# Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are a critical component of cybersecurity, monitoring networks and systems for unauthorized access or suspicious activity. By detecting and alerting on potential threats, IDS help organizations maintain the integrity and confidentiality of their digital assets.

**MRUNAL SINGH**

# WORKFLOW

**Data Collection:**

- The IDS collects data (network traffic or system logs).

**Data Analysis:**

- The IDS analyzes the data by comparing it with known signatures or detecting anomalies.

**Threat Detection:**

- The IDS identifies potential threats based on deviations from expected behavior or rule violations.

**Alert Generation:**

- The IDS sends an alert to the system administrator for further investigation and response.

**Response Action (Optional):**

- In some advanced systems (intrusion prevention systems), it might take immediate action, such as blocking traffic or isolating a system.

# TYPES OF IDS

**Network-based IDS (NIDS):**

- Monitors traffic on an entire network.
- Detects threats like DDoS attacks, malware, etc.

**Host-based IDS (HIDS):**

- Installed on individual systems (hosts).
- Monitors system calls, file modifications, etc.
- Include a comparison chart or table for clarity.

# Network-based IDS

## Definition

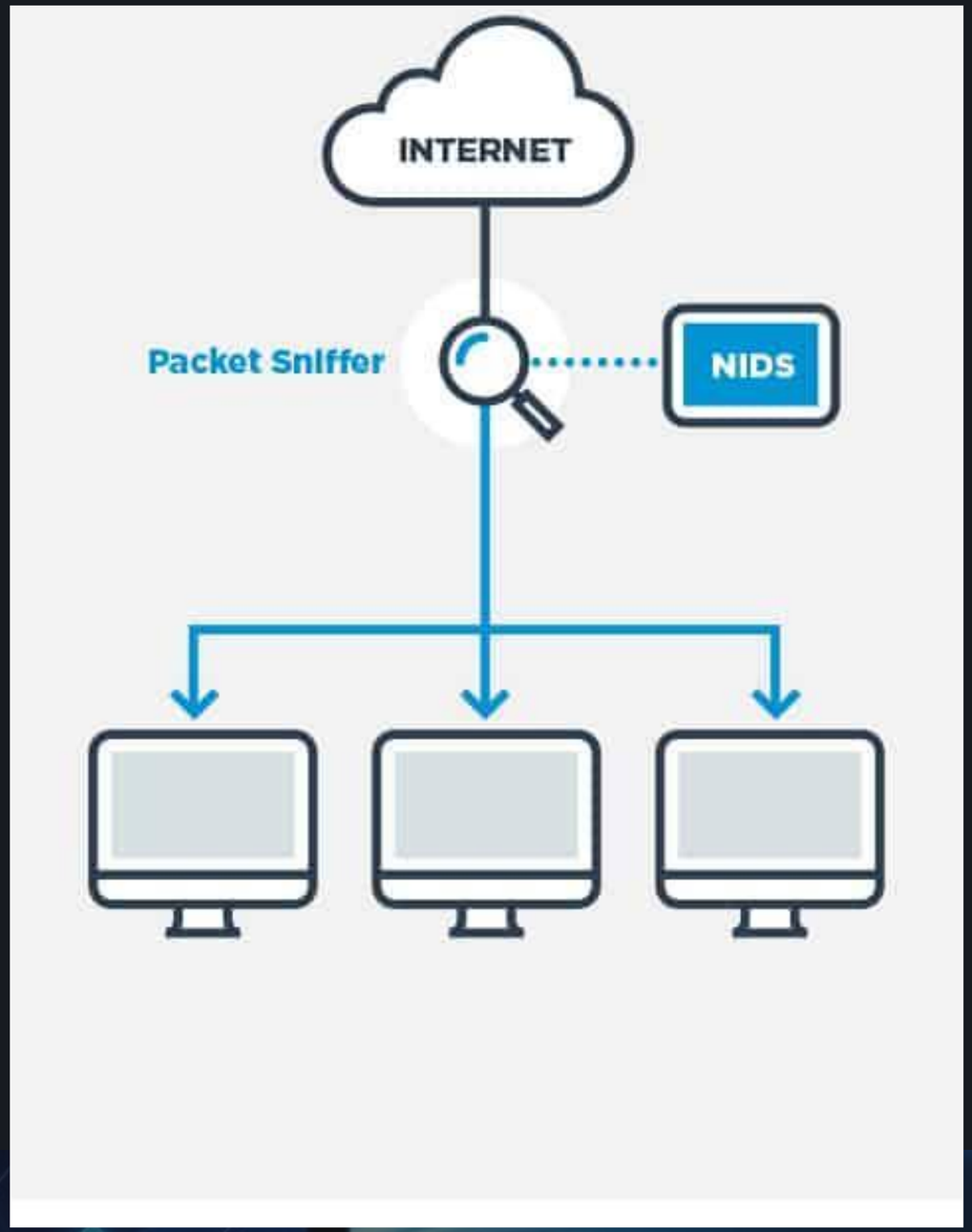
Network-based IDS monitor network traffic, analyzing packets to identify potential intrusions.

