

**Cognizant’s Response to Telefonica**

RFQ PART 3 TECHNICAL PROPOSAL

*Dated: 14th September 2018*

Proprietary Notice

The information and data furnished in this proposal shall not be furnished outside “Telefonica”. This information shall not be duplicated, used or disclosed in whole or part for any purpose other than to evaluate this proposal; provided, that if a contract is awarded to this offer or as a result of or in connection with the submission of this information/data. The customer shall have the right to duplicate, use or disclose the information/data to the extent provided in the contract. This restriction does not limit the customer right to use the information contained in the proposal if it is obtained from another source without restriction.

**© 2018 Cognizant Technology Solutions**

Contents

[1. Executive summary 4](#_Toc525118849)

[SUMMARY OF THIS PROPOSAL 5](#_Toc525118850)

[PART 2 GENERAL INFORMATION OF PROPOSER AND EXPERIENCE 7](#_Toc525118851)

[Industry Experience 9](#_Toc525118852)

[3.0 FUNCTIONAL REQUIREMENT SOLUTION 10](#_Toc525118853)

[3.1 Splunk Architecture: 10](#_Toc525118854)

[Search Head Instance specification 14](#_Toc525118855)

[Indexer Instance Breakdown 14](#_Toc525118856)

[Management Instance Breakdown 14](#_Toc525118857)

[Forwarder Quantity Information 16](#_Toc525118858)

[License Information 16](#_Toc525118859)

[Volume 17](#_Toc525118860)

[TEST SETUP: To be UPdated 18](#_Toc525118861)

[3.3 LOG SOURCE & CORRELATION SEARCHES: 19](#_Toc525118862)

[3.4 ALERTS 19](#_Toc525118863)

[3.5 DASHBOARDS 20](#_Toc525118864)

[3.6 SYSTEM HEALTH & performance MONITORING 20](#_Toc525118865)

[4.0 service requirement 22](#_Toc525118866)

[4.1 DEPLOYMENT APPROACH 22](#_Toc525118867)

[4.2 Supplied Resources 25](#_Toc525118868)

[4.4 Project Management 26](#_Toc525118869)

[4.5 Test and Acceptance Procedures 27](#_Toc525118870)

[4.6 RACI 28](#_Toc525118871)

[5.0 Support and Maintenance for SIEM Tool 30](#_Toc525118872)

[RACI 31](#_Toc525118873)

[SERVICE LEVELS 31](#_Toc525118874)

[6.0 Risk & MITIGATION 32](#_Toc525118875)

[8 Appendix 34](#_Toc525118876)

[8.1 Cognizant Quality Management System Framework 34](#_Toc525118877)

[8.2 NextGen SOC Framework 37](#_Toc525118878)

# Executive summary

Cognizant would like to thank Telefonica for providing an opportunity to participate in this RFP to standardize the logging infrastructure, mechanism and logging policies across the organization thereby standardizing the way it collects, consumes and discards the various logs coming from numerous devices in its datacentres.

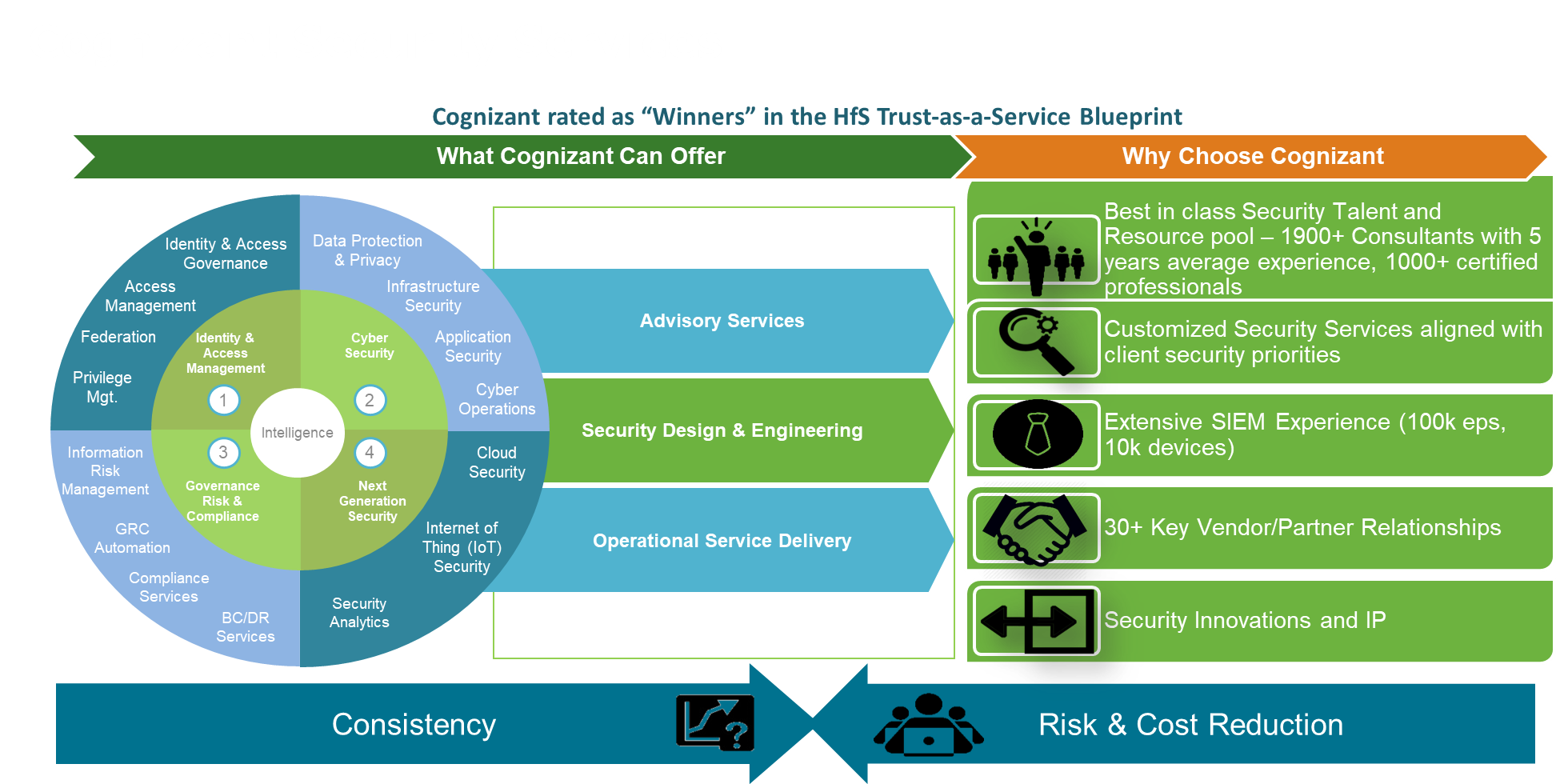
Cognizant is confident that it can deliver value and help to achieve Telefonica’s objectives based on its extensive experience and competency in delivering end to end solution around Infrastructure Security Designing, assessment and implementation.

For the purpose of this RFP, considering the objectives, business requirements of Telefonica and Telefonica’s choice, Cognizant is proposing Splunk based SIEM solution to meet the requirement.

With Cognizant’s extensive experience in handling similar threat management engagements with Splunk, we bring in our delivery experience to build a standardized SIEM technology to collect, analyse and store log data in a centralized manner. Following are Salient Features of our Solution

* Enterprise-scale, modular and resilient SIEM architecture to sustain event collection with minimal risk of data loss
* Cluster design allowing Telefonica to scale by introducing additional components in the cluster
* Experienced Splunk Certified skilled resource to help Telefonica meets its objective of robust SIEM platform
* Onsite Availability of Resources at Telefonica site 8x5 for high touch engagement with Telefonica
* Recommend readily available use cases based on Cognizant experience working with other customers
* SLA and KPI based service delivery during Maintenance phase

Cognizant believes that the following are some of the key Cognizant’s differentiators to bid this proposal and why we consider it a privilege to be a partner with Telefonica.



# SUMMARY OF THIS PROPOSAL

Telefonica is planning to deploy a standardized SIEM technology to collect, analyse and store log data that originate in network devices, servers, hosts, applications and other end-point log sources to effective means to identify and mitigate security events.

The objective of this project is to -

* Build a centralized SIEM platform for log-correlation and alerting and built in default Security use case templates enabling Telefonica SOC team to build use cases for Security Event Monitoring, triage, analysis and investigation
* Integration of log sources
* Handover to Telefonica SoC Team for Monitoring and Administration
* Post Deployment 8x5 SIEM Application components 2nd Level Maintenance & Support services [ Limited to Splunk Enterprise and Enterprise Security Application platform related issues]

**Activities in Scope**

* Design & Implementation of the proposed Splunk based SIEM solution Telefonica DC in Frankfurt
* Integration of Log Sources as mentioned in the “Systems to be connected” from the “functional requirements” document
* Deploy Splunk Enterprise security app that would enable Telefonica SOC team to build the correlation rules mentioned in the “Log correlation and use cases” from the “functional requirements” document
* Enable User Management and Authorization
* Handover to Telefonica SoC Team for Monitoring and Administration
* Post Deployment 8x5 SIEM Application components 2nd Level Maintenance & Support services [ Limited to Splunk Enterprise and Enterprise Security Application platform related issues]

**Out of Scope**

* VM, Backup & Network Infrastructure Deployment, Management and Troubleshooting
* Policy, standard and recommendation decisions
* Hands and Feet support
* Product evaluation for future state technology/migration
* Performing audit
* Procurement of License and Tools

The following table describes the Cognizant strategy to meet the high level objectives of Telefonica

|  |  |  |
| --- | --- | --- |
| Telefonica Objectives | Solution tenets | Benefits to Telefonica |
| SIEM Implementation and Design | Cognizant will provision a SIEM Architect with relevant experience of the proposed SIEM solution. The architect will be responsible for Design, Configuration, and Integration of agreed log sources, Customized Dashboard, Correlation rules and Reports creation as per Telefonica requirement. Fine-tuning of the platform. | Experienced and skilled resource helps Telefonica to meets its objective to robust SIEM design and implementation. |
| SIEM (security information and event management) deployment for Log Consolidation and detect and prevent potential security issues. | Cognizant proposes Splunk Enterprise Security SIEM solution that will be deployed at the datacentres of Telefonica located in Frankfurt that is capable enough to handle the initial 300 GB/Day capacity and scale further by onboarding additional component within the cluster.  The proposed solution provides a scalable, easy-to-use, intelligent and robust architecture for Security Incident Monitoring and Investigation that delivers-   * An architecture that is enterprise-scale, modular and resilient to sustain event collection with minimal risk of data loss * Enhanced incident management capabilities by supporting real-time detection of, investigation of emerging threats in the environment.   . | * An architecture that is enterprise-scale, modular and resilient to sustain event collection with minimal risk of data loss * Cluster design allows Telefonica to scale by adding additional components in the cluster * High Availability at the log collection level * Dedicated Search Head for Enterprise Security app |
| Integration | * Onboard Log Sources as mentioned in the “Systems to be connected” from the “functional requirements” document * Deploy Splunk Enterprise security app * Recommend additional use cases based on Cognizant experience with other customers during Implementation stage and during Operations stage as well * Configure dashboards and reporting | * Enable Telefonica SOC Team to leverage Splunk Enterprise security app or build correlation rules and use cases for Security Event Monitoring, triage, analysis and investigation. * Cognizant Splunk Experts Onsite providing second level support during maintenance phase based on change request initiated by Telefonica SOC team |
| Archiving for 6 Months | The solution is sized Virtual Environment with Required storage specification and parameters for Log Retention. | Enables Detection & Investigation possibilities for a longer period in the past in a central platform for all network elements |
| Reporting | Out-of-the-box content templates for reporting and dashboards for numerous regulatory compliance For example: NERC-CIP, HIPAA, SOX, PCI-DSS, EU 8th Directive etc. | Meets Telefonica’s compliance reporting requirement. |
| Handover to Telefonica SOC personnel | Handover to Telefonica SoC Team for Monitoring and Administration | Well defined Design and Build documents |
| Post Deployment Maintenance Support | Post Deployment 8x5 SIEM Application components 2nd Level Maintenance & Support | Experienced Splunk Certified Resource  SLA based delivery  Onsite Availability at Telefonica site 8x5 for high touch engagement with Telefonica  Gather feedback from Telefonica Operations, recommend appropriate changes |

