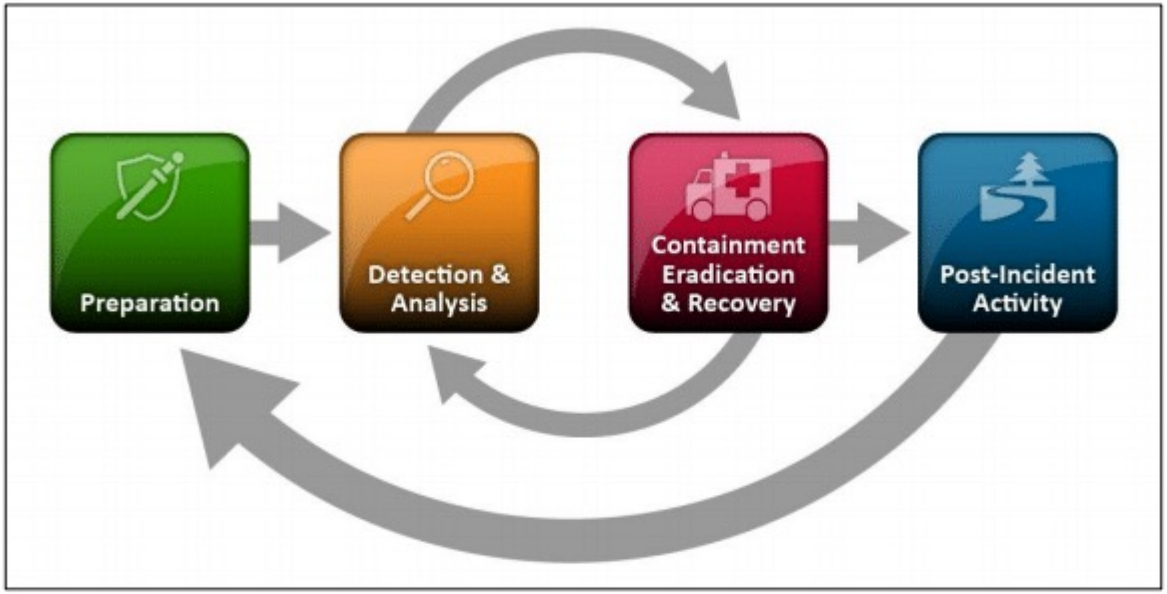
Incident Management

Investigations and Incident Handling

- Investigations and incidents have defined processes.
- For criminal investigations and best practices – ACPO Good Practice Guide
- For incident response – NIST 800-61r2

