

...

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

...

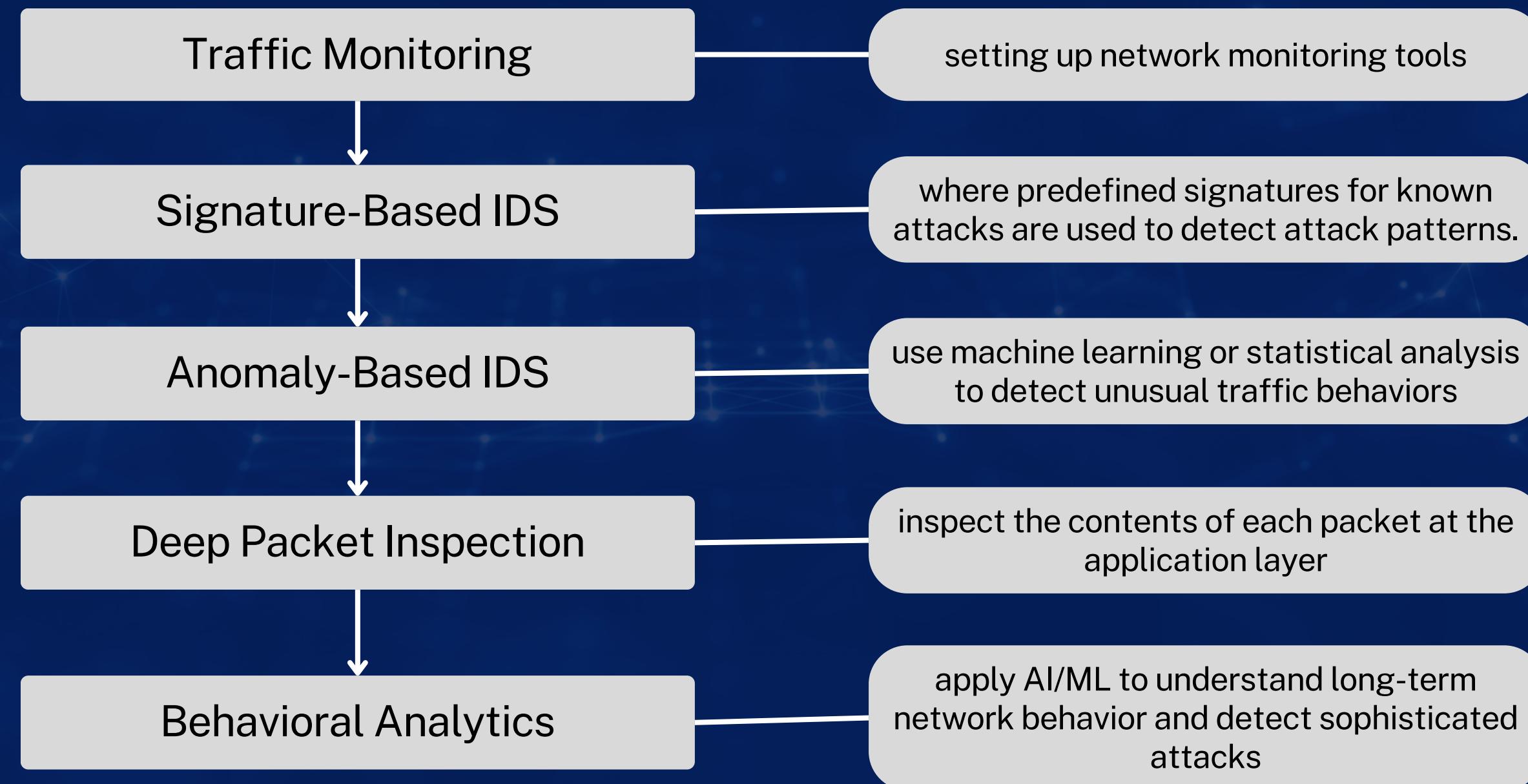
NETWORK BASED ATTACKS:

- 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:

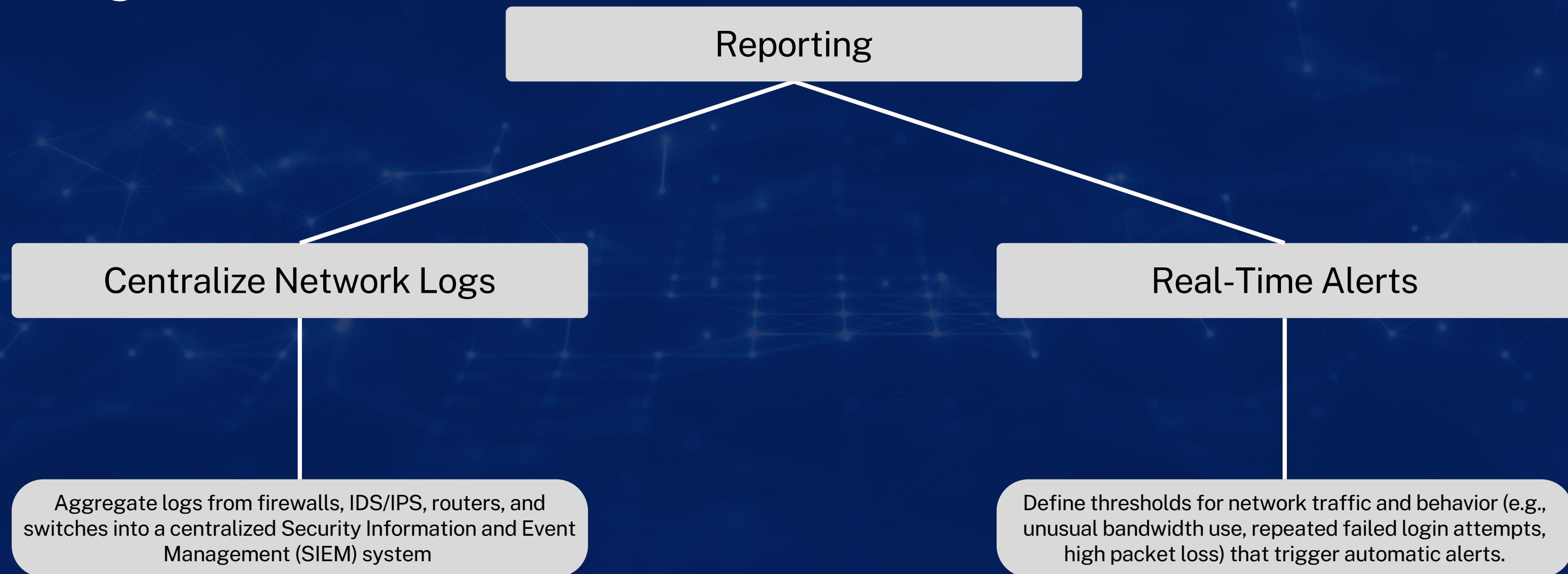
Detecting:



...