# PART 2 GENERAL INFORMATION OF PROPOSER AND EXPERIENCE

We believe that we are perfectly positioned to successfully deliver this project due to the following strong levers-

* **Cognizant’s Enterprise Risk & Security Solutions (ERSS) practice’s expertise:** Cognizant is one of the first large System Integrators to establish a dedicated Information Security Practice – Infrastructure security and Digital security under one umbrella named- Enterprise Risk & Security Solutions (ERSS). ERSS practice specializes in providing Information Security Solutions for Banking & Financial Services domain. ERSS practice focuses on mitigating enterprise IT risks to achieve a measurable ROI of security solutions that provide for Compliance, Risk Management and Business Enablement. ERSS has already served 400+ customers across the world. It has CISSP/CISA/CISM/CEH, Security+ certified associates along with vendor security product certifications. ERSS covers Governance, Risk & Compliance; Identity & Access Management; Application Security Services; Data Protection & Privacy; and Integrated Threat Management. ERSS has a long list of Banking, Financial Services & manufacturing industry clientele.
* **Domain Knowledge & similar engagements experience**: Integrated Threat Management (ITM) wing of ERSS has successfully completed similar engagements for various customers across geographies and has more than 1000+ years of man experience in SIEM consulting, implementation and support. This engagement will be completely led, managed and staffed by seasoned professionals from this practice, who will bring in relevant experience and best practices derived from similar implementations at other client organizations. Cognizant has experience of implementing right SIEM solution based on client Infrastructure, Network topology, Business Requirements, Reporting requirements. Cognizant has experience of implementing & managing following SIEM solutions- Splunk, RSA envision, IBM Q-Radar, SPLUNK SIEM etc. for 15+ Global customers across different verticals BFS, Insurance, Retail, Healthcare ,E&U etc.
* **Experience relevant to the Proposed Solution:** Cognizant has a pool of 20+ Splunk Certified Professionals that support existing customers and developed scripts and use cases on this platform. Apart from Cognizant being a Managed Service provider (MSP) partner for Splunk, Cognizant has expertise in implementing, monitoring and managing Splunk SIEM. Team has repository of developed scripts and use cases. Cognizant has 10+ SOCs which are both dedicated and shared SOC’s servicing global customers. The SOC for the customers are located both at US and India.
* **MSP partner for Splunk:** Being a MSP partner for Splunk, Cognizant has the partner enablement on new technologies, access to Splunk SME for any kind of support during implementation and solution validation by Splunk Architects. This will ensure enhanced design, implementation and support services to Telefonica.



# Industry Experience

**Case studies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Services Provided by Cognizant** | **Volumetric Information** | **Customer** | **Optimization** |
| SIEM, Vulnerability Management  DLP & Content Security Services  Incident Management & Remediation | * 5000 EPS * 5000 IP Addresses * 3000 devices * McAfee – Endpoint, IPS, DLP, Web Gateway, SIEM | Leading Financial Major in North America | 20 % Reduction in EPS after Noisy traffic Filtration and change in aggregation Parameters  3 to 4 New Correlation rules per Quarter being introduced to detect the latest threats  10 New log sources being integrated per month |
| SIEM, Vulnerability Management  Security Device Management  Incident Management & Remediation | * 10,000 EPS * 10,000 IP Addresses * 5000 devices * RSA, Qualys, Algosec, Cisco ISE | Leading Financial major in Europe | 40 % Reduction in EPS after Noisy traffic Filtration and change in aggregation Parameters  8 to 10 New Correlation rules per Quarter being introduced to detect /the latest threats  25 New log sources being integrated per month |
| SIEM Services | * 6700 log sources * 7500 EPS * QRadar | Leading Retailer in North America | 25 % Reduction in EPS after Noisy traffic Filtration and change in aggregation Parameters  5 to 6 New Correlation rules per Quarter being introduced to detect the latest threats  15 New log sources being integrated per Quarter |
| SIEM Services  Security Device Management | * 3500 Endpoints * 2500 EPS * RSA Security Analytics | Leading Healthcare Company in North America | 10 % Reduction in EPS after Noisy Traffic Filtration and change in aggregation Parameters  2 to 3 New Correlation rules per Quarter being introduced to detect the latest threats  5 New log sources being integrated per Quarter |

**References for each of the above experiences**

We have carefully identified some of our relationships from over 400+ customers we presently service. All customers provided as a reference in this section are currently active and are engaged with Cognizant in multiple initiatives across a spectrum of services. For all these valued customers, we are presently performing or have recently performed the services requested as part of this RFP. We believe these relationships will provide you with a clear perspective on Cognizant’s customer centricity and delivery capabilities. The repeat business we gain from our existing customers stands as a testament to our focus on the customer needs and delivery capability.

The customer contact and reference calls can be arranged on request. We will do our best to schedule the meetings within the stipulated time subject to customer availability.

| **Experience#** | **Customer** | **Services Provided** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

# 3.0 FUNCTIONAL REQUIREMENT SOLUTION

Based on the wide analysis and comparison across these SIEM projects, Cognizant has determined to propose the cost effective **Splunk** (Enterprise Security Manager) that would perfectly fit in for the requirement.

**Why Splunk?**

* Splunk can deliver the performance, actionable intelligence, and real-time situational awareness as required by Telefonica.
* The Solution brings in holistic management of Threats from a single console because of the integration capabilities it brings with other components.
* High event collection rate suited for very large scale deployment like Telefonica

SIEM TOOL:

There are two key aspects to a Splunk SIEM Solution:

1: Splunk Enterprise:

Splunk Enterprise is a software product that enables search, analysis and Visualization of data gathered from the components of IT infrastructure or business. Splunk Enterprise takes in data from websites, applications, sensors, devices, and so on. After you define the data source, Splunk Enterprise index the data stream and parses it into a series of individual events that you can view and search.

Users connect to Splunk Enterprise with a web browser and use Splunk Web to administer their deployment, manage and create knowledge objects, run searches, create pivots and reports, and so on. Users can also use the command-line interface to administer your Splunk Enterprise deployment.

2: Splunk Enterprise Security:

Splunk Enterprise Security is an app that is deployed on search head. It uses the Splunk platform's searching and reporting capabilities to provide the security practitioner with an overall view of their organization's security posture. Enterprise Security uses correlation searches to provide visibility into security-relevant threats and generate notable events for tracking identified threats.

A correlations search is a type of saved search that scans multiple data sources for defined patterns, to detect suspicious events or patterns in your data. If a suspicious event is detected, a notable event is created. The notable event can then be investigated using the Incident Review dashboard in ES.

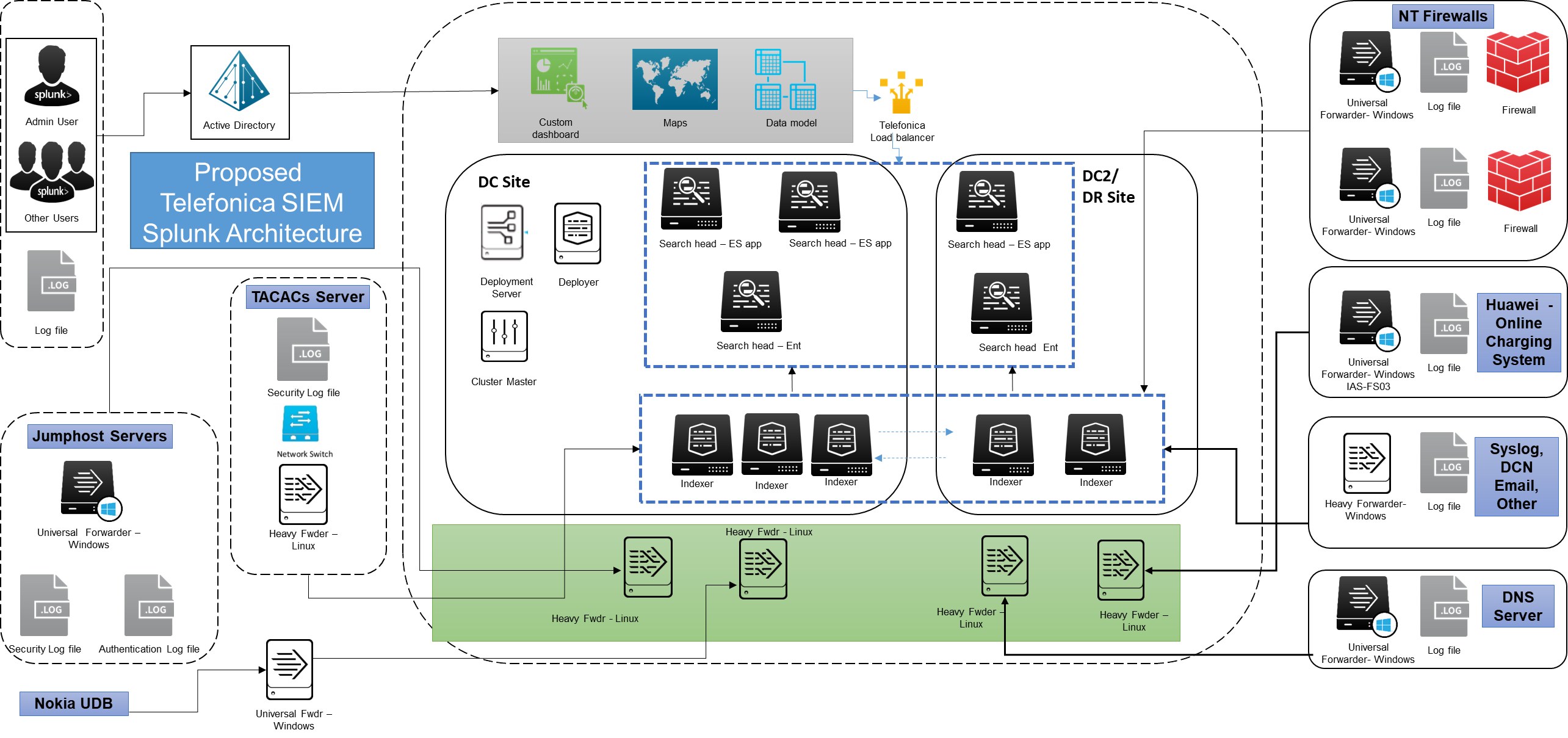
## 3.1 Splunk Architecture:

Cognizant recommends Telefonica to deploy Distributed, multi-site (dual site) clustered model of Indexers and Search Headers and integrate log sources across Enterprise. Strategic locations within multiple Data centers should be identified for the placement of Heavy forwarders and route the traffic to the central location after filtering out unwanted logs. Below is the Indicative architecture based on assumptions that the components will be deployed in two DC’s for cluster and continuity during DC Failure. The architecture is designed for high Availability at Indexer and Search head level. Universal Forwarder forwards logs to Heavy Forwarders and will be configured

For the easier administration of Universal forwarders and related configurations, Cognizant recommends to have “Deployment Server” or any other similar configuration management tools.

