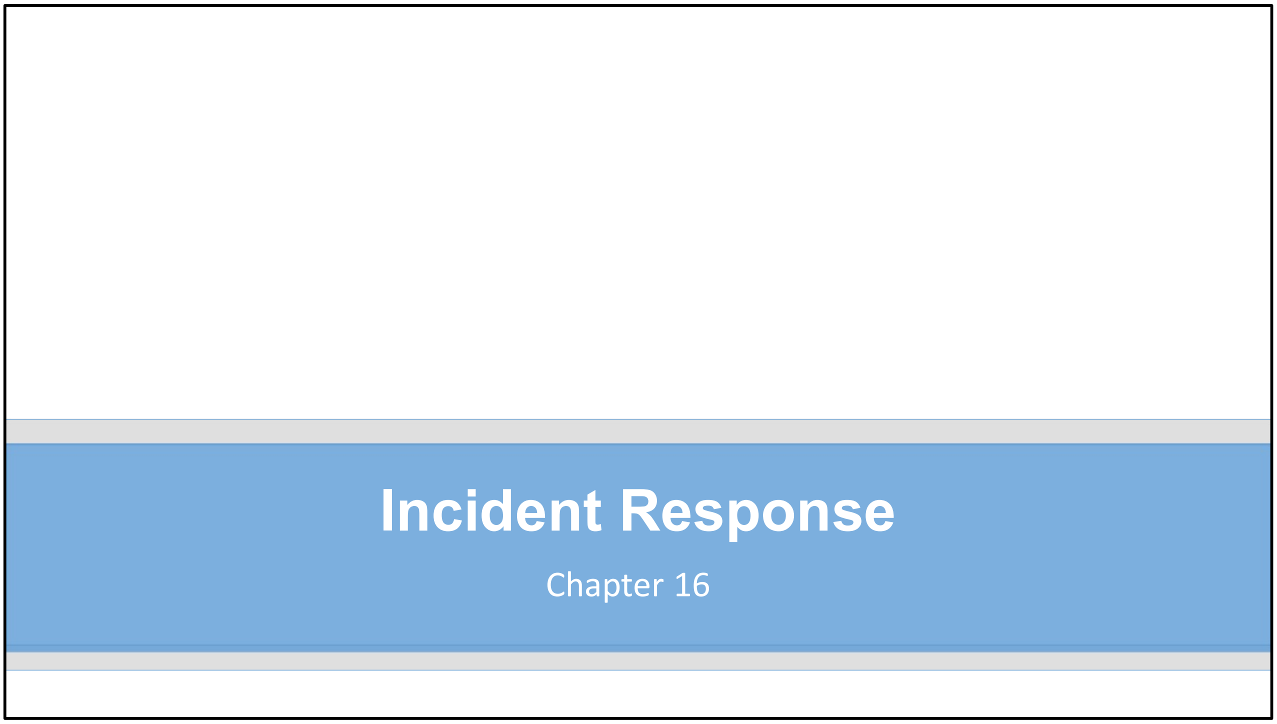


Incident Response

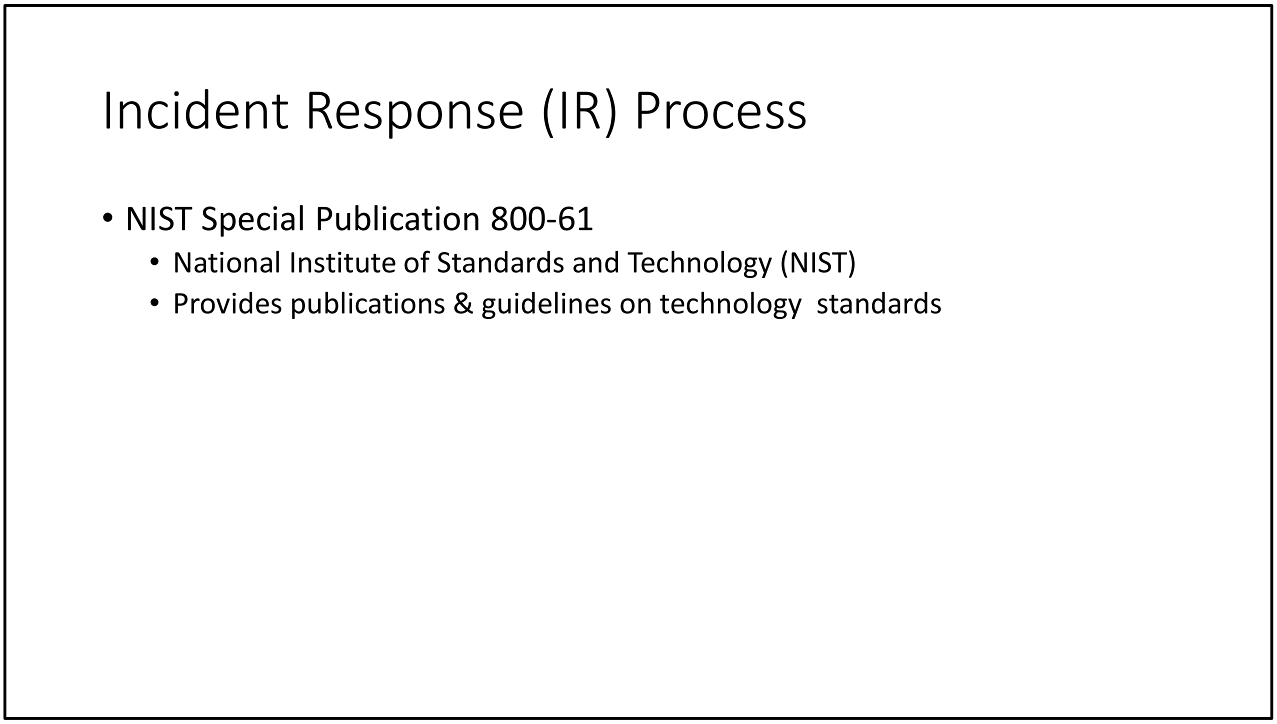
Chapter 16

Episode 16.01

Incident Response Process

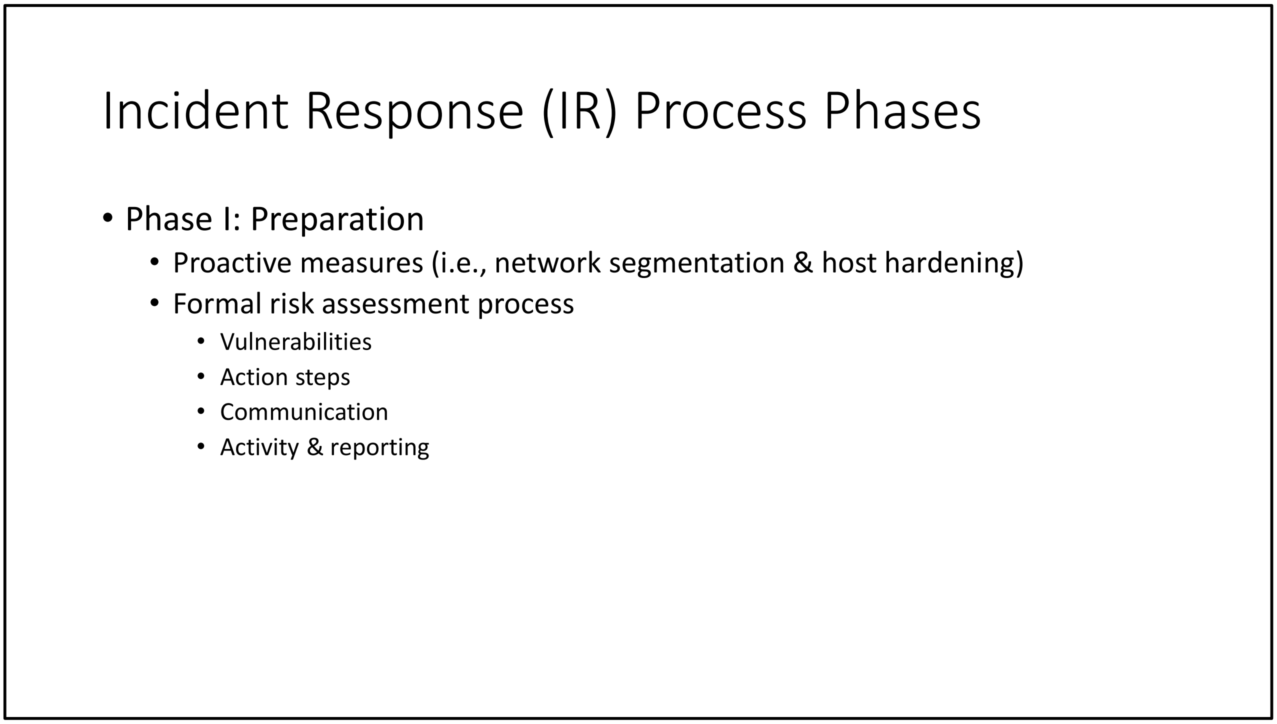
Objective: 4.2 Given a scenario, apply the appropriate incident response procedure.
• Preparation
- Training
- Testing
- Documentation of procedures
• Detection and analysis
- Characteristics contributing to severity level classification
- Downtime
- Recovery time
- Data integrity
- Economic
- System process criticality
- Reverse engineering
- Data correlation
• Containment
- Segmentation
- Isolation
• Eradication and recovery
- Vulnerability mitigation
- Sanitization
- Reconstruction/reimaging
- Secure disposal
- Patching
- Restoration of permissions
- Reconstitution of resources
- Restoration of capabilities and services
- Verification of logging/communication to security monitoring
• Post-incident activities
- Evidence retention
- Lessons learned report
- Change control process
- Incident response plan update
- Incident summary report
- IoC generation

