Secure Software Development Secure Software Deployments

Objectives

- Explain the security related problems of software installation
- Define hardening
- Understand the importance of continuous monitoring
- Explain the concept of a Bastion Host
- Define the terms event, alert, and incident
- Draw the incident response lifecycle
- Explain the incident risks at end of software life

Final Exam:
Wednesday of
Exam week
8:00–10:00
here (I think).....

Article Reviews

⇒ Lab

= pick best of 3 articles/podcast/etc

→ Explain in ≈ 5 minutes

Hardening

- The act of locking a system to the most restrictive level of access necessary to still maintain proper operation of the system
  - Refereed to as MSB
- Common errors:
  - Hardcoding credentials and cryptographic keys
  - Not disabling the listing of directories and files on a web server
  - Installation of software with default accounts and settings
  - Installation of admin console with default settings
  - Installation of unneeded services
  - Missing patches

Turn off debugging

maybe?

IT staff

Monitoring

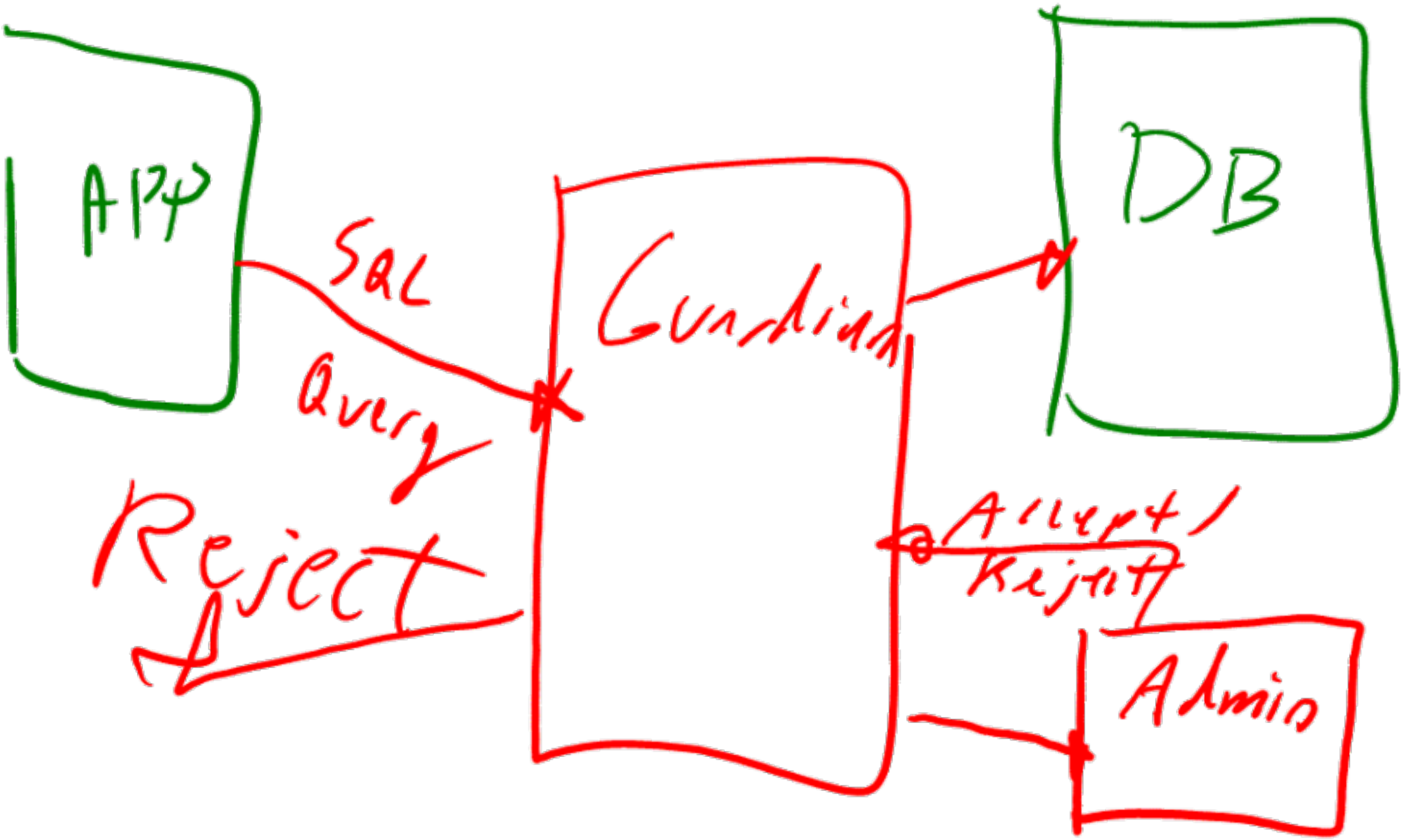
- "What is not monitored cannot be measured, and what is not measured can not be managed.
- Monitoring's purpose
  - Validate compliance with regulations
  - Provide evidence for audit defense
  - Assist forensics investigations
  - Assure that data confidentiality, integrety, and availability aspects are not impacted adversly
  - Detect insider and external threats that are orchestrated against the organization
  - Identify new threats
  - Validate the overall state of security