A search head cluster is a group of interchangeable and highly available and Splunk Enterprise search heads. For failover with clustering, three search heads are required

Indexer clusters consist of groups of Splunk Enterprise indexers configured to replicate each other’s data so that the indexes of the system become highly available. By maintaining multiple, identical copies of indexes, clusters prevent data loss while promoting data availability for searching.



**Solution Components & Description:**

1. The master node controls the entire cluster. Although the master resides physically on a site, the master is not actually a member of any site. However, each master has a built-in search head, and that search head requires that you specify a site for the master as a whole. Note that the master's search head is for testing purposes only. Do not use it in a production environment.
2. Concurrent search is support by no. indexers with cores per indexer, our solution is designed to handle more than 6 concurrent searches.
3. Universal forwarders use a lightweight version of Splunk Enterprise that simply inputs data, performs minimal processing on the data, and then forwards the data to a Heavy Forwarders. Because its resource needs are minimal, it can also be deployed on the machines that produce the data, such as web servers. During due diligence stage such system shall be identified.
4. Data enters the system through forwarders, which consume external data, perform a small amount of pre-processing on it, and then forward the data to the indexers.
5. A Cluster of Heavy forwarders will be deployed across the two DC’s. All data from one group of machines/Universal forwarders will be sent to one indexer and all data from a second group of machines to a second indexer. Heavy forwarders will parse data before forwarding it to the receiving indexer, thus allowing indexer to handle only the indexing segment. Heavy forwarders shall be configured to filter and route data to specific receivers based on source, source type, or patterns in the events themselves. Heavy forwarders can also look inside the events and filter or route accordingly.
6. Cognizant has assumed one DC and One DR wherein the heavy processing components – Search head and Indexers would be deployed.
7. Each of the two sites [DC and DR] has its own indexers deployed as a cluster. An indexer cluster is a group of Splunk Enterprise indexers that are configured to replicate each other’s' data, so that the system keeps multiple copies of all data. This process is known as index replication. Multiple clustered search-peers (indexers) improves performance both during data-ingest and search. This strategy reduces search time and provides redundancy of data-ingest and availability should a single server fail.
8. By maintaining multiple, identical copies of Splunk Enterprise data, the cluster prevents data loss while promoting data availability for searching. Splunk Enterprise clusters feature automatic failover from one indexer to the next. This means that, if one or more indexers fail, incoming data continues to get indexed and indexed data continues to be searchable.
9. Each of the two sites has its own search head, which searches the set of peer nodes on its site. This is an example of a cluster that has been configured for search affinity. A search head cluster is a group of search heads that serves as a central resource for searching. The search heads share knowledge objects, apps, and all other configurations. You can run the same searches, view the same dashboards, and access the same search results from any search head in the cluster.
10. A total of five search heads will be deployed with Splunk Enterprise Security app installed on Three search heads and other two with only Splunk Enterprise Search. Search specific to security can be executed on search head deployed with Splunk Enterprise Security app while basic search can be installed on Search head without ES app.
11. The peers replicate data across site boundaries. This behaviour is fundamental for both disaster recovery and search affinity.
12. Multisite replication and search factors determine the number of bucket copies and searchable bucket copies, respectively, in the cluster. Multisite replication and search factors also determine the number of copies on each site
13. Multisite clusters provide search affinity, which allows searches to occur on site-local data. Search affinity is always enabled in a multisite cluster, but you must perform a few steps to take advantage of it. Specifically, you must ensure that both the searchable data and the search heads are available locally
14. When a peer goes down, bucket fix-up happens within the same site, if possible. The cluster tries to replace any missing bucket copies by adding copies to peers remaining on that site. (In all cases, each peer can have at most one copy of any particular bucket.) If it is not possible to fix up all buckets by adding copies to peers within the site, then, depending on the replication and search factors, the cluster might make copies on peers on other sites
15. Site failure is just a special case of peer node failure. Cluster fix-up occurs following the rules described earlier for peer node failure. Of particular note, the cluster might hold copies in reserve against the eventual return of the site.
16. Cluster setup would require enough WAN bandwidth availability between the two DC’s.
17. The deployment server is not supported as a means to distribute configurations or apps to cluster peers. To distribute configurations across the set of cluster peers, instead use the configuration bundle method.
18. Traffic between forwarders and indexers is encrypted using SSL and TLS.
19. Heavy forwarders can be configured to parse and drop the traffic logs that are not relevant and configure to accept only the event of interest.
20. Monitoring Console will be configured on Deployment server that will act as diagnostic tools inward to analyse and troubleshoot problems in your Splunk environment.

**Benefits of (dual-site cluster)**

1. Cost of the deployment with high-availability for entire enterprise will be optimum
2. Easy management, one place to integrate different type of devices
3. Efforts during initial deployment and post-deployment activities like upgrade, patches etc. will be easy
4. Ongoing SOC efforts by Telefonica will be less – if Telefonica selects dual-site cluster instead of individual Splunk infrastructure per Data Centre
5. Rolling out organization wide lookup for malware or malicious detail capture will be easy

***Hardware sizing:***

Below specification are considering Splunk will be deployed on a Virtual environment provisionedby Telefonica.

Splunk Enterprise Security in a virtualized environment requires same memory and CPU allocation as a non-virtualized bare-metal environment and needs following to be considered.

* Reserve all CPU and memory resources.
* Do not oversubscribe hardware.
* Splunk indexers are usually CPU-and disk I/O-intensive, so disk exposed to these indexers within virtual machines should be capable of 1200+ random seeks per second

Cognizant assumes that Telefonica will validate VM hardware sizing and UNICA compatibility with OEM – Splunk during due diligence phase through professional services.

Considering the Splunk Data Load from all the logs is around 300 GB / Day

|  |  |  |
| --- | --- | --- |
| Instance Family | Quantity | Location |
| Search Heads | 5 | Frankfurt [ 3 in DC and 2 in DR Site] |
| Indexers | 4 | Frankfurt [ 2 in DC and 2 in DR Site] |
| Deployment Servers | 1 | Frankfurt |
| Deployer | 1 | Frankfurt |
| Cluster Master | 1 | Frankfurt |
| License Servers | 1 | Frankfurt |
| Distributed Management Console | 1 | Frankfurt |
| Heavy Forwarders | 6 | Frankfurt |
| Universal Forwarders | 6 | Frankfurt |

# Search Head Instance specification

|  |  |
| --- | --- |
| Search Head Cluster | Description |
| Processors Info | 32 CPU cores at 2GHz or greater speed per core |
| Operating System | 64-bit Linux distribution |
| Disk Subsystem | 800+ random seeks per second |
| Disk Info | 416 GB virtual Disk (SSD) |
| RAM | 64 GB |
| Number of Instances | 6 |

# Indexer Instance Breakdown

|  |  |  |
| --- | --- | --- |
| Indexer Cluster | Description | |
| Processors Info | 48 CPU cores at 2GHz or greater speed per core | |
| Operating System | Linux RedHat Enterprise 7 | |
| Disk Subsystem | | 1200+ random seeks per second |
| Disk Info | Please see below table on Data Input and Data Retention | |
| RAM | 128 GB | |
| Number of Instances | 5 | |

# Management Instance Breakdown

|  |  |
| --- | --- |
| License Master | Description |
| Processors Info | 4 Core |
| Operating System | Linux RedHat Enterprise 7 |
| Disk Info | 125 GB virtual disk (SAS) |
| RAM | 8 GB |
| Number of Instances | 1 |
| Notes | Virtual Machine |

|  |  |
| --- | --- |
| Deployment Server | Description |
| Processors Info | 12 CPU cores at 2GHz or greater speed per core |
| Operating System | Linux RedHat Enterprise 7 |
| Disk Info | 356 GB virtual disk (SAS) |
| RAM | 16 GB |
| Number of Instances | 1 |
| Notes | Virtual Machine |

|  |  |
| --- | --- |
| Cluster Master | Description |
| Processors Info | 4 shared Core |
| Operating System | Linux RedHat Enterprise 7 |
| Disk Info | 356 GB virtual disk (SAS) |
| RAM | 4 GB |
| Number of Instances | 1 |
| Notes | Virtual Machine |

|  |  |
| --- | --- |
| Deployer | Description |
| Processors Info | 4 shared Core |
| Operating System | Linux RedHat Enterprise 7 |
| Disk Info | 356 GB virtual disk (SAS) |
| RAM | 4 GB |
| Number of Instances | 1 |
| Notes | Virtual Machine |

|  |  |
| --- | --- |
| Distributed Management Console | Description |
| Processors Info | 4 Core |
| Operating System | Linux RedHat Enterprise 7 |
| Disk Info | 121 GB virtual disk (SAS) |
| RAM | 4 GB |
| Number of Instances | 1 |
| Notes | Virtual Machine |

# Forwarder Quantity Information

|  |  |  |
| --- | --- | --- |
| Item | Amount | Specifications |
| Universal Forwarders | 6 +  Additionally, Universal forwarders can also be deployed on the machines that produce the data, such as web servers. During due diligence stage such system shall be identified. | 6 CPU 12 GB Memory 300 GB Disk |
| Heavy Forwarders | **6** | 12 CPU 24 GB Memory 800 random seeks per second 300 GB Disk |

# License Information

|  |  |
| --- | --- |
| Module | Volume |
| Splunk Enterprise | 300GB/Day |
| Splunk Enterprise Security | 300 GB/Day |

**Data Input:**

|  |  |
| --- | --- |
| Daily Volume | 300GB |
| Raw Compression | .15 % |
| Metadata Size Factor | .35% |

**Data Retention:**

|  |  |  |  |
| --- | --- | --- | --- |
| Hot / Warm Bucket | 7 Days | 350.0 GB per Indexer | Hot Data Contains newly indexed data. Open for writing. One or more hot buckets for each index.  Warm Data rolled from hot. There are many warm buckets. Data is not actively written to warm buckets. |
| Cold | 30 Days | 1.5 TB per Indexer | Data rolled from warm. There are many cold buckets. |
| Frozen | 6 Months | 2.6 TB per Indexer | Data rolled from cold. The indexer deletes frozen data by default, but you can choose to archive it instead. |
| Total Retention | 7 Months |  |  |

Storage requirement per Indexer: 4.8 TB

Total Storage requirement: 24 TB

**NETWORK LATENCY LIMIT**

For indexer cluster nodes, network latency should not exceed 100 milliseconds.

For search head clusters, latency should not exceed 200 milliseconds.

