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

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

System protection. Unused and Patches.

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

techniques:
Scanning, Loggings, intrusion
Detection

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

Installation

- Why does this happen?

People don't know about the SW they are installing or how to set it up properly.

Principles of Least Privilege and Deployment

- What is the principle of least privilege?

Who needs to be able to circumvent binaries?
Administrator
Users (if personal installs are allowed)

From a security standpoint: Admin should have full access to Program Files and no one else should.

Principles of Least Privilege and Deployment

- What is the principle of least privilege?

Who should be able to write/edit files into an install directory?

⇒ No one

Data files should be in a profile/home directory

Installation Directory and its impact on security

Cleaning Up after the install

1. Delete installer files which have been extracted
2. Dismount any mounted drives from installer...

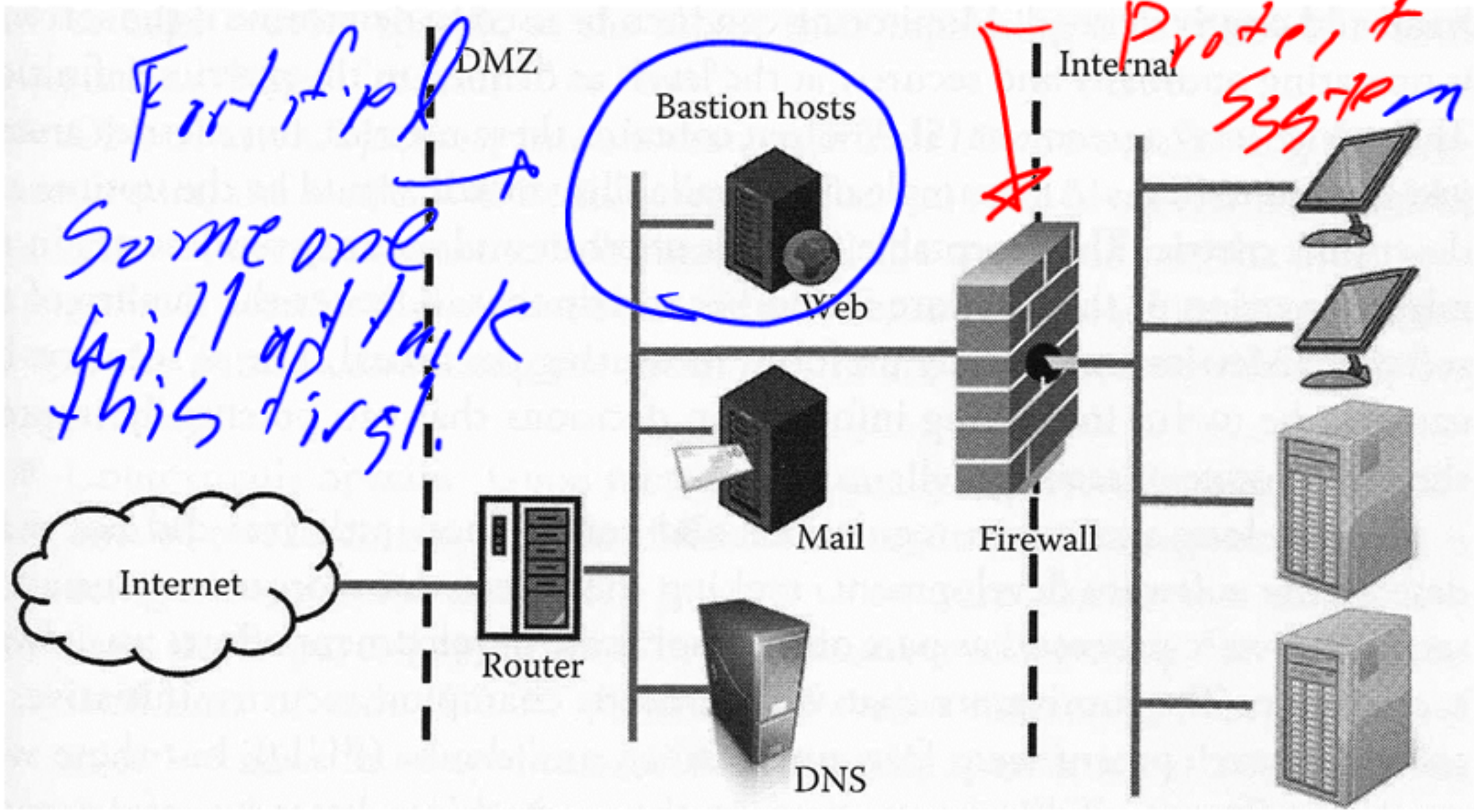
what if installer crashes?