what attacked us?

IBM Guardian

Scanning, loggin monitoring, intrusion detection

MSOE


App
SQL
Query
Reject
Guardian
DB
Allow/
Reject
Admin

Installation

- The most overlooked aspect of application security
  - Accounts for a sizable proportion of security patches

- Why does this happen?

End of the product!

Principles of Least Privilege and Deployment

- What is the principle of least privilege?

Installation Directory and its impact on security

How many programs should be able to save to the install directory?

Dumb idea!

Cleaning Up after the install

What happens if install aborts?

- Clean up

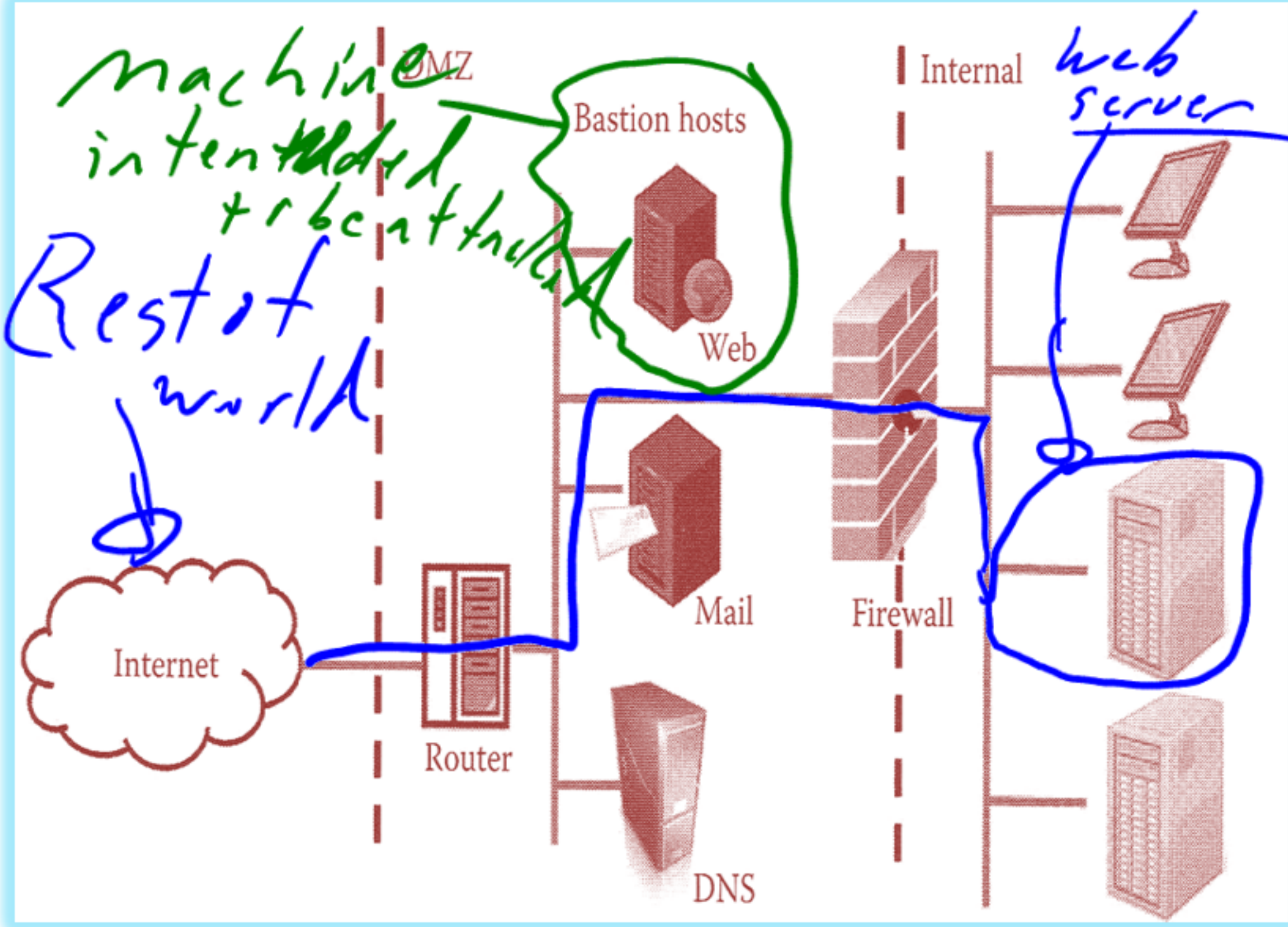
⇒ NW paths?