## LOG SOURCE VOLUME

|  |  |  |  |
| --- | --- | --- | --- |
| **Log Source** | **Type of Logs** | **Volumes** | **Estimated log size by Telefonica in GB/Day** |
| NT-Firewalls [Checkpoint, Juniper (Netscreen/SRX), CISCO(ASA/PIX) | Security Logs, Authentication Logs, Application Logs | 100 | 250 |
| Jumphost Server | Security Logs, Authentication Logs | 41 | 2 Gb/day |
| TACACS Server | Security Logs, Authentication Logs, Application Logs | 15 | 2 Gb/day |
| DNS | Security Logs (contains Authentication Logs). | 26 | 0.1 Gb/day |
| Management Systems Nokia Netact, Huawei U2000 | Security Logs, Authentication Logs | Assuming 4 Systems | 1 Gb/Day (Assumed) |
| Nokia UDB - Routing DSA, Backend DSA, PGW, Frontend HLR, Frontend HSS | Security Logs, Authentication Logs. For PGW the syslogs (applications logs) | 264 Unix servers | ~25 Gb/Day (Assumed) |
| Huawei OCS (Online Charging System), Huawei Voucher Management | Security Logs, Authentication Logs |  | 1 Gb/Day (Assumed) |
| Syslog Servers and others central log collectors [These Servers collect logs from multiple routers] | Syslog |  | 15 Gb/day |
| DCN E-mail Relay Server & Proxy Server | Security Logs (Access Logs) and E-mail logs | 1 | 1 Gb/Day (Assumed) |

TOTAL EXPECTED LOG VOLUME: **~300 GB/Day**

**Future Log Sources:**

* UNICA Server (Operating System logs, Security Software logs, Application logs)
* UGW-s Huawei, SGW-s (Security Gateway), SBG-s, AAA-s fixed & mobile, PCRF-s, GGSN-s, Charging GW-s, MSS-s, PKI-s, E-PDG-s (voiceover WIFI), ARBOR, SESAM. Type of logs needed: Security Logs, Authentication Logs

## TEST SETUP: To be UPdated

|  |  |  |
| --- | --- | --- |
| Instance Family | Quantity | Location |
| Search Heads | 2 | Frankfurt |
| Indexers | 2 | Frankfurt |
| Deployment Servers | 1 | Frankfurt |
| Deployer | 1 | Frankfurt |
| Cluster Master | 1 | Frankfurt |
| License Servers | 1 | Frankfurt |
| Distributed Management Console | 1 | Frankfurt |
| Heavy Forwarders | 1 | Frankfurt |
| Universal Forwarders | 1 | Frankfurt |

## 3.3 LOG SOURCE & CORRELATION SEARCHES:

Splunk offers a number of mechanisms for ingesting data—from reading simple, well-known log file formats, to invoking programs to handle custom data formats. In cases where input data cannot be loaded using standard Splunk Enterprise inputs, Cognizant will leverage scripted or modular inputs to parse the data, One of the resource deployed by Cognizant will be a Splunk developer to take care of such activities.

A correlation search is a type of search that evaluates events from one or more data sources for defined patterns. When the search finds a pattern, it creates a notable event, adjusts a risk score, or performs an adaptive response action.

Splunk allows correlation searches to be created manually or you leverage guided search creation wizard to create a correlation search. The guided search creation wizard allows you to create a correlation search that uses data models or lookups as the data source. The wizard takes your choices about the data source, time range, filtering, aggregate functions, split-by fields, and other conditions and builds the syntax of the search for you.

During the Build stage Cognizant will deploy Splunk Enterprise Security which is a premium app for the Splunk platform that addresses SIEM use cases by providing insight into machine data from security sources. The app includes pre-packaged dashboards, correlations, and incident response workflows to help security teams analyze and respond to their network, endpoint, access, malware, vulnerability, and identity information. Splunk Enterprise Security is supported by a set of frameworks. These frameworks implement the functional areas of Splunk Enterprise Security. Together, the frameworks support the monitoring and alerting content packaged within Splunk Enterprise Security, as well as external content provided in other security apps. Splunk Enterprise Security has five frameworks that are available for integration

* The Notable Event framework provides a way to identify noteworthy incidents from events and then manage the ownership, triage process, and state of those incidents.
* The Asset and Identity framework performs asset and identity correlation for fields that might be present in an event set returned by a search.
* The Threat Intelligence framework is a mechanism for consuming and managing threat feeds, detecting threats, and alerting.
* The Risk Analysis framework provides the ability to identify actions that raise the risk profile of individuals or assets, and accumulate that risk to allow identification of people or devices that perform an unusual amount of risky activities.
* The Adaptive Response framework provides a mechanism for running preconfigured actions within the Splunk platform or by integrating with external applications. These actions can be automatically triggered by correlation search results or manually run on an ad hoc basis from the Incident Review dashboard.

Cognizant will integrate Log sources as described in in “Systems to be connected” from the “functional requirements” document. Cognizant understands that expectation from Telefonica from vendor is to build a SIEM platform that enables Telefonica to build use case as described in Functional Requirement Document.

Cognizant will Deploy Splunk Enterprise security app that would enable Telefonica SOC team to build the correlation rules mentioned in the “Log correlation and use cases” from the “functional requirements” document.

These available correlation, dashboard and Integration can be leveraged by Telefonica SOC team to build use case for Security Event Monitoring, triage, analysis and investigation. Cognizant Splunk Experts at Onsite will provide required second level support during maintenance phase based on change request initiated by Telefonica SOC team to support this activity.

## 3.4 ALERTS

Splunk Alerts module will be configured to monitor for and respond to specific events. Alerts uses a saved search to look for events in real time or on a schedule. Alerts trigger when search results meet specific conditions. You can use alert actions to respond when alerts trigger. Alert actions help you respond to triggered alerts. You can enable one or more alert actions.

Splunk Enterprise Security detects patterns in your data and automatically reviews events for security-relevant incidents using correlation searches. When a correlation search detects a suspicious pattern, the correlation search creates an alert called a notable event. The Incident Review dashboard surfaces all notable events, and categorizes them by potential severity so analysts can quickly triage, assign, and track issues.

All notable events generate alerts based on the configurations and could vary from Emails, Integration to 3rd party ITSM tools, SMS event population in the Dashboard etc.

Moreover, the alerts can also be configured to send them further to other platforms, using standard interfaces such as Webhooks that allow you to define custom callbacks on a particular web resource. For instance, you can set up a webhook to make an alert message pop up in avchat room or post a notification on a web page. When an alert trigger, the webhook makes an HTTP POST request on the URL. This action writes the results of a triggered alert or a run of a scheduled report to a CSV lookup file that you specify

The system will alert on increase EPS and Data /day, through the license module alert. Alarm will be triggered when license exceeded and data will be processed as backlog on the next day if license not increased.

## 3.5 DASHBOARDS

Proposed dashboard will facilitate identification and investigation security incidents, reveal insights in your events, accelerate incident investigations, monitor the status of various security domains, and audit your incident investigations and your ES deployment. The Security Posture dashboard will be designed to provide high-level insight into the notable events across all domains of your deployment, suitable for display in a Security Operations Center (SOC). Splunk offers easy to create new reports or modify existing ones. Data can be visualized in many ways including tables, charts or scatterplots

Domain dashboards provided with Splunk Enterprise Security will facilitate monitoring the events and status of important security domains.

The Access Protection domain monitors authentication attempts to network devices, endpoints, and applications within the organization. Access Protection is useful for detecting malicious authentication attempts, as well as identifying systems users have accessed in either an authorized or unauthorized manner.

The Port and Protocol Tracker tracks port and protocol activity specifies the network ports that the enterprise allows and will facilitate visibility into new activity by port to identify devices that are not in compliance with corporate policy, as well as detect prohibited traffic.

Web Center dashboard will be leveraged to profile web traffic events. This dashboard reports on web traffic gathered by Splunk from proxy servers. It is useful for troubleshooting potential issues such as excessive bandwidth usage, or proxies that are no longer serving content for proxy clients. The Web Center can profile the type of content that clients are requesting, and how much bandwidth is being used by each client.

Malware Center dashboard can be leveraged to identify possible malware outbreaks in the environment. It displays the status of malware events in your environment, and how that status changes over time based on data gathered by Splunk. Shows all malware detected over the specified time period, split by action (allowed, blocked, deferred). Shows all malware detected over the specified time period, split by signature.

## 3.6 SYSTEM HEALTH & performance MONITORING

The Monitoring console turns Splunk's diagnostic tools inward to analyze and troubleshoot problems in your Splunk environment. This module will be deployed on Master Node. It will provide a detailed topology and performance information view of Splunk Enterprise deployment.

The available dashboards provide insight into the following areas of your deployment or instance:

* search performance and distributed search framework
* indexing performance
* operating system resource usage
* Splunk app key value store performance
* search head and indexer clustering
* index and volume usage
* forwarder connections and Splunk TCP performance
* HTTP Event Collector performance
* license usage.

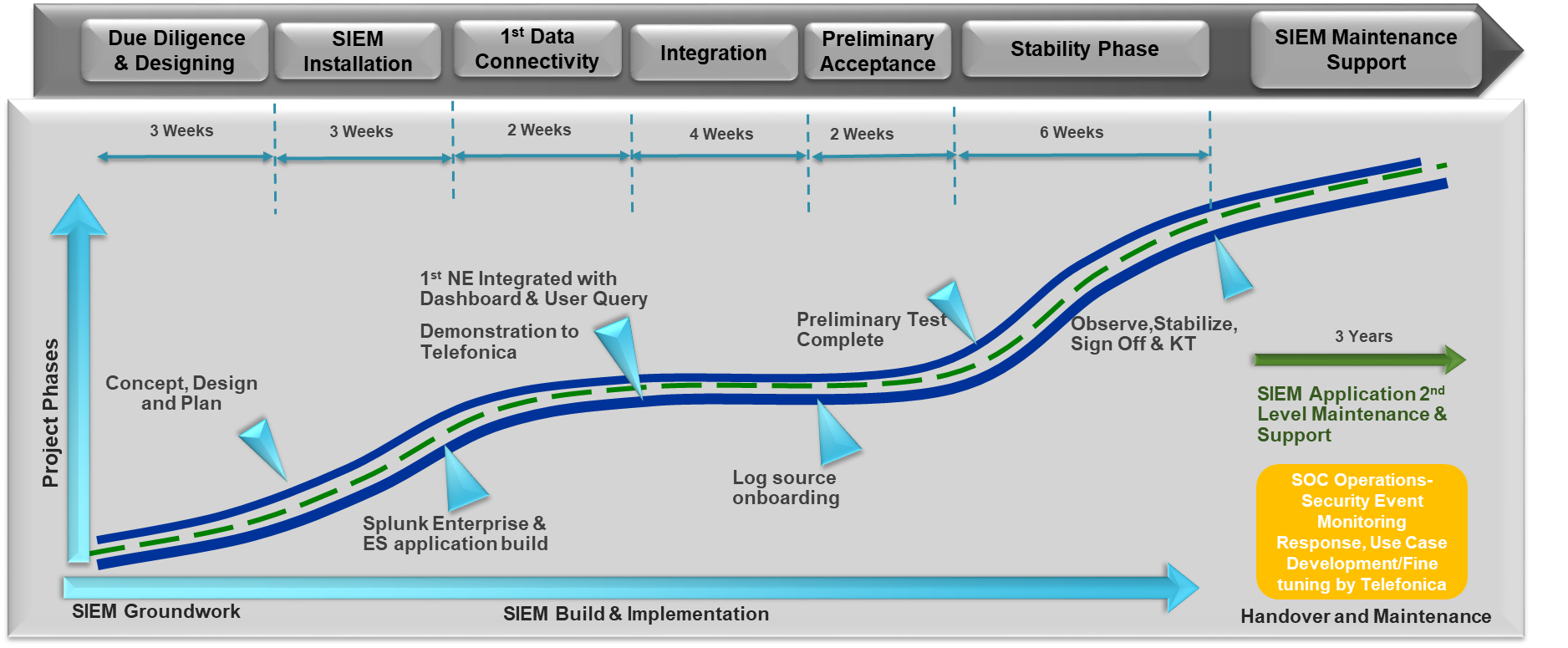
Cognizant will configure Splunk to send alerts to Telefonica ITSM tool for alerting Cognizant Support engineers when an performance or health related event occurs.

# 4.0 service requirement

## 4.1 DEPLOYMENT APPROACH

The proposed Splunk solution deployment will undergo the following phases. The phased approach provides a systematic deployment of the solution considering the business requirements and the network architecture. This is critical in providing an optimized implementation of SIEM component deployment. This framework will serve as building blocks across people, process and technology aspects. The process followed here is a sequential building of SIEM Solution.

