IDS TECHNOLOGIES

Sahil Pokharkar (21102A0006)
Deep Salunkhee (21102A0014)
Omkar Patil (21102A0003)
Pranav Redij (21102A0005)

OBJECTIVES

Section 1: Introduction to IDS Technologies

- Overview of IDS technologies
- Typical components
- Network architectures in the context of IDS

Section 2: Security Capabilities of IDS

- Security Capabilities
  - Information Gathering
  - Logging Capabilities
  - Detection & Prevention Capabilities

SECTION 3: ADVANCED IDS TECHNOLOGIES

- Intrusion Prevention Systems (IPS)
- Network Protocol based IDS
- Hybrid based IDS

Section 4: Analysis Schemes for Intrusion

- Analysis Schemes for Instrusion
- Model Intrusion analysis

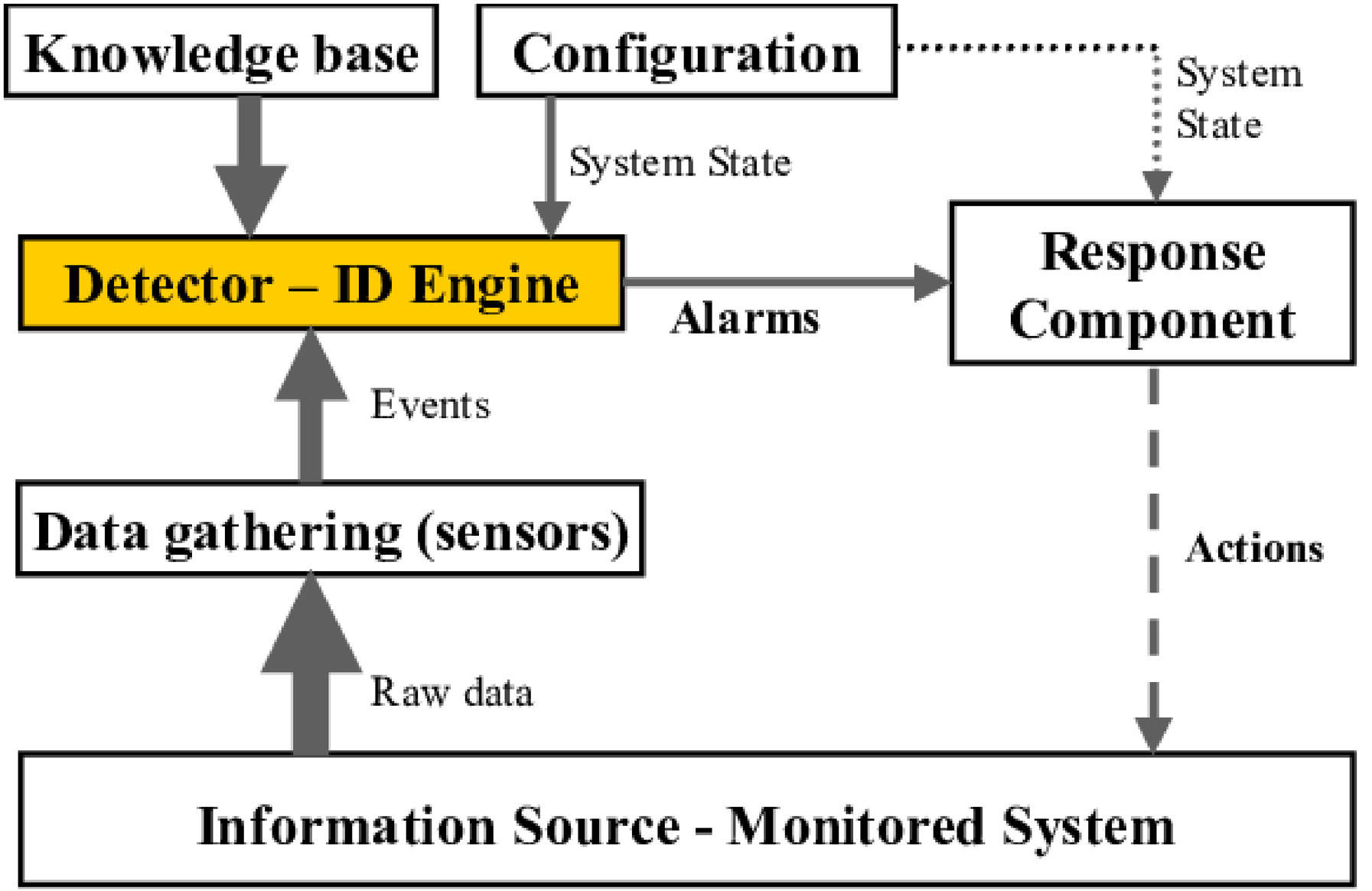
Section 5: Security Assessments

- Techniques for Intrusion Analysis
- Mapping Responses to Policy
- Vulnerability Analysis
- Credential Analysis