## Placement

Network-based IDS are typically deployed at strategic points within the network infrastructure.

## Advantages

Ability to detect attacks across the entire network, not limited to a single host.



# HOST-BASED IDS

1

## Definition

Host-based IDS monitor activity on individual computers or servers to identify potential threats.

2

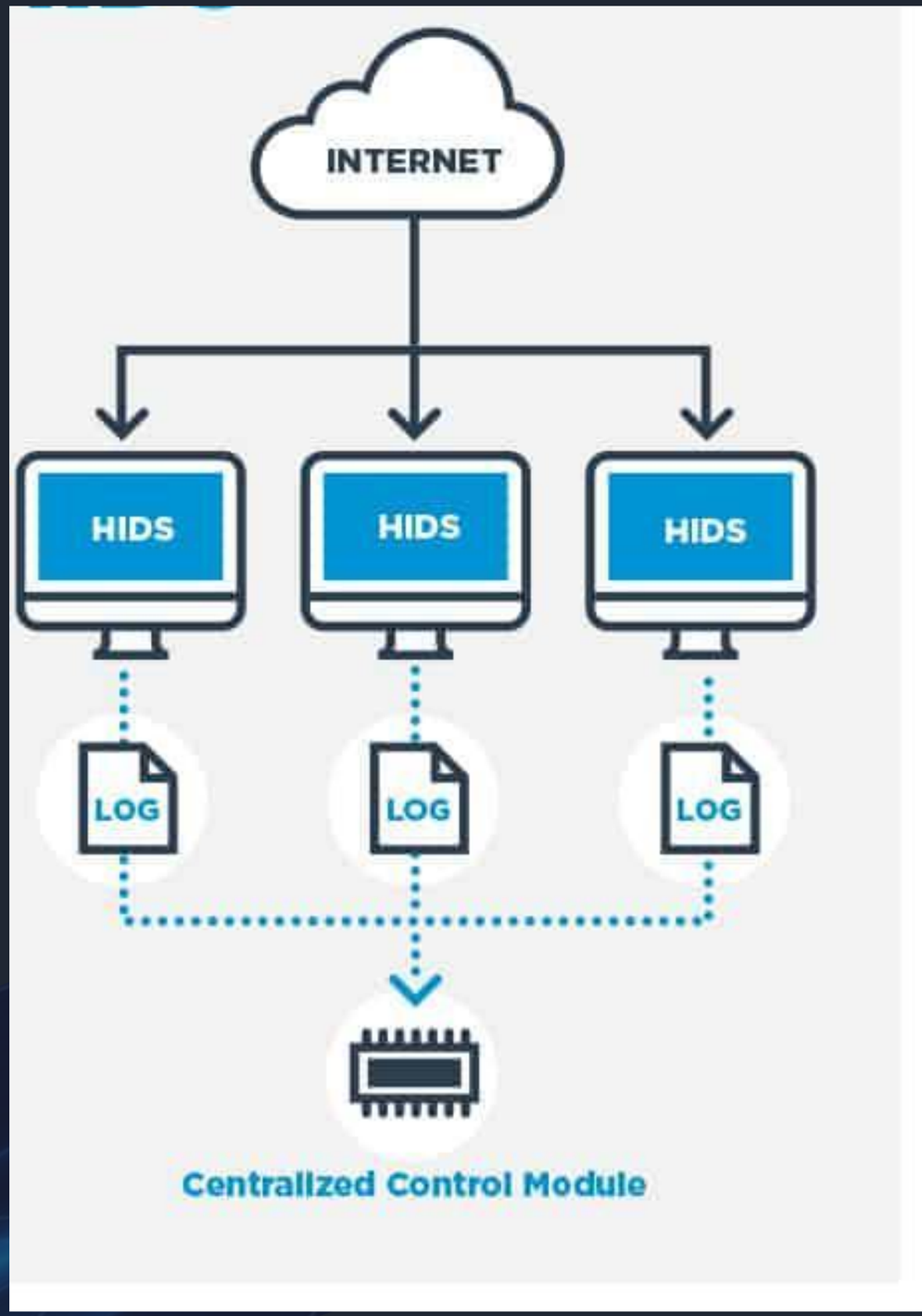
## Placement

Host-based IDS are installed directly on the systems they are designed to protect.

3

## Advantages

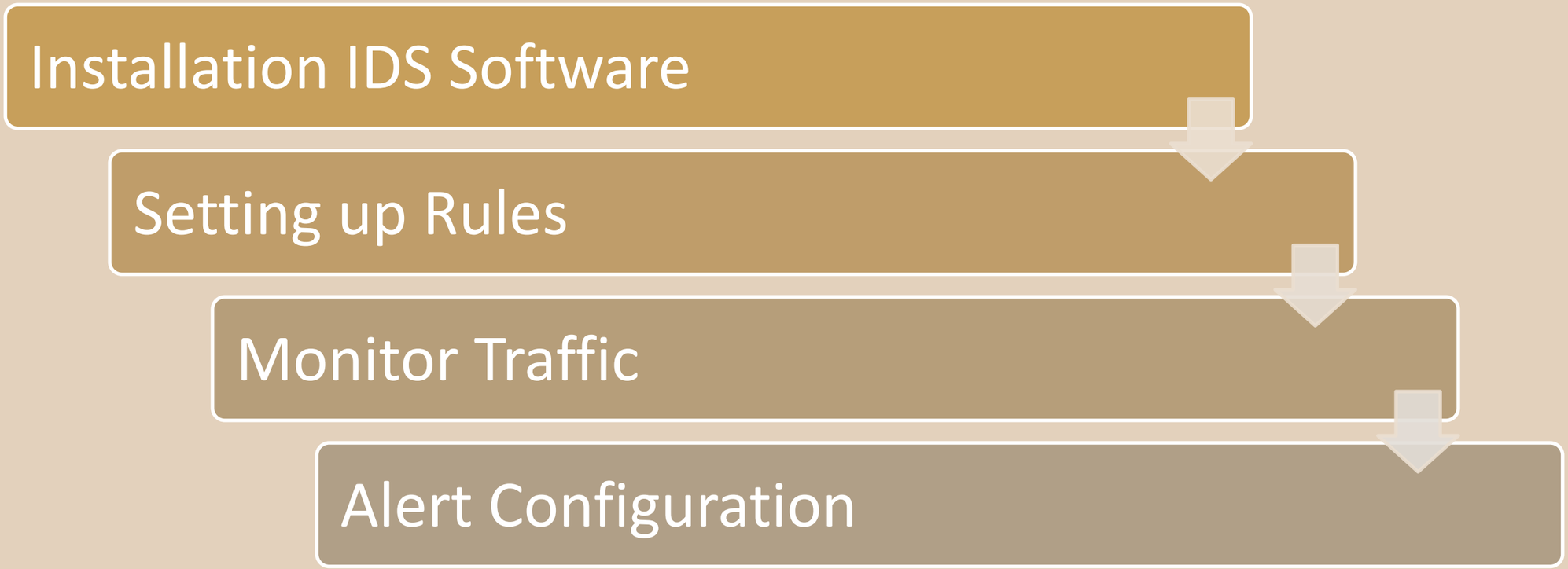
Can detect threats that may be missed by network-based IDS, such as insider threats or local attacks.