NIST 800-61r2

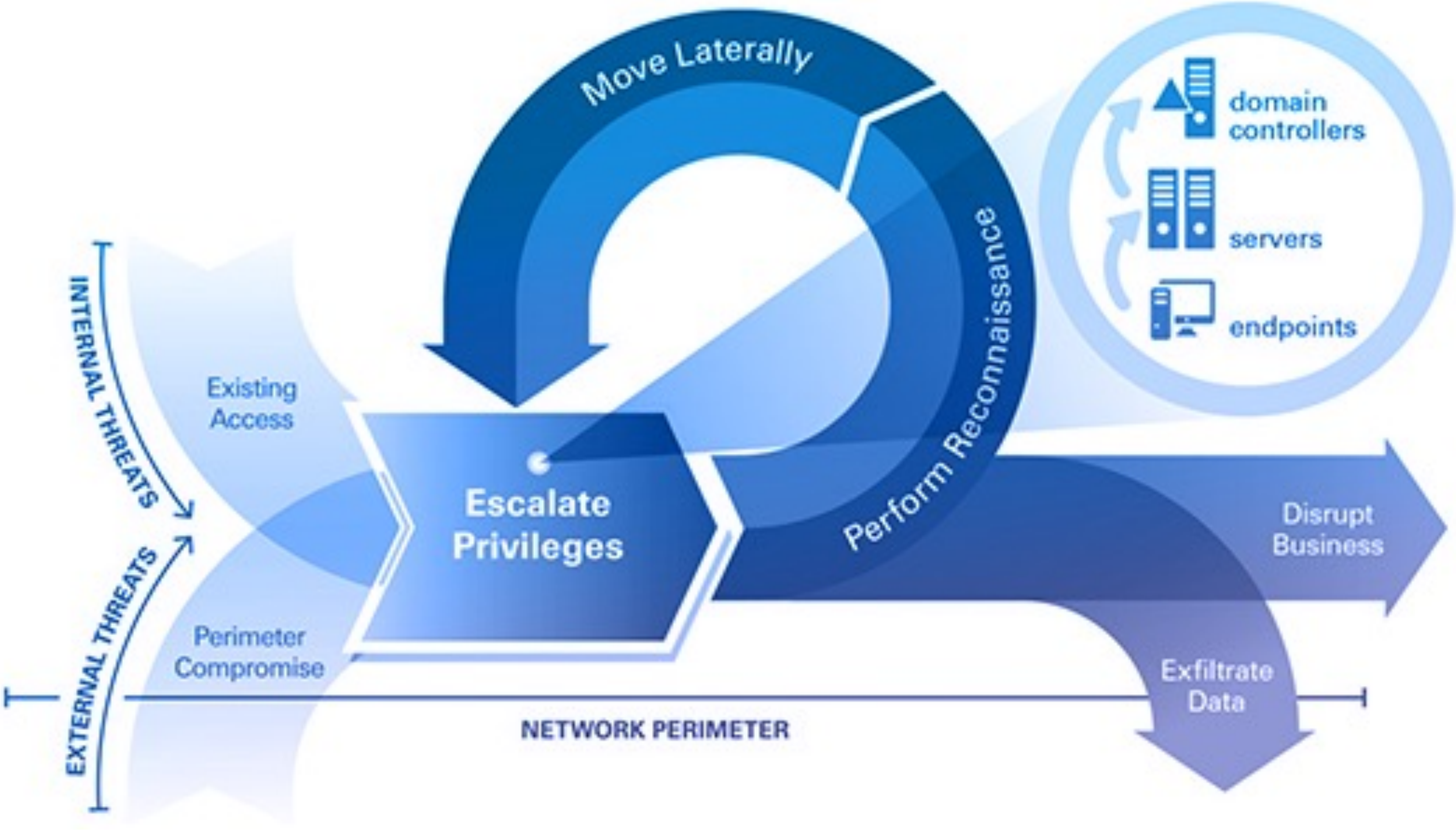
- NIST 800-series – information security series.
- 800-61r2 – Computer Security Incident Handling Guide



Investigation Preparation

- Communications:
  - Contact information
  - On-call information
  - Incident reporting mechanisms
  - Issue tracking systems
  - Encryption software
  - War room
  - Secure storage facility

Attack Lifecycle



Attack Vectors

- External/Removable Media
- Web-based attacks
- Email attacks
- Impersonation
- Improper usage
- Loss or theft of equipment
- Other

Signs of an Incident

Precursors

- Web server logs indicate the presence of unauthorized vulnerability scanning.
- Announcement of a new, relevant vulnerability.
- A threat group stating privately or publicly that they are targeting the organization

Signs of an Incident

Indicators of Compromise

- Alerts from a NIDS or HIDS
- Suspicious log / audit log entries for key services.
- Configuration changes
- Multiple failed login or access attempts

Analysis

- Profile networks and systems.
- Baseline normal behavior
- Perform event correlation
- Maintain and use a knowledge base of information
- Use Internet search engines for research
- Collect additional data
- Filter the data
- Seek assistance from others

Documentation

- Current status of the incident
- Summary of the incident
- Indicators of the incident
- Other related incidents
- Actions taken by incident handlers
- Chain of custody, if applicable
- Impact assessments related to the incident
- List of gathered evidence
- Next steps to be taken

