



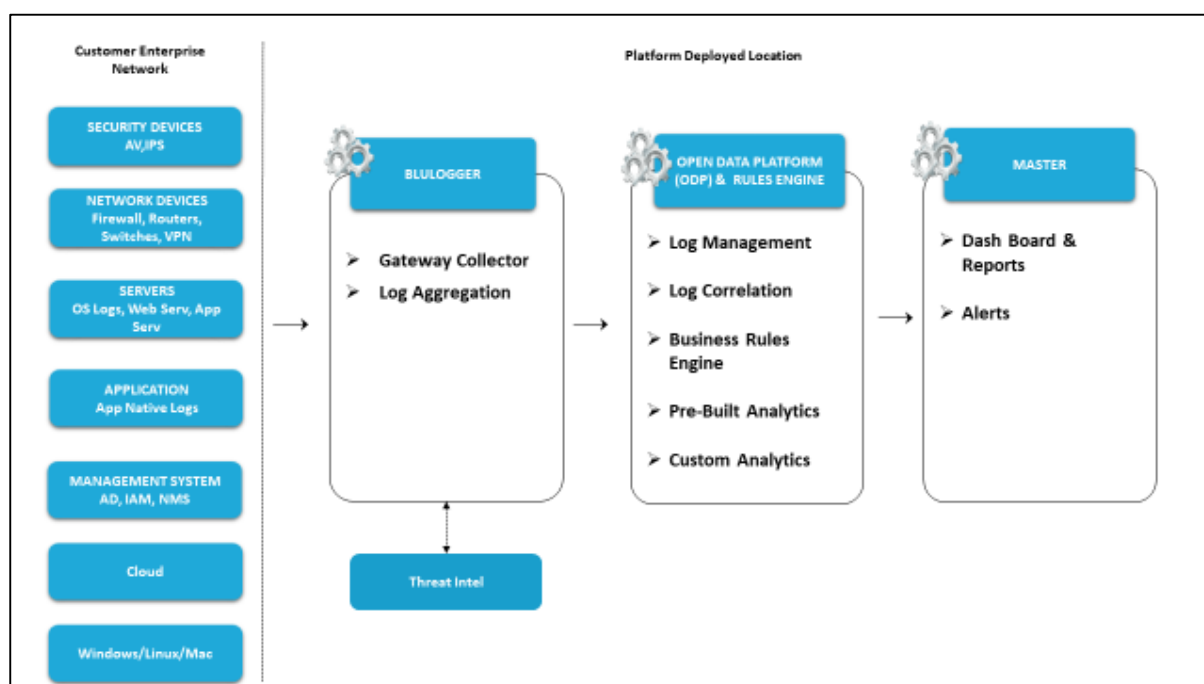
**BLU**SAPPHIRE  
INTELLIGENT CYBER DEFENSE

## BLUSIEM

Next-Gen Security Incident & Event Management System

## BluSIEM - (Next Gen SIEM)

BluSIEM brings you cutting edge SIEM capabilities with augmented ML-based detection models. It offers out of the box Predictive Analytics, MITRE ATT&CK Matrix mapping and Customizable Dashboards. Event Correlation and Analytics Event Correlation is an integral part with 1350+ built in uses cases / analytical models; option for flexible custom use case/rule building feature, which helps security teams to respond swiftly. The entire functionality is built on Big Data Platform which is horizontally scalable ensuring seamless operations.



### Log Forwarding & Processing Mechanism:

Log ingestion from but not limited to:

- Desktops/ Laptops (Example – Windows/Linux/Mac)
- Thin Clients
- Servers
- Virtual Machines
- Security Infrastructure (Example: Existing AV Solution, NTA, Firewall, Web Proxy, IDS Etc.)
- Network Infra- Syslog (Example: Switch, Router Etc.)
- Net-flow from Access & Core Switch

- h) Application Log
- i) Configuration Management systems

**Log Forwarding Agent:** BluSapphire's Log Telemetry Agent to be deployed in Desktop/ Laptop/ Thin Clients/ Servers and Virtual Machines in collecting advanced security log data and point it to BluSapphire BluLogger.

**Gateway and Streaming:** Organization's Log Sources are pointed towards BluSapphire's BluLogger which acts as a Gateway between Customer's Site & Central console of BluSapphire platform deployed site.