The proposed time lines and milestones for each phase is provided below-



**Due Diligence & Designing Phase**

The Due Diligence phase consists of gathering the requirements from Telefonica and architecture design as it pertains to deployment of the SIEM tool. The key activities that will be performed includes understanding current setup, network connectivity across Telefonica Data centers and validate log source inventory. One another key aspect of this phase is to revise project plan and sign off with the stake holders. Post Due diligence Cognizant will create a Low level implementation Architecture diagrams, Technical design documents, Finalizing the VM Requirement design and storage requirements for log retention.

Deliverables:

* Detailed concept created for the configuration and integration of the network elements
* System Architecture design created
* Test Plan
* Project framework aligned and ready

Procedure:

* Joint verification of the created design/concept

Pre-requisites/Dependency

* Purchase order is out

**SIEM Installation**

The primary objective of this phase is to fulfil design and architectural requirements for Implementation/Build and of SIEM tool

Activities/deliverables:

* The Main system is implemented in the virtual environment end SIEM platform tested successfully by Cognizant

Procedure:

* Cognizant presents the overview about the basic platform test cases which are necessary for the installation verification as per agreed Test Plan

Pre-requisites/Dependency

* Virtual and storage environment is provisioned, deployed and tested by Telefonica or its Third party vendor
* IP design and connection for SIEM platform.
* Network Infrastructure and Backup Tools provisioned, deployed and tested by Telefonica or its Third party vendor

**First Data Connectivity**

This phase targets First data connectivity for1 Firewall & 1 Jump-host along with software framework installed, firewall and Jump-host log file received

Activities/deliverables:

* IP connection, Firewall & Jump-host, monitoring data flow between the SIEM platform in the datacentre and first NEs
* User Interface available and data can be used for analysis

Procedure:

* Vendor presents the complete log file of one Firewall and one Jump-host that is available in the backend platform to TEF
* Dashboard, reporting and user query will be presented by the vendor
* Log Source end configuration is performed by Telefonica admin on the respective log sources as per recommendation from Cognizant Splunk SME.

Pre-requisites/Dependency

* The connections to the network elements are established, technical information for integration is provided to the vendor, log file transfer is enabled on the NE.
* Log Source end configuration is configured by Telefonica admin on the respective log sources

**Integration**

This Phase targets mainly on SIEM platform and Integration of Critical Log Sources to enable Security Posture visibility across IT Security infrastructure.

Activities/deliverables:

* At least 75% of network element types mentioned in the functional requirements are onboarded on SIEM platform.
* Platform basic functions regarding functional requirements are present. The Vendor internal factory test procedure was internal accepted by the Vendor.
* The Vendor provided a detail Factory Test Protocol.

Procedure:

* At least 75% of network element types mentioned in the functional requirements
* The Vendor distributes to TEF the internal detail test document. The test document contains test case name, test case procedure description, test date, pass/ fail criteria.
* The test cases are provided by the Vendor and mutually agreed between both parties.

Pre-requisites/Dependency

* The definition of the detailed technical integration scenario with all network elements is documented
* The connectivity to the network elements is prepared and available
* Any dependency on Third party to fulfil the requirement will be coordinated and closed by Telefonica during this phase.
* ITSM tool configuration

**Ready for Preliminary Acceptance Certificate**

Activities/deliverables:

* The UCs are validated and approved by Telefonica
* Cognizant provided operational status report of the SIEM Platform (health check report: eg. data availability, log flows, system status, system capacity utilization)
* The User Acceptance Tests (UAT) as agreed during Concept phase is signed off Purchaser.

Procedure:

* Cognizant presents to TEF that the configuration on the system took place and monitoring data of all interfaces are available and complete.
* Acceptance will be done according to an acceptance criteria list mutually agreed upon between Telefonica and Cognizant Acceptance processes and procedures

Pre-requisites/Dependency

* Telefonica will verify the implementation and confirm that the acceptance can be started
* All Telefonica Use Cases (UC) according to functional requirements are fully implemented at the SIEM System.
* The SIEM functional requirements defined in the functional requirements are implemented
* The northbound interface to the alarming system is established
* The connectivity to the network elements is prepared and available

**Successful stability phase, final acceptance**

A stability period of 6 weeks shall be successfully passed.

Criteria for milestone completion:

* The stability period was successfully passed without complete or critical system outages.
* 98% Data Availability for raw and history data.
* The system performance has to be accepted by the customer as per Cognizant response to compliance on functional requirement and in the service requirement document.
* All Major issues from the UAT are solved.
* Test system is running and configured (e. g. same software version, features) as the main system

Procedure:

* The Cognizant shall prepare and present a status overview covering the criteria for milestone completion.

Pre-requisites/Dependency

* UAT results are available and the severity of open tickets is jointly agreed
* Any dependency on Third party to fulfil the requirement to be coordinated and closed by Telefonica.

## 4.2 Supplied Resources

|  |  |  |
| --- | --- | --- |
| Role | Responsibilities | Location |
| Cognizant – SIEM Architect | * Design of the SIEM Architecture * Develop Test and Acceptance Plan * Implementation of the agreed upon SIEM architecture * Integration of the agreed log sources to the SIEM Infrastructure and test as per agreed acceptance criteria * Define and test correlation search * Participate in project status reviews & meetings | Onsite |
| Cognizant – Splunk Developer | * Build User Interface, dashboard and Report Templates * Build parsers * Configure correlation search rules * Configure Log sources | Onsite |
| Cognizant - PMO | * Project Management * Quality Assurance Tracking | Onsite |

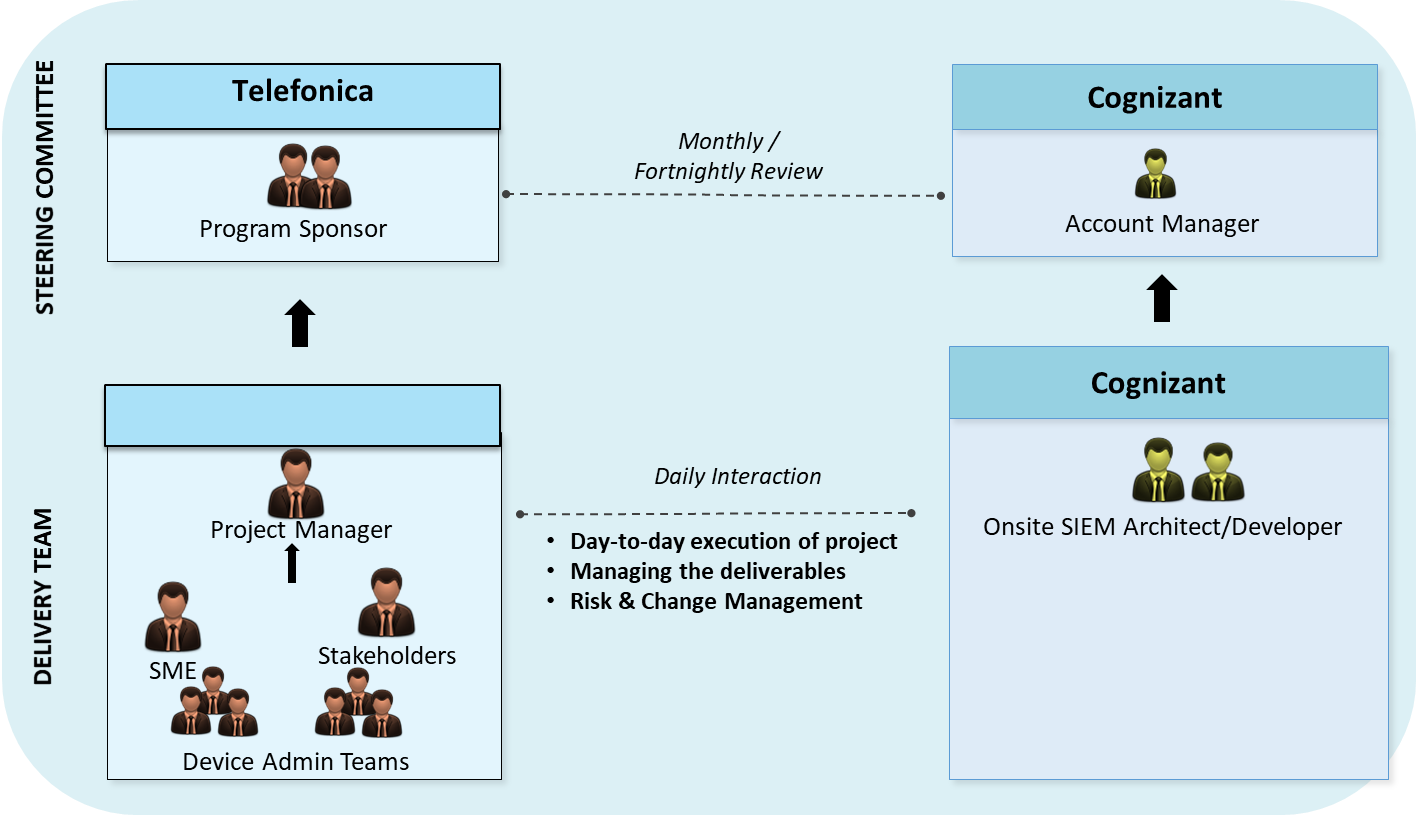
Hours of Work: Telefonica Germany business hours – 8 x 5 basis

Mode of Communication: English

## 4.4 Project Management

**Proposed Governance**

The following is the proposed governance structure for the project-



* Delivery team manage the day-to-day operations with respect to the project
* Cognizant would leverage centers of excellence (CoE) as needed during various phases of the project
* Cognizant team will closely work with the SIEM product vendor for this project

**Steering committee**

* To assess and monitor the strategic direction and health of the project
* Weekly checkpoint meetings

**Delivery Team**

* Implementation of the Proposed SIEM solution

**Communication and Reporting**

Communication will happen at various levels between Telefonica, Cognizant Onsite and Cognizant Offshore teams. Primary contacts for Telefonica will be the Cognizant onsite team; however, offshore team members will be present during key discussions as required.

Following is the communication plan suggested for Telefonica-

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Meeting** | **Frequency** | **Attendees** | | **Focus Area** |
| **Cognizant** | **Telefonica** |
| **Account Management Review** | Monthly/  Fortnightly | * Account Manager | IT Director | * Discuss overall strategic business, financial decisions * Discuss overall account management relationship * Project status discussion |
| **Status Review** | Daily | Onsite SIEM Consultant | Project Manager | * Previous day's tasks, critical updates, status update |

## 4.5 Test and Acceptance Procedures

The Acceptance Process ensures prompt Telefonica acceptance of key project deliverables.

Cognizant will develop test and acceptance model with test concept. Acceptance will be formally defined when the contract is agreed. The result of the UAT is the basis for the final acceptance of the project. The formal testing with respect to user needs, requirements, and business processes will be conducted to determine whether a system satisfies the acceptance criteria and to enable the user, customers or other authorized entity whether or not to accept the system.