Prioritization

- Prioritization of incidents is critical
- Functional impact
  - impact of the incident on IT systems functionality
- Information impact
  - What’s the impact on confidentiality, integrity and availability of information
- Recoverability
  - Size of the incident, degree of compromise, and type of resources it affects will impact the amount of resources needed for recovery

Notification

- Key stakeholders must be notified based on the incident severity and impacts
- This is typically documented in an organization’s incident response plan
- Notification requirements may vary by the data involved in the incident or contractual requirements

Containment

- Containment strategies vary and they must balance the need to prevent additional damage or theft with a need to maintain and collect evidence
- Premature containment can lead to situations where an adversary is thought to be “evicted” but is not
- Containment cannot occur without root cause analysis
- Containment typically involves parallel network and identity efforts
- Example: APT actor war stories

Evidence Collection

- Once containment is established / it’s time to figure out what happened, and to do that a scope of systems and a collections plan are needed
- Scoping systems is critical while prioritizing timelines and resources for collection

Analysis

- Identify attacking hosts
- Identify the root cause of the incident
- Build a timeline of the incident including the sequence of events from the root cause of the incident

Eradication and Recovery

- Similar to containment strategies, good eradication and recovery strategies will take inputs from evidence collection and analysis and balance the business capabilities against attacker access
- Phased approaches generally work better
- Eradication - removing adversary access
- Recovery - ensuring systems are functional within expected parameters
- Don’t forget to address the root cause!

Lessons Learned

- What happened, when?
- Did staff and organizations perform as expected?
- What would staff do differently the next time an incident like this occurs?
- What corrective actions can prevent similar incidents in the future?

Post-incident Analysis

- Prioritization of incidents is critical
- Functional impact
  - impact of the incident on IT systems functionality
- Information impact
  - What’s the impact on confidentiality, integrity and availability of information
- Recoverability
  - Size of the incident, degree of compromise, and type of resources it affects will impact the amount of resources needed for recovery

Conducting an Investigation: Investigation Models

Formal Investigation Process Models

- Digital investigations must uncover and produce the truth
- Early models described a stepwise approaches to specific investigative problems (and focused solely on computer crime on networked computer systems)
- Real-world digital investigations are diverse

