Information Assurance and Security – ACIT 4630

Hesam Alizadeh

Week 4 – Winter 2024

Learning Outcomes

- Security incident identification & response process
- Log tampering
- Logging laws
- Different backup approaches

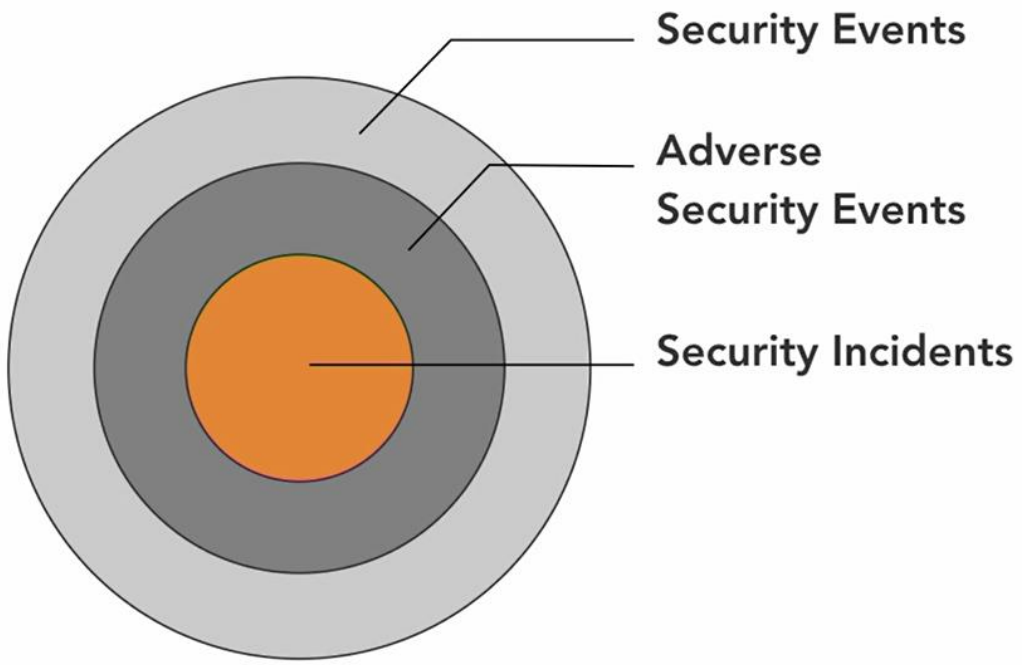
Notes from previous weeks

- **CVSS Scope**:

  Does it impact items outside security authority?
- **Workaround**: *avoiding the problem*
  - Cleanup, delete files, disable feature, etc.
- **Mitigation:** *eliminate or minimize the vulnerability*
  - Configuration update, replace certificate, password update, etc.