- Monitoring



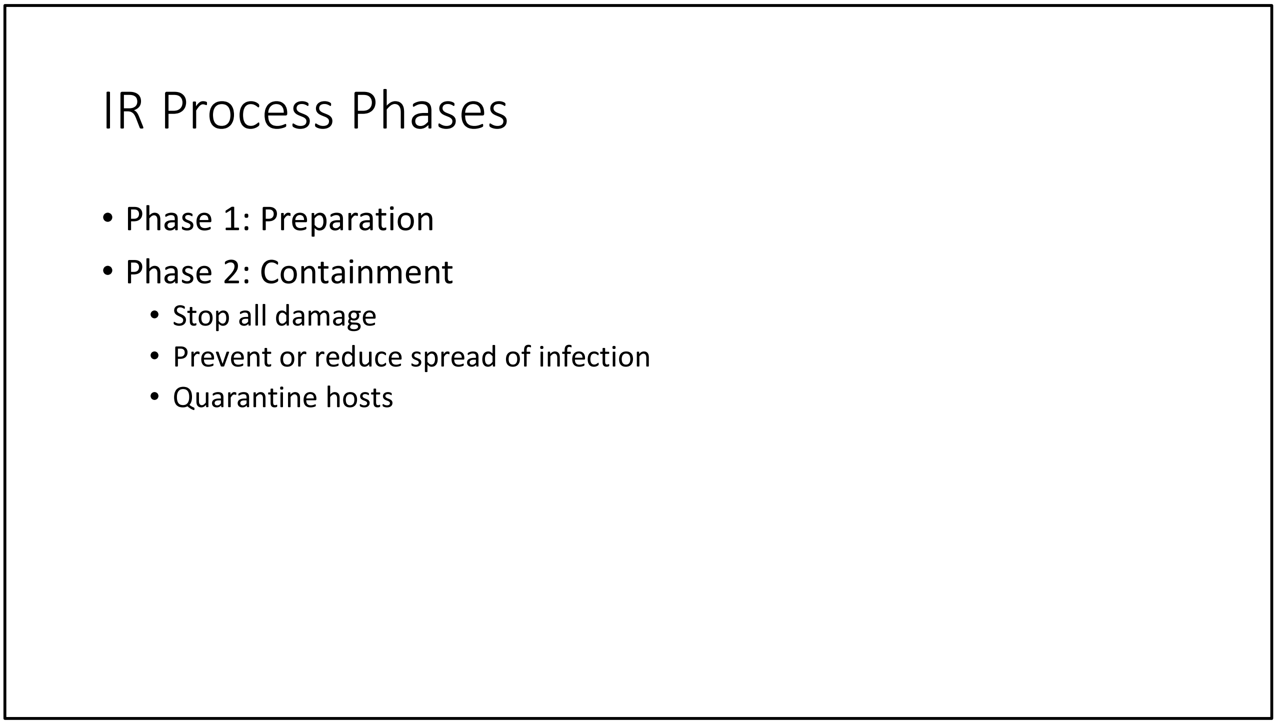
Incident Response (IR) Process

- NIST Special Publication 800-61
  - National Institute of Standards and Technology (NIST)
  - Provides publications & guidelines on technology standards



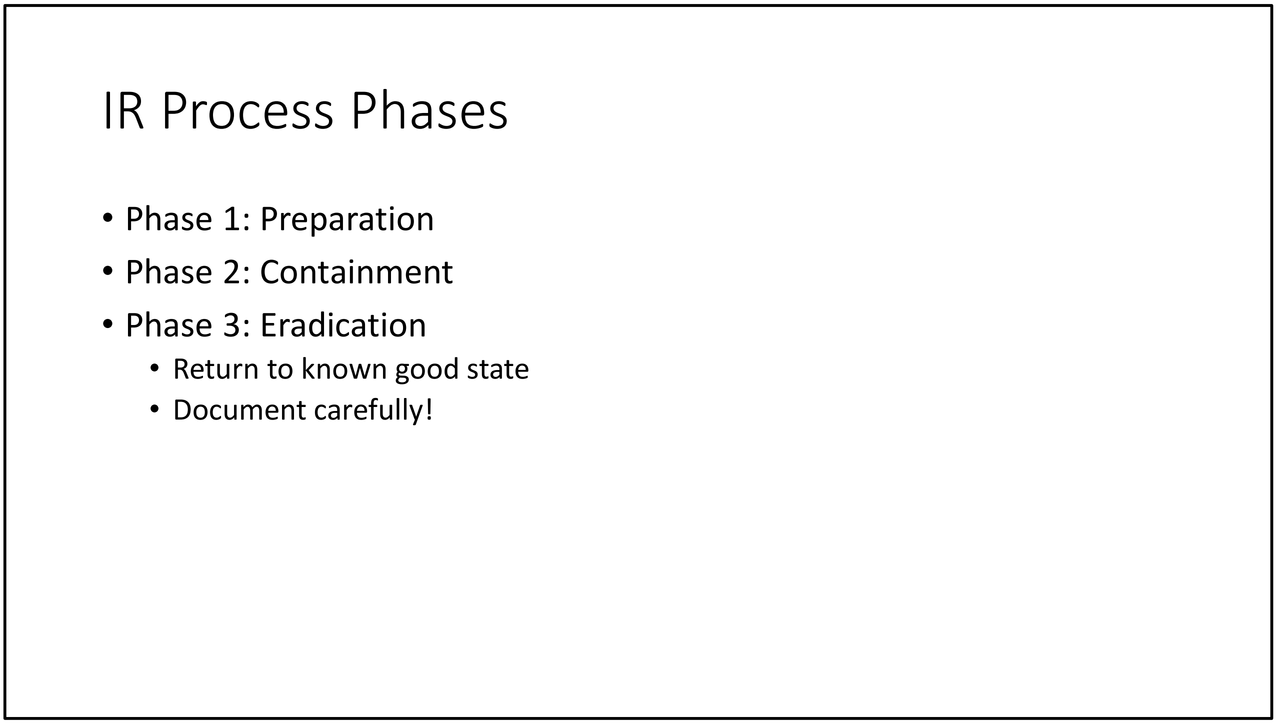
Incident Response (IR) Process Phases

- Phase I: Preparation
  - Proactive measures (i.e., network segmentation & host hardening)
  - Formal risk assessment process
    - Vulnerabilities
    - Action steps
    - Communication
    - Activity & reporting