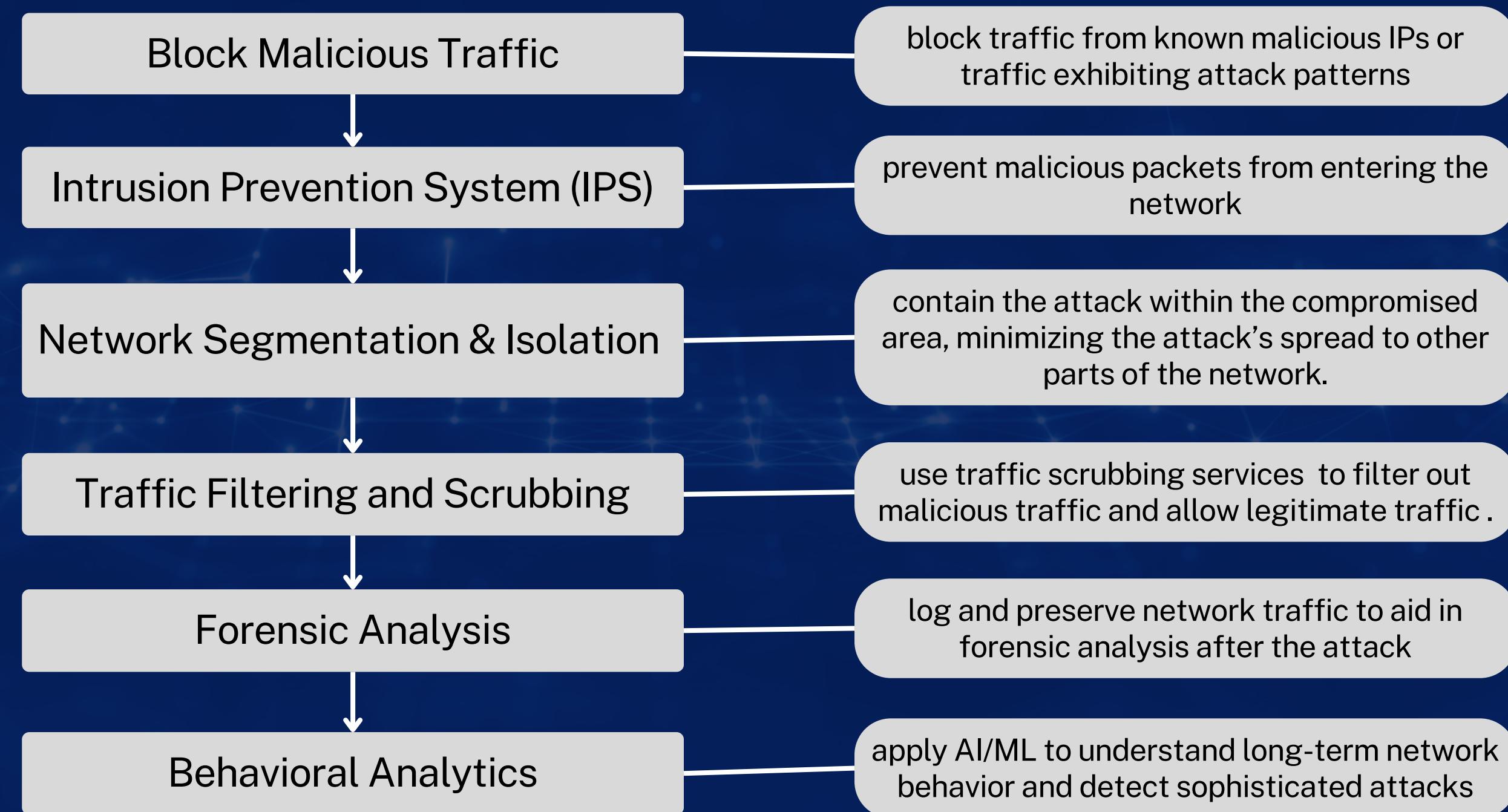
NETWORK BASED ATTACKS:

Reporting:



NETWORK BASED ATTACKS:

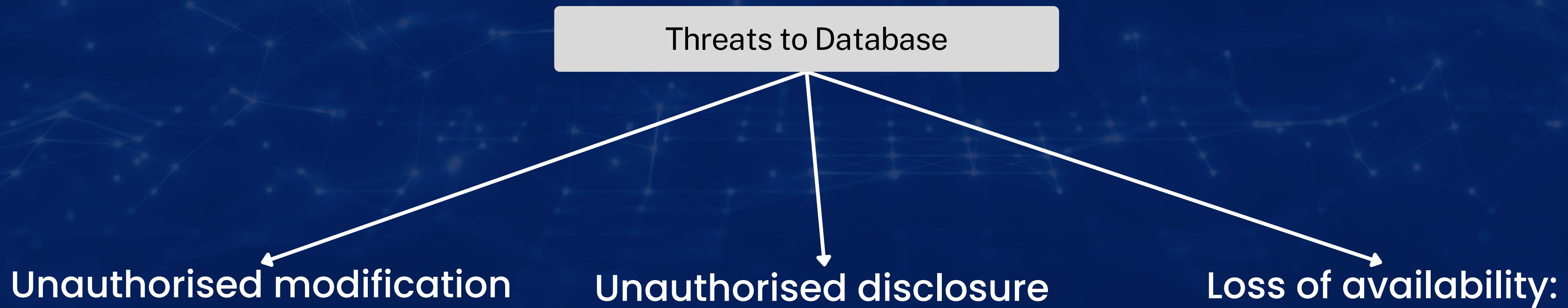
Responding:



...