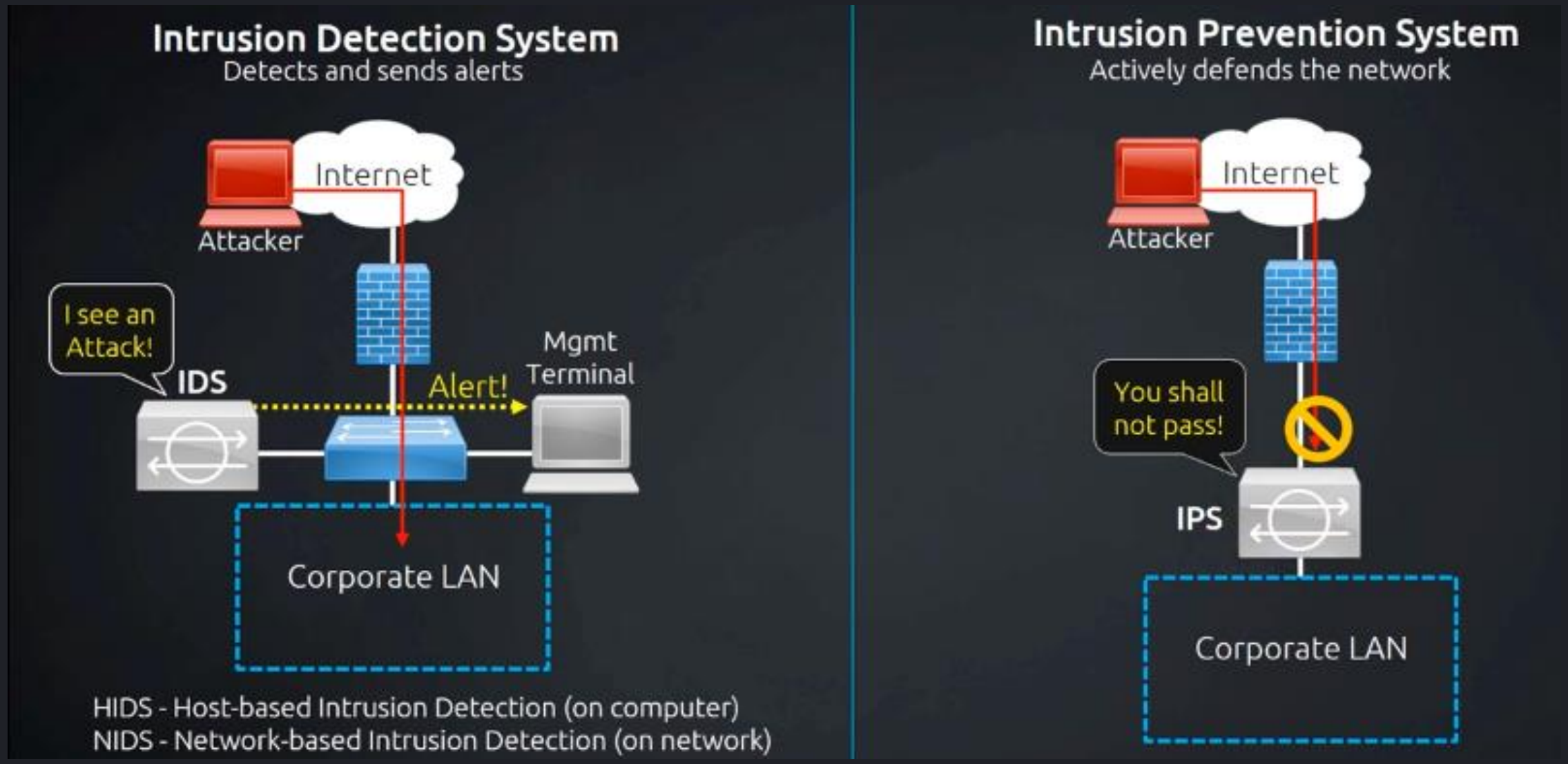
Incident Identification

- Are all security events considered incidents?
- How do we identify a security incident?
- How are the identified incidents assigned severity ratings?



Incident Data Sources

- IDS/IPS
- Firewalls
- Authentication systems
- Integrity monitors
- Vulnerability scanners
- System event logs
- NetFlow records
- Anti-malware packages



Source: [Intrusion Detection and Intrusion Prevention Systems]