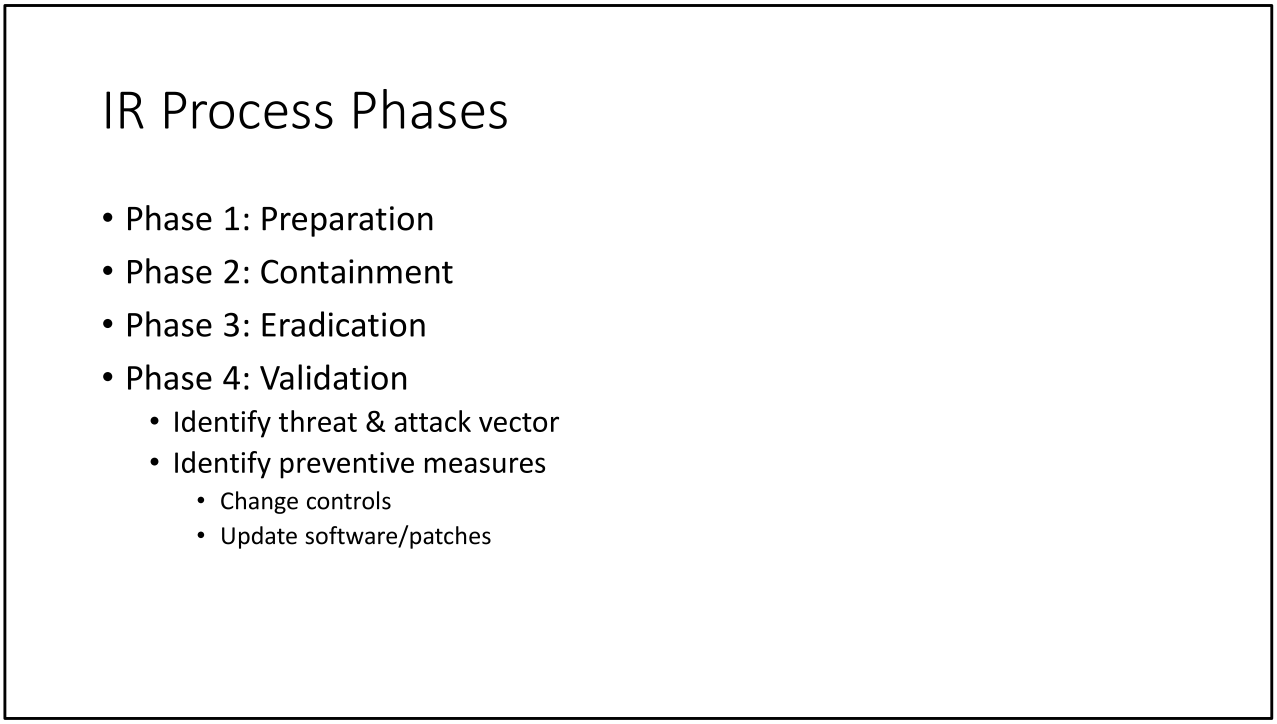
IR Process Phases

- Phase 1: Preparation
- Phase 2: Containment
  - Stop all damage
  - Prevent or reduce spread of infection
  - Quarantine hosts