SECTION 1: INTRODUCTION TO IDS TECHNOLOGIES

1.1 OVERVIEW OF IDS TECHNOLOGIES

Intrusion Detection System (IDS) is a security technology that monitors network or system activities for malicious or suspicious behavior. It identifies potential security threats, such as unauthorized access attempts, malware infections, or abnormal network traffic patterns, by analyzing collected data against predefined rules or signatures. IDS helps organizations detect and respond to security incidents promptly, enhancing overall cybersecurity posture

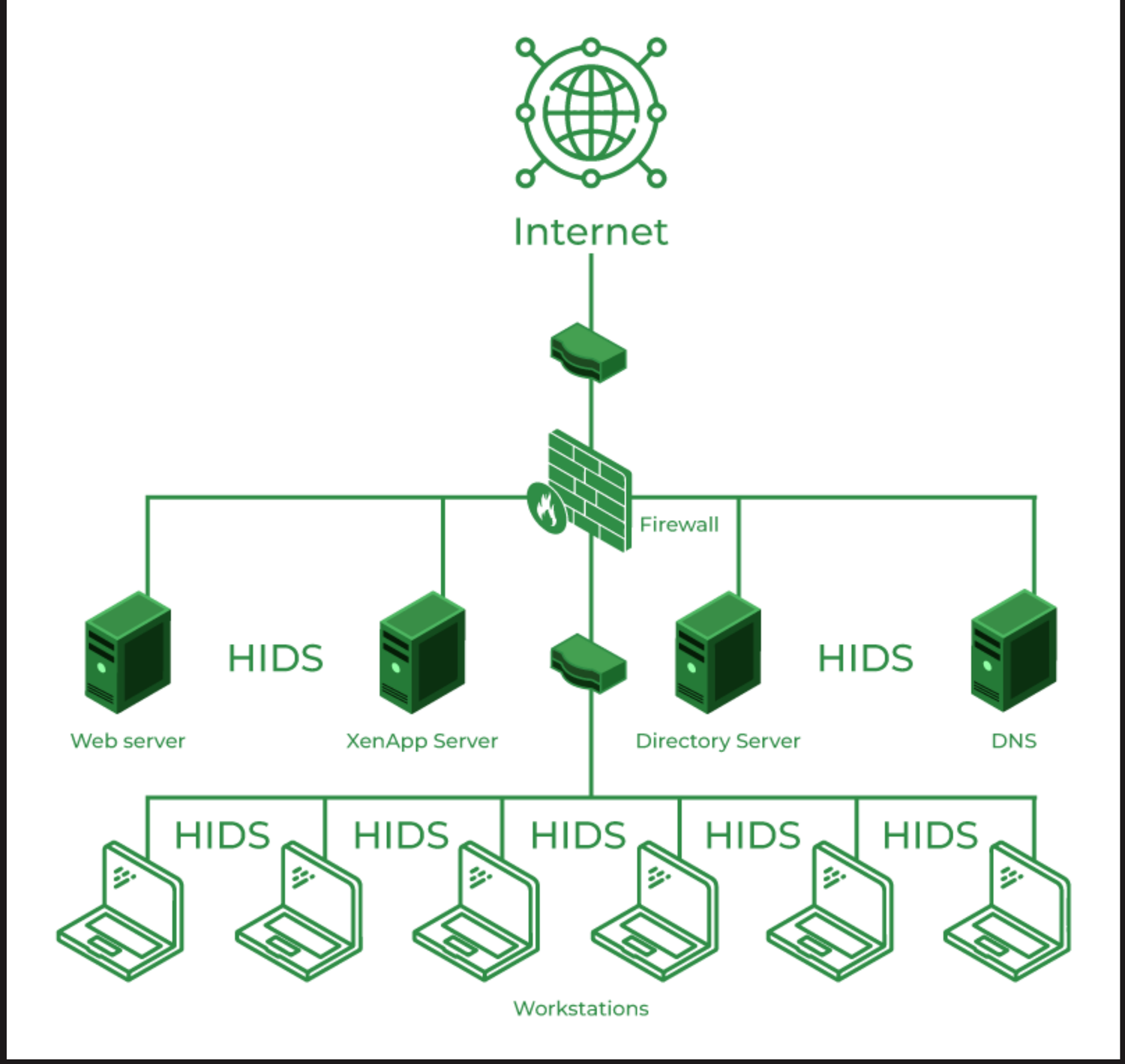

Knowledge base
Configuration
System State
System State
Detector – ID Engine
Alarms
Response Component
Events
Data gathering (sensors)
Actions
Raw data
Information Source - Monitored System