# CONFIGURING AN INTRUSION DETECTION SYSTEM (IDS)

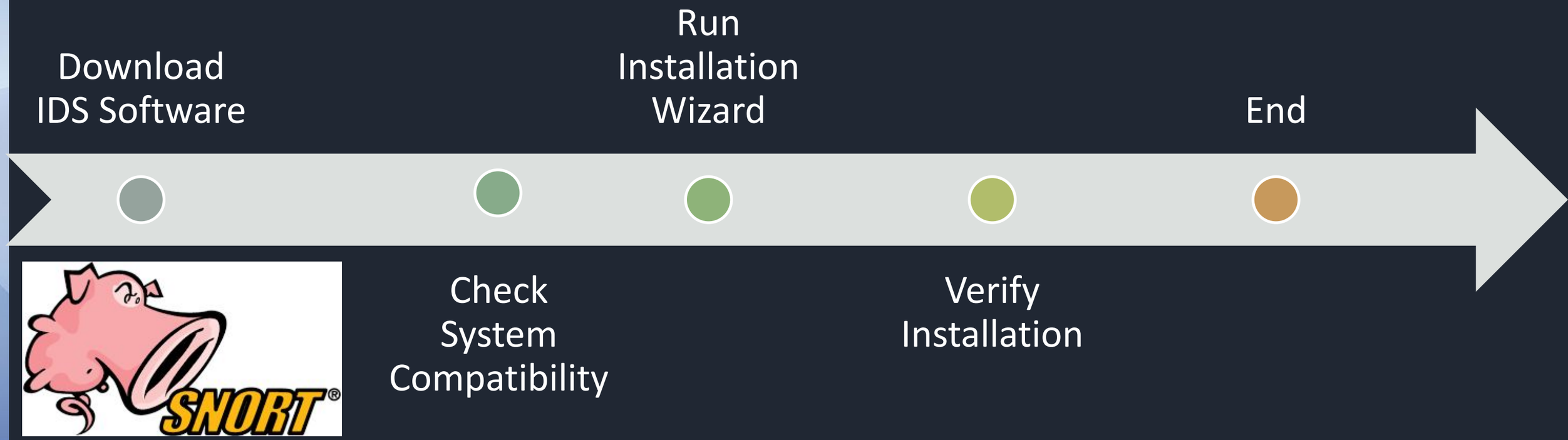
**INTRODUCTION**

Proper configuration of an Intrusion Detection System (IDS) is crucial for effective network and host security. This guide covers the essential steps for configuring both Network-based IDS (NIDS) and Host-based IDS (HIDS).



# INSTALATION

- Download IDS software (e.g., Snort for NIDS, OSSEC for HIDS)
- Follow vendor-specific installation instructions
- Ensure compatibility with your operating system and hardware



# Configuring Network-based IDS

## Sensor Placement

Deploy network sensors at key network choke points to maximize visibility and coverage.

## Rule Configuration

Carefully craft IDS rules to detect known attack signatures and anomalous behavior.

## Tuning and Optimization

Continuously monitor and adjust IDS configurations to minimize false positives and improve detection accuracy.

## Integration

Integrate the network IDS with other security tools for enhanced threat detection and response.

# Configuring Host-based IDS

## Agent Installation

Deploy the host-based IDS agent on each targeted system to monitor local activity.

## Policy Configuration

Define host-based IDS policies to detect suspicious user actions and file modifications.