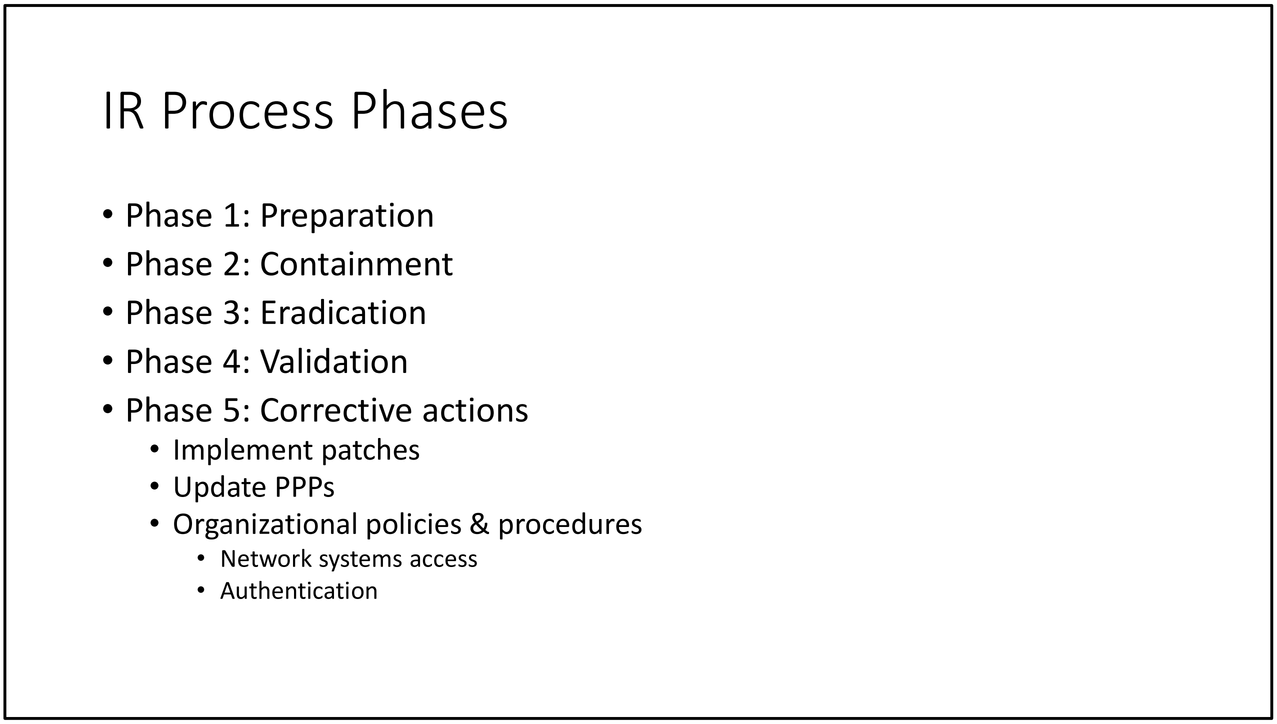
IR Process Phases

- Phase 1: Preparation
- Phase 2: Containment
- Phase 3: Eradication
  - Return to known good state
  - Document carefully!