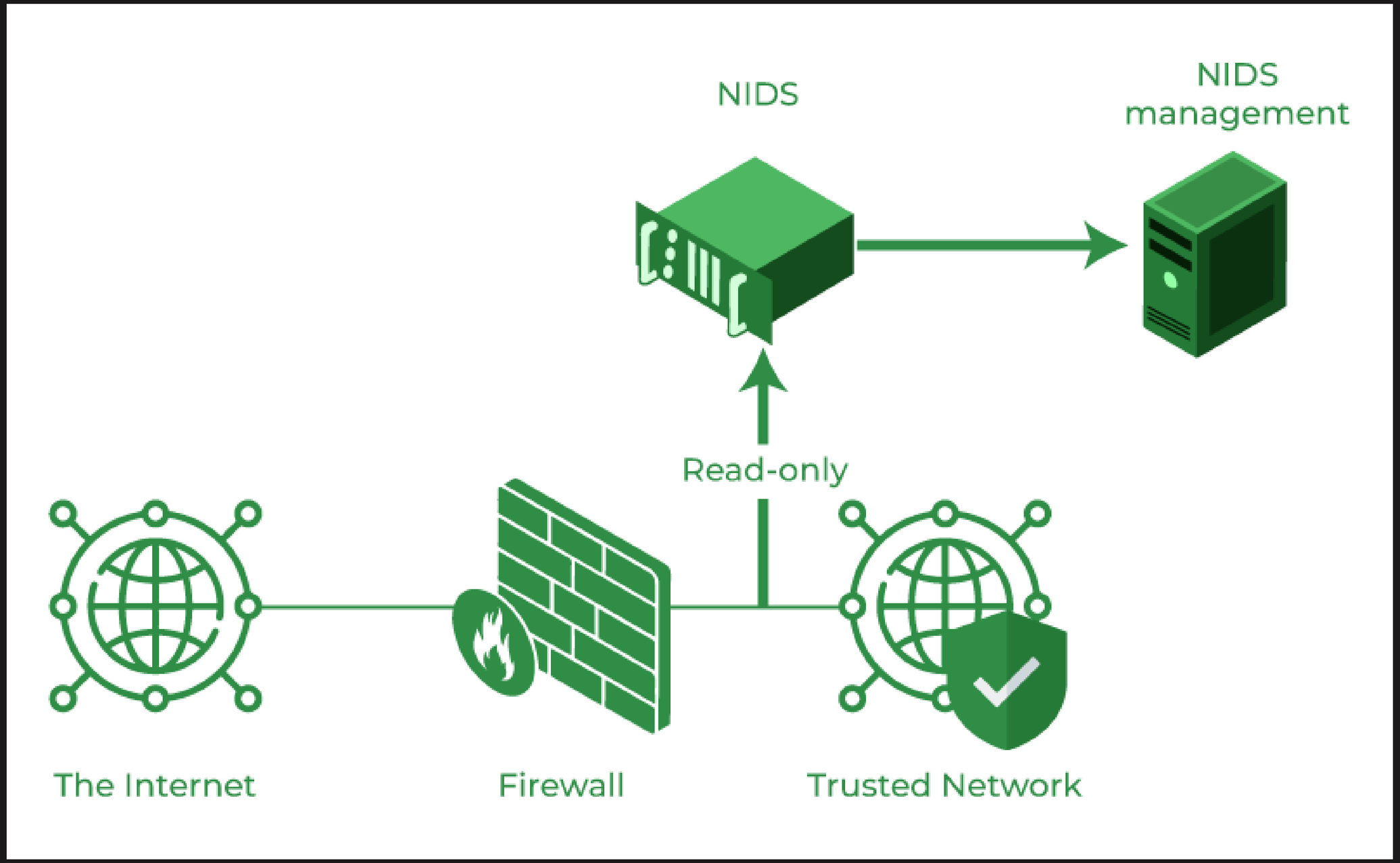
1.2 TYPICAL COMPONENTS

sensors (hardware or software)
analyzers
consoles

1.3 NETWORK ARCHITECTURES IN THE CONTEXT OF IDS

host-based
network-based
hybrid IDS setups


Internet
Firewall
HIDS
HIDS
Web server
XenApp Server
Directory Server
DNS
HIDS
HIDS
HIDS
HIDS
HIDS
Workstations