Example of collection from Log Sources:

- a) Logs from End Points via agent shall be pointed to BluLogger.
- b) Application specific Log information can be consumed into BluLogger by utilizing native log forwarding mechanism of respective application.
- c) Security Infrastructure such as Firewall can be consumed directly via native log forwarding mechanism. (Example: Firewall log consumption by pointing logs to BluLogger via UDP Protocol)

#### **Log Streaming & Processing Within BluLogger:**

BluSapphire's BluLogger has streaming capabilities which ensures that there is No Delay in log forwarding from IT assets for analysis.

Within BluLogger, there is a two-way check established which checks if log data has reached Big Data Index within BluSapphire platform deployed site. If the check fails, in that case, the log data shall be buffered for later consumption at a later point of time which ensures there is No Log information lost even if the connectivity between BluLogger in customer's premise and BluSapphire platform deployed site is lost.

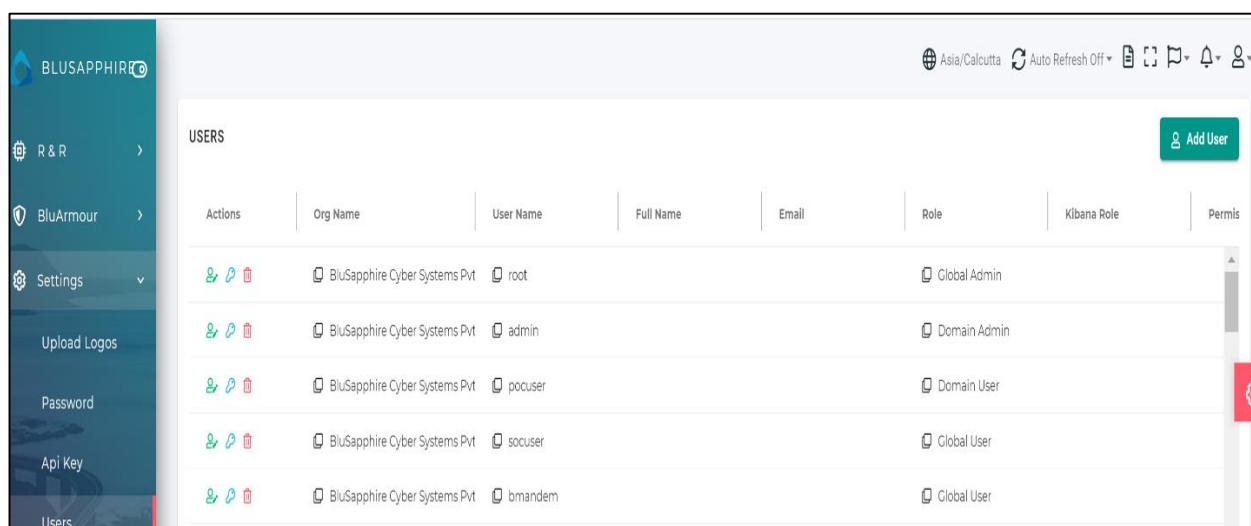
In a scenario where customer is expects BluLogger to consume Custom Log sources where a parser is yet to be developed; The functionality of consuming Non-Parsed Log is very much available within BluSapphire. It can ingest raw log and position it within a separate index of big data lake. Once parser is built, we can normalize and consume it back for analysis.











BluLogger utilizes customer's LAN to transfer the log data from source to BluSapphire's Open Data Platform. It normalizes and enriches the data for consumption by the platform.