Windows Installer

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

=> Fail w/ Admin access in a cmd Shell

Bastion Host

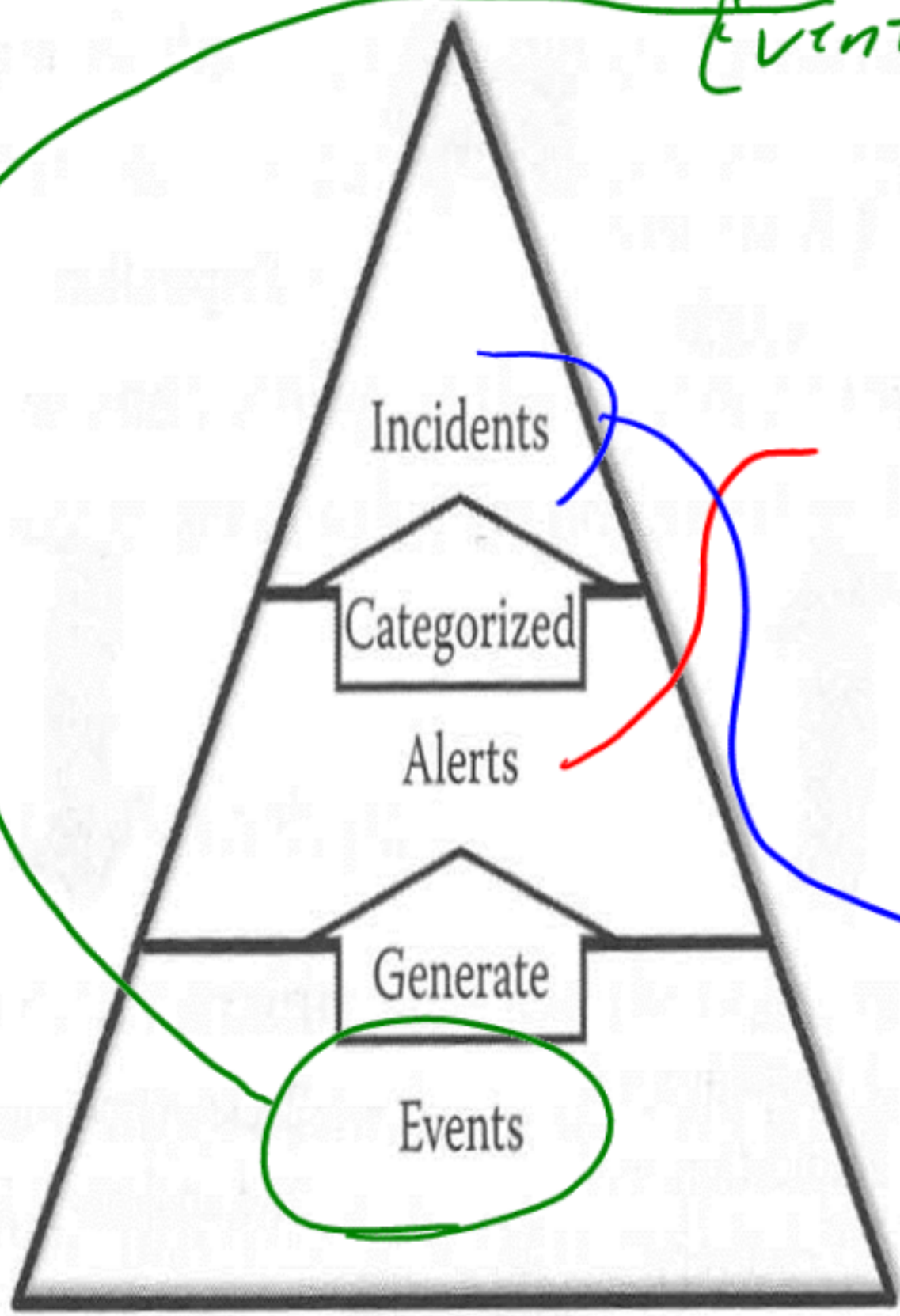


First step → Someone will attack this first.