NIDS
NIDS management
Read-only
The Internet
Firewall
Trusted Network

SECTION 2: SECURITY CAPABILITIES OF IDS

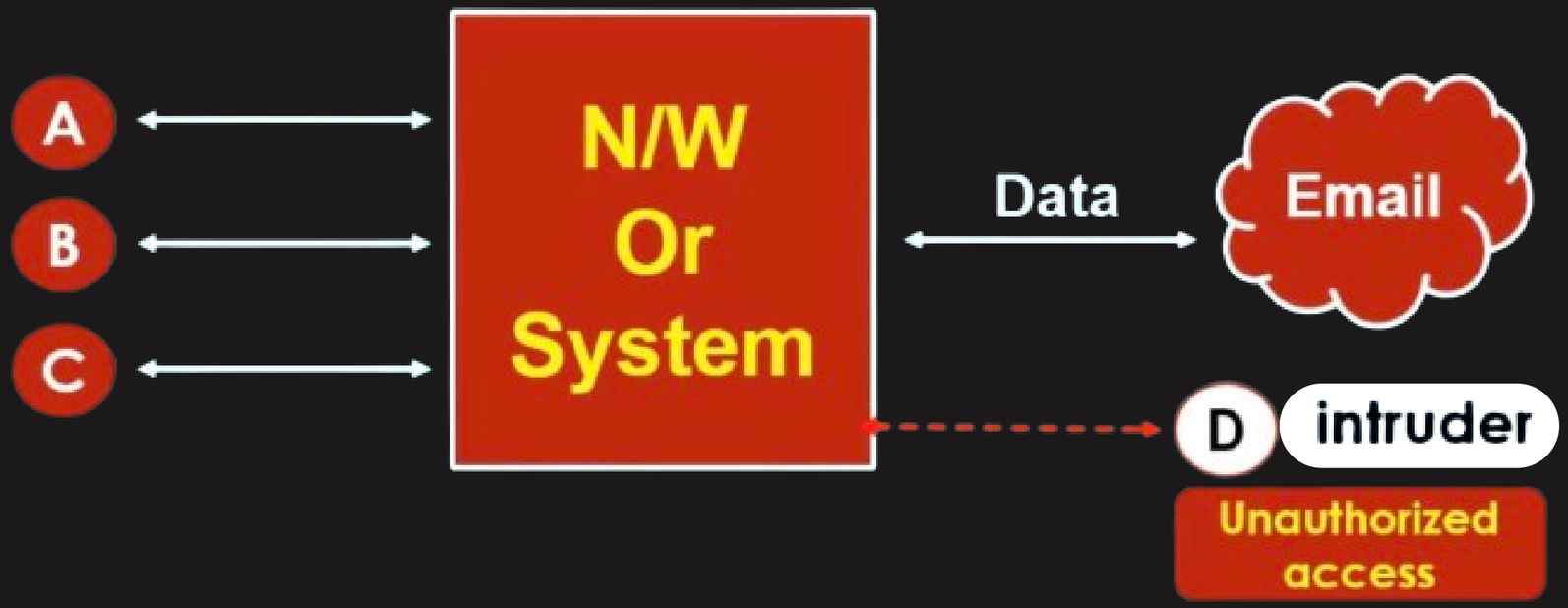
2.1 SECURITY CAPABILITIES

- Information Gathering
- Logging Capabilities
- Detection & Prevention Capabilities

SECTION 3: ADVANCED IDS TECHNOLOGIES

INTRUSION

intruder’s -> intrusion
(ghuskhor) (ghuskhori kar raha)



