Software Architecture
Assignment : 1

BITS Pilani

Submitted by:
Vatsal Jain
2021MT12071
BITS Pilani, WILP

What is an SIEM? (Purpose)

innovate achieve lead

- Security Information and Event Management (SIEM) is a term for software and products services combining security information management (SIM) and security event management (SEM).

- The acronyms SEM, SIM and SIEM have been sometimes used interchangeably.
  - SEM → Real time reporting, log collection, normalization, correlation, aggregation
  - SIM → Log collection, archiving, historical reporting, forensics and backtracking of events.

- SIEM is capable of :
  - Data Aggregation : Collection of data from different sources like firewalls, NIDS, etc.
  - Correlation : A part of SEM, it means to look for common attributes and link events together in meaningful bundles.
  - Alerting : An automated analysis of correlated events to make more substantial & detailed report and then alerting the admin to take necessary actions.
  - Retention : preserving the logs for long time so that they could be used for forensic examination.
  - Forensics Analysis : To search & analyse the stored logs and backtrack the attacker.
  - Dashboards : Taking the raw security data and converting it to easily readable, understandable and relatable charts and graphs.

Key Requirements : Functional & Non-Functional

Functional requirements	Non functional requirements
• Log correlation • Anomaly detection • Alerting • Integration with various log sources • Open API integration capability • Log normalization • Dashboard view for admins	• Automatic & Elastic Scaling • Multiple views/roles • Customization of the dashboard

Utility Tree

Understanding business value & Impact on architecture

Quality attribute	Attribute refinement	Scenario	Business value	Architecture impact
Security	Integrity	The log data should not be lost or tampered with by unauthorized people, including those working in the company	High	High
Performance	Service Availability	System should support 99.999% Availability	High	High
Usability	User Experience	Alerts should be generated real-time or near real-time.	High	High
Usability	Correctness	System should accurately show alerts without false positives.	High	High
Modifiability	Criteria specification	User should be able to modify use cases.	Medium	Medium
Interoperability	Notification	The system should send real time notification to the admins.	High	Medium
Performance	Response time	System should be able to support 1000 CAPS.	Medium	High
Interoperability	Unified User Experience	System should be able to integrate with multiple log sources	High	High
Interoperability	User Experience	The user should be able to build on use cases and dashboards	High	High
Performance	Scalability	System should support 1Gbps of data ingestion and should be scalable further.	High	High
Maintainability	Easy Operation & Maintenance	System should support easy monitoring, alarms , deployment using micro service based architecture using Docker Container.	High	High
Availability	Data backup	System should keep back up of complete system data including configuration and logs	Medium	High

Tactics used to achieve the top 5 ASRs : Security

Quality Attribute	Scenario (ASR)	Tactics
Security	The log data should not be lost or tampered with by unauthorized people, including those working in the company	No direct access database by any user, all system user can access backend data through system business process with respective access rights.
		Web Service Interfaces will be authenticated with User/Password
		Coding security includes security methods during programming of codes
		Access security includes identification, authentication, authorization, access control, session control etc.
		Block multi session login from different devices and session time out after 5 minute (default time) for system user.
		Store data on a separate database server cluster and protect the server using an appropriate security zones using firewall technologies

Tactics used to achieve the top 5 ASRs : Performance

Quality Attribute	Scenario (ASR)	Tactics
Performance & Scalability	System should support 99.999% Availability	• Buy scalable licence • Deploy server in HA mode • 99.999% Availability based on Distributed Architecture and Active-Active GDR

Tactics used to achieve the top 5 ASRs : Interoperability

Quality Attribute	Scenario (ASR)	Tactics
Interoperability	The system should send real time notification to the admins.	Develop use cases to trigger email and SMS alerts to admins for critical events

