PROBLEM STATEMENT 3

Approach for application development that leads to applications having features to detect, report and respond to attempts of attacks.

TYPES OF ATTACKS:

Classification of attacks based on the attack vector and the target areas

- Network Based attacks
- Database Based attacks
- Application Based attacks
- Host Based attacks

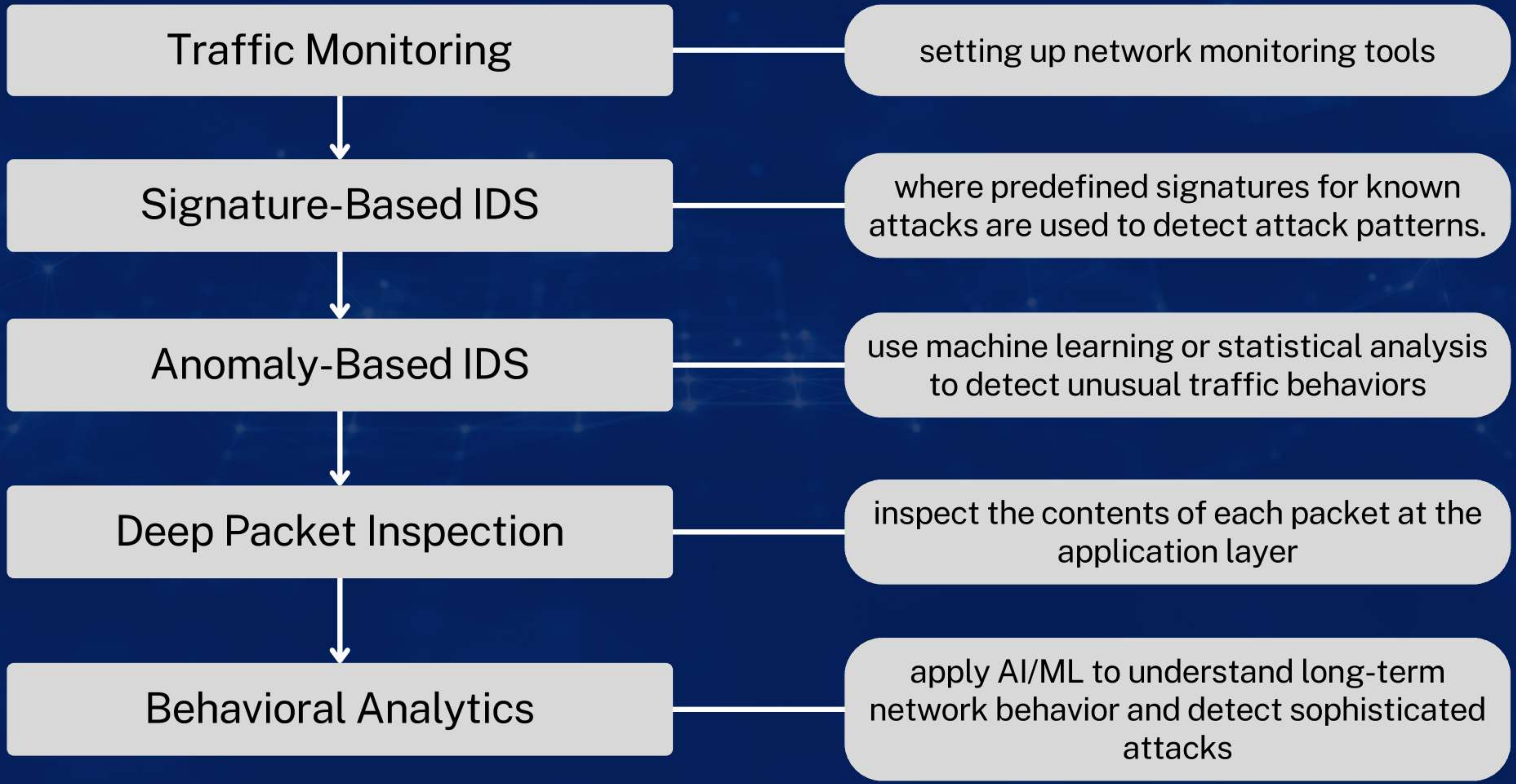
NETWORK BASED ATTACKS:

- Attacks focus on compromising the network infrastructure, including routers, switches, communication channels, and network protocols.
- They aim to disrupt or gain unauthorized access to a network or intercept data transmitted between systems.

Some of the common network based attacks include Denial of Service (DoS) and Distributed Denial of Service (DDoS), Port Scanning, SYN flood etc.

NETWORK BASED ATTACKS:

Detecting:



Traffic Monitoring — setting up network monitoring tools

Signature-Based IDS — where predefined signatures for known attacks are used to detect attack patterns.