Real life and funny example to understand

difference

B/W

FIREWALL,IDS and IPS

Intruder’s

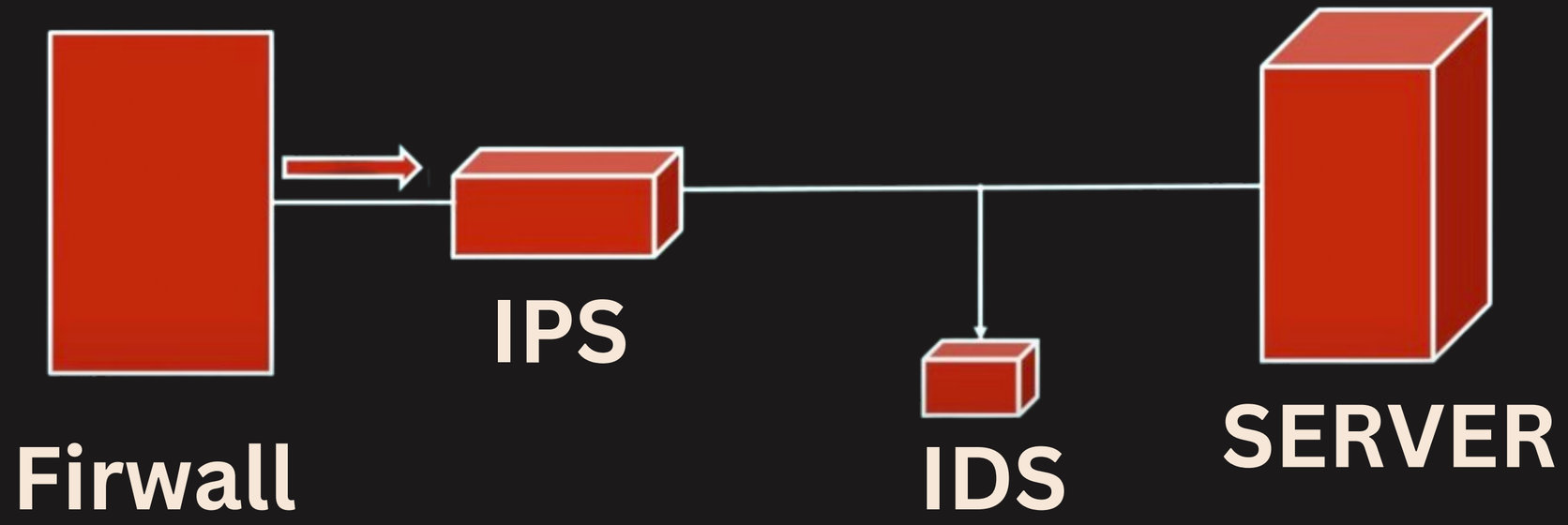

FIREWALL
they are INTRUDER'S
they are
AUTHORIZED USERS
अरे! ओ उंकल

IDS(intrusion detection system)

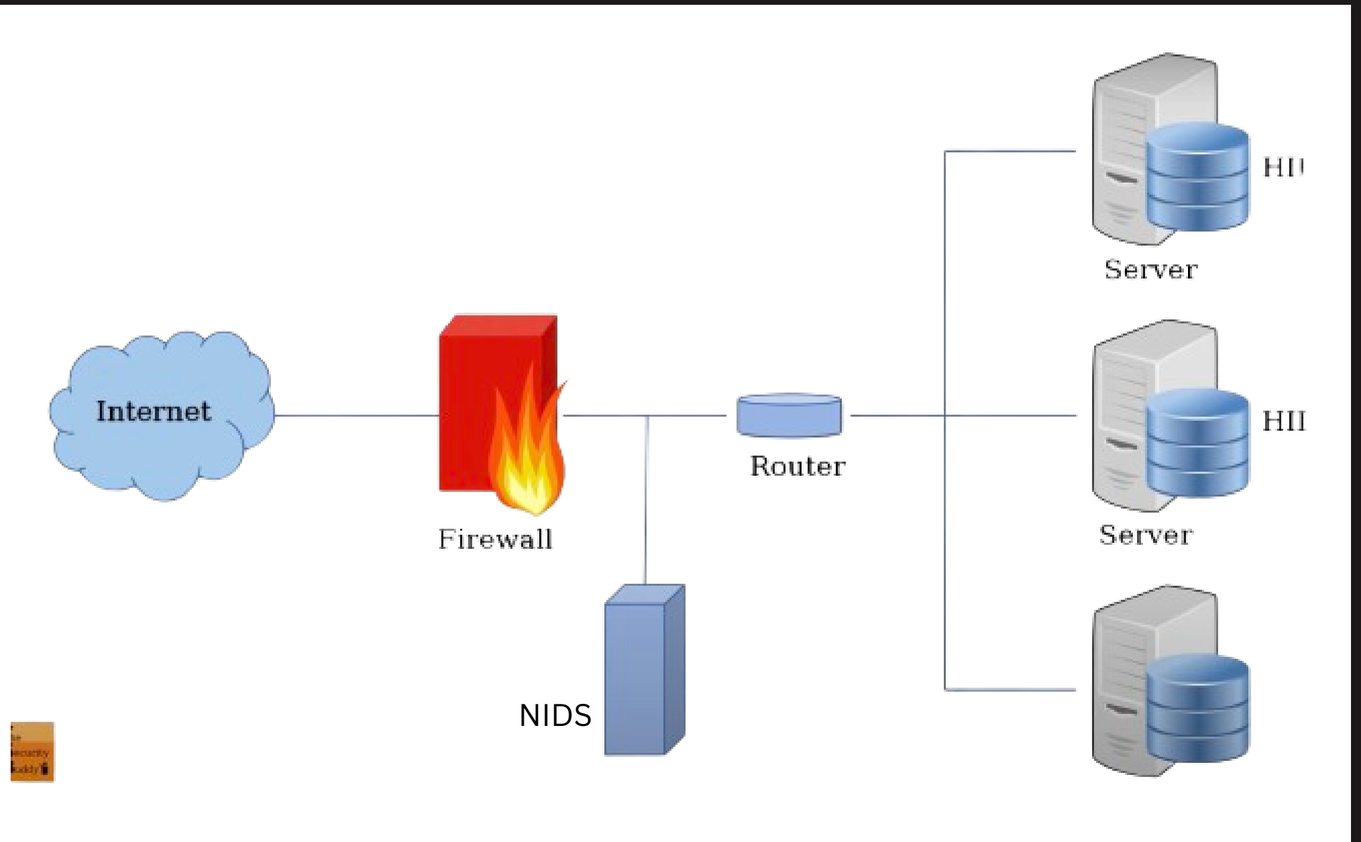
IPS(intrusion prevention system)

