Types of Firewall

Created by: Shubham Kumar Soni

Table of Contents

Details of Firewalls and L1 SOC Analyst Role

Hardware Firewalls

Hardware Firewalls are security devices that represent a separate piece of hardware placed between an internal and external network. This type is also known as an Appliance Firewall.

L1 SOC Analyst Role:

L1 SOC Analyst Role: Monitor alerts related to hardware firewalls, identify unauthorized access attempts, and escalate issues if any anomalies are detected.

Software Firewalls

A software firewall is installed on the host device. Since it is attached to a specific device, it has to utilize its resources to work. Therefore, it is inevitable for it to use up some of the system's RAM and CPU.

L1 SOC Analyst Role:

L1 SOC Analyst Role: Ensure endpoint security by reviewing software firewall logs, identifying malware activity, and responding to security events on host machines.

Cloud Firewalls

A Cloud firewall or firewall-as-a-service (FaaS) is a cloud solution for network protection. Like other cloud solutions, it is maintained and run on the internet by third-party vendors.

L1 SOC Analyst Role:

L1 SOC Analyst Role: Monitor cloud firewall logs, detect suspicious activities in cloud environments, and report unauthorized access attempts.

Proxy Firewalls

It serves as an intermediate device between internal and external systems communicating over the internet. It protects a network by forwarding requests from the original client and masking it as its own.

L1 SOC Analyst Role:

L1 SOC Analyst Role: Analyze web proxy logs, detect anomalies in user web traffic, and block malicious URLs or connections.

Circuit-Level Firewalls

Circuit-Level gateways are a type of firewall that work at the session layer of the OSI model, observing TCP (Transmission Control Protocol) connections and sessions.

L1 SOC Analyst Role:

L1 SOC Analyst Role: Monitor TCP sessions, identify unauthorized or suspicious connections, and escalate cases of potential data exfiltration.

Stateful Inspection Firewalls

A stateful inspection firewall keeps track of the state of a connection by monitoring the TCP 3-way handshake.

L1 SOC Analyst Role:

L1 SOC Analyst Role: Investigate anomalies in stateful firewall logs, detect unusual connection patterns, and take necessary action on suspicious network sessions.

Packet-Filtering Firewalls

Packet-Filtering Firewalls serve as an inline security checkpoint attached to a router or switch. As the name suggests, it monitors network traffic by filtering incoming packets according to the information they carry.

L1 SOC Analyst Role:

L1 SOC Analyst Role: Review firewall packet logs, identify unauthorized access attempts, and report unusual traffic patterns.

Next-Generation Firewalls

The next-generation firewall is a security device that combines a number of functions of other firewalls. It incorporates packet, stateful, and deep packet inspection.

L1 SOC Analyst Role:

L1 SOC Analyst Role: Analyze advanced firewall logs, monitor for deep packet inspection alerts, and correlate security events to detect threats.