Cognizant’s responsibilities are to:

* Provide formal notification to Telefonica of the impending deliverable delivery
* Conduct internal quality assurance review and approve deliverable for Telefonica
* Present deliverable for acceptance and
* Incorporate agreed upon comments and changes

Telefonica’s responsibilities are to:

* Review the deliverable
* Provide consolidated and written feedback and comments within agreed time frame and
* Formally accept the deliverable upon incorporation of agreed upon comments and changes
* Any dependency on Third party to fulfil the requirement to be coordinated and closed by Telefonica.
* Engage a Point of Contact and arrange for any resource if required to perform test on systems not managed by Cognizant

Unless a different review period is specified for a deliverable, within three (3) business days of the receipt of each deliverable, the Telefonica’s Acceptor, with assistance from the Telefonica’s team, will do the following:

* Notify Cognizant in writing of Telefonica’s full acceptance, conditional acceptance, or non-acceptance of the deliverable
* If the deliverable is not fully accepted, return to Cognizant a single annotated copy of the deliverable, indicating the unacceptable portions, any required corrections or additions
* Assign a Telefonica point of contact for corrections / adjustments to specific comments per deliverable (this helps expedite the update process for Telefonica and Cognizant)

It is assumed all subsequent iterations needed for deliverable acceptance will be completed within 7 business days or lesser. Any outstanding sign-offs and potential or actual delays after these iterations will be handled through Change Management process.

In the absence of a consolidated set of feedback within this timeframe, the deliverable will be deemed to have been accepted.

Specific acceptance criteria will be mutually defined before the beginning of each deliverable. The criteria will be reasonable and consistent with industry standards. Acceptance of the project deliverables will not be unreasonably withheld by Telefonica.

The test concept will include

1. Definition of acceptance criteria's model for the UAT
2. Definition of the organization, coordination and user communication of the UAT
3. Acceptance Test Plan
4. Acceptance Test Cases/Checklist
5. Definition of a ticket handling process - ITSM tool configuration that Telefonica is required to fulfil.
6. Automated ticket status reporting - ITSM tool configuration to be fulfilled by Telefonica
7. Consideration of performance tests leveraging Splunk Built in Monitoring console

The test cases will cover the following areas:

1. Product (Enterprise Security application) functionalities
2. Use Cases
3. Interfaces
4. Platform Security (platform hardening)
5. Backup and recovery

Any dependency on Third party to fulfil the requirement of test cases will coordinated and closed by Telefonica.

Splunk Built in Monitoring console shall be leveraged to measure below performance parameters. Performance tests consideration will be limited to feature set offered by Splunk Built in Monitoring console

• search performance and distributed search framework

• indexing performance

• operating system resource usage

• Splunk app key value store performance

• search head and indexer clustering

• index and volume usage

• forwarder connections and Splunk TCP performance

• HTTP Event Collector performance

Cognizant recommends Telefonica to leverage its Vulnerability Management tool and perform Infrastructural security test.

Any Vulnerabilities identified will be rectified by Cognizant within the ability of proposed toolset. Where Product Vendor dependency is required Cognizant will provide Product Vendor roadmap to address the Vulnerability based on Product Vendor response.

## 4.6 RACI

R-> Responsible

A-> Accountable

C-> Consulted

I-> Informed

F

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Activities** | **Vendor (Cognizant)** | **CUSTOMER** |
|  | Strategy, Policy guidance | C,I | R,A |
|  | Nominate one single-point-of-contact for interfacing with Cognizant for all project related activities | C,I | R,A |
|  | Coordinate Requirement Workshops | C,I | R,A |
|  | Analyse Requirements - Conduct technical assessment, Create requirements list | R,A | C,I |
|  | Design Final SIEM Architecture | R,A | C,I |
|  | Develop and share Virtual Machine, Network and Storage Infrastructure requirement | R,A | C,I |
|  | Develop Project, Implementation and test plan | R,A | C,I |
|  | Review and Sign off on Architecture, Project, Implementation and test plan | C,I | R,A |
|  | Provide timely approval | C,I | R,A |
|  | Develop HLD and LLD for SIEM solution | R,A | C,I |
|  | Build and Deploy Virtual Machine and Network Infrastructure | C,I | R,A |
|  | Deploy and configure Backup Tools | C,I | R,A |
|  | Install Splunk Components | R,A | C,I |
|  | Onboard Log Sources on Splunk | R,A | C,I |
|  | Configuration on Log sources to enable logging and forward as per requirement | C,I | R,A |
|  | Build Dashboard and Reports on Splunk | R,A | C,I |
|  | Configure Console Performance Monitoring | R,A | C,I |
|  | Configure Splunk for Integration with ITSM Tool | R,A | C,I |
|  | ITSM tool Configuration | C,I | R,A |
|  | Validate as per Test Plan | R,A | C,I |
|  | Review and Sign off on Implementation | C,I | R,A |

# 5.0 Support and Maintenance for SIEM Tool

Cognizant proposes SIEM Infrastructure support and maintenance based on the RFP requirement from Telefonica. We understand that Telefonica has an existing Run team (SOC) and assume that the team will provide 24x7 SIEM monitoring services that include Monitor, analyse triage and alerting services.

Cognizant proposes Post Deployment 8x5 SIEM Application components 2nd Level Maintenance & Support. Post Deployment 8x5 SIEM Application components 2nd Level Maintenance & Support services will be limited to Splunk Enterprise and Enterprise Security Application platform related issues. This excludes VM/Backup/Network/Storage/any Hardware Infrastructure Platform

Two dedicated Security Analysts with Splunk SIEM experience will be deployed at Onsite, Germany with 8x5 EST coverage. Below are the roles and responsibilities of Splunk

Resource 1:

Primary Roles/Responsibilities: Architecture, SIEM app Platform Incident Management, Problem Management & Maintenance

Secondary Roles/Responsibilities: SIEM Platform Health Checkup

Resource 2:

Primary Roles/Responsibilities: SIEM Platform Health Checkup, SIEM app Platform Incident Management, Parser Development [Phython, Regex]

Secondary Roles/Responsibilities: Architectural Understanding; SIEM app Platform Problem Management & Maintenance

In-Scope Activities for Support phase includes.

1. Incident management:
   1. Incident management (ticket resolution, ticket tracking)- Reaction & resolution to incident tickets in given SLA time frame
   2. Incident and ticket reports - Ticket processing along the Telefonica processes, Documentation of taken actions in the UTS ticketing tool or other appointed Telefonica tools
   3. SLA and KPI reporting leveraging Telefonica ITSM Tool
2. Problem management
   1. Analysis of repeated systematic errors or issues
   2. Identification of workarounds for problems
   3. Identification of problem areas and their solutions
   4. Implement measures of preventive maintenance
3. Change request handling
4. Monitoring (e. g. application and data flows) on Splunk Monitoring Console.
5. Preventive Maintenance, House Keeping & Proactive system maintenance
   1. Development and continuous improvement of solutions/tools (scripts, etc.) for system and application landscape health checks
   2. Run regular (daily, weekly, monthly, on-demand) health checks and housekeeping activities in order to ensure error free and performant operation of system and application
   3. Creation of system/application state and health reports and joint evaluation with Telefonica application owner
   4. Proactive resolution of system and application problems
6. Software Updates - Coordination with 3rd level support partners and developers to prepare hot-fixes, Updates and Upgrades
7. Software patches - Coordination of timing for patches to production as per Telefónica change management process
8. System configuration as per Telefonica’s inputs
9. Rollout of feature requests – Cognizant will assess feature rollout request on case to case basis, validate efforts required to deliver features and if existing resource has bandwidth to deliver the ask along with validating license requirement and other pre-requisite. If additional resource or effort is required, then this will be serviced through a new change order process.
10. Communication:

a. Deliver communication content relevant for all impacted organizational units within Telefonica and external partners

b. Synchronization of communication content with NT Service Desk

c. Proactive information to NT Operations management and NT Service desk with regard to planned downtimes and maintenance windows

## RACI

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Responsible Party** | |
| **Ref** | **Tower/Process/Sub-Process/Activity** | **Vendor (Cognizant)** | **CUSTOMER** |
|  | Strategy, Policy guidance | C,I | R,A |
|  | Nominate one single-point-of-contact for interfacing with Cognizant for all support related activities | C,I | R,A |
|  | 2nd Level Maintenance & Support services limited to Splunk Enterprise and Enterprise Security Application platform related issues – Incident management | R,A | C,I |
|  | Splunk Enterprise and Enterprise Security Application related Problem Management | R,A | C,I |
|  | Splunk Enterprise and Enterprise Security Application: Preventive Maintenance & Health Checks | R,A | C,I |
|  | VM/Backup/Network Infrastructure Platform Maintenance | C,I | R,A |
|  | Backup as per Schedule | C,I | R,A |
|  | Security Event Monitoring and Response | C,I | R,A |
|  | Fine Tune Policies/Correlation searches | C,I | R,A |
|  | Provide second level configuration support during maintenance phase based on change request initiated by Telefonica SOC team | R,A | C,I |
|  | Use Case Management | C,I | R,A |
|  | ITSM tool Management | C,I | R,A |

## SERVICE LEVELS

Availability of Onsite Engineer: (P1/P2/P3/P4: 8x5 Business Hours)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Response** | **Recovery** | **Resolution** | | | |
| **1** | **2** | **3** | **4** |
| **CRITICAL** | 15 min | 14 hrs. | 45CD | 60CD | 90CD | 90CD |
| **MAJOR** | 30 min | 72 hrs. | 60CD | 90CD | 120CD | 120CD |
| **MINOR** | 1 hr | 30 CD | 90CD | 120CD | 150CD | Next Release |

CD = Calendar Days

WD =Working Days

Exception:

* Where there is a dependency on SIEM Vendor to provide fix
* Platform Availability as VM Infrastructure is not under Cognizant Scope.
* Availability of backup configurations

# 6.0 Risk & MITIGATION

Cognizant shall perform Risk Management as a continual activity to identify risks, access and discuss with Telefonica to mutually agree for a response and recommend the mitigation strategies.

Cognizant shall also report all risks as and when identified.

|  |  |  |  |
| --- | --- | --- | --- |
| **Identified Risk** | **Impact of Risk** | **Likelihood of Risk occurrence** | **Mitigation** |
| Network Connection – IT Infra | Medium | Connection timeout, Latency & Intermittent connection | Redundancy link, High Bandwidth |
| Event Source Integration | Low | Non-availability of SME | Advance notification / Calendar blocking |
| Event Source Integration | Low | Non-support event Sources | Develop a custom parser |
| Change Management | Low | Delayed Approvals | Approvals in time / Emergency CAB |
| Hardware/VM availability | High | 6-8 Weeks delivery timelines from OEM | Order processing ahead of time to comply with the expected handover of the SIEM infrastructure |

# 7.0 Key assumptions

* Enough bandwidth is available between the Datacentres for log forwarding,
* Log Source end configurations required for logging will be performed by Telefonica Application owners / administrators
* Log Size calculation is done based on log size estimation provided in Functional requirement document by Telefonica. For log sources where estimation was not provided such as Management Systems (Nokia Netact, Huawei U2000), Nokia UDB, Huawei OCS (Online Charging System) & Huawei Voucher Management, Cognizant has assumed average of 2 events per second per log source and maximum event size in bytes at 600. During Due Diligence Cognizant will access the required log size and any increase in Log Volume will be intimated to Telefonica for purchase of additional licenses.
* Cognizant assumes that Telefonica will validate VM hardware sizing and UNICA compatibility with OEM – Splunk during due diligence phase through professional services.
* Load Balancing service to balance SOC admin traffic across search heads will be provisioned and managed by Telefonica.
* Cognizant onsite personnel will be provided with required work space, laptop and phones as necessary for executing this project
* Hardware/Virtual Platform, Network and Backup Platform Infrastructure will be deployed and managed by Telefonica
* Relevant ITSM Tool configuration to measure Service Levels
* There will be a stabilization period of around 90 days during which the SLA for the steady state will not be applicable
* Any dependency on Third party to fulfil the requirement of deployment will be coordinated and closed by Telefonica.
* Any dependency on Third party to fulfil the requirement of test cases will have coordinated and closed by Telefonica.
* Post Deployment 8x5 SIEM Application components 2nd Level Maintenance & Support services will be limited to Splunk Enterprise and Enterprise Security Application platform related issues. This excludes VM/Backup/Network/Storage/any Hardware Infrastructure Platform
* Cognizant will assess feature rollout request on case to case basis, validate efforts required to deliver features and if existing resource has bandwidth to deliver the ask along with validating license requirement and other pre-requisite. If additional resource or effort is required, then this will be serviced through a new change order process.