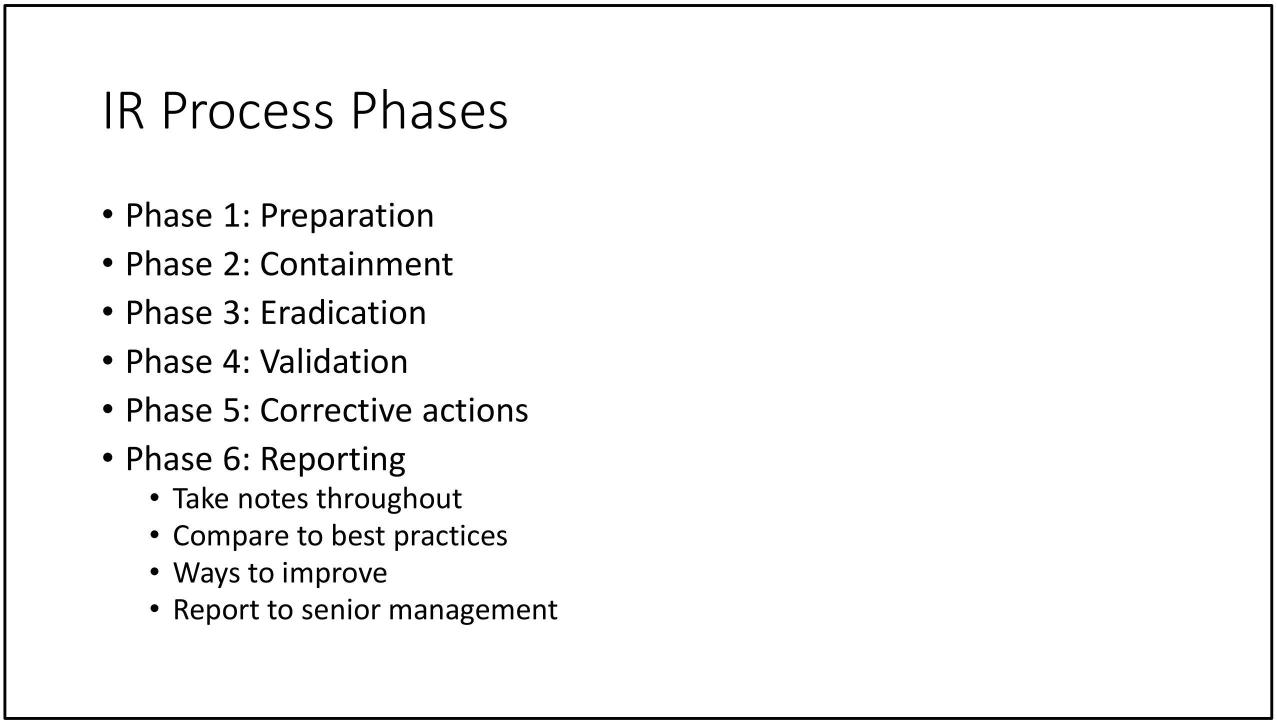
IR Process Phases

- Phase 1: Preparation
- Phase 2: Containment
- Phase 3: Eradication
- Phase 4: Validation
  - Identify threat & attack vector
  - Identify preventive measures
    - Change controls
    - Update software/patches



