Dated 12/09/2018

BARCLAYS BANK PLC



WORK ORDER



|  |  |
| --- | --- |
| **Activity/Project** | Splunk Enterprise Core & SIEM |
| **Commencement Date** | 01/10/2018 |
| **Site/location for delivery of the Services/Deliverables** | London |
| **Barclays contact** | Name: Yaman Saqqa  Tel: + 44 (0) 207 116 1810  Email: [Yaman.Saqqa@barlcays.com](mailto:Yaman.Saqqa@barlcays.com) |

1. Scope of Work - Description of Deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Task** | **Expected Artefact** | **Notes** |
| **1** | **Data-Onboarding** | Data and indices created into the System (Operational) | Minimum of 5 data sets ingestion and normalised expected.  Types:   * Firewall * Network * Endpoint (Windows)   Anticipated activities for this task are:   * Creation of indices * Normalising the data * Field extraction based on the business specification * Ingestions pattern advice based |
| **2** | **Integrations** | Integrations in the systems working as per the specifications articulated by users (Operational) | Anticipated integrations tasks are - Minimum of 5 integration expected with code base handed over and transitioned into the RTB Team (See below detail)   * Integration with Databases via DB Connect * Integrations with Hadoop * Integration with Incident management platform i.e. Resilient * Integrations with Intelligence platform e.g. ThreatConnect |
| **3** | **Dashboard Creation** | Dashboards in the systems working as per the specifications articulated by users (Operational) | Build of 10+ Dashboards to support:   * Support monitoring of data feeds |
| **4** | **Data Reconciliation** | * Document with a plan * Document with Hosts reconciled against the original expected | Reconcile data for 3 main ingested data sets from Firewall and Endpoint (Windows desktop events)   * Delivery of a plan of work with internal infrastructure teams to reconcile data coming from our estate e.g. Reconcile hosts from Firewall * Delivery of reconciled hosts from those data sets |
| **5** | **Metadata extraction** | * Document/Knowledge Base article with the Metadata and their definitions | * Creation of an internal knowledge base of the metadata ingested into the Splunk tool |
| **6** | **Splunk ES** | * Document/Knowledge Base article with the ES best practices | * Splunk ES best practise for data utilisation |