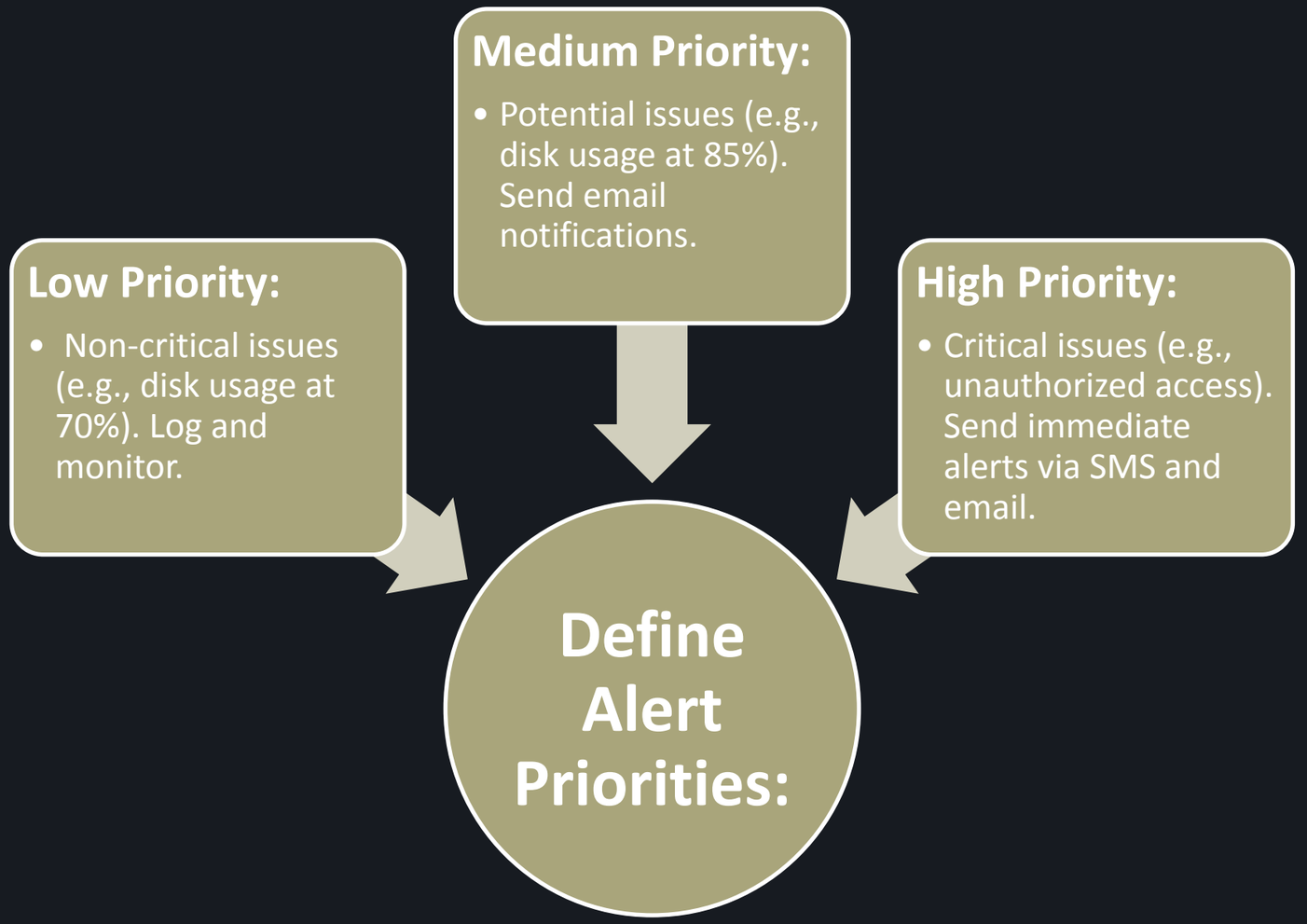
## Logging and Reporting

Configure comprehensive logging and generate alerts for security events on the host.

## Automated Response

Implement automated response actions to quickly mitigate detected threats on the host.

# ALERT CONFIGURATION SIMPLIFIED



# USING IDS FOR MAX. PROTECTION

# Advantages and Disadvantages of IDS Types

## 1 Network-based IDS

Advantages: Comprehensive network visibility, can detect a wide range of attacks. Disadvantages: May miss threats specific to individual hosts, can be resource-intensive to deploy and manage.

## 2 Host-based IDS

Advantages: Able to detect local threats, can provide detailed event logging. Disadvantages: Limited to individual hosts, can be complex to configure and maintain across multiple systems.

# Monitoring and Analysing IDS Alerts

1

## Alert Aggregation

Collect and consolidate IDS alerts from network and host-based systems.

2

## Alert Prioritization

Analyze and prioritize alerts based on severity, threat intelligence, and potential impact.

3

## Incident Response

Investigate high-priority alerts and initiate appropriate incident response procedures.

# Best Practices for Effective IDS Implementation

| | |
|---|---|
| Comprehensive Coverage | Deploy both network-based and host-based IDS to maximize visibility and protection. |
| Continuous Tuning | Regularly review and fine-tune IDS configurations to minimize false positives and improve detection accuracy. |
| Threat Intelligence | Integrate threat intelligence to enhance IDS capabilities and stay ahead of evolving threats. |
| Incident Response | Establish well-defined incident response protocols to effectively investigate and mitigate detected threats. |