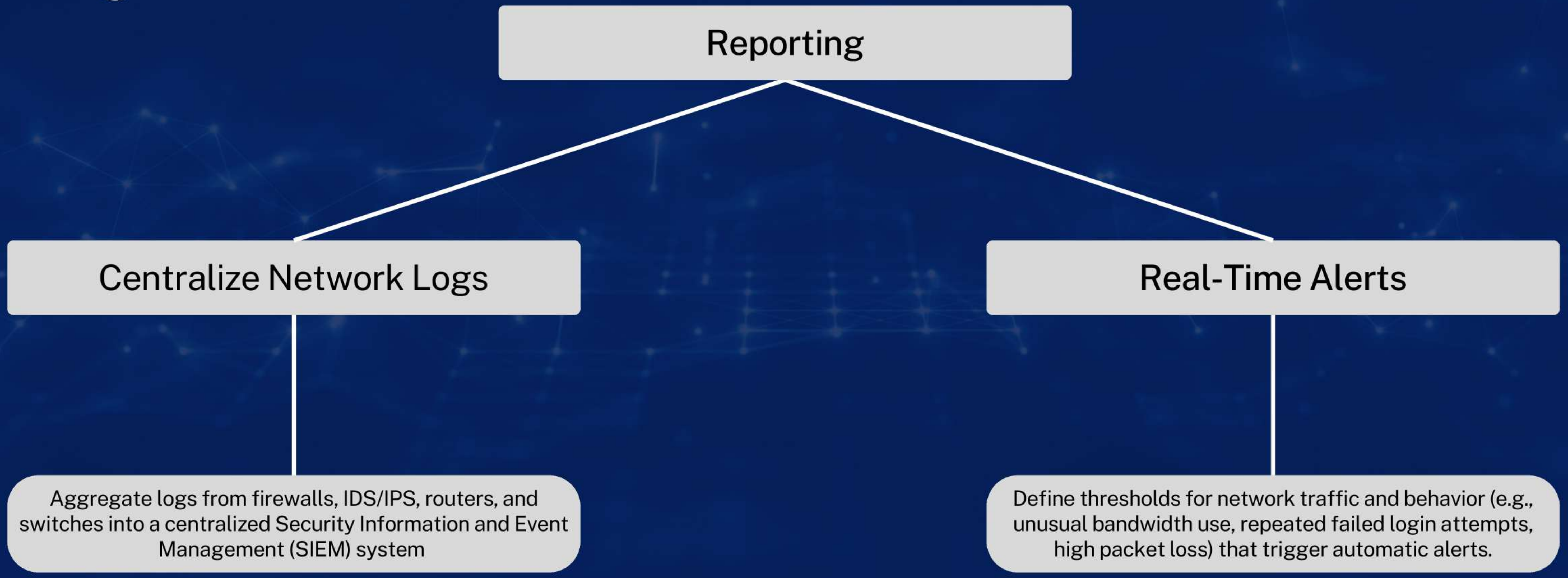
Anomaly-Based IDS — use machine learning or statistical analysis to detect unusual traffic behaviors

Deep Packet Inspection — inspect the contents of each packet at the application layer

Behavioral Analytics — apply AI/ML to understand long-term network behavior and detect sophisticated attacks

NETWORK BASED ATTACKS:

Reporting:



Reporting

Centralize Network Logs

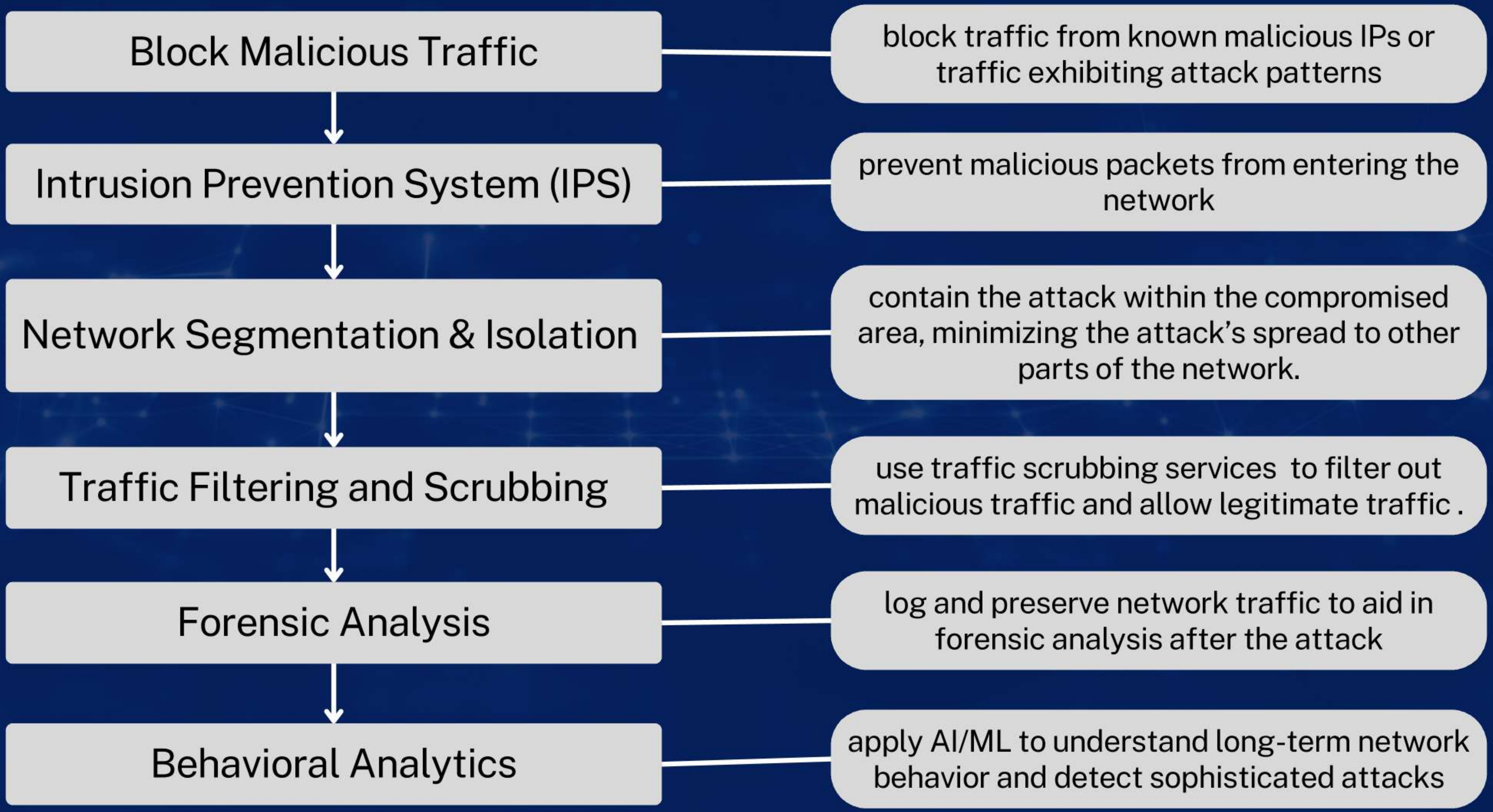
Aggregate logs from firewalls, IDS/IPS, routers, and switches into a centralized Security Information and Event Management (SIEM) system