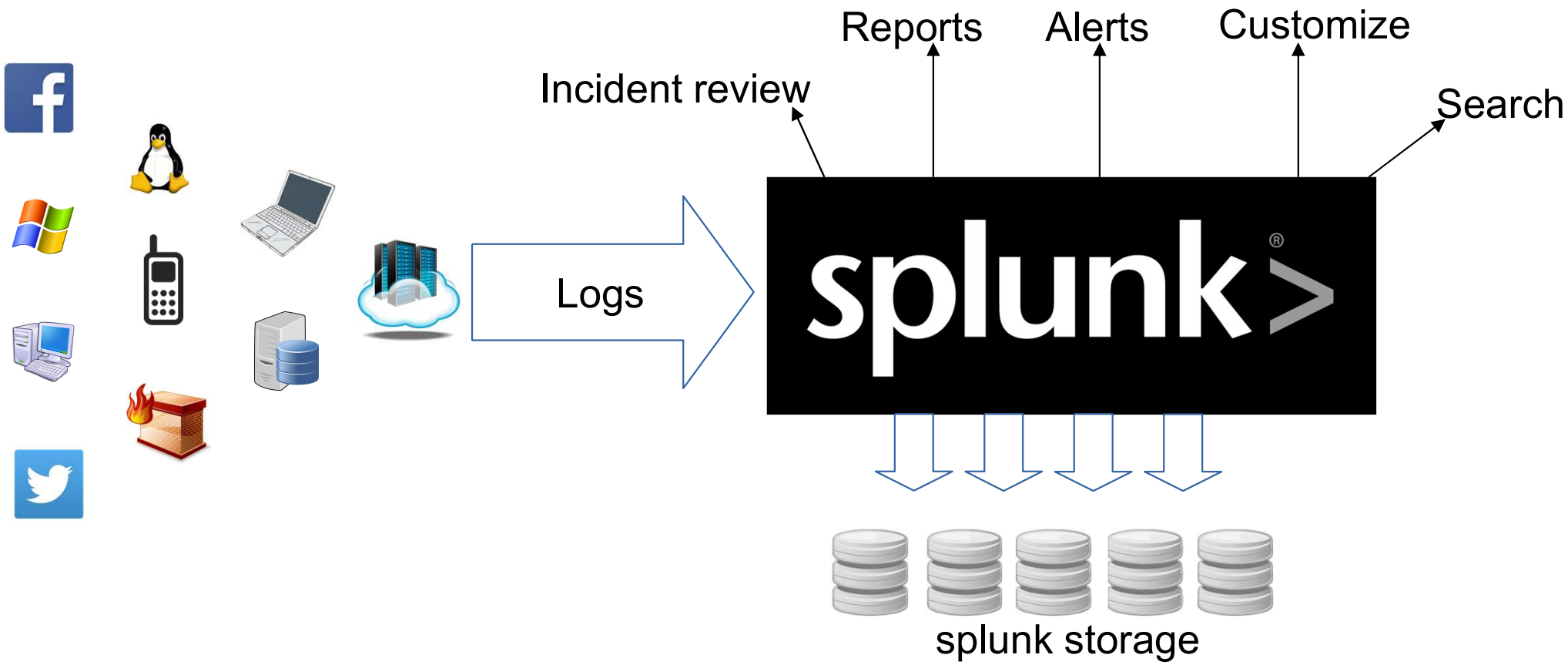
Tactics used to achieve the top 5 ASRs : Modifiability

Quality Attribute	Scenario (ASR)	Tactics
Modifiability	User should be able to modify use cases.	Provide the admins with ability to modify the use cases and add as per need.

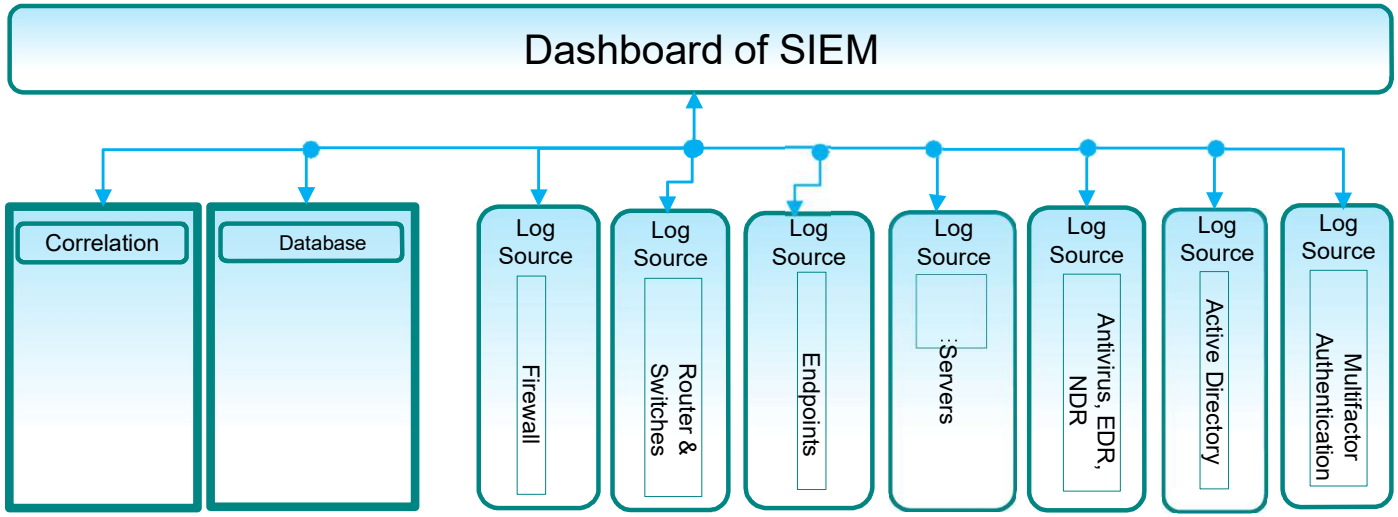
Tactics used to achieve the top 5 ASRs : Availability