# 8 Appendix

## 8.1 Cognizant Quality Management System Framework

The Contractor’s quality assurance strategy with regard to all activities related to the performance of this Contract shall be formulated and detailed in a Quality Plan by Contractor that will:

* not contain any obligation for Telefónica Germany.
* be provided to Telefónica Germany by a date to be agreed.
* be maintained by the Contractor and followed for the duration of the Contract.
* identify the quality assurance objectives, strategy and measures employed by the Contractor to ensure the quality of the Deliveries provided under the Contract.
* Describes the Contractor’s organisation, responsibilities and resources involved in Contractor’s fulfilment of its obligations under this Contract including subcontractors and/or third parties and their QMS in detail.

**Quality Management System**

Cognizant has a robust Quality Management System (QMS) that has evolved and matured over the last 20 years.  Our QMS subscribes to industry standards like ISO (27001:2013, 20000-1:2011, 9001:2015, 14001:2004, 13485:2003) and CMMI v1.3.  It is hosted in a web-based platform and enforced through an independent Quality function called Delivery Excellence (DE).  It is well orchestrated and institutionalized through internal process tools.  There is a robust mechanism for continuous process improvement that aligns with industry trends and aims to meet growing needs of our clients’ expectations.  Implementation of the QMS is subject to periodic internal and external audits.

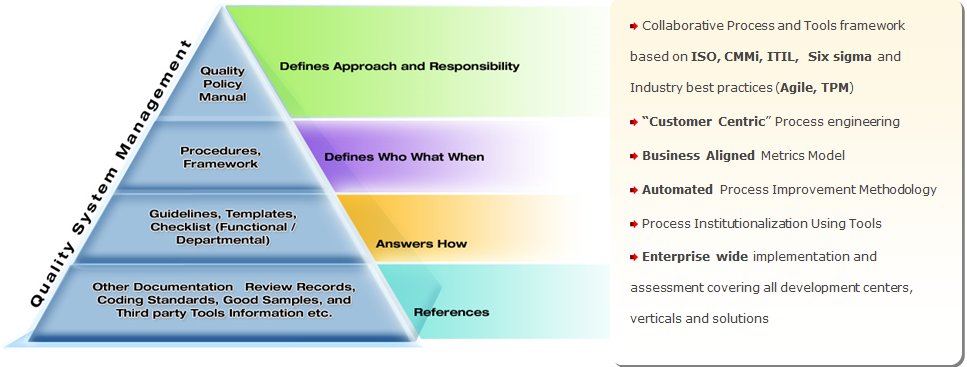


Figure 1: Cognizant’s Quality Framework

QMS provides comprehensive process framework with detail procedures, guidelines, templates and checklists addressing the various service offerings. It covers all aspects of project and Service Delivery Management, software engineering for various solution offerings. These processes are matured and adaptable to integrate with Telefonica specific processes such that the best practices defined by you are being implemented without compromising on high maturity practices defined for Cognizant. The software engineering processes provide a focus on solution development, testing and delivery emphasizing on problem prevention rather than problem correction. The quality management process embodies the processes for expectation identification, quality planning, performance measurement and continuous improvement. Combined, these provide a solid foundation for the management and delivery of high quality services and deliverables.

**Delivery Excellence**

Delivery Excellence (DE) is an independent function, associated with every project in the organization, which

* Ensures that processes are enriched in accordance with industry trends
* Ensures that projects conform to the defined processes
* Provides facilitation and training for process setup and implementation to meet client, as well as, the regulatory/statutory requirements
* Monitors the effectiveness of process implementation through audits
* Facilitates continuous improvement to the QMS by identifying opportunities for improvement and implementation of best practices
* Uses organization’s metrics program and performance analysis
* Checks adequacy of the implementation of information security policy and procedures at engagement level
* Supports in tailoring of the organization’s process to meet the project’s needs

DE team is structured into Envision, Industrialize and Enable - to ensure that best standards are adapted for project delivery, to arrive at a coherent delivery strategy and to assure consistent delivery.

* **Envision** - *continuously scan the horizon for contemporary ideas and concepts related to delivery, contextualize it for Cognizant and construct the framework for broader awareness, acceptance and adoption across the organization*
* **Industrialize** *- Provide a scalable delivery enabling infrastructure by channeling the outputs of Envision and making them available to the Enable through Platforms, Audit & Assurance Processes, Performance Accelerators and Training*
* **Enable** *- To be the link between DE & business units (BU) in a pro-active, consultative and facilitation role to ensure design & components of DE model are consistently implemented in every part of the BU, Accounts, Shores & Centers*

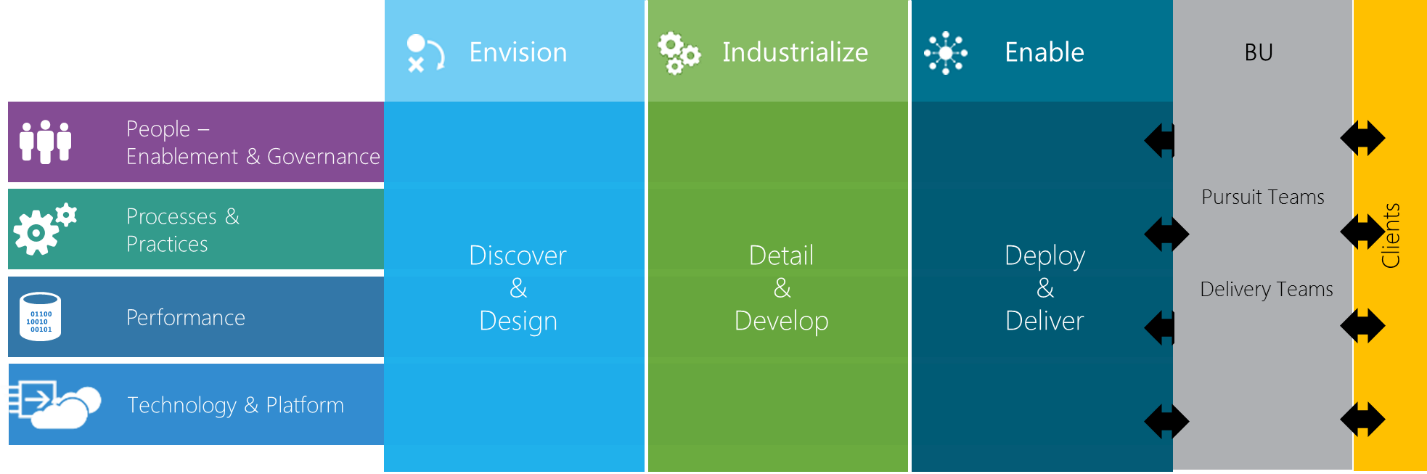


Figure 2: Delivery Excellence structure enabling business units to deliver best in class solutions to clients

**Quality Plan**

Quality planning is ensured through the Delivery Assurance plan. Every project will have a delivery assurance plan, which is part of the integrated software project plan which also encompasses other plans such as Risk Plan, Staffing Plan, Configuration Plan, Infrastructure Plan, Business Continuity Plan and Disaster Recovery Plan and Knowledge Management Plan.

The Delivery Assurance Plan covers the below sections:

* **Metrics Plan**- Identifies the controls/benchmarks related to process execution and product quality. Responsibility for ensuring abidance to the same is also identified as part of the plan. Quality goals for the project will be defined based on business objectives, project objectives and Telefonica needs.
* **Review Plan**-To document the critical deliverables of the project which undergoes the formal acceptance review and any additional reviews apart from those mentioned in the process or lifecycle model.
* **Audit Plan**-To document details of the audits applicable for the project.
* **Defect Prevention Plan and Causal Analysis**- To document the defect type, defect cause, root cause, preventive action planned, responsibility and target date stage wise.
* **Problem Prevention Plan**-To document the problems / repeated risks and issues faced in the project, which requires careful evaluation to arrive at the solution.

**Quality Objective and Measures**

During the onset of the project, the list of project deliverables along with their acceptance criteria will be defined and will be mutually agreed by Cognizant and Telefonica. We follow a metrics-based project management approach, where a project’s progress is tracked and quality of service delivered is measured using metrics. Based on the nature of the project, a list of mandatory metrics along with goals are identified. The expectations of Telefonica from a quality perspective will also be fed into the metrics plan. We will identify your business objectives and translate them into Key Performance Indicators (KPIs). These KPIs will be further translated into Project/ Sub process performance goals and SLAs.

There are various DE levers that focus on key areas enabling project teams to achieve excellence. Few of them are

|  |  |  |
| --- | --- | --- |
| **Programs/Tools** | **Description** | **Benefits** |
| Audits and Reviews | * Assess quality of project and deliverables through different type of audits (startup audit, transition audit, delivery audit etc.) * Center of Excellence (CoE) and expert group involvement * Experienced leaders/ SME review though Project/Service Management Review (PMR)/ (SMR) | * Delivery risk identification and mitigation * Ensure the project deliverables are on time, within budget and are of acceptable quality |
| SLA Management | * Ensures that SLAs identified addresses all aspects of the spectrum like business relevance, measures vendor performance, focusses on service outcomes * Ensure OLA’s are established with other dependent services * SLA baselines are established with defined targets | * Quality of services are tracked in terms of KPIs, SLAs and reported in multiple governance forums * Governance mechanism with appropriate corrective and preventive actions in case of any deviations |
| Continuous Improvement and Innovation (CII) | Our CII framework will optimize the existing operation to deliver service reliability and cost control by adopting a well-executed approach by:   * Aligning the existing processes to ConEd business objectives and Industry best practices * Improving the quality of services by bringing together the varied innovation levers like Lean-Six- Sigma, Managed Innovation, Best-In-Class and Continuous Service Improvement | * Optimize the existing operation, deliver cost control and service reliability * Enhance the existing operation to deliver organizational value and customer growth in alignment with business objectives |
| Knowledge Management(KM) | * Organization wide knowledge like reusable assets, best practices, solution accelerators, other collaterals are available in **Know Hub**, our KM portal. * Team can also create, maintain and govern their own knowledge using know Hub. | * Improve productivity and deliverable quality through structured reuse and best practice sharing * Centralized Knowledge repository and knowledge dissemination process |
| Delivery Risk Management (DRM) | * Focus on early risk identification, mitigation and contingency planning | * Ensure success of the engagement by Identifying and handling events that affect the likelihood of engagement’s success |