3.1 INTRUSION PREVENTION SYSTEMS (IPS)

These systems not only detect but also actively prevent intrusions by blocking or filtering malicious traffic.



3.2 NETWORK PROTOCOL BASED IDS

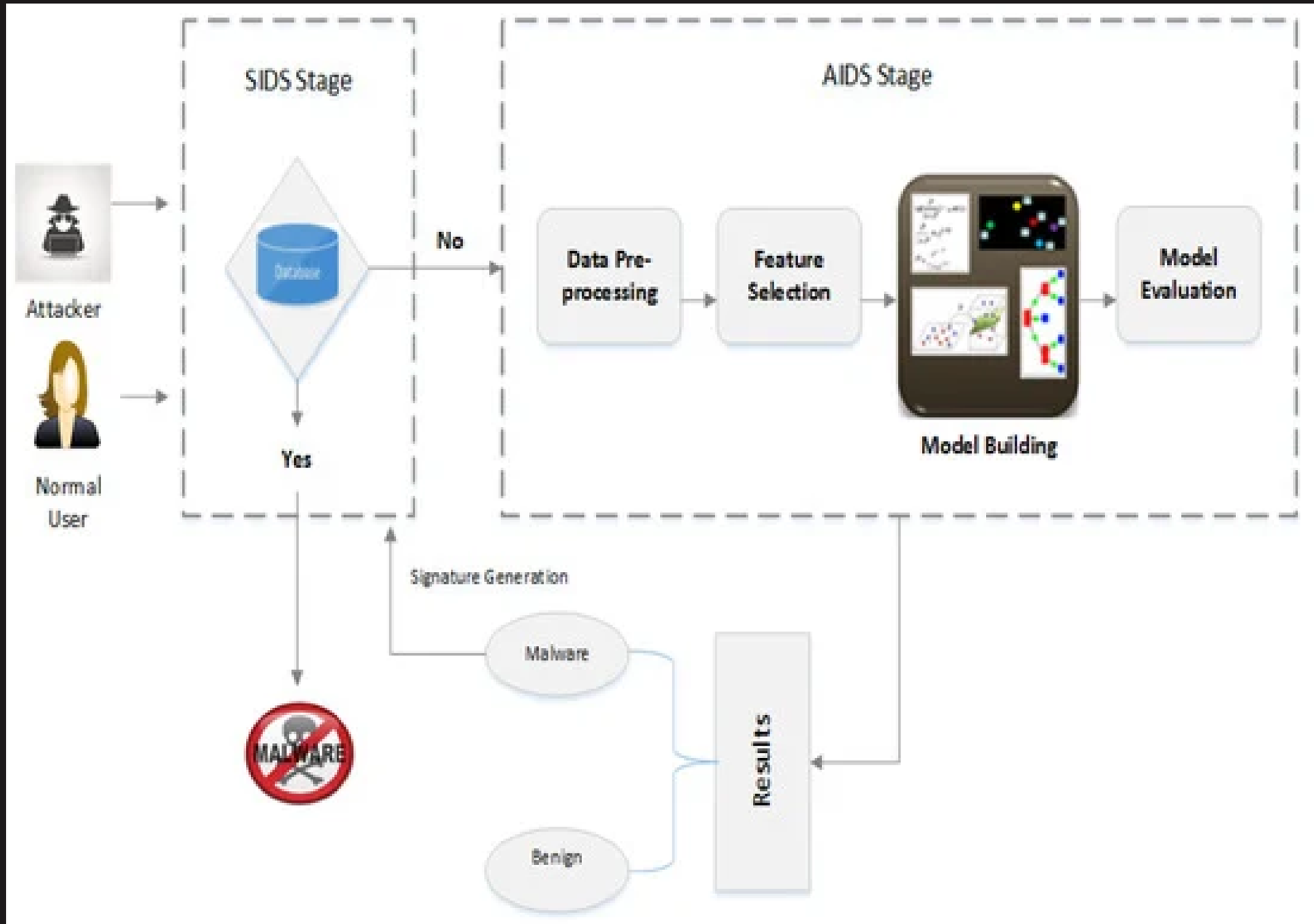


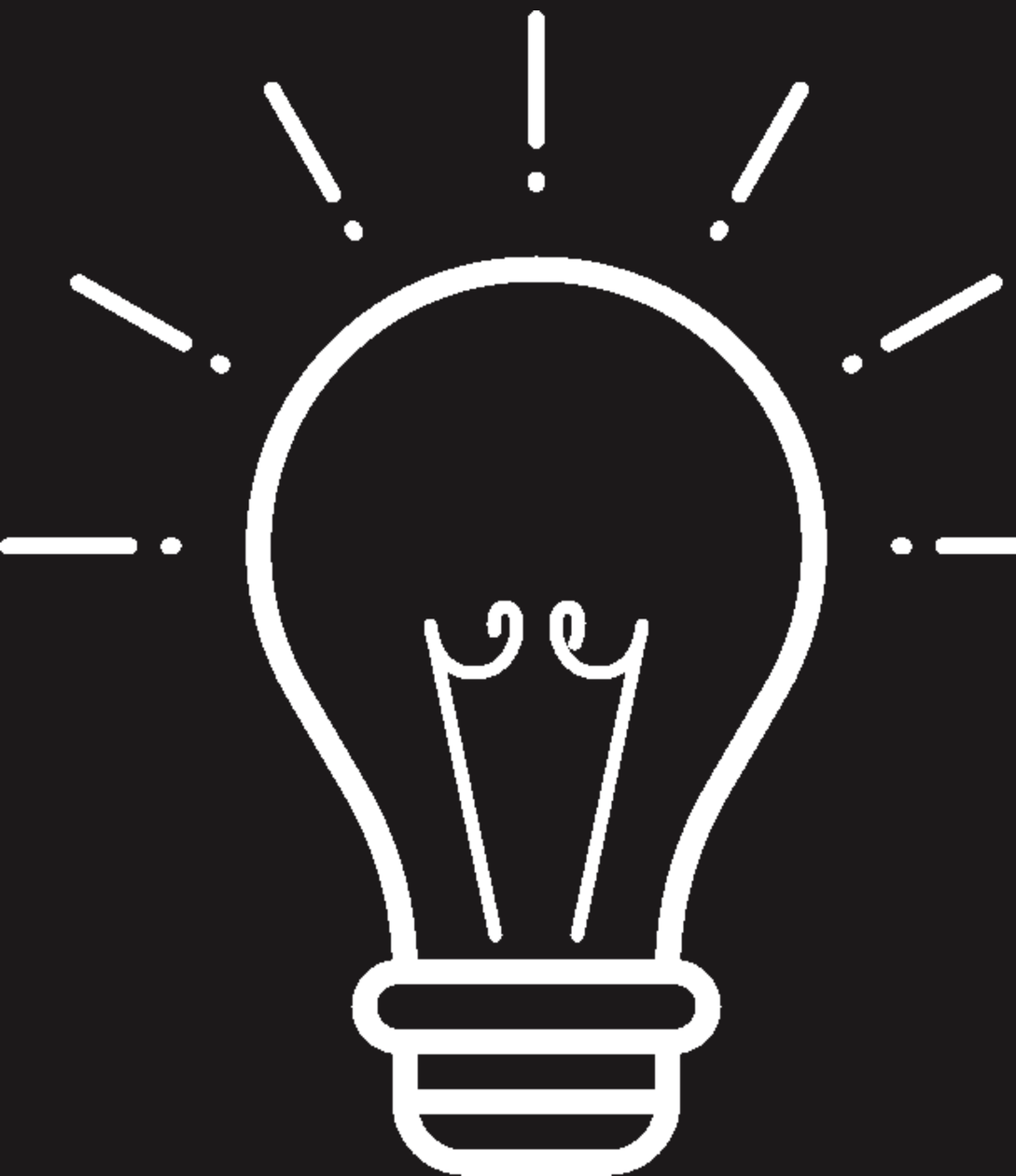
examines network traffic, protocols, and behaviors to identify and alert administrators to suspicious activities or potential security threats within the overall network.

- eg.The IDS, monitoring HTTP behavior, detects an anomaly: an HTTP request attempting to access data without going through the usual login process.

3.3 HYBRID IDS

Hybrid IDS is developed to integrates (signature)SIDS and (anomaly)AIDS to detect both unknown and known attacks.





