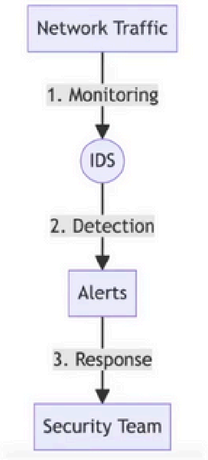
IDS, NIDS and HIDS

- **IDS**

An Intrusion Detection System (IDS) is a security software or hardware designed to detect and respond to malicious activities or security breaches within a computer network.

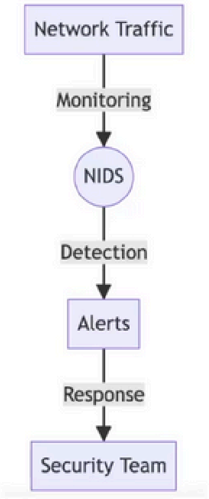


Picure source: own creation

IDS, NIDS and HIDS

- **NIDS**

A Network Intrusion Detection System (NIDS) is a security tool designed to monitor and analyze network traffic for suspicious or malicious activity in real-time.

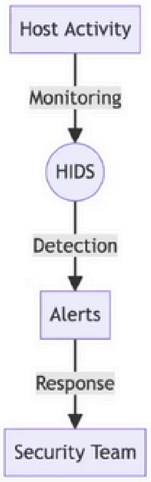


Picure source: own creation

IDS, NIDS and HIDS

- **HIDS**

A Host Intrusion Detection System (HIDS) is a security tool that monitors and analyzes activity on an individual device to detect and prevent intrusions or malicious behavior.

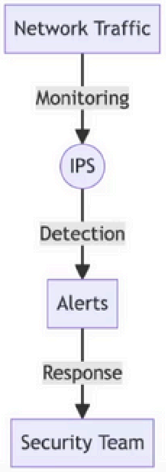


Picure source: own creation

IDS, NIDS and HIDS

- **IPS**

An Intrusion Prevention System (IPS) is a security tool designed to actively detect and block potential threats or malicious activities in real-time on a network or system.

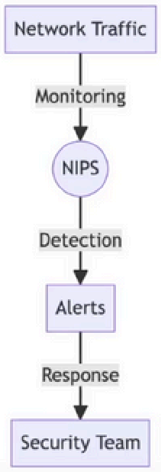


Picure source: own creation

IDS, NIDS and HIDS

- **NIPS**

A Network-based Intrusion Prevention System (NIPS) is a security tool designed to actively detect and block malicious network traffic in real-time, thereby preventing potential threats from reaching target systems or networks.

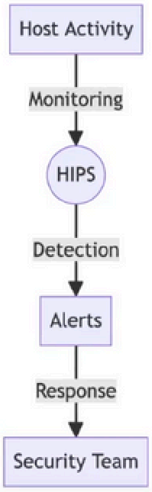


Picure source: own creation

IDS, NIDS and HIDS

- **HIPS**

A Host-based Intrusion Prevention System (HIPS) is a security software that actively monitors and defends individual computer systems against unauthorized access and malicious activities.

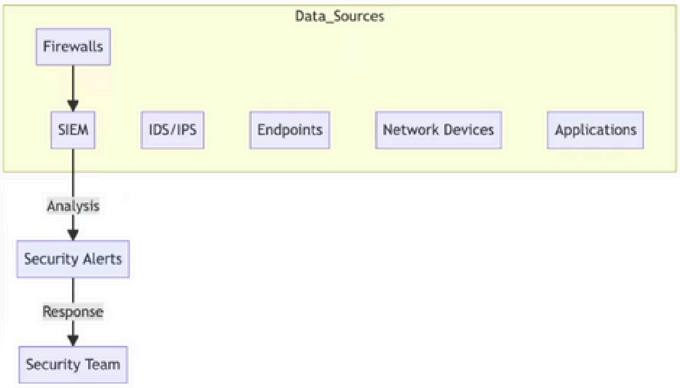


Picure source: own creation

IDS, NIDS and HIDS

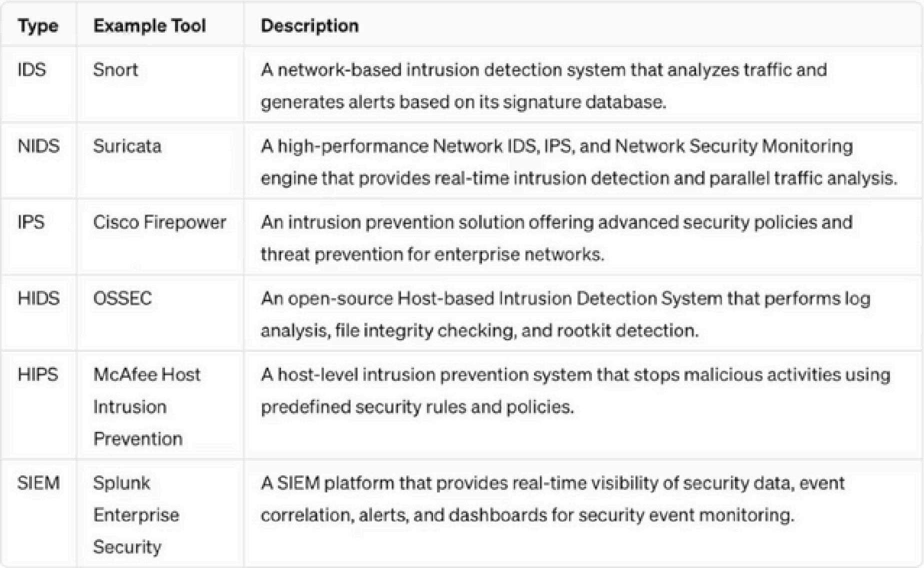
- **SIEM**

SIEM (Security Information and Event Management) is a security solution that provides real-time analysis of security alerts generated by network devices and applications, offering centralized visibility into an organization's security posture.