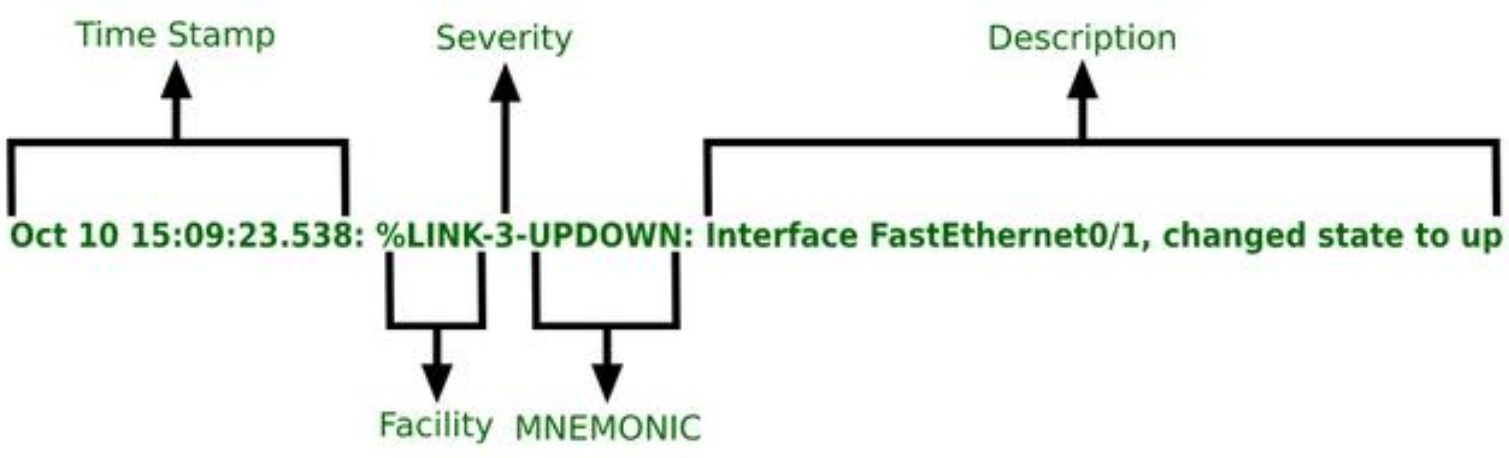
SIEM

“A solution that helps organizations detect, analyze, and respond to security threats before they harm business operations”

- Centralized Log Management
  - All system send logs directly to the SIEM platform.
- AI-Driven Threat Detection
  - Correlate and analyze log in data that could indicate a malicious activities.

Syslog

“The de facto standard for sending and receiving log messages between applications, systems and devices on Linux.”



How could severity of messages be used for incident monitoring?

Image source: [What is Syslog server and its working?]

Determining Incident Severity

Assessment Based on the CIA Triad:

- **Confidentiality**: Does the incident expose sensitive information to unauthorized parties?
- **Integrity**: Are there alterations or potential damage to the accuracy and completeness of data?
- **Availability**: Is there any disruption in access to critical systems or data?

Incident Severity Levels 1-5

Severity Description	
SEV 1	A critical incident that affects a large number of users in production.
SEV 2	A significant problem affecting a limited number of users in production.
SEV 3	An incident that causes errors, minor problems for users, or a heavy system load.
SEV 4	A minor problem that affects the service but doesn't have a serious impact on users.
SEV 5	A low-level deficiency that causes minor problems.

Data Sensitivity Focus:

- **PII**: Personally identifiable information
- **PHI**: Personal health information
- **SPI**: Sensitive personal information (e.g., genetic or sexual orientation data)
- **PCI**: Payment card industry data

- Severity Assessment Criteria:
  - Downtime, Recovery Time, Data Integrity Breach, Economic Impact, Business Processes Criticality
- Adapt criteria to specific needs and environment
- Apply consistent criteria for effective incident management and resource allocation