Real-Time Alerts

Define thresholds for network traffic and behavior (e.g., unusual bandwidth use, repeated failed login attempts, high packet loss) that trigger automatic alerts.

NETWORK BASED ATTACKS:

Responding:



Block Malicious Traffic — block traffic from known malicious IPs or traffic exhibiting attack patterns

Intrusion Prevention System (IPS) — prevent malicious packets from entering the network

Network Segmentation & Isolation — contain the attack within the compromised area, minimizing the attack’s spread to other parts of the network.

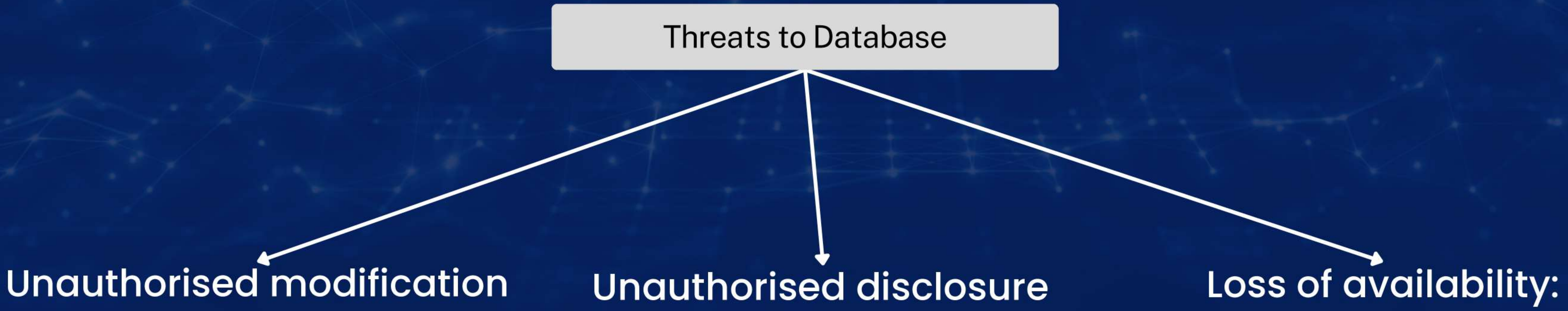
Traffic Filtering and Scrubbing — use traffic scrubbing services to filter out malicious traffic and allow legitimate traffic .

Forensic Analysis — log and preserve network traffic to aid in forensic analysis after the attack

Behavioral Analytics — apply AI/ML to understand long-term network behavior and detect sophisticated attacks

DATABASE BASED ATTACKS

- Attacks targeting databases that store structured or unstructured data.
- The aim is to extract, modify, or destroy data, often focusing on breaching the confidentiality, integrity, or availability of the database.