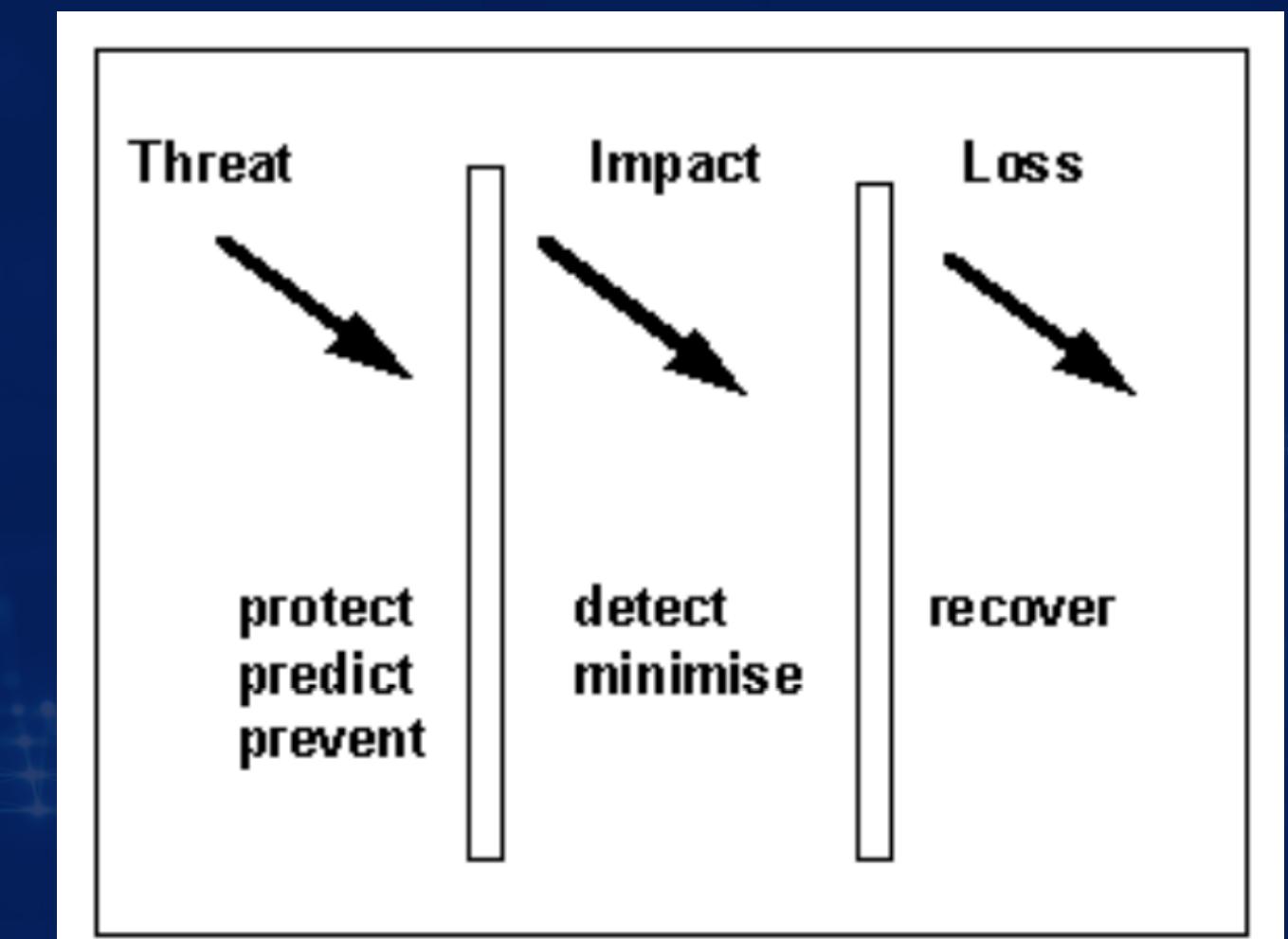
DATABASE BASED ATTACKS

- 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.