Staircase Model

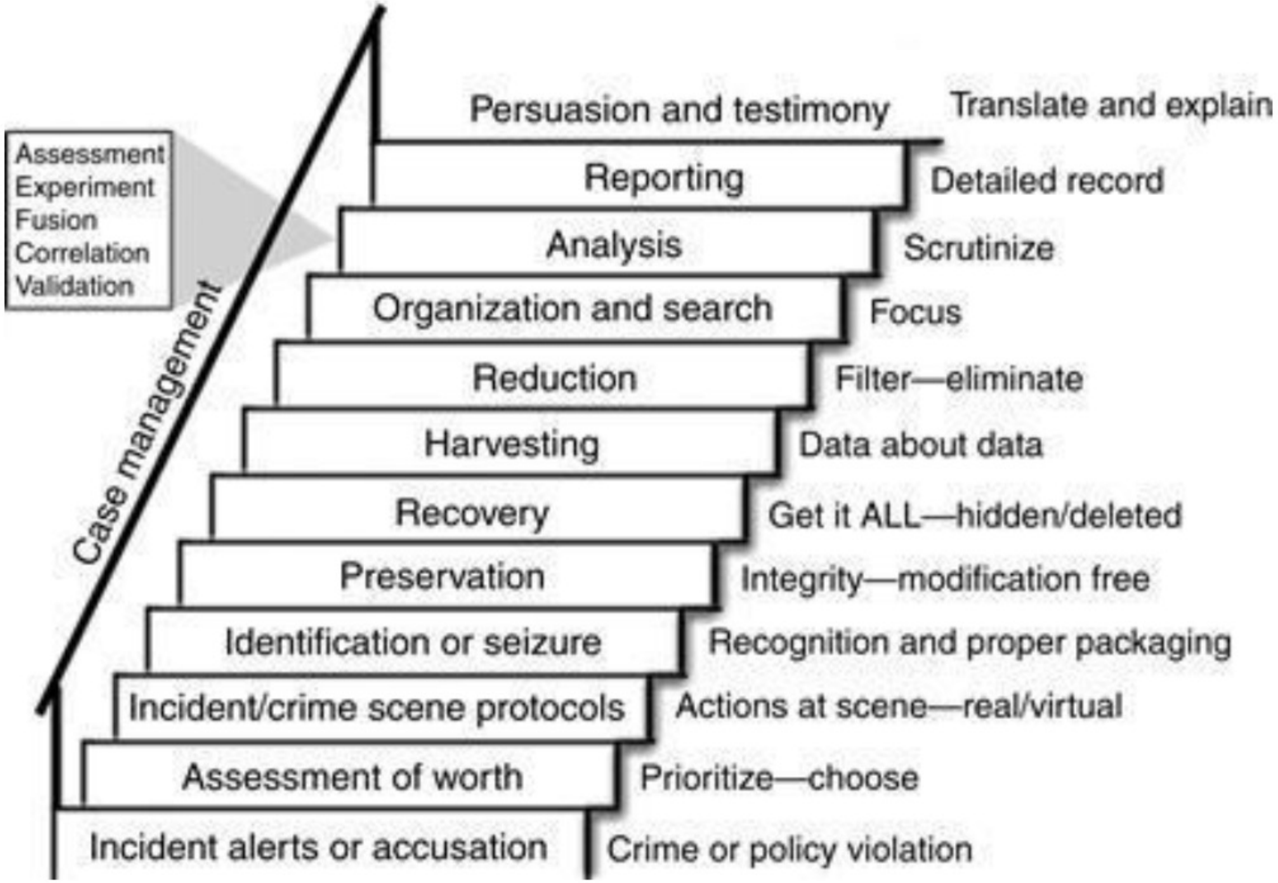


Figure 6.2 Categories of the investigative process model (depicted as a flight of stairs) from Digital Evidence and Computer Crime, 2nd edition.

Distillation

- Preparation
- Survey / Identification
- Preservation
- Examination and Analysis
- Presentation (Reporting)

Preparation

- Plan of action, tool preparations and resource preparation
- Case management (or case management preparation)
- Logistical / collection considerations

Survey / Identification

- Review all potential sources of digital evidence to get a familiarity with the totality of evidence
- Determine which items may be of potential relevance to the investigation
- Example: compromised systems vs. all systems

Preservation

- Preventing changes of *in-situ* digital evidence
- Critical for maintaining the integrity of the investigation

Investigation Scoping

In-depth Investigations

Overview

- Forensic policy approach
- Digital evidence maps
- Scope of an investigation
- Forensic preparedness
- Real-world lessons learned on investigation scoping

Realities of Real-world Forensics

- Surveys by nature must be initially broad
- Once the investigation starts, it will be constrained by the law, time, resources and the interests of the victim (person, business, or organization)