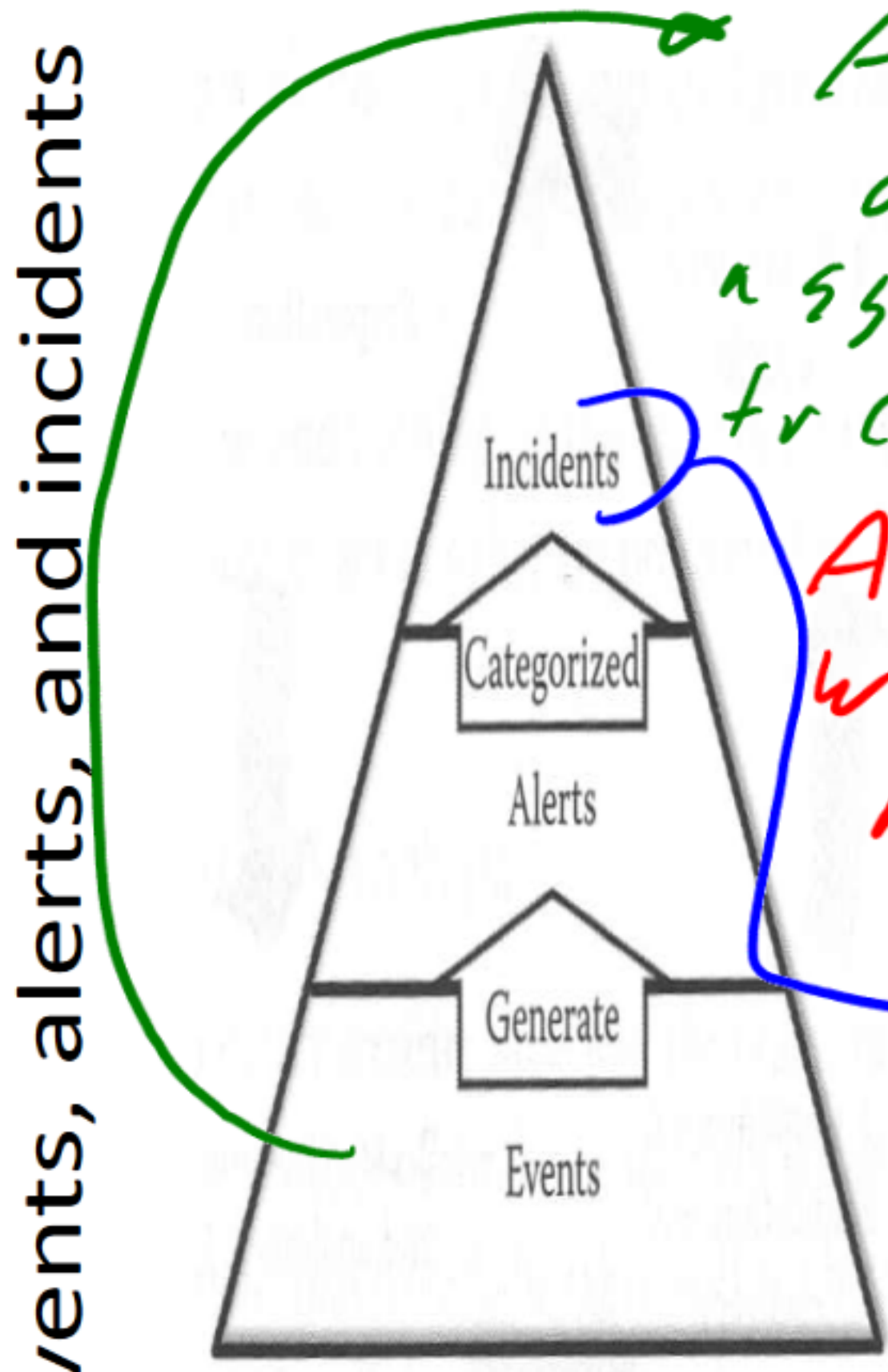
⇒ Root privileges?