SECTION 4: ANALYSIS SCHEMES FOR INTRUSION

4.1 ANALYSIS SCHEMES FOR INSTRUSION

- Intrusion analysis involves examining the data collected by the IDS to determine the nature and severity of detected threats.
- IDS typically employs various analysis schemes such as signature-based analysis, anomaly-based analysis, or stateful protocol analysis to identify potential intrusions.

4.2 WHY ANALYSIS SCHEMES ?

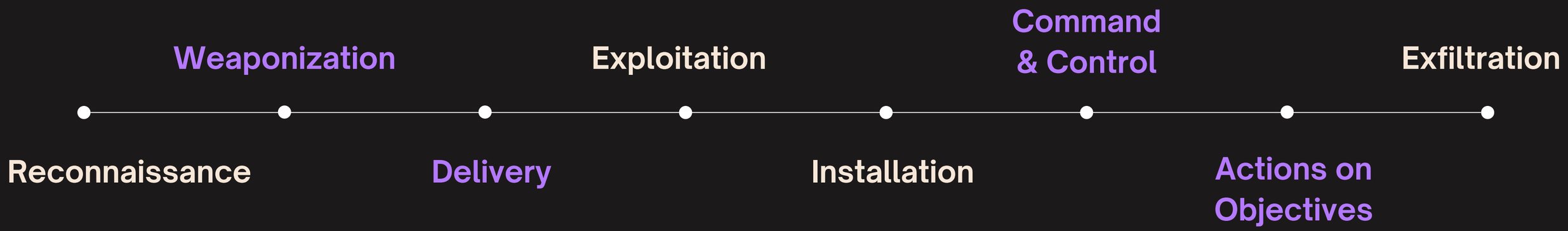
- Threat Detection
- Contextual Awareness
- Early Warning System
- Comprehensive Protection
- Investigation Aid

4.3 CYBER KILL CHAIN MODEL

- The Cyber Kill Chain model is a framework developed by Lockheed Martin to illustrate the lifecycle of a cyber attack. It provides a structured approach for understanding the various steps that an attacker typically goes through during the course of an intrusion.

- By analyzing the attack lifecycle, organizations can better detect, prevent, and respond to cyber threats, thereby enhancing their overall cybersecurity posture.

4.3 STEPS CYBER KILL CHAIN MODEL



1. Reconnaissance: Attackers gather information about the target organization, including network architecture and potential vulnerabilities.

2. Weaponization: Attackers create or obtain malware to exploit identified vulnerabilities.

3. Delivery: Malware is delivered to the target environment through various means like phishing emails or malicious websites.

4. Exploitation: Vulnerabilities within the target environment are exploited to gain unauthorized access.

5. Installation: Attackers install and execute malicious code or tools on compromised systems to establish persistence.

6. Command and Control (C2): Attackers establish communication channels with external servers to remotely manage compromised systems.

7. Actions on Objectives: Attackers carry out their intended goals, such as data theft or disruption of operations.

8. Exfiltration: Stolen data is transferred out of the target environment to complete the intrusion cycle.

SECTION 5: SECURITY ASSESSMENTS

5.1 TECHNIQUES FOR INTRUSION ANALYSIS

- Log Analysis
- Network Traffic Analysis
- Memory Forensics
- Attacker Profiling
- Endpoint Detection and Response (EDR)
- Threat Intelligence

5.2 MAPPING RESPONSES TO POLICY

- Identify relevant policies: Align incident response actions with established policies like AUP, SIRP, and data breach notification policies.
- Map policies to response actions: Create a clear matrix linking specific response actions to the policies they uphold.
- Train and communicate: Educate all personnel on policy alignment to ensure everyone understands their roles and response actions.
- Benefits:
- 1. Consistency: Uniform approach to handling incidents.
- 2. Efficiency: Streamlined response process.
- 3. Transparency: Builds trust through adherence to established policies.

5.3 VULNERABILITY ANALYSIS

- Proactive Security Measures: Highlight the proactive nature of vulnerability analysis in identifying and addressing weaknesses before they can be exploited.
- Tools and Methodologies: common tools and methodologies used for vulnerability analysis (e.g., vulnerability scanners, penetration testing).
- Risk Mitigation: Emphasize how vulnerability analysis contributes to risk mitigation and overall security enhancement.

5.4 CREDENTIAL ANALYSIS

- Authentication Security: Stress the importance of secure authentication mechanisms and the role of credential analysis in maintaining their integrity.
- Common Vulnerabilities: common vulnerabilities associated with credentials, such as weak passwords, credential reuse, and password storage practices.
- Access Control Enhancement: effective credential analysis contributes to strengthening access controls and preventing unauthorized access.

Thank you!