

WHAT IS A SIEM SOLUTION- HOW SIEM WORKS AND ARCHITECTURE

WHAT IS SIM?

Security information management (SIM) refers to the collection of log files and storage in a central repository for later analysis. SIM is therefore also referred to as log management.

WHAT IS SEM?

Security event management (SEM) is the identifying, gathering, monitoring, evaluating, correlating and monitoring of system events and alerts. In a sense, SEM is an improvement of SIM, though the two are seen as distinct areas of security management.

WHAT IS SIEM?

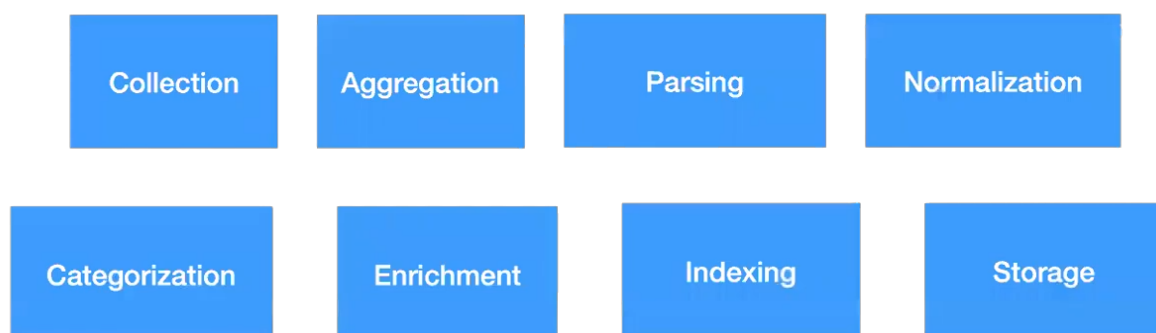
$SIM + SEM = SIEM$

SIEM is a tool that collects, aggregates, normalizes the data and analyses it according to pre-set rules and presents the data in human readable format.

Garbage In = Garbage Out

1. Log Collection
2. Log Aggregation
3. Rule Based Alerts
4. Artificial Intelligence
5. Response

SIEM FUNCTIONS



COLLECTION

I. Agent Based

- Agent Collected on each device collects, parses and forwards the logs.
- Windows Servers, Web Servers, Other file-based logs Sysmon, NXLog, OSSEC, etc.

II. Agent Less

- Devices send the logs to the servers.
- Windows Hosts WMI, Cloud Environments (APIs), Firewalls, Switches.

AGGREGATION

Process of collecting logs from multiple computing systems, parsing them and extracting structured data, and putting them together in a format that is easily searchable and explorable by modern data tools.

Methods

- I. **Push.** Logs are pushed from source to server.
- II. **Pull.** Logs are pulled by server from source.

PARSING

Software component that can take a specific log format and convert it to structured data. Multiple parsers are used for different systems

Example Log:

Sep 28 16:39:03 app_server sshd[8677] Failed password for invalid user icecast2 from 10.72.109.227 port 57238 ssh2

After parsing

host = app_server

process = sshd

source_user = icecast2

source_ip = 10.72.109.227

source_port = 57238

NORMALIZATION & CATEGORIZATION

Normalization:

Merges events containing different data into a reduced format which contains common event attributes. Following a standard for reducing records to common event attributes i.e., common field names and values.

Categorization:

Categorization involves adding meaning to events - identifying log data related to system events, authentication, local/remote operations, etc.

Host=app_server

Process=sshd

source_user=icecast2 → Authentication|Login|SSH Login

source_ip=10.72.109.227

source_port= 57238

ENRICHMENT

Log enrichment involves adding important information that can make the data more useful.

host = app_server

process = sshd

source_user = icecast2 → (Administrator)

source_ip = 10.72.109.227 → (Internal IP)

source_port = 57238

CORRELATION RULES & ALERTS

A correlation rule is a logical expression that causes the system to take a specific action if a particular event occurs. For example, "Anonymous logon, alert the user".

In other words, a correlation rule is a condition (or set of conditions) that functions as a trigger for alert.

INDEXING

Effectively search and explore log data, there is need to create an index of common attributes across all log data.