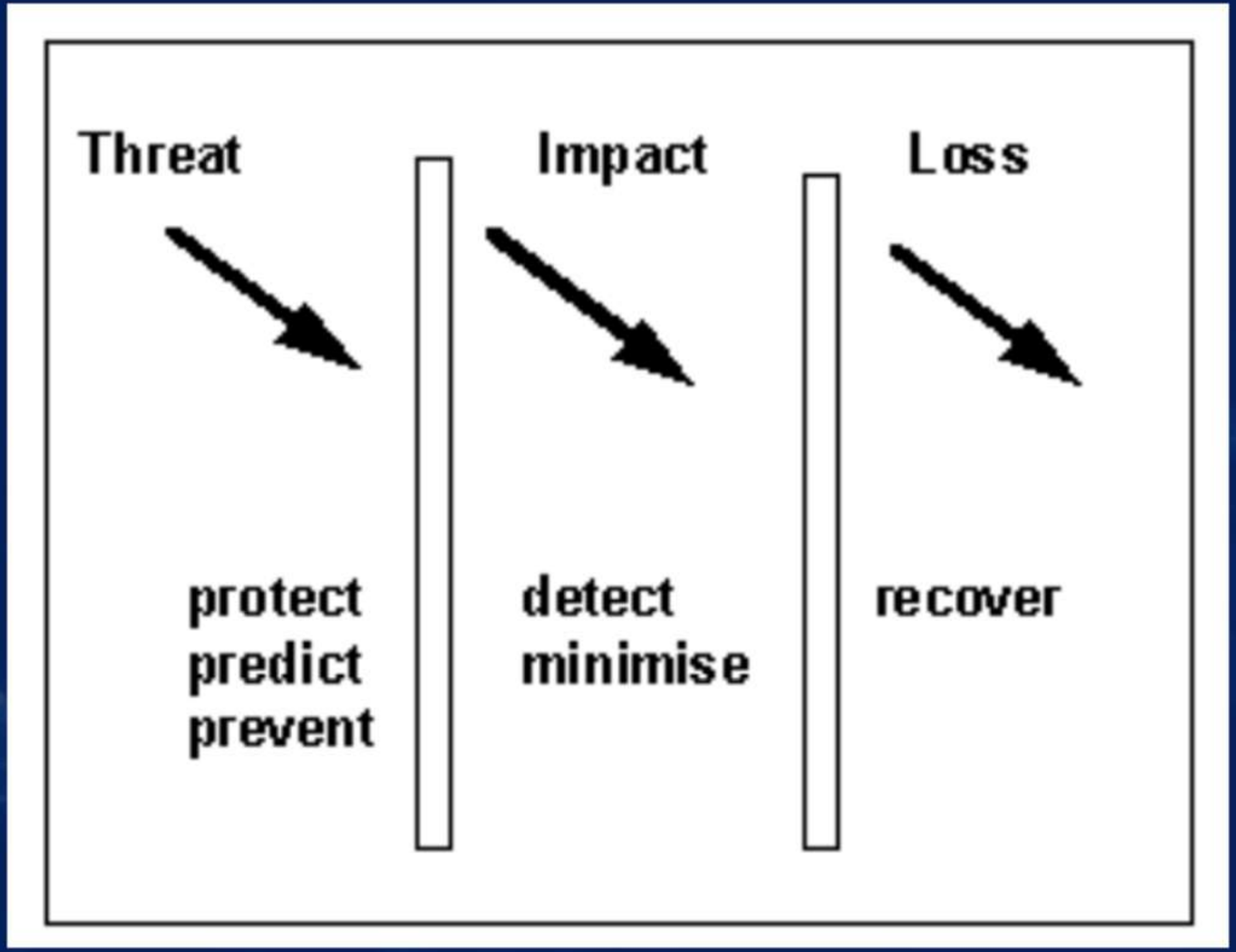
Threats to Database

Unauthorised modification

Unauthorised disclosure

Loss of availability:

PROBLEM	TOOL	TECHNIQUE
RELIABILITY	Recover from corruption loss and damage	back -ip ,logging checkpoints
Access Security	control Acess	Password Dialouges
Integrity	Ensure internal Consistensy	Validation rules, Constraints



Process	Technique
Detection	• Intrusion Detection Systems (IDS), • Database Activity Monitoring (DAM), • SQL Injection Tools • Anomaly Detection, Logs Monitoring
Reporting	• Automated Alerts • Log Reporting • Incident Reports • Regulatory Notifications
Responding	• Isolation • Backup Restoration • Patching • Root Cause Analysis • Data Integrity Checks • Credential Updates • Continuous Monitoring

SECURITY MODEL:

Authentication:

- The client has to establish the identity of the server and the server has to establish the identity of the client.
- This is done often by means of shared secrets (either a password/user-id combination, or shared biographic and/or biometric data).
- The result, as far as the DBMS is concerned, is an authorisation-identifier. Authentication does not give any privileges for particular tasks.
- It only establishes that the DBMS trusts that the user is who he/she claimed to be and that the user trusts that the DBMS is also the intended system. Authentication is a prerequisite for authorisation.

SECURITY MODEL:

Authorization:

- Authorisation relates to the permissions granted to an authorised user to carry out particular transactions, and hence to change the state of the database (writeitem transactions) and/or receive data from the database (read-item transactions). The result of authorisation, which needs to be on a transactional basis, is a vector:
- Authorisation (item, auth-id, operation). A vector is a sequence of data values at a known location in the system. At a logical level, the system structure needs an authorisation server, which needs to co-operate with an auditing server. There is an issue of server-to-server security and a problem with amplification as the authorisation is transmitted from system to system. Amplification here means that the security issues become larger as a larger number of DBMS servers are involved in the transaction.
- To be safe, you need to log all accesses and log all authorisation details with transaction identifiers. There is a need to audit regularly and maintain an audit trail, often for a long period.