• • •

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

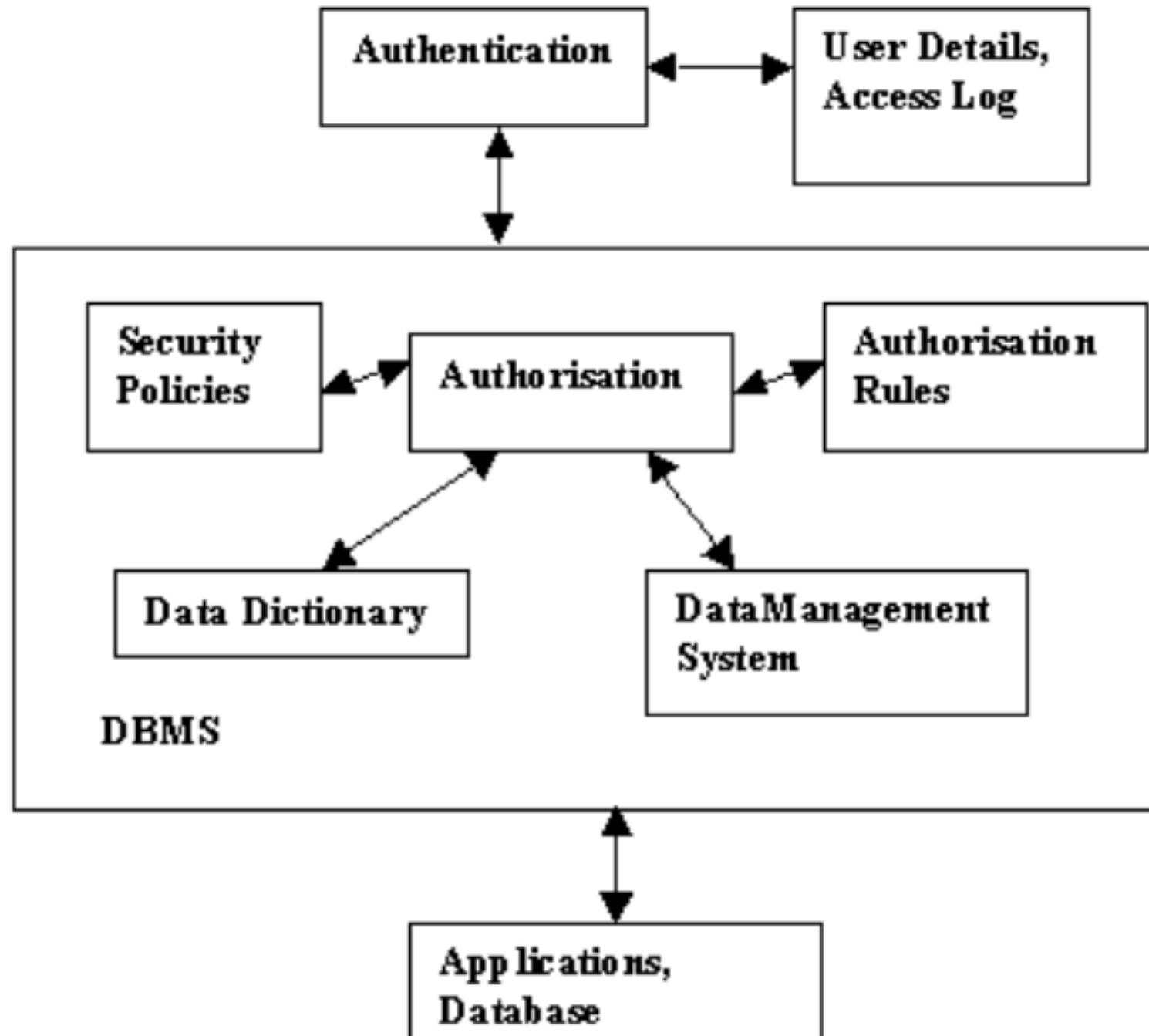
•••

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 AUTHORIZATION U1;
```