Quality Attribute	Scenario (ASR)	Tactics
Availability	System should keep back up of complete system data including configuration and logs	Provide for provisions of complete configuration and log backup using real-time mirroring techniques

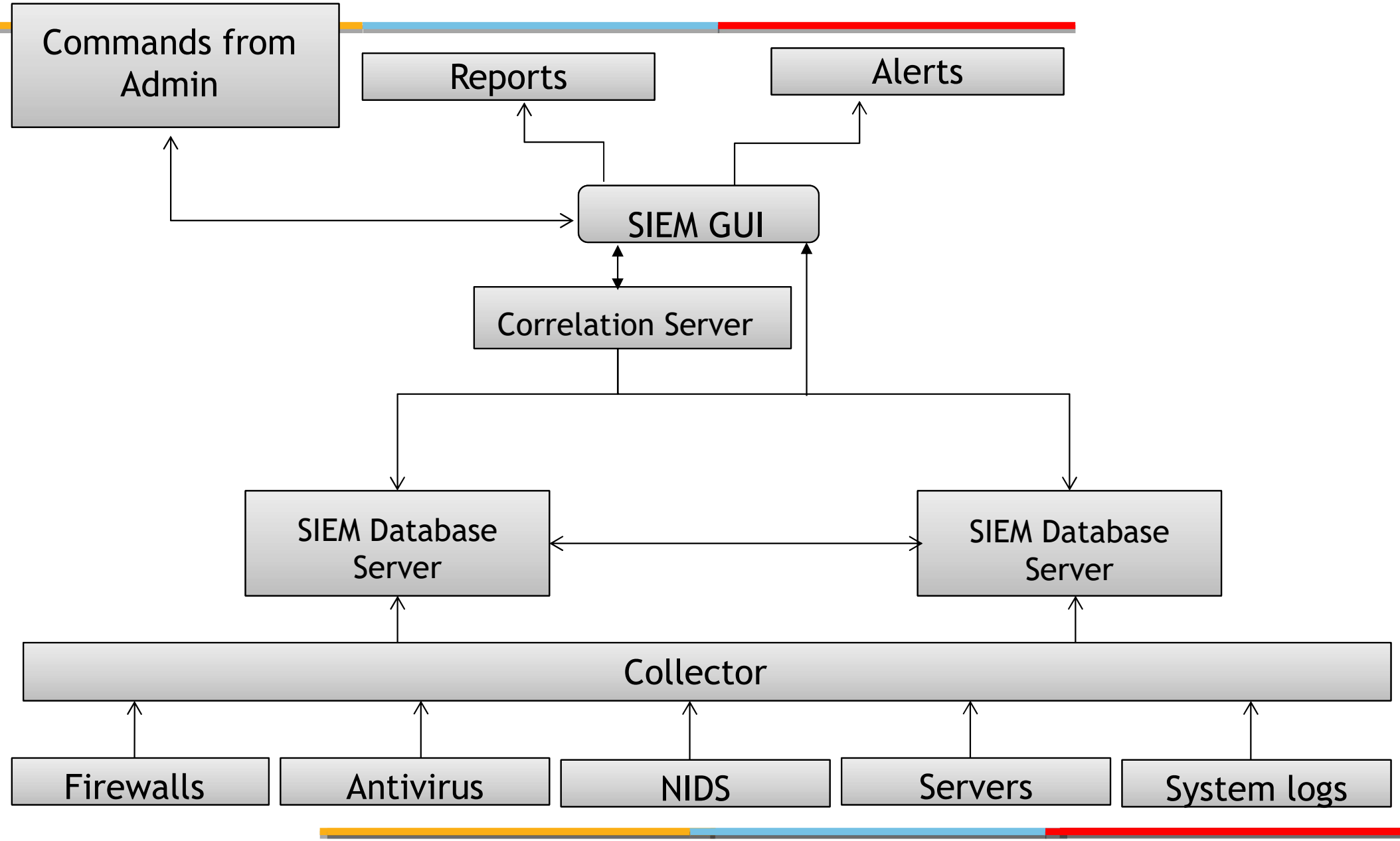
System Context Diagram