Protect system

A fortified computer system exposed to external attack and illegal entry

Events, alerts, and incidents



Event: Any act action directed toward a system attempting to change its state.

Random event which matches expressed pattern or condition.

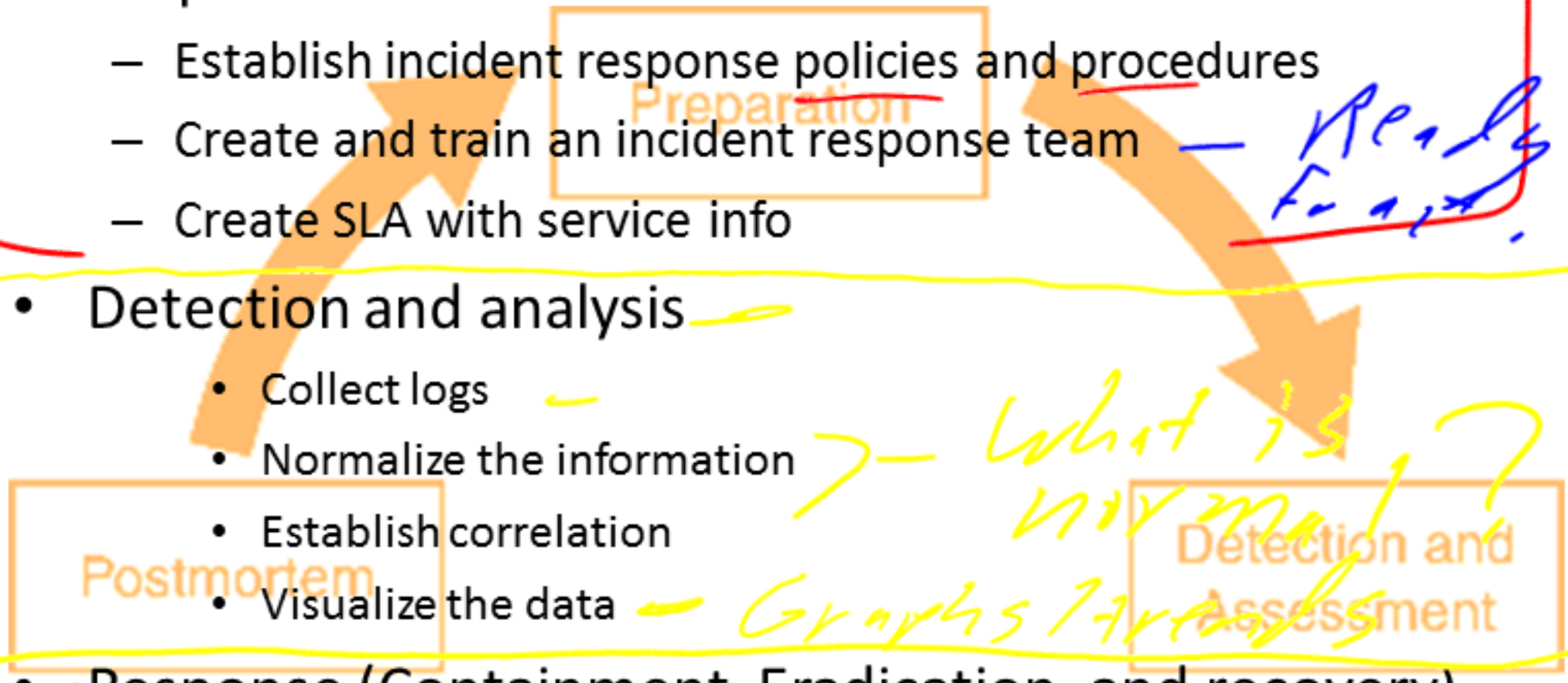
An attempt to violate or threaten the security of the system.