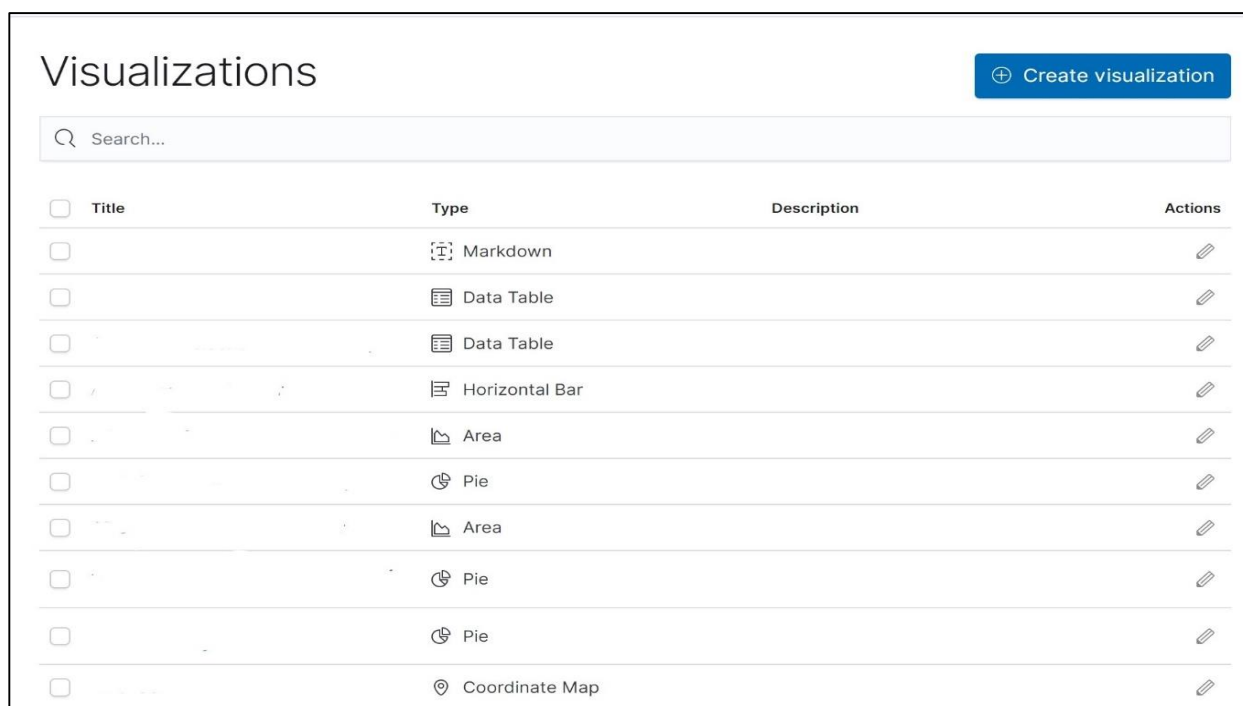
**Storage:** BluSapphire is bundled with an "Open Data Platform"(ODP) that leverage the new age Big Data technologies providing horizontal scalability, flexibility and raw on-demand analytical capabilities. Logs from the customer's site are shipped via BluLogger to central ODP. Our ODP provides Instant search results, even across terabytes of data. It can easily store & fetch the data available from any external storage device. It also enables infinite storage capabilities with near zero maintenance and management as an appliance.











**Authorization:** Role Based Authorization is available for manual access of log data within the index. (Potentially during manual log analysis. Forensic or Threat Hunt Activity).

Different roles & actions they can perform are shown as below:



Actions	Org Name	User Name	Full Name	Email	Role	Kibana Role	Permis
 	BluSapphire Cyber Systems Pvt	root			Global Admin		
 	BluSapphire Cyber Systems Pvt	admin			Domain Admin		
 	BluSapphire Cyber Systems Pvt	pocuser			Domain User		
 	BluSapphire Cyber Systems Pvt	socuser			Global User		
 	BluSapphire Cyber Systems Pvt	bmandem			Global User		



Title	Type	Description	Actions
<input type="checkbox"/>	Markdown		
<input type="checkbox"/>	Data Table		
<input type="checkbox"/>	Data Table		
<input type="checkbox"/>	Horizontal Bar		
<input type="checkbox"/>	Area		
<input type="checkbox"/>	Pie		
<input type="checkbox"/>	Area		
<input type="checkbox"/>	Pie		
<input type="checkbox"/>	Pie		
<input type="checkbox"/>	Coordinate Map		

**Log Format:** Both Raw & Normalized log are being stored within ODP which can be furnished on Demand.

**SIEM Rules, Analytics and Threat Intelligence Feeds:**

BluSapphire SIEM utilizes over 750+ rules which are built over Behaviour driven activity and are also mapped via MITRE ATT&CK. The rules also built-in detecting Advance persistent threat activity. This behaviour driven activity along with log & packet data will help in enriching the context for better insights

With this capability, the solution offers proactive anomaly detection.

**Custom Rule build:** The Engine allows to build custom rules based on the customers ask on demand.

**Threat Intelligence:** BluSapphire by design ingests Threat Intelligence from over 100+ sources (Combination of Commercial and Open-Source Feeds); currently, BluSapphire has active integration with MISP, and can consume feeds in the format of STIX, TAXII & CSV formatted threat intel sources.

**Sample Screenshots**

