Tools	Description	Identifies Threats	Prevent Threats
Intrusion Detection System (IDS)	A form of monitoring to detect abnormal activity; it detects intrusion attempts and system failures.	✓	
Host-basaed IDS (HIDS)	Monitors activity on a single computer.	✓	
Network-based IDS (NIDS)	Monitors and evaluates network activity to detect attacks or event anomalies.	✓	
SIEM	Gathers log data from sources across an enterprise to understand security concerns and apportion resources.	✓	
Anti-malware/Antivirus	Seeks to identify malicious software or processess.	✓	✓
Scans	Evaluates the effectiveness of security controls.	✓	
Firewall	Filters network traffic - manages and controls network traffic and protects the network.	✓	✓
Intrusion Protection System (IPS-NIPS/HIPS)	An active IDS that automatically attempts to detect and block attacks before they reach target systems.	✓	✓