Security in SQL:

As an example , the supplied roles in Oracle include

SYSOPER : Starts and stop the DBMS

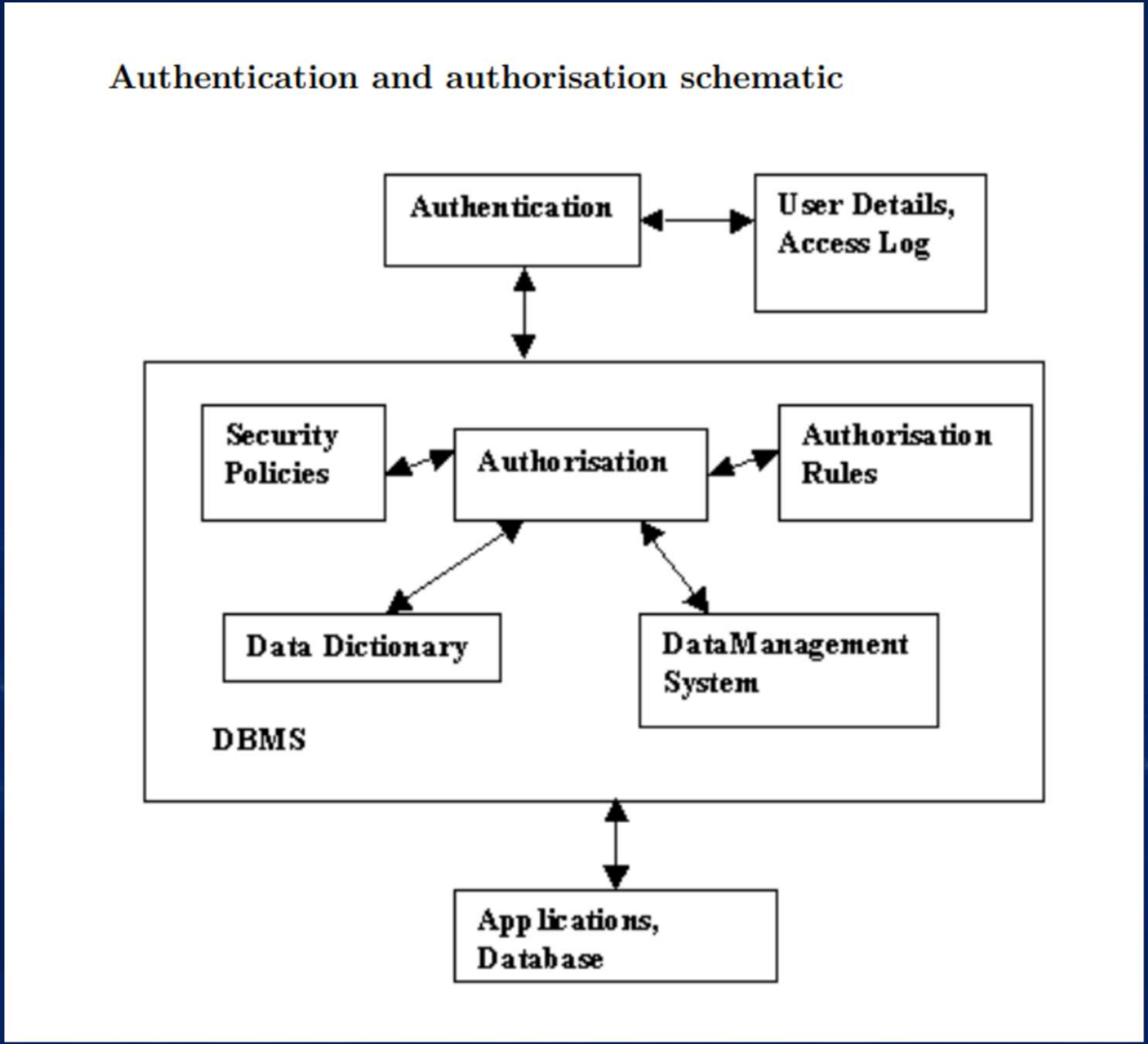
DBA : Authority to create users and to manage the database and existing users .

SYSDBA : All the DBA's authority plus the authority to create , start , stop and recover

Schema Level:

The first security-related task is to create the schema. The authorisation is optional and will default to the current user if it is not specified. Only the owner of the schema is allowed to manipulate it. Below is an example where a user is given the right to create tables. The creator of the table retains privileges for the tables so created.

