MORE DATA = MORE TELEMETRY BUT MORE $$$

SIEM

LOG INGESTION & COMMON COSTING FACTORS

@URVESH_THAKKAR

Understanding log ingestion metrics is critical for cybersecurity professionals experimenting with to maximise their SIEM tools. Here's how five top SIEM tools and insights on how they handle log ingestion, with examples to clarify:

splunk>

Splunk: Splunk log ingestion is based on the volume of daily indexed data, with a 50% compression rate. For example, if you're ingesting 100GB of data per day, you should budget for 50GB of storage due to compression. This calculation assists in determining the storage and performance requirements for your Splunk environment.

IBM QRadar

QRadar uses EPS (Events Per Second) to measure log ingestion. For example, if you observe 360,000 events in one hour, the EPS calculation is 360000 events / 3600 seconds = 100 EPS. This metric aids in understanding the volume of data that QRadar processes over time, as well as capacity planning.

ELK

The ELK Stack provides several ingestion methods, including Beats, Logstash, and the direct Elasticsearch API. For example, if you are using Filebeat to ship logs, you could set it up to monitor and send 10,000 log lines to Elasticsearch every 5 minutes. This setup demonstrates the flexibility and scalability of data ingestion.

ArcSight

ArcSight, similar to QRadar, uses EPS for log ingestion metrics. For example, if ArcSight processes 1,800,000 events during a 2-hour peak period, the EPS is calculated as 1,800,000 events / 7200 seconds = 250 EPS. This figure aids in determining the system's ability to handle large amounts of data during peak periods.

wazuh.

Wazuh collects data using an agent-based model. For example, a Wazuh agent installed on a server could collect 500,000 events per day. These events are then sent to the Wazuh manager for processing and analysis. This example demonstrates the distributed nature of Wazuh's data collection.

COMMON COSTING FACTORS

Vendor Pricing Models: SIEM costs vary by vendor, influenced by factors such as data volume, EPS, user count, and others, which affect total ownership cost.

Discounts and Licensing Agreements: Negotiated discounts or licensing agreements can help to reduce costs, with volume and contract length being important considerations.

Add-ons and Feature Packs: Some SIEM functionalities, such as advanced analytics or integrations, may necessitate additional fees or feature packs.

Data Retention Policies: Longer data retention necessitates more storage, which directly impacts costs due to compliance or forensic requirements.

Infrastructure and Maintenance Costs: The deployment model (on-premises, cloud, or hybrid) has a significant impact on infrastructure and maintenance expenses.