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

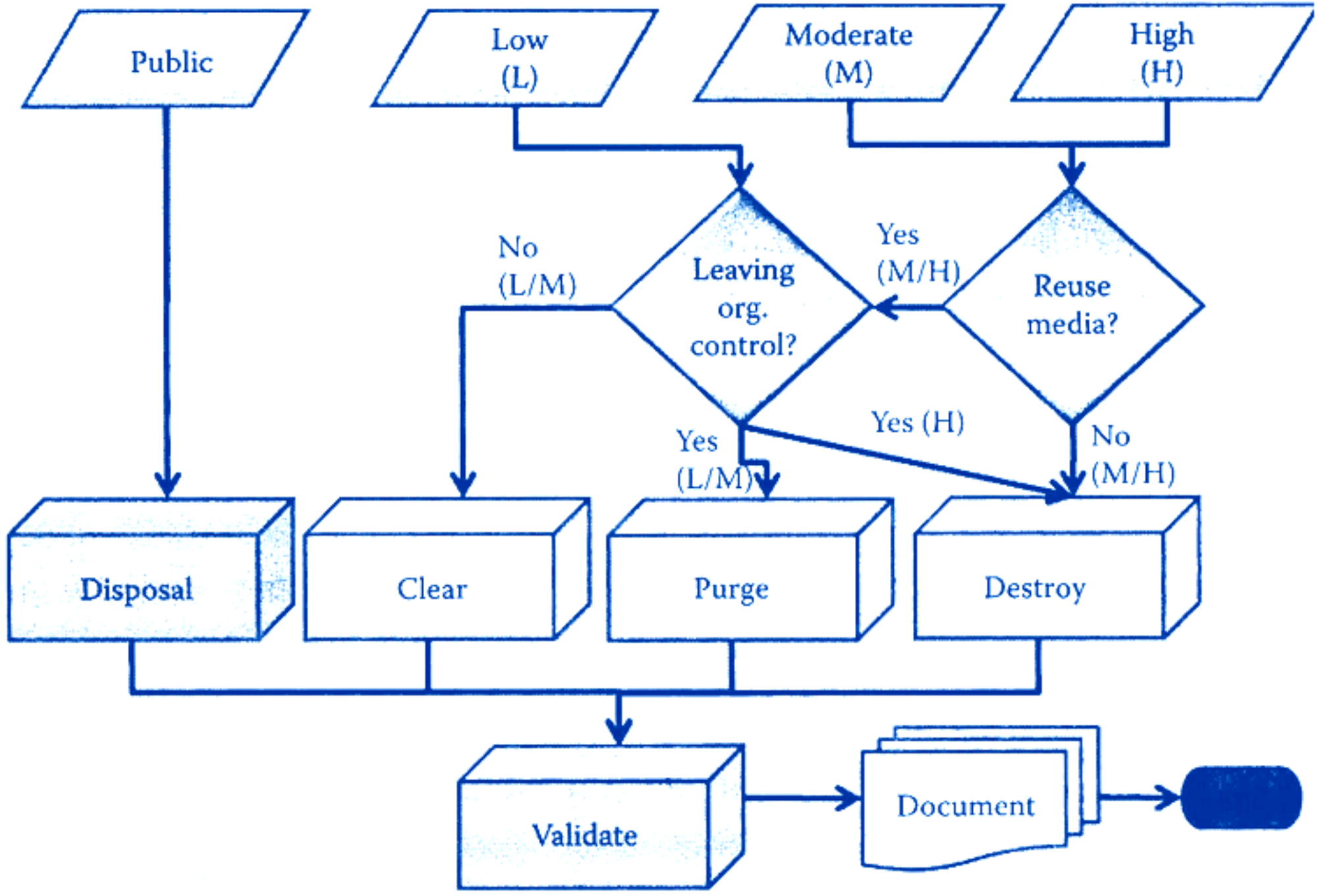
- Preparation:
  - Establish incident response policies and procedures
  - Create and train an incident response team
  - Create SLA with service info
- Detection and analysis
  - Collect logs
  - Normalize the information
  - Establish correlation
  - Visualize the data
- Response (Containment, Eradication, 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



Disposal

- 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

Information Disposal and Media Sanitization



Configuration keys and the Windows Registry

- HKEY_CURRENT_USER versus HKEY_LOCAL_MACHINE

Windows System Management Server (SMS) Remote Agent

Windows Systems Management Server (SMS) Remote Agent