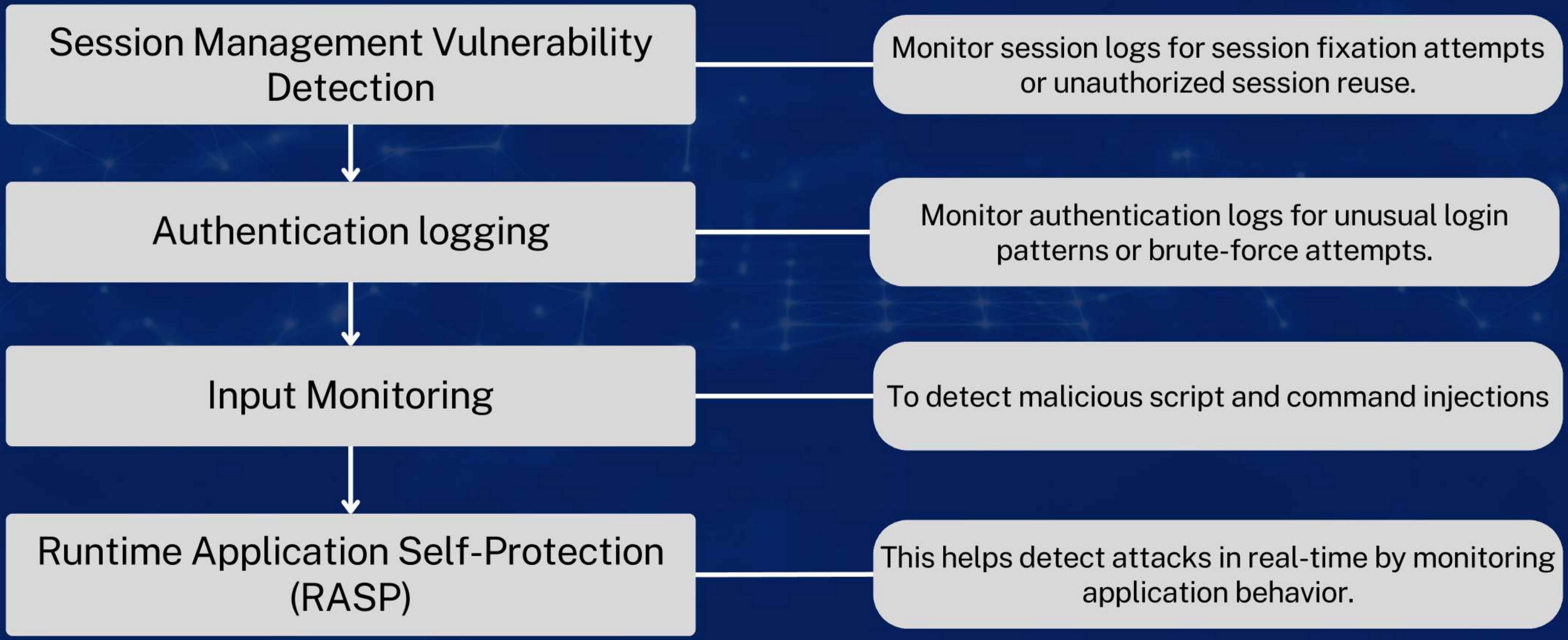
```
CREATE SCHEMA student_database AUTHORISATION U1;
```



Authentication and authorisation schematic

APPLICATION BASED ATTACKS:

Detecting:



Session Management Vulnerability Detection

Monitor session logs for session fixation attempts or unauthorized session reuse.

Authentication logging

Monitor authentication logs for unusual login patterns or brute-force attempts.

Input Monitoring

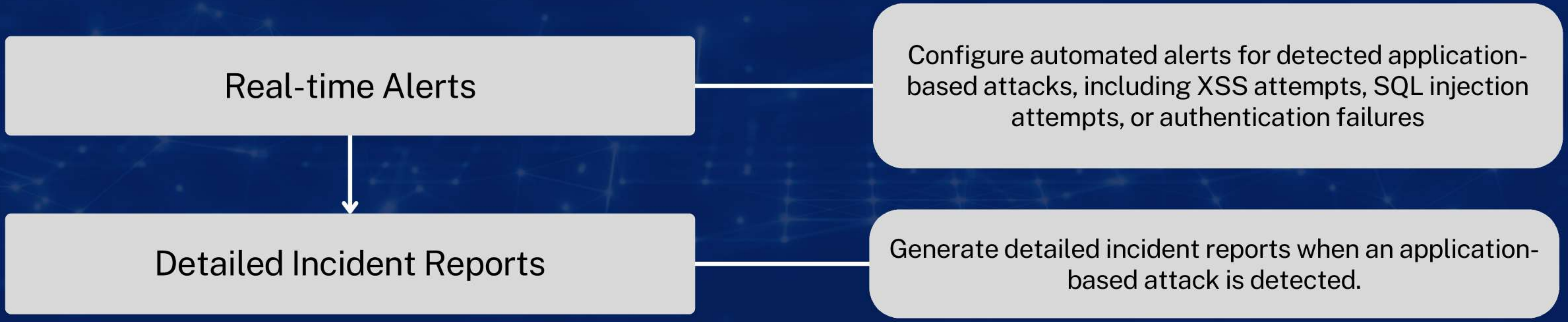
To detect malicious script and command injections

Runtime Application Self-Protection (RASP)

This helps detect attacks in real-time by monitoring application behavior.