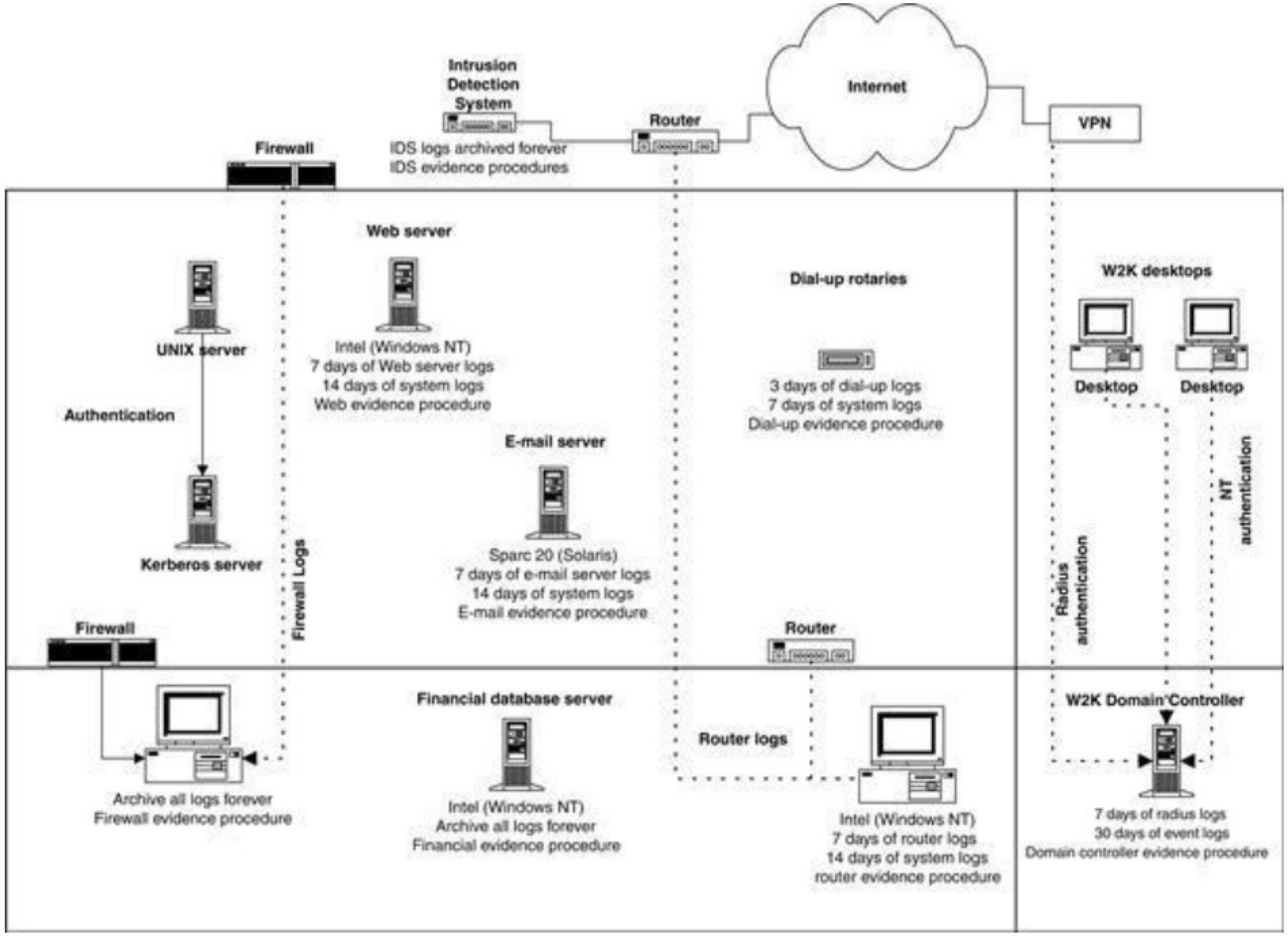
Forensic Policy Approach

- Specification and enforcement of policies
- What events must be handled
- What data surrounding events must be preserved
- What logs are collected, how long are they retained, do they have required detail

Digital Evidence Maps

- Layout of evidence survey
  - Systems
  - Network layout
  - How they relate
  - What data we have from each
- Can help with rapid scoping / targeting and prioritization of analysis

Digital Evidence Maps



Investigation Critical Focus Areas

Common Core Investigation Areas

- Despite every investigation being unique, there are core investigation focus areas almost all investigations include
- Core areas:
  - Customer data
  - Intellectual property
  - Payments and financial systems

Core Investigation Functions

- Difficult to affect CIA triad (confidentiality, integrity, availability) without accessing systems and data.
- Core functions:
  - Local authentication
  - Remote authentication
  - Data access (application logs)

Core Investigation Tech

- Certain systems appear in investigations more often than not
- Core systems:
  - Active Directory Domain Controller(s)
  - Email Server (could be server or SaaS)
  - Web Application Servers
  - Remote Access Servers (Virtual Private Network (VPN) or Remote Desktop / Secure Shell)