Sprint 1 Requirements Descriptions

Requirement 1

Overview

Design and configure a secure, scalable cloud-hosted environment that will serve as the central platform for the network monitoring system. This includes provisioning compute, storage, and networking resources required to collect, process, and store monitoring data.

Detailed Description

This requirement involves establishing a robust cloud infrastructure that forms the foundation of the entire network monitoring system. The environment must be architected with security, scalability, and reliability as core principles.

Requirement 4

Overview

Implement a network traffic sensing component that continuously captures and collects network traffic from monitored hosts. The sensor should reliably gather packet data or flow information without disrupting normal network operations.

Detailed Description

This requirement focuses on developing or deploying lightweight, efficient traffic capture agents that operate on monitored hosts or network segments. The sensors must operate transparently without impacting application performance or user experience.

Requirement 5

Overview

Ensure that all network traffic and monitoring data transmitted between monitored hosts and the central monitoring system is securely encrypted. This requirement aims to protect data confidentiality, integrity, and prevent unauthorized interception or tampering.

Detailed Description

This requirement establishes end-to-end encryption for all monitoring data in transit, protecting sensitive network information from eavesdropping and manipulation. The solution must balance security with performance to avoid becoming a bottleneck.

Requirement 6

Overview

Develop functionality to extract relevant metadata from PCAP packets, such as source/destination addresses, ports, protocols, and timestamps. This reduces the need to store full packet payloads while still enabling effective traffic analysis and monitoring.

Detailed Description

This requirement focuses on intelligent data reduction through metadata extraction, balancing forensic capability with storage efficiency. By capturing packet headers and flow characteristics rather than full payloads, the system can achieve massive storage savings while retaining analytical value.