Lesson 14 – Incident investigation

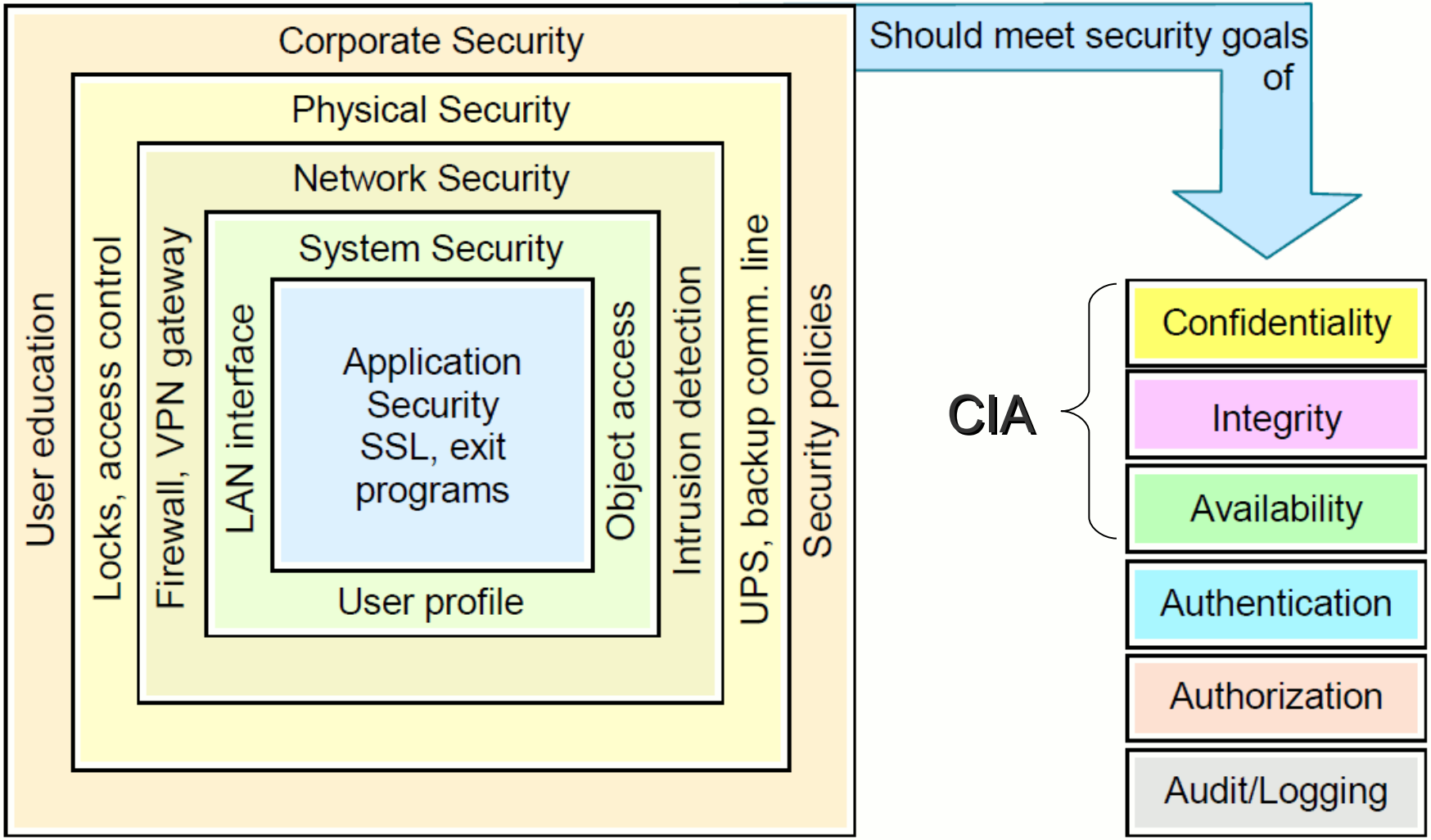
Security management – review

- An organization protects its assets by implementing security management practices
- The security management practices include
  - Identification of
    - Assets
    - Vulnerabilities
    - Threats
    - Risks
    - countermeasures
  - Security controls
  - Information classification
  - Roles and responsibilities

Securing management process – review

- An organization achieves its desired level of security by:
  - Defining a security policy
  - Implementing the security policy
  - Monitoring for compliance with the security policy
  - Obtaining independent confirmation that the security policy is sufficient and has been properly implemented

