SIEM Architecture: Technology, Process and Data

IN THIS SIEM EXPLAINER, HOW SIEM SYSTEMS ARE BUILT, HOW THEY GO FROM RAW EVENT DATA TO SECURITY INSIGHTS, AND HOW THEY MANAGE EVENT DATA ON A HUGE SCALE.

info@techgek.co.in

SIEM

- Security information and event management (SIEM) platforms collect log and event data from security systems, networks and computers, and turn it into actionable security insights
- SIEM technology can help organizations detect threats that individual security systems cannot see.
- Investigate past security incidents, perform incident response and prepare reports for regulation and compliance purposes.

12 Components and Capabilities in a SIEM Architecture

Threat Intelligence

Collects and aggregates data from security systems and network devices.

Threat Intelligence Feeds

Combines internal data with third-party data on threats and vulnerabilities.

Correlation and Security Monitoring

Links events and related data into security incidents, threats or forensic findings.

Analytics

Uses statistical models and machine learning to identify deeper relationships between data elements.

Alerting

Analyses events and sends alerts to notify security staff of immediate issues.

Dashboards

Creates visualizations to let staff review event data, identify patterns and anomalie.

Compliance

Gathers log data for standards like HIPAA, PCI/DSS, HITECH, SOX and GDPR and generates reports.

Retention

Stores long-term historical data, useful for compliance and forensic investigations

info@techgek.co.in

Forensic Analysis

Enables exploration of log and event data to discover details of a security incident.

Threat Hunting

Enables security staff to run queries on log and event data to proactively uncover threats.

Incident Response

Helps security teams identify and respond to security incidents, bringing in all relevant data rapidly.

SOC Automation

Advanced SIEMs can automatically respond to incidents by orchestrating security systems in an approach known as security orchestration and response (SOAR).

info@techgek.co.in

SIEM Logging Process

- A SIEM server, at its root, is a log management platform. Log management involves collecting the data, managing it to enable analysis, and retaining historical data.

Data Collection

- SIEMs collect logs and events from hundreds of organizational systems (for a partial list, see Log Sources below).
- Each device generates an event every time something happens, and collects the events into a flat log file or database.

The SIEM can collect data in four ways:

1. Via an agent installed on the device (the most common method)
2. By directly connecting to the device using a network protocol or API call
3. By accessing log files directly from storage, typically in Syslog format
4. Via an event streaming protocol like SNMP, Netflow or IPFIX

The SIEM is tasked with collecting data from the devices, standardizing it and saving it in a format that enables analysis.