Windows Installer

- Make sure installation does not cause setup to fail in a manner compromising security

Bastion Host





Any action directed towards a system attempting to change the state.

Alert: Random events which match a preset condition or pattern.

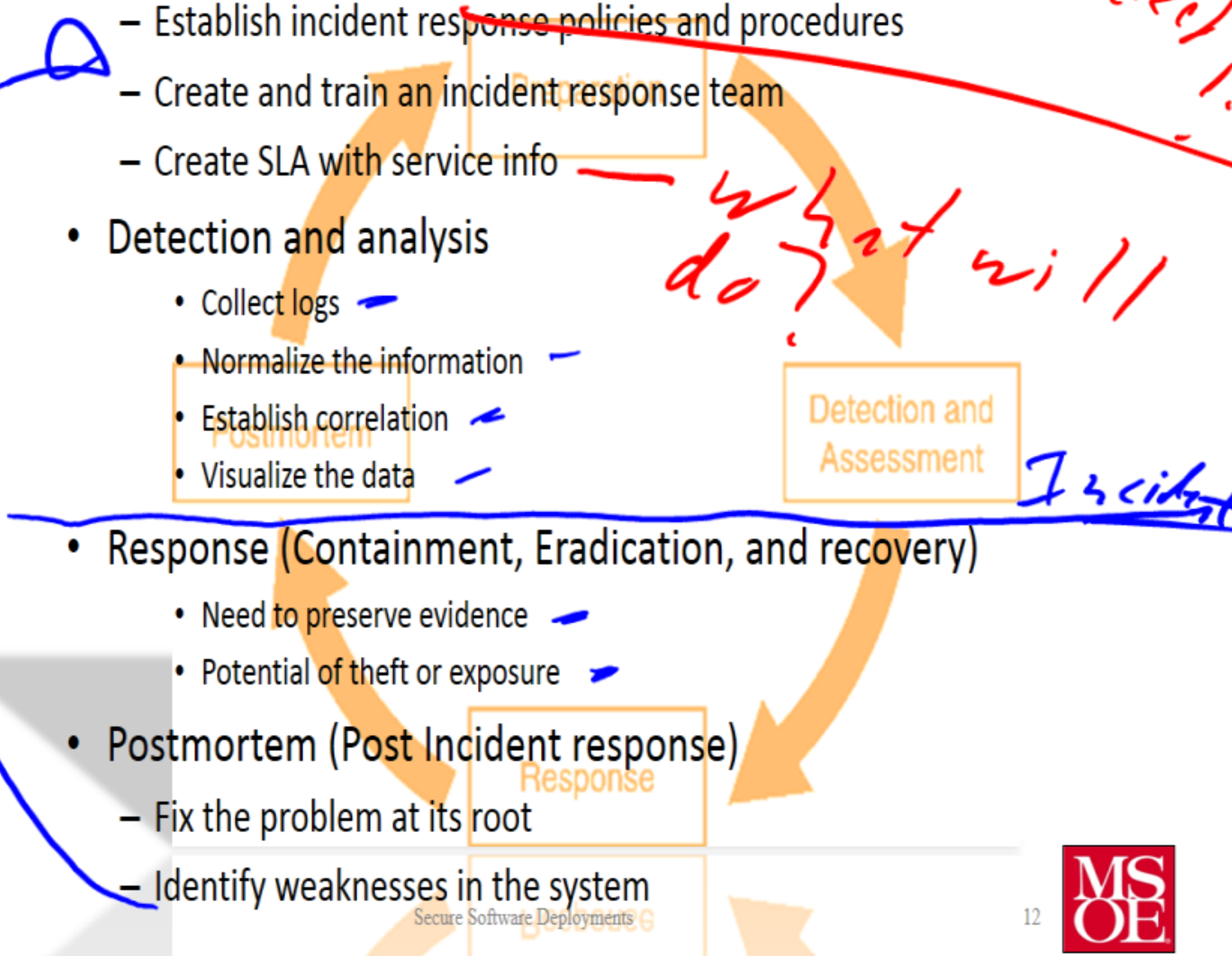
An attempt to violate or threaten security policy of the system.

Incident Types

- Denial of service
  - An attack that prevents or impairs an authorized user from using the network, system, or software application
- Malicious code
  - Code based malicious entities (viruses, worms) which infect a host
- Unauthorized access
  - Access control related events on a system where an unauthorized person gains logical or physical access to a system
- Inappropriate usage
  - A person violates proper usage of the software system
- Multiple components
  - Incidents which include two or more incidents