APPLICATION BASED ATTACKS:

Reporting:



Real-time Alerts

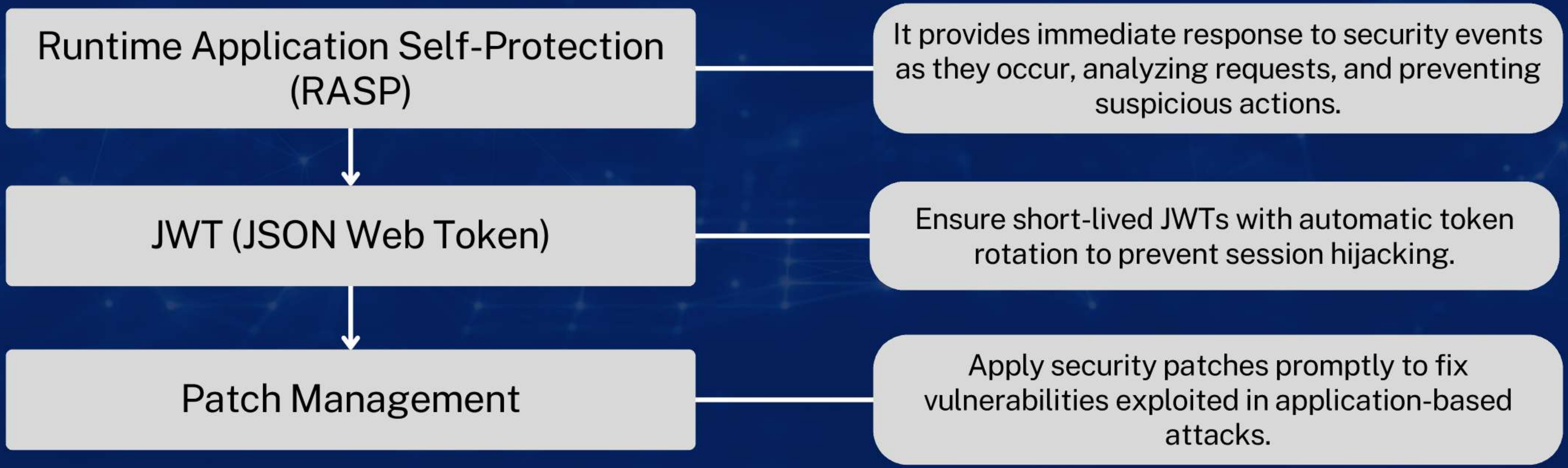
Configure automated alerts for detected application-based attacks, including XSS attempts, SQL injection attempts, or authentication failures

Detailed Incident Reports

Generate detailed incident reports when an application-based attack is detected.

APPLICATION BASED ATTACKS:

Responding:



Runtime Application Self-Protection (RASP)

It provides immediate response to security events as they occur, analyzing requests, and preventing suspicious actions.

JWT (JSON Web Token)

Ensure short-lived JWTs with automatic token rotation to prevent session hijacking.

Patch Management

Apply security patches promptly to fix vulnerabilities exploited in application-based attacks.

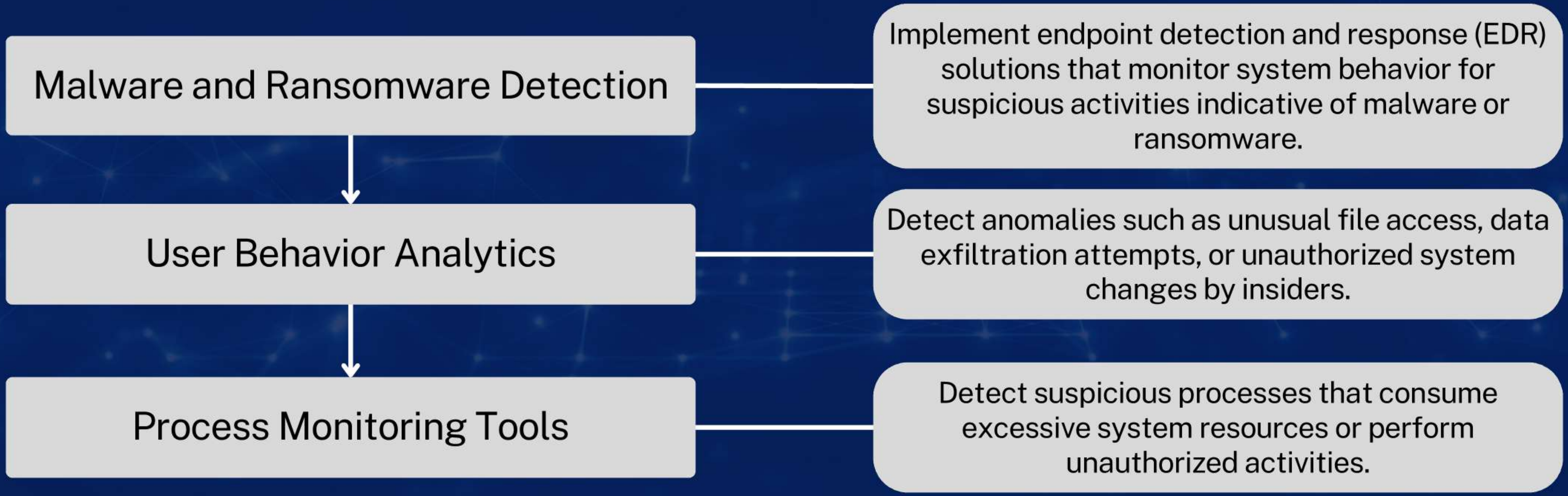
HOST BASED ATTACKS:

- These attacks are directed at individual host machines or operating systems (e.g., desktops, servers, or mobile devices).
- The goal is to compromise the host’s security to gain unauthorized control, install malicious software, or extract sensitive information.

- Examples of these attacks are Ransomware, Rootkits, Privilege Escalation etc..

