**Splunk SIEM Questionnaire**

1. Does Splunk Infra Architecture already exists?
2. What are all different types of logs? Is the data coming from mainframe systems?
3. What are total number of Applications?
4. How much data per day ingested? What is the data Volume?
5. What is the strategy for installation/configuration of forwarder (GitHub or Linux)?
6. Do we need to check feasibility in terms of forwarder installation and configuration on each Application Server.
7. Is SMTP configured for Alerting?
8. Is the Data Correlated? Rules and standard defined properly as per logging format?
9. What is the Retention and Archiving Policy on Logs?
10. What are all external systems involved? Antivirus or something like that?
11. How is access control methods for Splunk Users (For authentication and authorization)?

**Input on Sizing**

Considering the Splunk Data Load from all the logs is around 450 GB / Day

Due to the performance and worst case scenario I’m considering as 1 TB / Day

The Following Splunk sizing would be recommended

Data Input :

|  |  |
| --- | --- |
| Daily Volume | 1000GB |
| Raw Compression | .15 % |
| Metadata Size Factor | .35% |
|  |  |

Data Retension :

|  |  |
| --- | --- |
| Hot / Warm Bucket | 7 Days |
| Cold | 30 Days |
| Frozen | 6 Months |
| Total Retention | 7 Months |

Architecture ( for ES kind of App )

|  |  |
| --- | --- |
| Max Volume per Indexer | 260 GB |
| Number of Nodes – Clustered | 4 Nodes |
|  |  |

Storage Required : ( Per Indexer )

|  |  |
| --- | --- |
| Hot | 875 GB |
| Cold | 3.7 TB |
| Archived | 6.6 TB |
| Total | 11.1 TB |

Sample Index Configuration will look alike as shown here :

indexes.conf

# volume definitions

[volume:hotwarm\_cold]

path = /mnt/fast\_disk

maxVolumeDataSizeMB = 4980736

# index definition (calculation is based on a single index)

[main]

homePath = volume:hotwarm\_cold/defaultdb/db

coldPath = volume:hotwarm\_cold/defaultdb/colddb

thawedPath = $SPLUNK\_DB/defaultdb/thaweddb

homePath.maxDataSizeMB = 896000

coldPath.maxDataSizeMB = 3840000

maxWarmDBCount = 4294967295

frozenTimePeriodInSecs = 3196800

maxDataSize = auto\_high\_volume

coldToFrozenDir = /mnt/big\_disk/defaultdb/frozendb

**Proposed Splunk Architectural Diagram for SIEM ES Platform**