Incident Response lifecycle

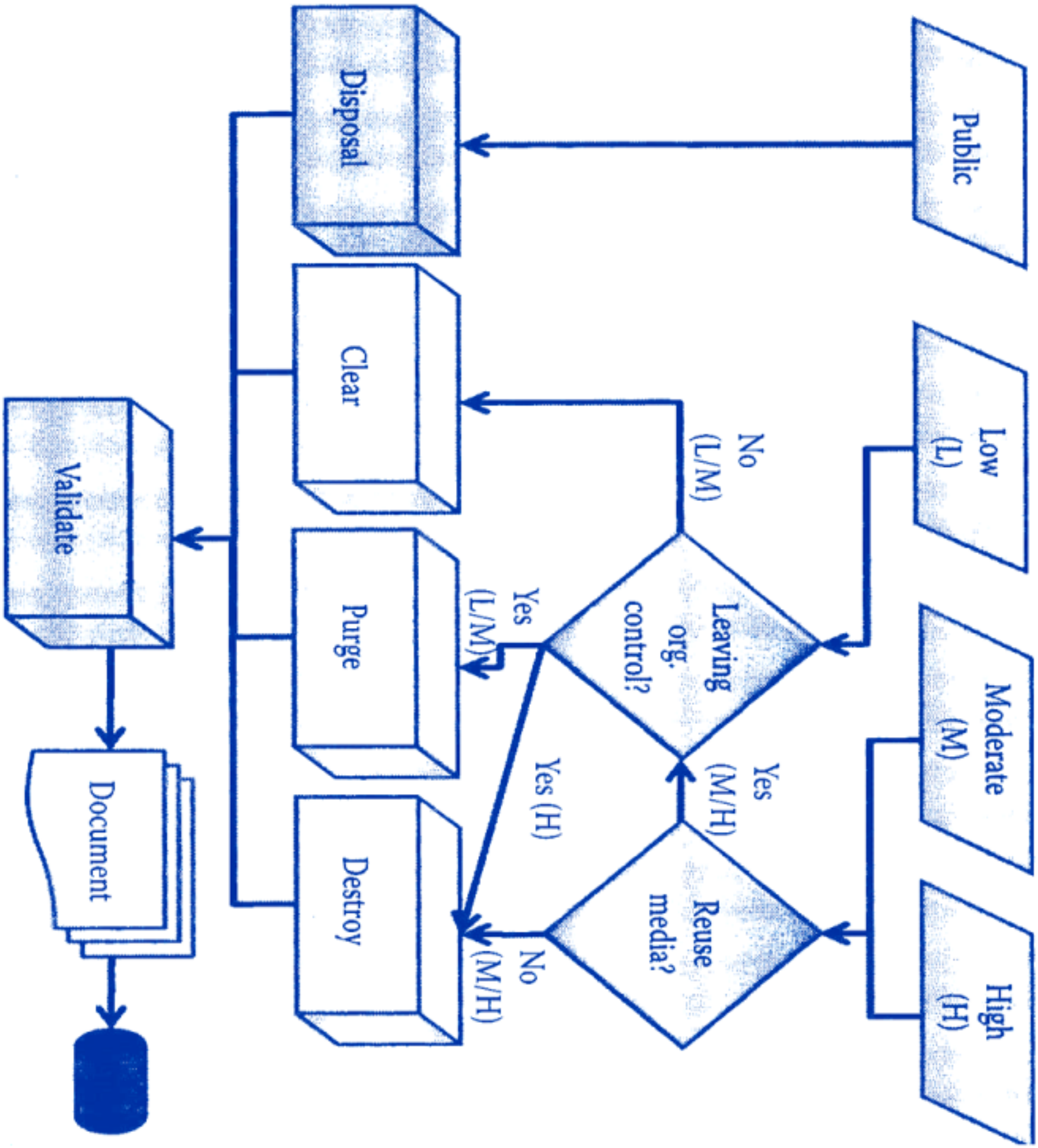
- Preparation:
  - Establish incident response policies and procedures
  - Create and train an incident response team
  - Create SLA with service info
- Detection and analysis
  - Collect logs
  - Normalize the information
  - Establish correlation
  - Visualize the data
- Response (Containment, Eradication, and recovery)
  - Need to preserve evidence
  - Potential of theft or exposure
- Postmortem (Post Incident response)
  - Fix the problem at its root
  - Identify weaknesses in the system



- Sunsetting criteria
  - When a specific hardware or software product must be disposed
- Reasons:
  - New threats against software are discovered
  - Contractual end of usage
  - Software has reached end of warranty period
  - Software has reached end of product support
  - Software is no longer compatible with hardware
  - Software which can provide same functionality in a more secure fashion is available

Disposal

Information Disposal and Media Sanitization



Configuration keys and the Windows Registry

- HKEY_CURRENT_USER versus HKEY_LOCAL_MACHINE

Windows Systems Management Server (SMS) Remote Agent

Windows Systems Management Server (SMS) Remote Agent