HOST BASED ATTACKS:

Detecting:



Malware and Ransomware Detection

Implement endpoint detection and response (EDR) solutions that monitor system behavior for suspicious activities indicative of malware or ransomware.

User Behavior Analytics

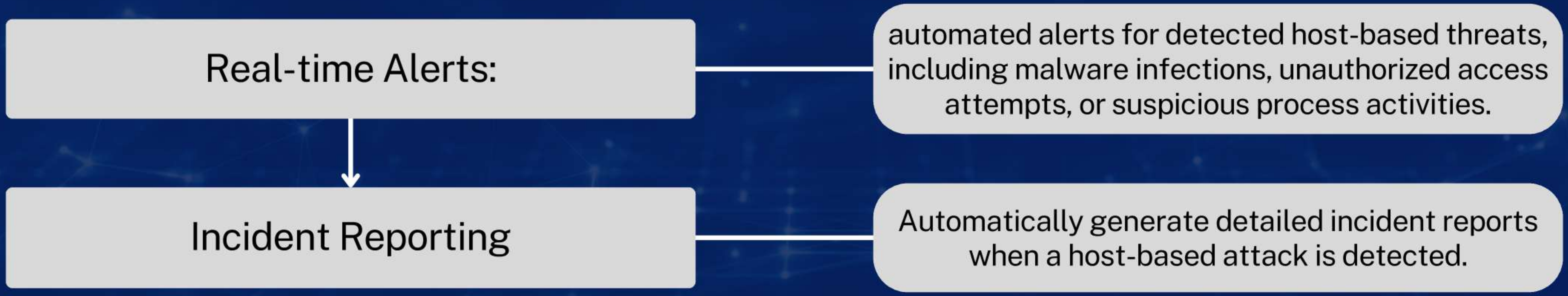
Detect anomalies such as unusual file access, data exfiltration attempts, or unauthorized system changes by insiders.

Process Monitoring Tools

Detect suspicious processes that consume excessive system resources or perform unauthorized activities.

HOST BASED ATTACKS:

Reporting:



Real-time Alerts:

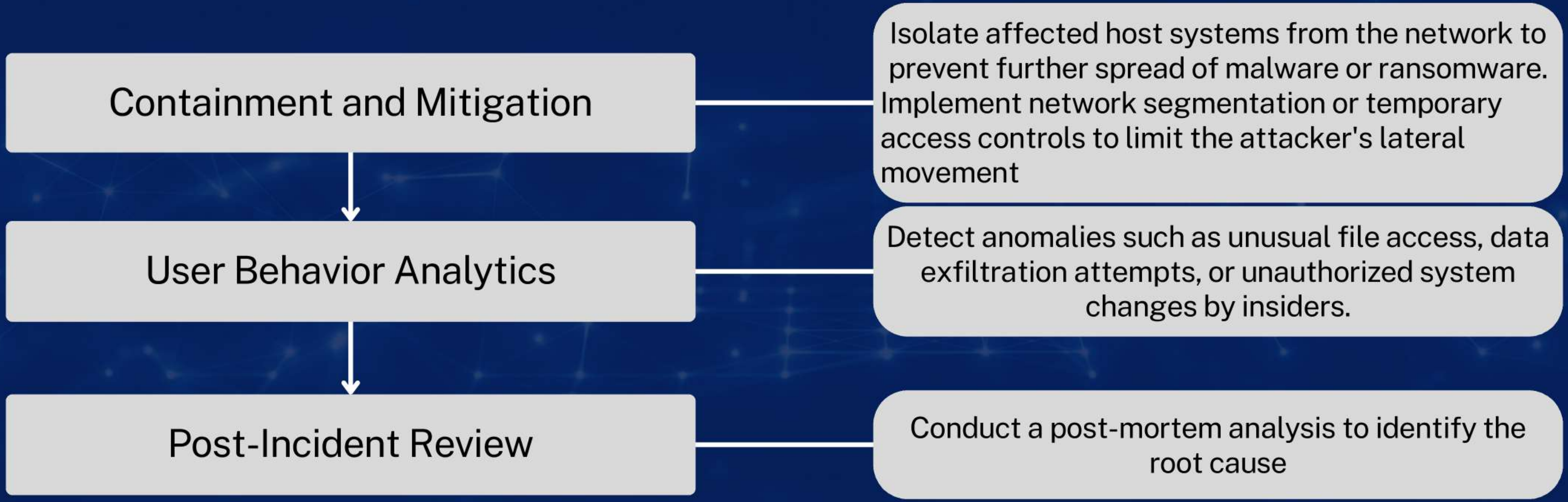
automated alerts for detected host-based threats, including malware infections, unauthorized access attempts, or suspicious process activities.

Incident Reporting

Automatically generate detailed incident reports when a host-based attack is detected.

HOST BASED ATTACKS:

Responding:



Containment and Mitigation

Isolate affected host systems from the network to prevent further spread of malware or ransomware. Implement network segmentation or temporary access controls to limit the attacker's lateral movement

User Behavior Analytics

Detect anomalies such as unusual file access, data exfiltration attempts, or unauthorized system changes by insiders.

Post-Incident Review

Conduct a post-mortem analysis to identify the root cause

THANK YOU