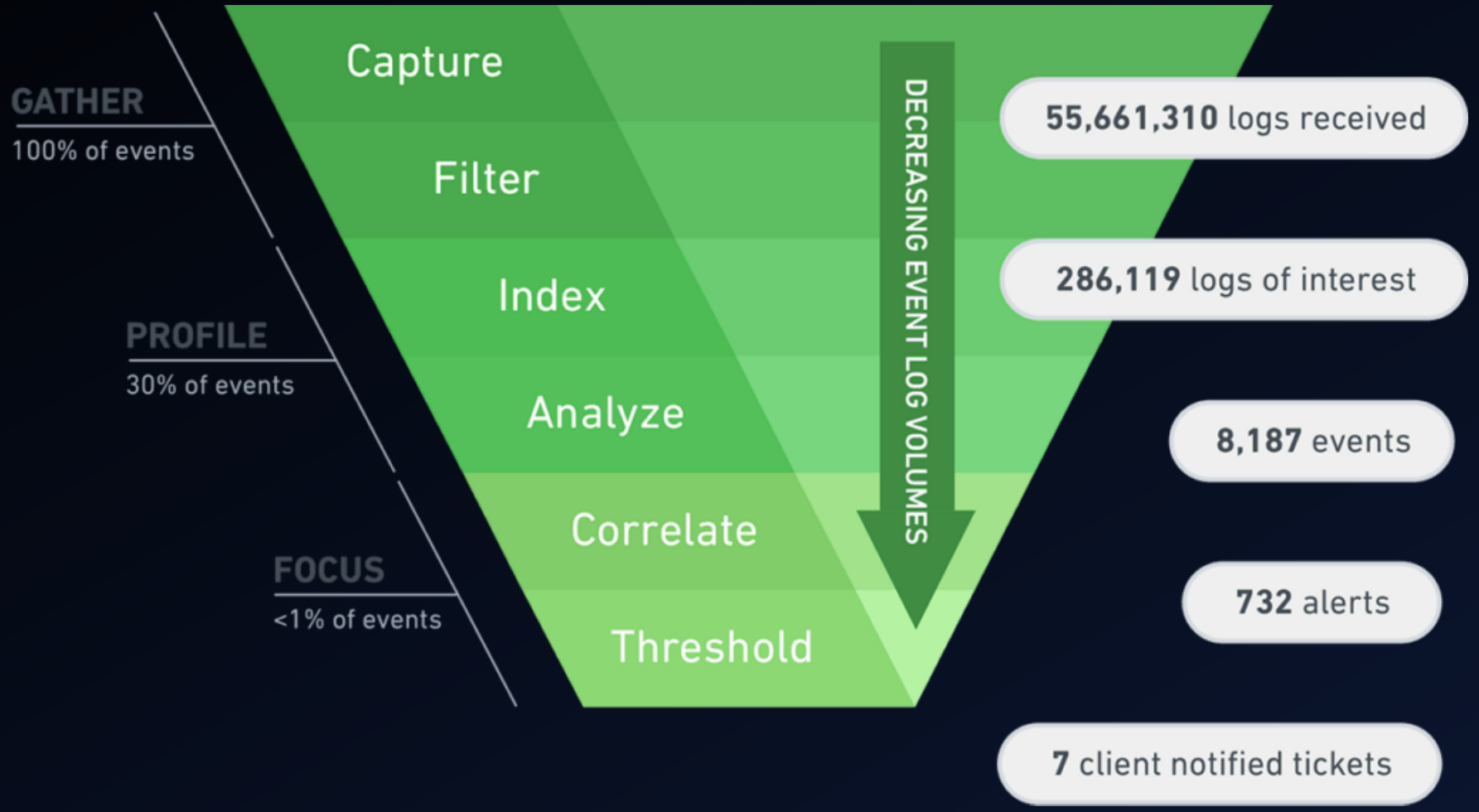
Data Management

SIEMs, especially at large organizations, can store mind-boggling amounts of data. The data needs to be:

- **Stored** – Either on-premises, in the cloud or both
- **Optimized and Indexed** – To enable efficient analysis and exploration
- **Tiered** – Hot data necessary for live security monitoring should be on high-performance storage,
- whereas cold data, which you may one day want to investigate, should be relegated to high-volume inexpensive storage mediums

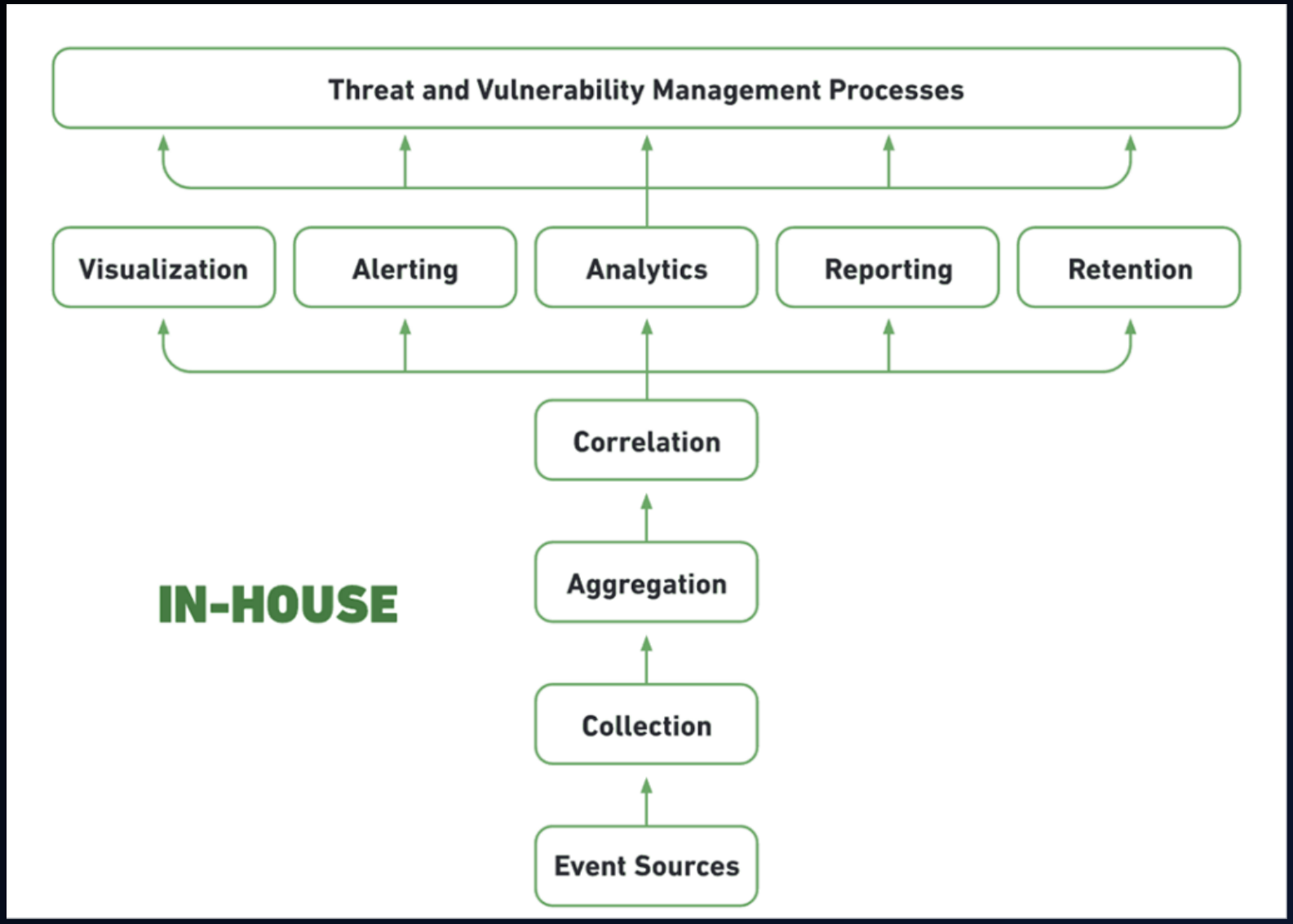
info@techgek.co.in

The Log Flow



info@techgek.co.in

SIEM Integrations



info@techgek.co.in

Thanks

info@techgek.co.in