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

Image source: ISO 27001 A.16 – How to handle security incidents

NIST Incident Response

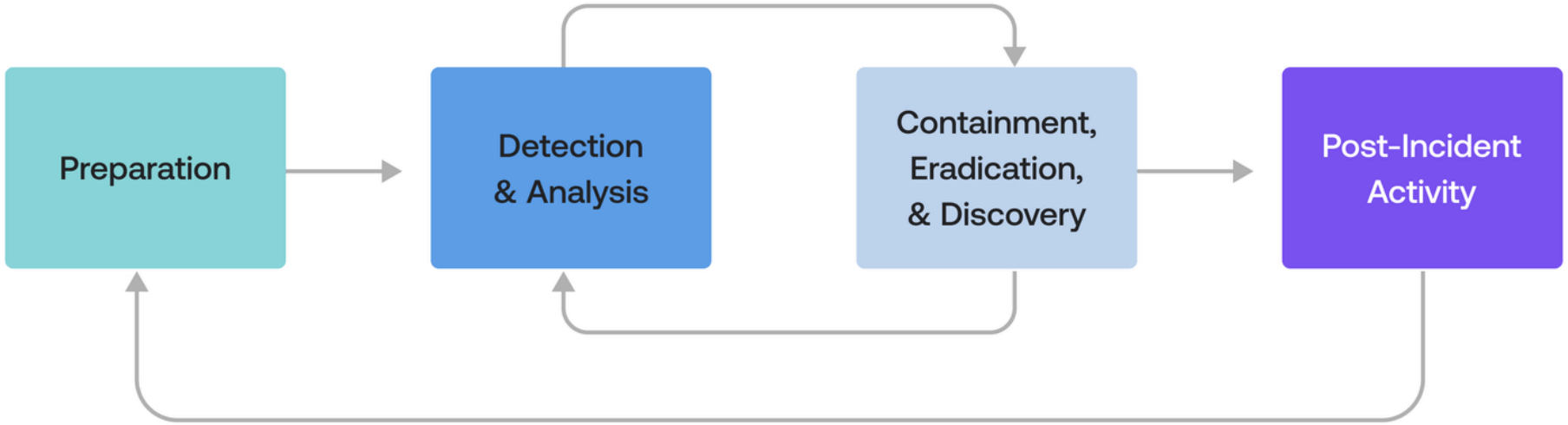


Image source: NIST Incident Response: Your Go-To Guide to Handling Cybersecurity Incidents

Choosing a Containment Strategy

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy
  - (e.g., partial containment, full containment)
- Duration of the solution
  - (e.g., **emergency workaround** to be removed in four hours, **temporary workaround** to be removed in two weeks, **permanent solution**).

Containment Techniques

- **Segmentation**: Dividing networks into logical segments.
- **Isolation**: move compromised systems to a network completely disconnected from the main network.
- **Removal**: Completely disconnects impacted systems from any network to cut off the attacker's access.

Incident Eradication & Recovery

- Eradication Goals:
  - Remove incident traces.
  - Secure user accounts, system configs.
- Recovery Objectives:
  - Restore normal operations.
  - Simultaneous activities with eradication.
- Rebuild systems to prevent backdoors.
- Media Sanitization Techniques: Clear, Purge, Destroy

Validation Process

- Verify the secure configuration of every system
- Run the vulnerability scans
- Perform account and permission reviews
- Verify that systems are logging and communication to the SIEM

Post-mortem Best Practices

- Don’t assign blame
- Do take responsibility
- Don’t procrastinate
- Do gather information
- Don’t be vague
- Do define clear owners
- Don’t lose focus
- Do use a consistent template

Log Tampering

- Why would malicious users/malwares want to tamper with logs?
- What are some processes mentioned in this article that hackers might do for log tampering?
- From this list look up some Event IDs that might indicate log tempering

Logging Laws

- **Law of Collection**:

  "*Do NOT collect/generate log data that you NEVER plan to use.*"

- **Law of Retention**:

  "*Retain log data for as long as it is conceivable that it can be used—or longer if prescribed by regulations.*"

- **Law of Monitoring**:

  "*Log all you can (which is as much as possible), but alert only on what you must respond (which is as little as possible).*"

Logging Laws (Cont.)

- **Law of Availability**:

  "*Don't pay to make your logging or monitoring system more available than your business systems.*"

- **Law of Security**:

  "*Don't pay to protect your log data more than you pay to protect your critical business data.*"

- **Law of Constant Changes**:

  "*Logs sources, log types, and log messages change.*"

Backups

- How are **full**, **differential**, and **incremental** backups different?
- How many backup files are needed for recovery from each kind of backup?
- How would you sort different kinds of backups according to following criteria:
  - Storage capacity, Recovery speed, Backup time

Lab 4

- Locate log files and their configuration on a Linux machine
- Perform manual log query to extract useful information from the logs

Assignment 1

- Keep Secrets Secret!
- How to avoid leaking credentials?

  “Keep secrets out of your source code”
- Due next week and individual