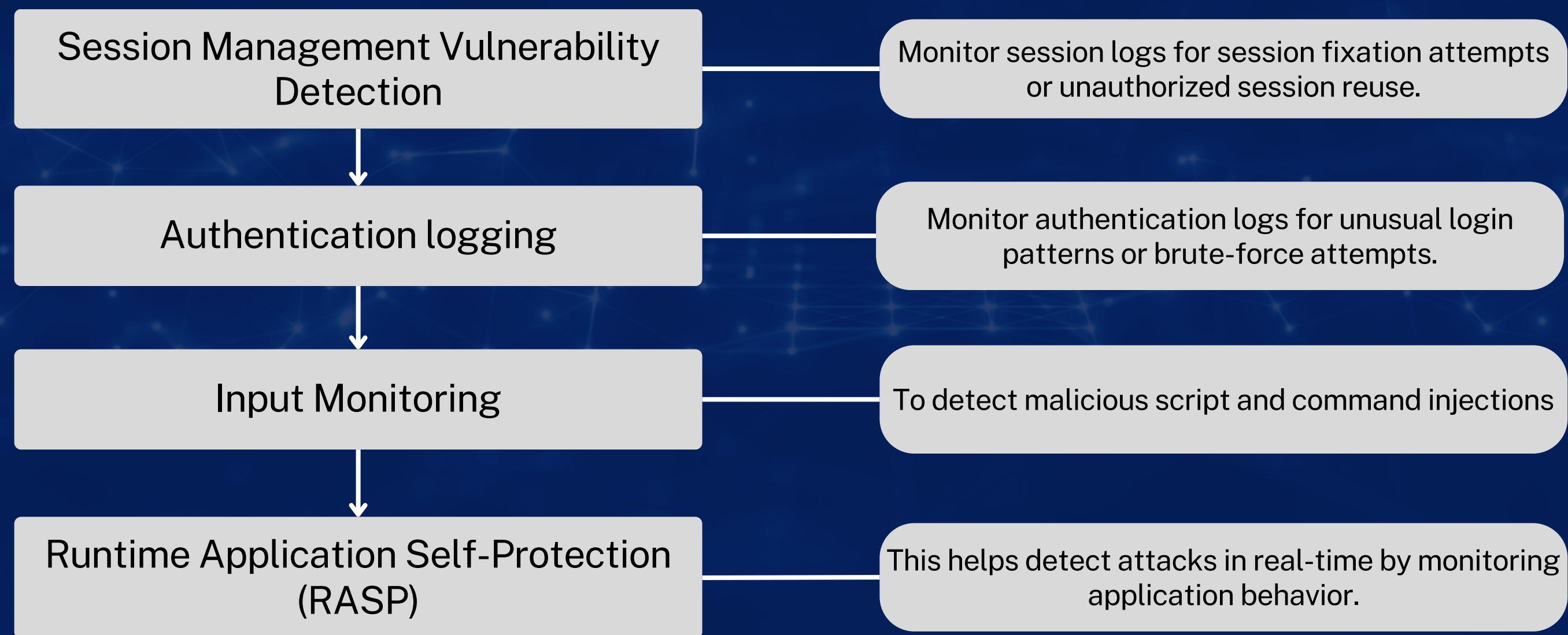
Authentication and authorisation schematic



...

APPLICATION BASED ATTACKS:

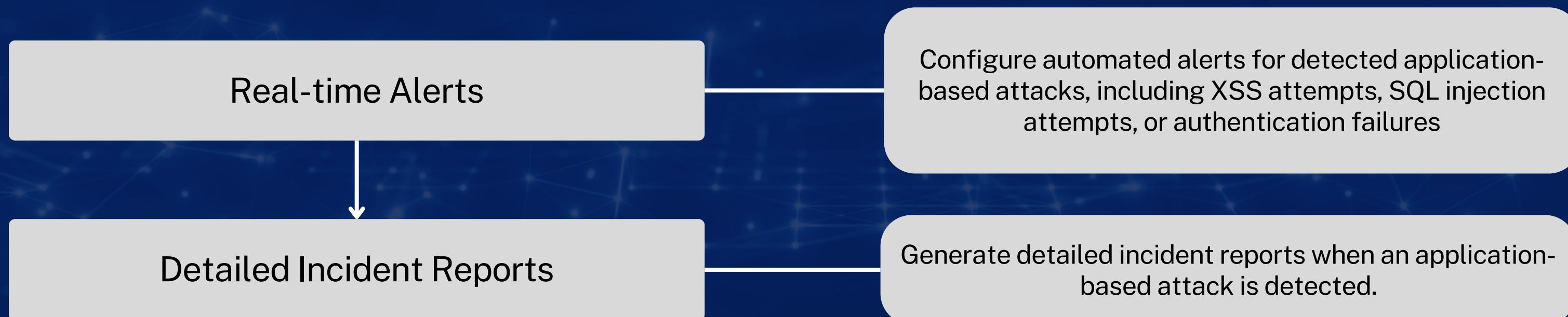
Detecting:



...

APPLICATION BASED ATTACKS:

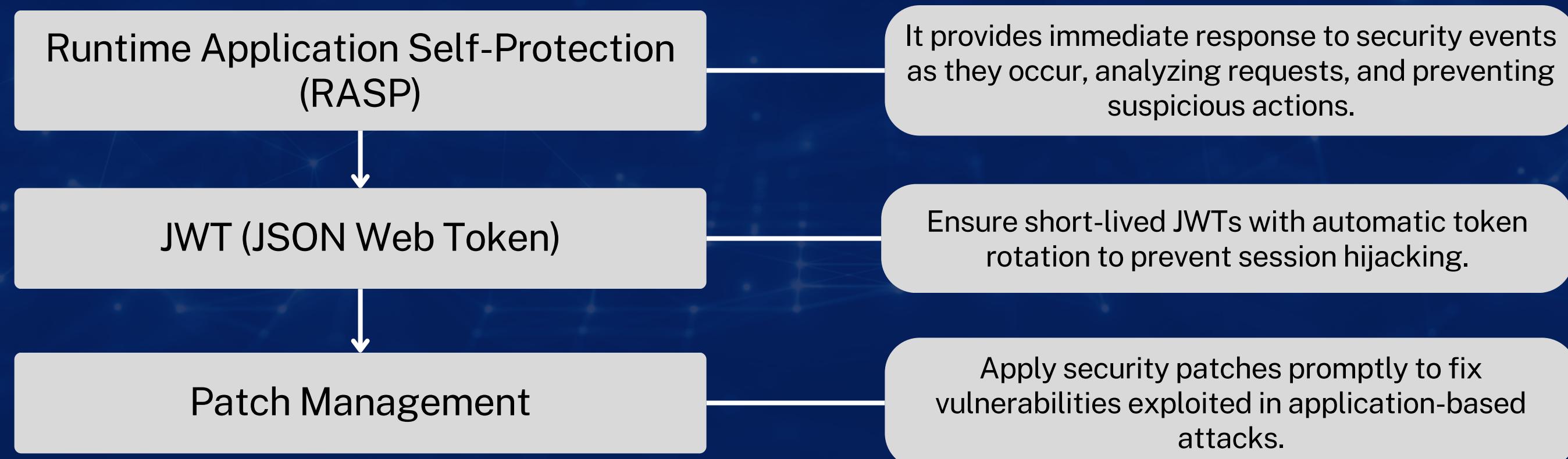
Reporting:



...

APPLICATION BASED ATTACKS:

Responding:



...

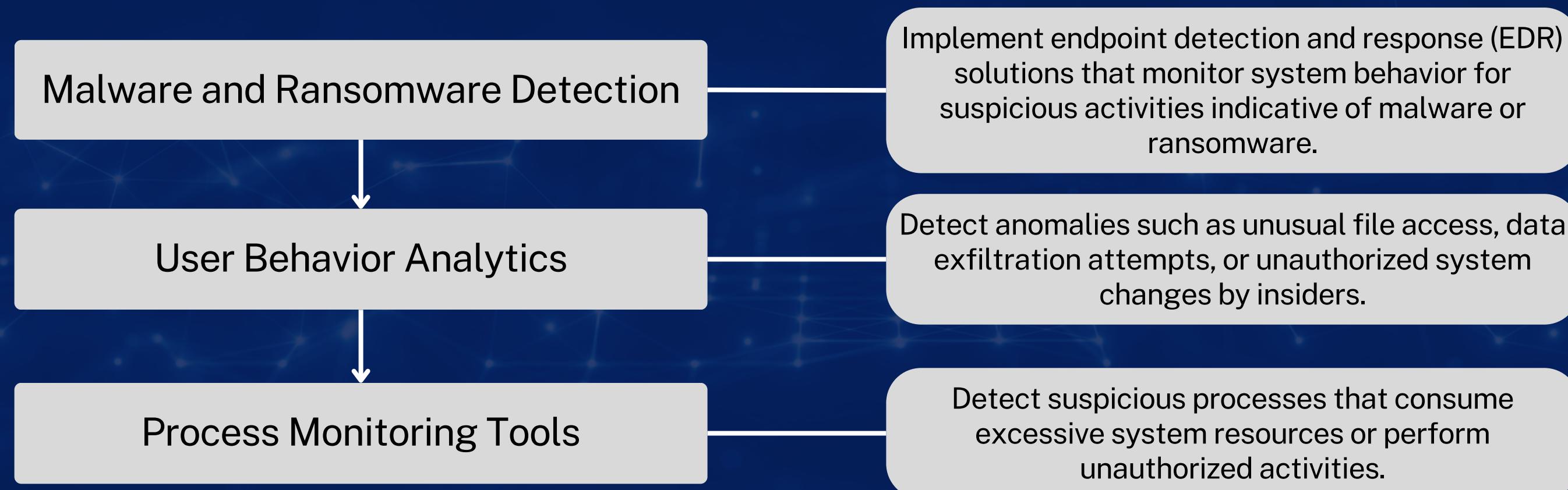
HOST BASED ATTACKS:

- 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:

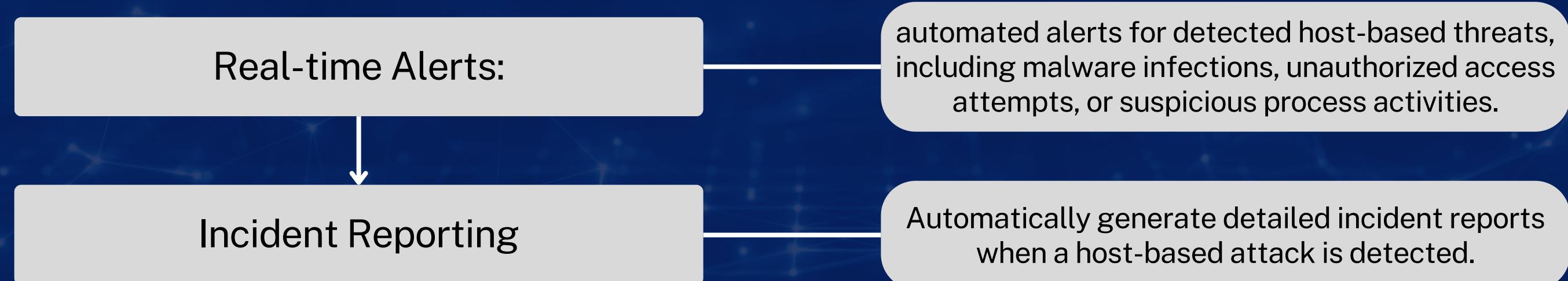
Detecting:



...

HOST BASED ATTACKS:

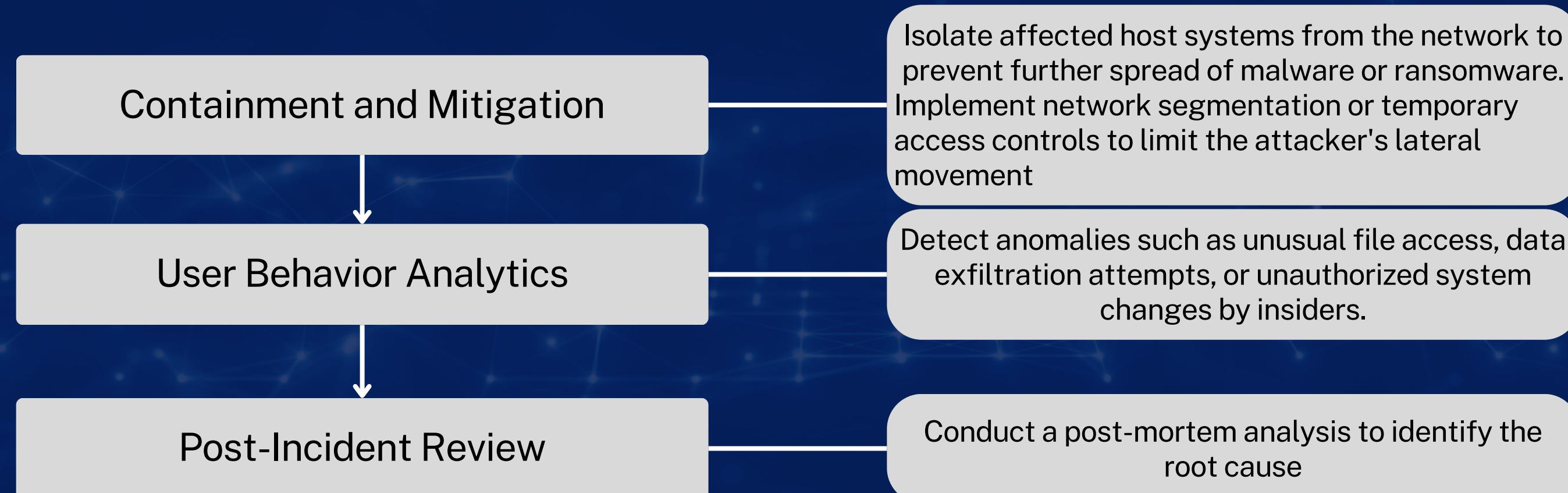
Reporting:



...

HOST BASED ATTACKS:

Responding:





THANK YOU