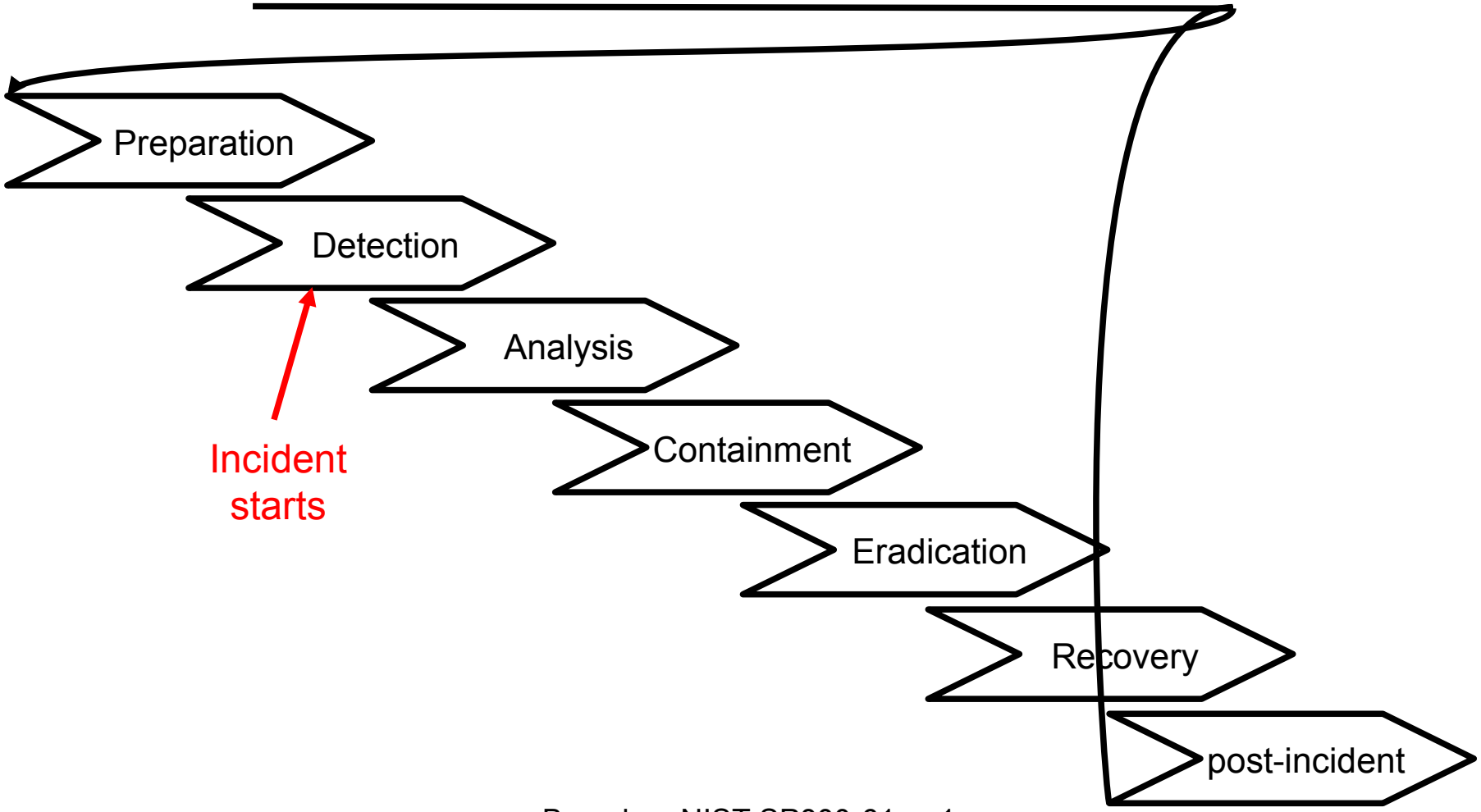
Security implementation layers – review



Security incident

- A violation or imminent threat of violation of security policies, acceptable use policies, or standard security practice
- Examples
  - Denial of Service
  - Malicious code
  - Unauthorized access
  - Inappropriate usage

Incident investigation lifecycle



Based on NIST SP800-61rev1

(http :// csrc.nist.gov/publications/PubsSPs.html)

Preparation

- Organization should have
  - A security policy with incident handling procedures
  - A trained incident response team
  - Prevention measures in place
    - Anti-virus, firewalls, etc.
- Incident response team should
  - Know the system and networks
  - Know existing policies and laws

Detection

- Detect deviation from normal
  - Alerted by a user or external entity
  - anti-virus alert
  - Network tool alert
  - System or firewall logs
  - Etc.
- If detected, then declare an incident
  - Notify senior management
  - Start following incident handling procedures

Analysis

- Forensic analysis
  - Aim to obtain sound evidence
- Evidence acquisition
  - volatile data collection
  - Hard disk images (if needed)
- Log and time-line analysis
- Document everything
  - Maintain “chain of custody”

Containment

- Try to prevent
  - The attacker from doing further damage
  - Other systems from being infected
- Take decisions on
  - Isolating the infected machines
    - Removing the machine from the network
    - Turning some machines off

Eradication

- Run anti-virus and cleanup software
- Remove
  - Compromised accounts
  - Malware or other artifacts left by the attacker
- Revoke compromised credentials
- Reinstall compromised software (if needed)

Recovery

- Restore data from backups
- Start the process of getting the software and systems back into production
  - Must be done in a control manner
  - Monitor to detect any anomaly

Post-incident

- Conduct a postmortem analysis
  - Identify the root cause of the incident
  - Evaluate the incident response team response
- Update security policy and incident handling procedures based on the findings

The End