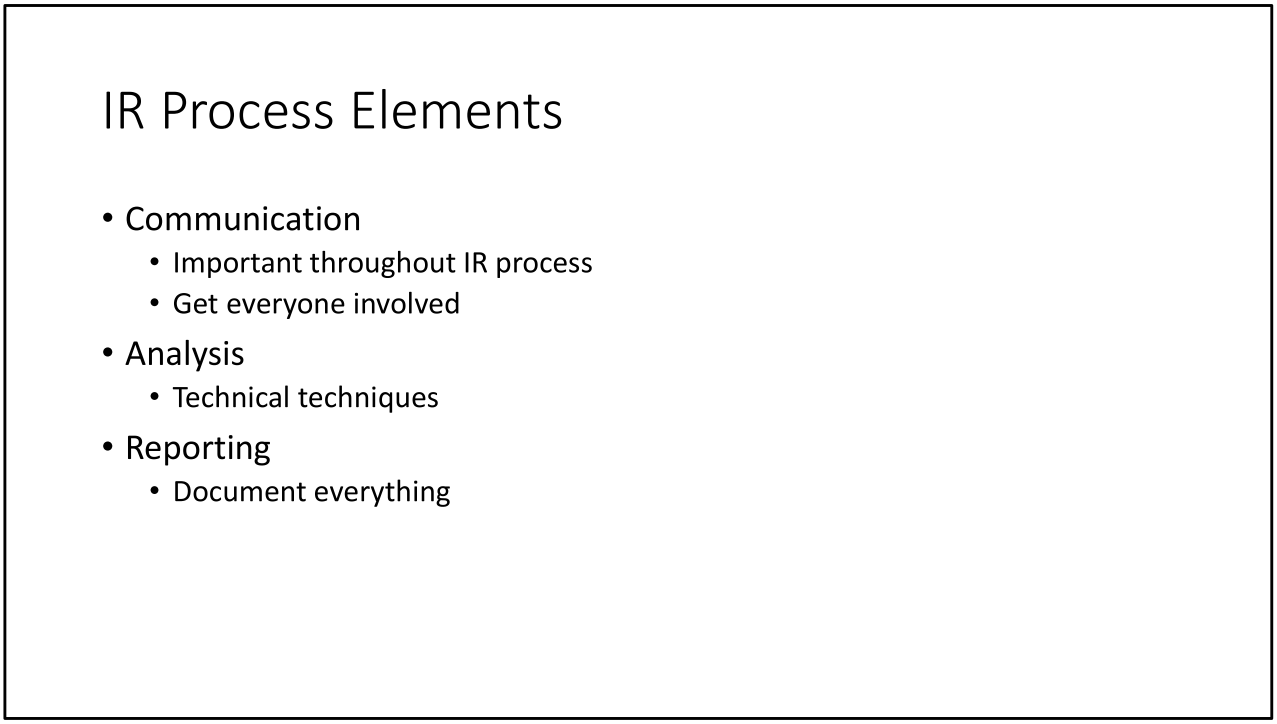
IR Process Phases

- Phase 1: Preparation
- Phase 2: Containment
- Phase 3: Eradication
- Phase 4: Validation
- Phase 5: Corrective actions
  - Implement patches
  - Update PPPs
  - Organizational policies & procedures
    - Network systems access
    - Authentication