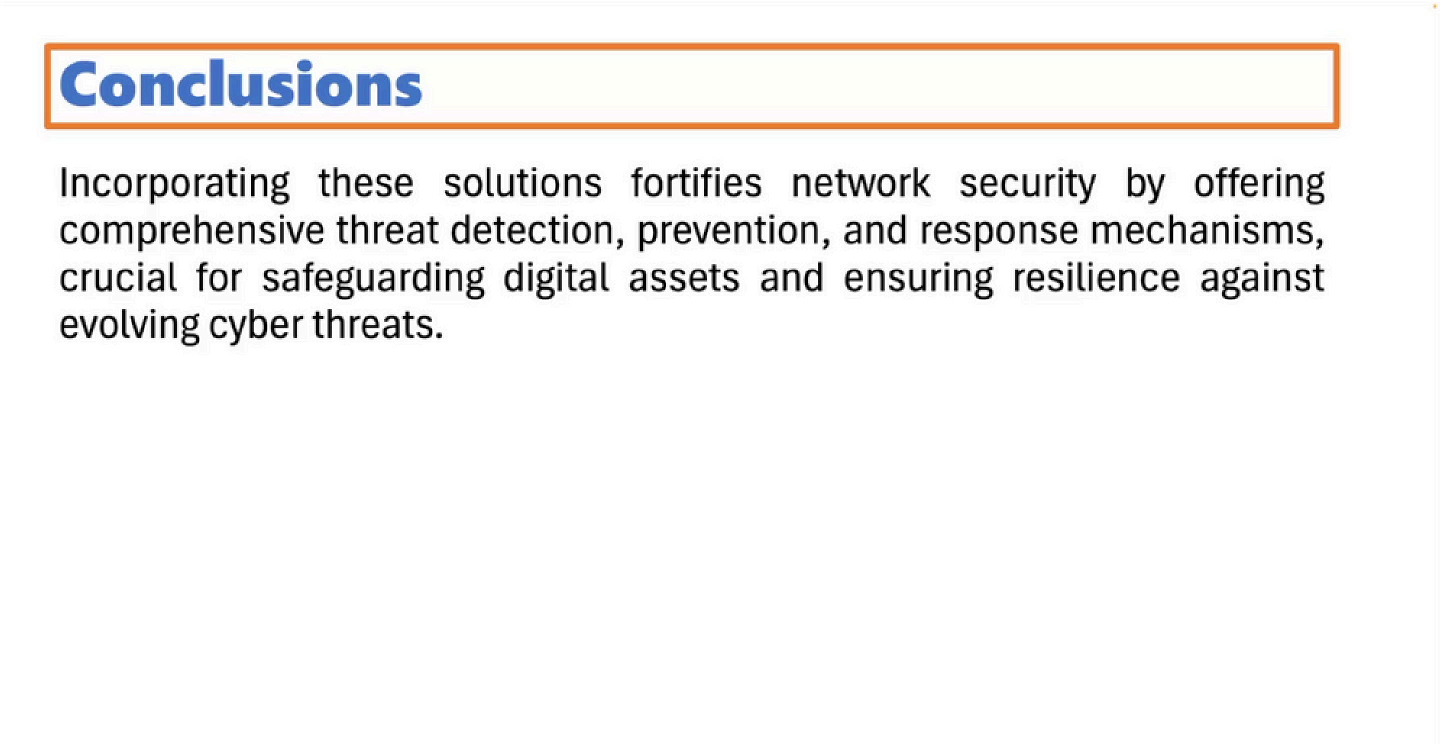


Picure source: own creation

IDS, NIDS and HIDS



Type	Example Tool	Description
IDS	Snort	A network-based intrusion detection system that analyzes traffic and generates alerts based on its signature database.
NIDS	Suricata	A high-performance Network IDS, IPS, and Network Security Monitoring engine that provides real-time intrusion detection and parallel traffic analysis.
IPS	Cisco Firepower	An intrusion prevention solution offering advanced security policies and threat prevention for enterprise networks.
HIDS	OSSEC	An open-source Host-based Intrusion Detection System that performs log analysis, file integrity checking, and rootkit detection.
HIPS	McAfee Host Intrusion Prevention	A host-level intrusion prevention system that stops malicious activities using predefined security rules and policies.
SIEM	Splunk Enterprise Security	A SIEM platform that provides real-time visibility of security data, event correlation, alerts, and dashboards for security event monitoring.



Conclusions

Incorporating these solutions fortifies network security by offering comprehensive threat detection, prevention, and response mechanisms, crucial for safeguarding digital assets and ensuring resilience against evolving cyber threats.