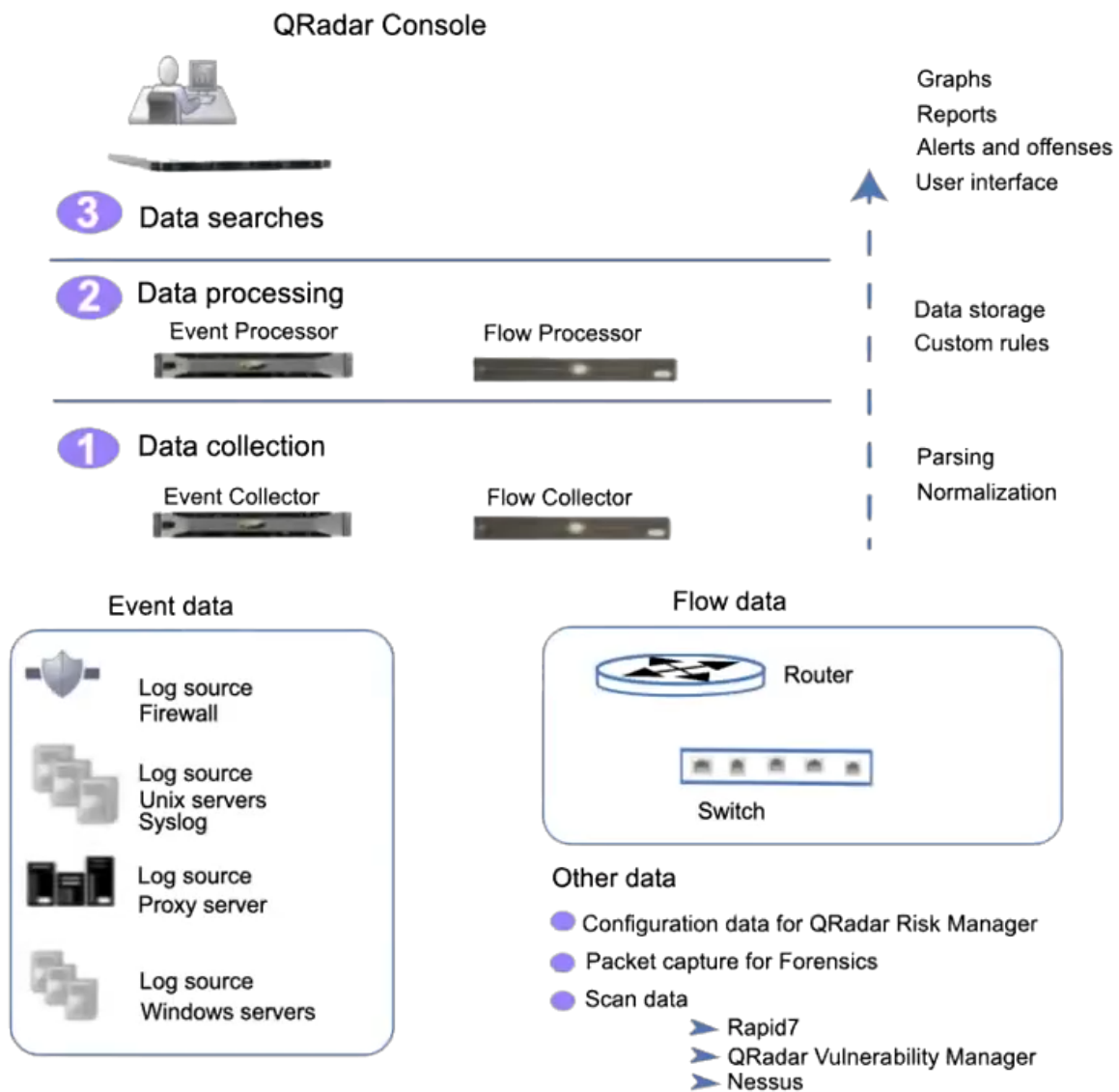
Searches or data queries that use the index keys can be an order of magnitude faster, compared to a full scan of all log data.