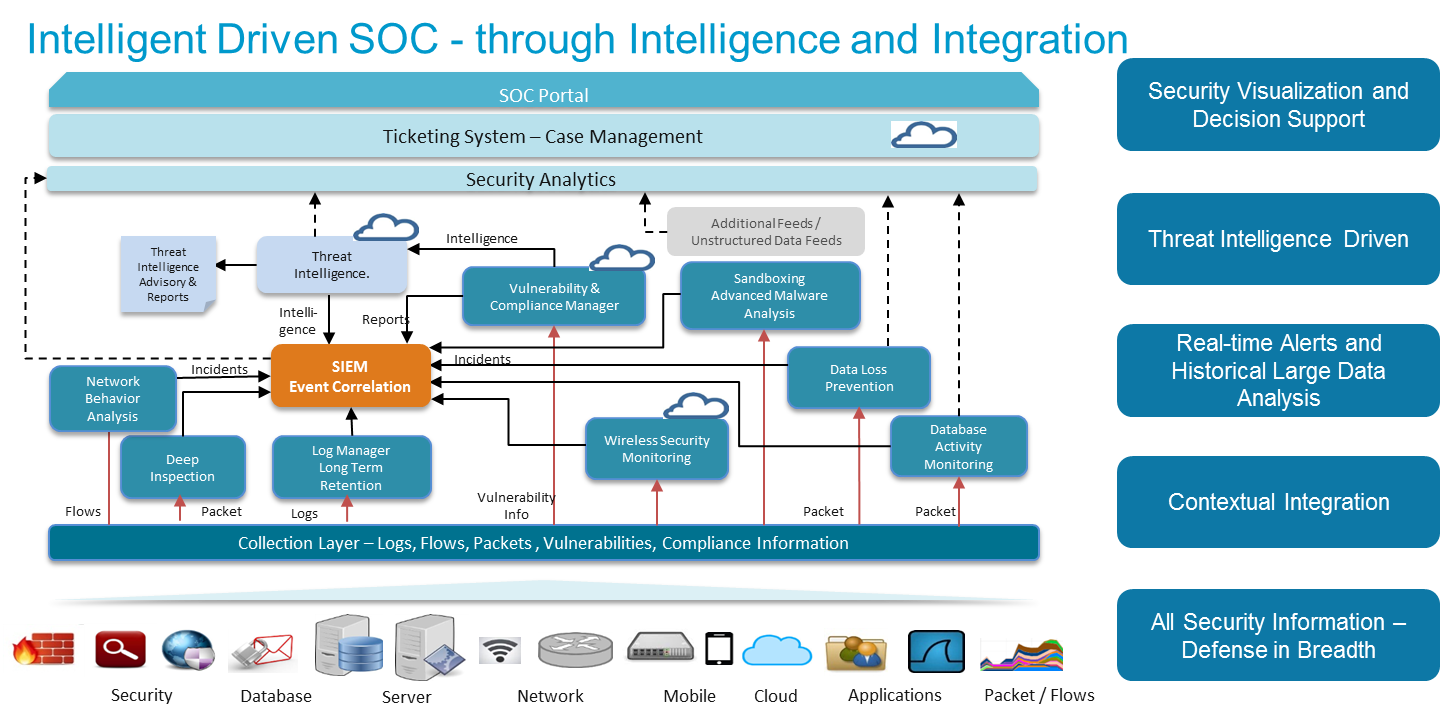
In addition to standard levers, certain engagements will have customized DE programs in alignment to business need / customer’s vision on the program, bringing in rigor on certain aspects, customize certain programs to suit the needs of the engagement over and top of the conventional quality assurance activities.

## 8.2 NextGen SOC Framework

Cognizant Visualizes the NextGen SOC framework for its Customers which is architected for intelligence, embracing an adaptive security architecture to become context-aware and intelligence-driven.

The intelligence-driven SOC approach with these five characteristics-

* Use multi-sourced threat intelligence strategically and tactically
* Use advanced analytics to operationalize security intelligence
* Automate whenever feasible
* Adopt an adaptive security architecture
* Proactively hunt and investigate incidents



The NextGen SOC framework is realized with three major building blocks-

**Adaptive Security Architecture**

Next Generation SIEM platform, SIEM Enterprise Security which takes feeds from various elements including infrastructure, flow telemetry, machine learning, environment, vulnerability assessment , data, identify and Threat Intelligence.

Advanced Threat Detection to correlate and contextualize these inputs to identify and access threats, anomalies and attacks in the environment and use this information for effective breach response. Global Intelligence feed integrated into SIEM for threat profiling, reputation filters, and Advanced correlation.

Leverage Next generation firewall services with Threat Prevention capabilities and Advanced Malware inspection for unknown malwares

Closed loop security Intelligence sharing between Perimeter controls and Endpoint Controls

Advanced Threat protection at network entry point including Internet (Wildfire) and Email (O365)

Towards innovation in future Cognizant proposes to introduce deception based security tools using arrays of decoys (Traps) and breadcrumbs (tokens) that would be deployed over the network to enable a pro-active security posture and provide visibility into ongoing attacks while luring attackers away from valuable assets.

Deception Security is designed to thwart or misdirect an attacker's cognitive processes, disrupt an attacker's automation tools or delay an attacker's activities or disrupt breach progression. Distributed decoys leverage the use of deception and fake decoy endpoint systems distributed across the enterprise for detection. Distributed decoy offers enhanced detection and stronger fidelity than other traditional security solutions because when an attacker touches a decoy, it is immediately recognized as an unwanted interaction, and likely an attacker or insider threat. Real-time detection of malware movement and lateral movement anywhere within the VLAN is possible with such decoys. Moreover it provides automated, highly accurate insight into malware and malicious activity unseen. Alerts from deception based security tools such as trapX networks or illusive networks is very unlikely to be a false positive and immediately actionable.

**Threat Intelligence Platform**

Integration of Threat intelligence inputs within the SIEM system for automated correlation of Network traffic against bad actors.

Integrate Vulnerability and Compliance Data with SIEM and use this data to identify impact and applicability of threat in IT Landscape

Leverage the threat feed subscriptions (FireEye, Palo Alto & Tanium) for threat intelligence and also bring additional open source threat feeds like abuse.ch, Malware domain list, Zeus Tracker, Cisco Botnet Filter for better threat monitoring.

Threat feeds from Dark Web Monitoring (Hold Security) leveraged to identify domain and industry specific threats along with specific threats targeted on customers.

Leverages the intelligence of monitoring large enterprise customers, and leverages the threat indicators identified

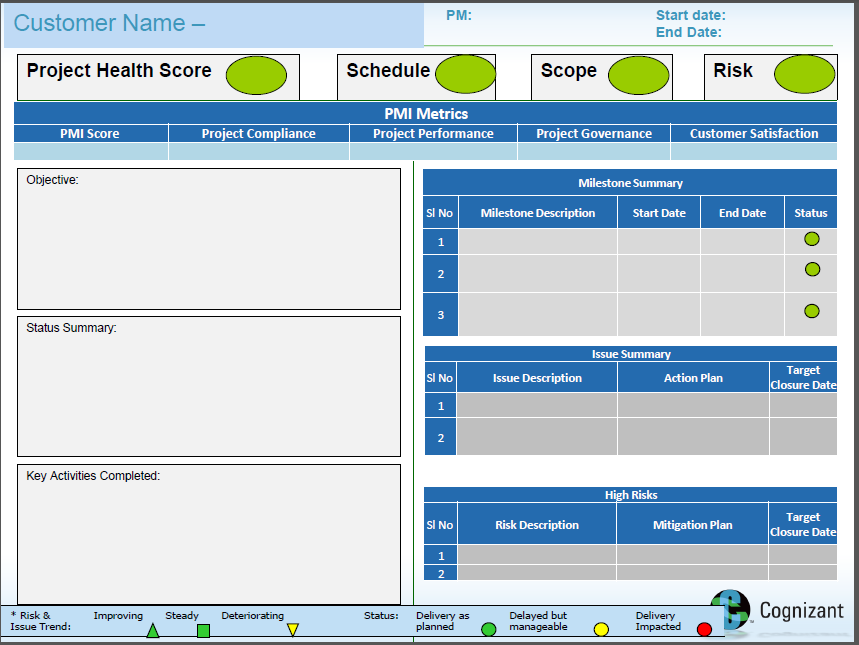
**Security Workflow Orchestration and Automation**

Leverage Servicenow Secops for automating security incident response through integration with SIEM.

Create workflow automation for security incident management, prioritization, records of engagement , resolution and reporting

Leverage Tools like Ayehu for orchestration and automation of basic device management tasks improving response time and resource optimization over a period of time.

1. **Sample PMR Report**



1. **Indicative Profiles**

Following are couple of indicative profiles as a reference to the Cognizant supplied resources.

|  |  |
| --- | --- |
| Indicative Profile 1 | Title: SIEM Architect |
| Skillset :   * IT Security & Technical Support * Security consulting (SIEM, VA, Endpoint Security, CSP, IDS ) * Implementation & Commissioning * Security operations management * IT Infrastructure |
| **Proposed Role and Responsibilities in the Engagement** | * Design of the SIEM Architecture * Implementation of the agreed upon SIEM architecture * Integration of the agreed log sources to the SIEM Infrastructure * Build the correlation rules & Reports * Co-ordinate with Splunk * Participate in project status review meetings |
| **Experience** | The architect has 10+ years of IT experience in Managing IT Infrastructure and Consulting services. Extensive experience in requirements gathering, Designing, Tool deployment and team management, Well versed in using SIEM tools, requirement gathering, Design (LLD / HLD) tools deployment like Splunk, RSA envision, Symantec MSSP Operations, Qualys Qradar VA, Endpoint Security tools SEPM / Splunk ePO and also familiar in managing the Qradar and Strong skills in Security / Threat Management. Proficient in tool deployment of Splunk, RSA envision, QualysGuard, SCSP, Splunk ePO, Symantec End point security 11.x 10.1/10.0 and 9.0, Trend Micro, ArcSight 4.5, Microsoft Forefront client security, Sygate Firewall 4.1  **Key Project Delivered:**   * Design and implement Splunk in HA mode * Splunk hosted in Datacenters and placed the Receivers in all the Remote offices to sends logs to main server on a periodic basis. * Deploy comprehensive [SIEM](http://www.bullhornreach.com/job/266611_siem-analyst-security-information-event-mgmt-austin-tx) architecture to support real-time security monitoring operations * Develop filters and correlated event rules to reduce false-positive alerts. * Created the Security management process document. * Monitor and recommend improvements for security breaches in areas including networks, systems, and endpoints * Provide level 3 [SIEM](http://www.bullhornreach.com/job/266611_siem-analyst-security-information-event-mgmt-austin-tx) support to manage SIEM components, IDS/IPS, parsing/normalization of logs, rule engine, log storage, source device, log collection and event monitoring |
| **Location** | **USA** |

|  |  |
| --- | --- |
| Indicative Profile 2 | Title: SIEM Architect |
| Skillset :   * Splunk, RSA Envision, NetForensics, SSIM, RSA Security Analytics |
| **Proposed Role and Responsibilities in the Engagement** | * Design of the SIEM Architecture * Implementation of the agreed upon SIEM architecture * Integration of the agreed log sources to the SIEM Infrastructure * Build the correlation rules & Reports |
| **Experience** | The architect has 11+ years of expertise in IT predominantly in Information Security Domain. Experience across diverse organizations involving Security Consulting, Security Services, Security Compliance and Incident Response. Proficient in analyzing information system needs, evaluating end-user requirements, custom designing solutions, troubleshooting for complex issues.  Hands on experience on SIEM Tools Deployments, Gateway Devices Up gradation Planning, Implementation & maintenance, Process Mapping and Information Security Risk Assessments.  Service Desk Co-ordination to get Aligned with Security teams and Quality initiative.  **Key Project Delivered:**   * Design and Deployment of Splunk SIEM * Implementing the proposed and approved viable on the Customer Infrastructure with integrating the security and Splunk SIEM components. * Deliver and provide the Customized Correlation, Dashboard and reports * Integration of customized feeds to the Splunk SIEM platform * Configuration of rules for alerts * Customization and Configure rules, offenses and alerts for Log flows and events in SIEM, monitor logs and events. |
| **Location** | **India** |