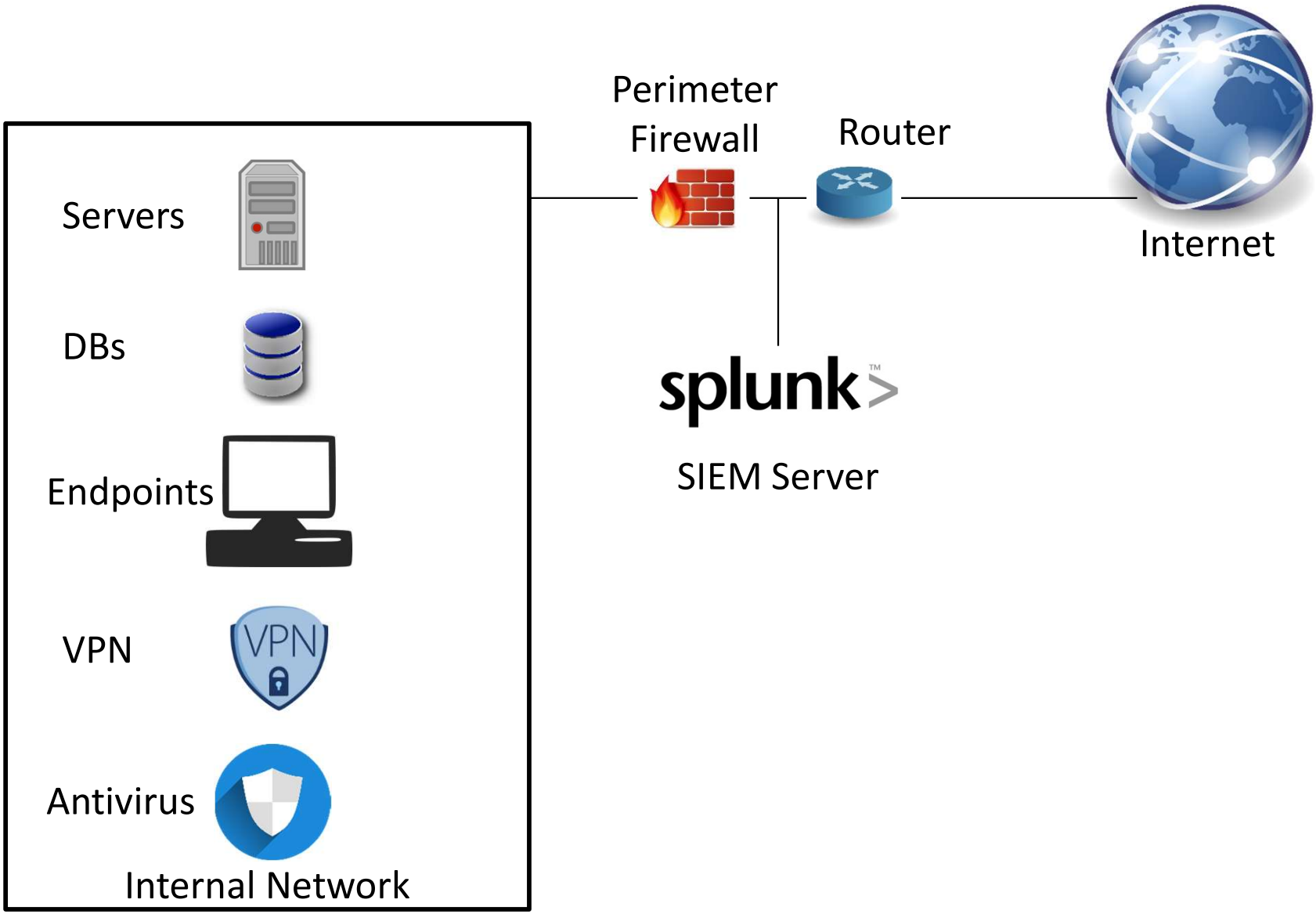
Module Decomposition Diagram



Component & Connection diagram



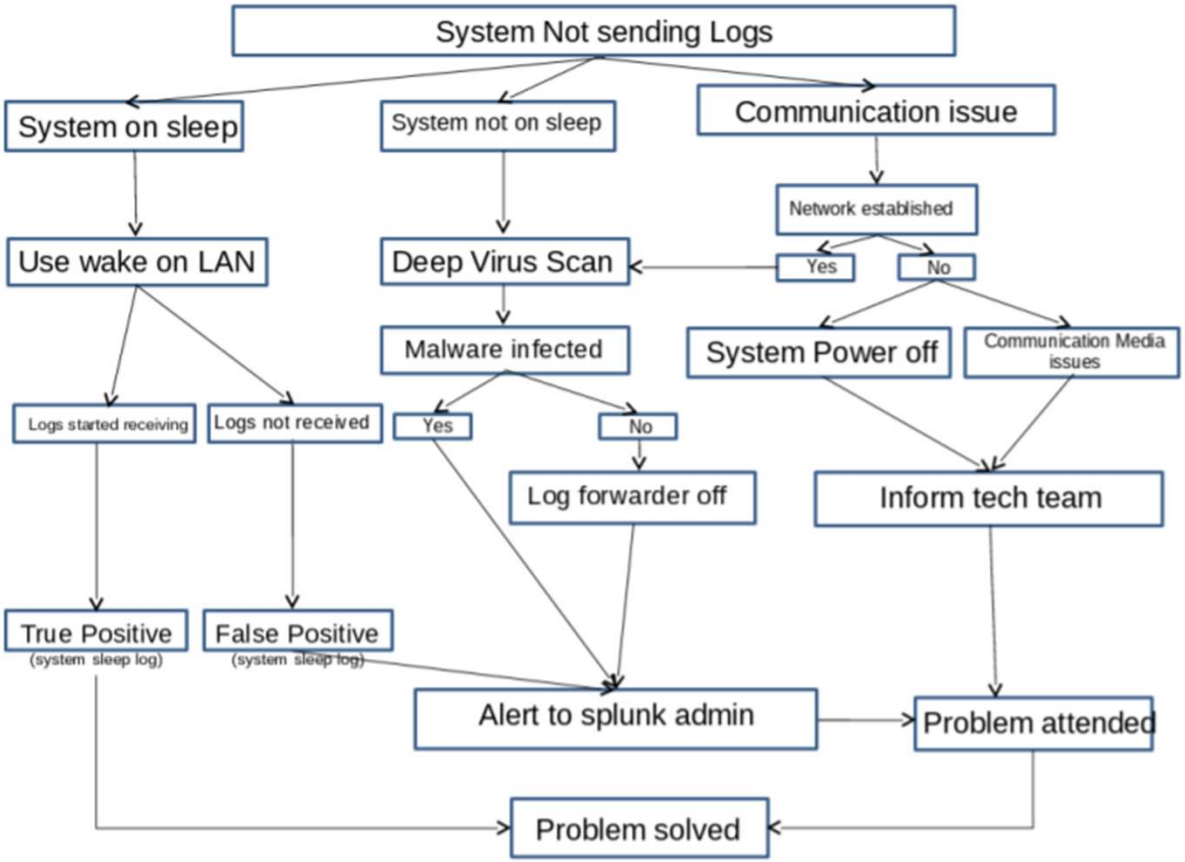
Deployment diagram



How SIEM works?

innovate achieve lead

SIEM correlates logs from various sources and presents it in a dashboard. Below is a sample working of very basic SIEM use case working.



Key Learnings

1. Learnt about key requirements and how they are categorized into functional and non-functional requirements
2. Understood the different types of diagrams and how they play a role in software architecture
3. Architecturally Significant Requirements documentation