STORAGE

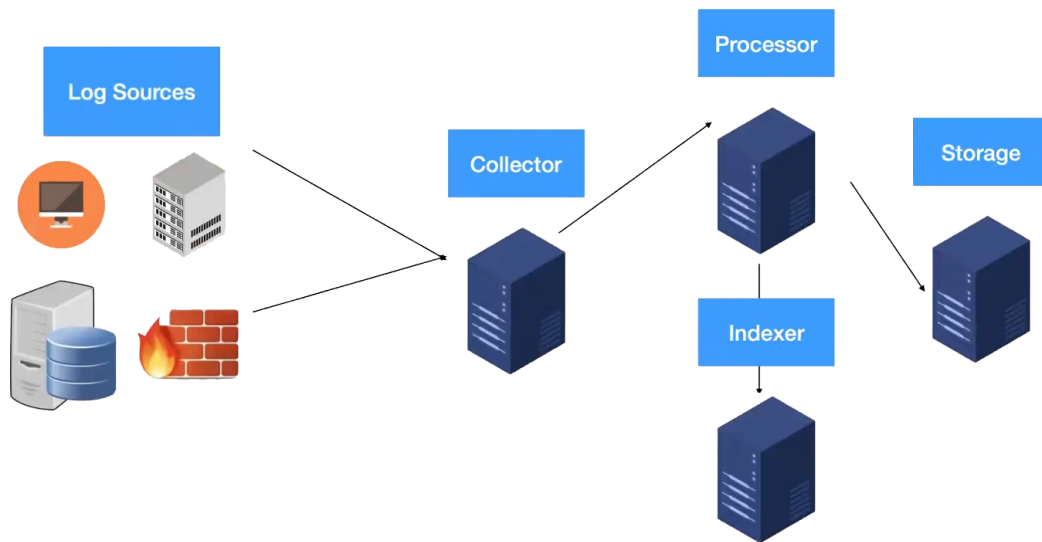
Logs are stored for different purposes such as compliance and sometimes for later retrieval. They can be kept as Hot Storage or Cold Storage.

SIEM ARCHITECTURES

Example: QRadar



DEPLOYMENT



How to convince non-technical stakeholders about the need for a Security Information and Event Management (SIEM)?

When trying to convince non-technical stakeholders about the need for a Security Information and Event Management (SIEM) solution, it's important to focus on the business benefits and address their concerns in a language they understand. Here are some approaches you can take:

1. **Start with the business impact:** Highlight the potential consequences of a cybersecurity breach, such as financial losses, reputational damage, legal liabilities, and operational disruptions. Explain how a SIEM solution can proactively detect and respond to threats, minimizing the impact and reducing the likelihood of such incidents.
2. **Emphasize regulatory compliance:** Many industries have specific regulatory requirements regarding data protection and security. Explain how implementing a SIEM solution helps meet these compliance obligations, avoiding penalties and legal complications. Emphasize that a SIEM solution provides the necessary audit trails and reporting capabilities to demonstrate compliance to auditors and regulators.
3. **Discuss risk mitigation:** Non-technical stakeholders are often concerned about managing business risks. Illustrate how a SIEM solution reduces the risk of cyber threats by actively monitoring the network, identifying suspicious activities, and enabling timely response and mitigation. This can prevent costly data breaches, operational downtime, and potential legal ramifications.
4. **Showcase incident response capabilities:** Non-technical stakeholders may worry about the organization's ability to respond to security incidents effectively. Explain how a SIEM solution provides real-time alerts, automated incident response, and centralized visibility into security events. Demonstrate how it enables faster detection, investigation, and remediation of threats, reducing the impact of security incidents.
5. **Quantify the ROI:** Non-technical stakeholders often respond well to concrete numbers and measurable benefits. Explain how a SIEM solution can help save costs by reducing incident response time, minimizing downtime, and preventing data breaches. Provide case studies or industry benchmarks to illustrate the potential return on investment (ROI) from implementing a SIEM solution.
6. **Address scalability and growth:** Non-technical stakeholders may be concerned about the scalability of security measures as the organization grows. Highlight how a SIEM solution can adapt to the organization's evolving needs, supporting increased data volumes, expanding infrastructure, and emerging security challenges. Position the SIEM solution as a long-term investment that can scale alongside the business.
7. **Leverage industry best practices and standards:** Reference widely accepted frameworks and industry best practices, such as the NIST Cybersecurity Framework or ISO 27001, to support your argument for a SIEM solution. Demonstrate how a SIEM aligns with these standards, ensuring a robust security posture and instilling confidence in stakeholders.
8. **Use visual aids and non-technical language:** Simplify complex technical concepts and present them using visual aids, diagrams, or infographics. Avoid jargon and acronyms that may confuse non-technical stakeholders. Focus on conveying the core benefits and outcomes in a clear and understandable manner.
9. **Engage in open dialogue:** Encourage non-technical stakeholders to ask questions and express their concerns. Listen actively and address their specific doubts or reservations. Tailor your explanations to their level of understanding and provide examples or analogies to clarify technical concepts.

10. Leverage external expertise: If necessary, consider bringing in external consultants or experts who can provide independent validation of the need for a SIEM solution. Their objective insights and industry experience can lend credibility to your case.

By emphasizing the business value, risk reduction, compliance, and incident response capabilities of a SIEM solution, you can effectively communicate its importance to non-technical stakeholders and gain their support.