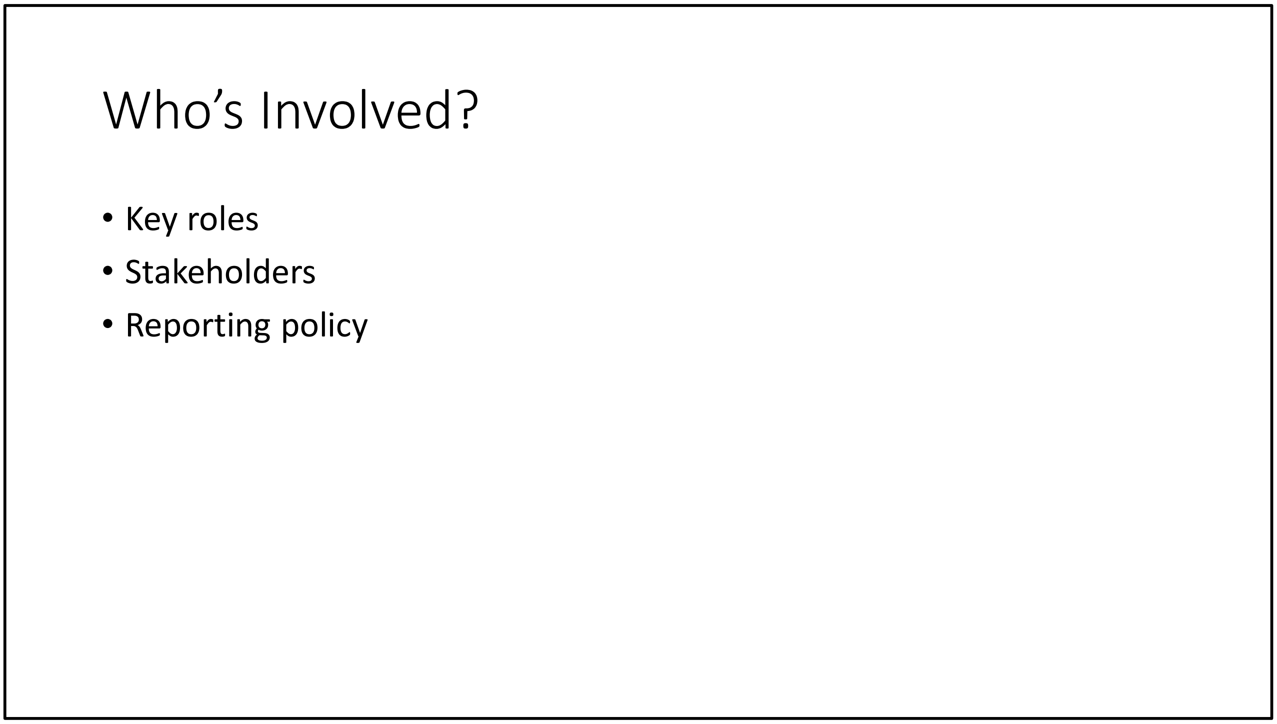
IR Process Phases

- Phase 1: Preparation
- Phase 2: Containment
- Phase 3: Eradication
- Phase 4: Validation
- Phase 5: Corrective actions
- Phase 6: Reporting
  - Take notes throughout
  - Compare to best practices
  - Ways to improve
  - Report to senior management



IR Process Elements

- Communication
  - Important throughout IR process
  - Get everyone involved
- Analysis
  - Technical techniques
- Reporting
  - Document everything



Who’s Involved?

- Key roles
- Stakeholders
- Reporting policy