August 06

2020

QRadar Scope of Work Document

Project/Solution: SIEM Solution (QRadar)

Prepared for : ABK

Table of Contents

Company Profile

IT Valley is a leading system integrator in Egypt & UAE arming the Egyptian and regional Markets with huge varieties of technologies, platforms and business solutions that serve the Banking, money services, government, defense, telecommunications, oil and gas, and General business sectors

IT Valley ’s Solutions & Services helps organizations & companies to step over their Challenges and problems, and realize their possibilities, aspirations and visions. IT Valley Applies new motivational thinking and ideas to create more simple, valuable and trusted Experiences with Information technology, continuously improving the way our customers develop their business.
Summary

We enable people to do business by planning, supplying, integrating and managing their IT. We make IT work through partnership, knowledge and passion: trusted to run IT services for leading business across Middle East and GCC for 15 years.

- IT Valley solutions started as Infrastructure Services & Solution Provider Company. Today IT Valley is a well-known IT solution provider offering support to various technologies.
- Our collaborative approach with our customers, successful relationships with world-classed technology providers and our ability to be agile and flexible enable us to create innovative solutions, which get you the value you need from your data.
- We plan, supply, integrate and manage IT, so when people do business, we make it work.

Executive Summary

This Scope of work has been submitted based on project’s main objectives and ABK team’s vision in order to define all executive tasks mentioned in the project management time plan for the required upgrade \ Migration Services.
Implementer Installation and Configuration Services provide the customer with the right solution, resulting in successful service ensures that your equipment is up-and-running correctly through this service, organizations have access to the best of Implementer experts who can rapidly install and configure all that is needed for a successful project. Implementer experts will also ensure that knowledge is transferred to organization’s technicians to ensure quality of services continuity.

Scope of Work

In this document we will explain the below:

- Preparation for Migration
- Installation and Migration
- Creating Custom DSM
- Fine Tuning and KT

Migration Method and Implementation Plan

1- Preparation for Migration

1.1 Gathering Information
✓ Solution Architecture
✓ Current Version & Patches
✓ Current IP/s Addresses
✓ Log\Flow Sources with their status
✓ Sample of Logs for unsupported Log Sources
✓ Installed Apps
✓ Any Current Integrations

1.2 Taking Backup
✓ Configuration Backup
✓ Full Back up of Data
✓ Export Network Hierarchy
✓ Export Applications
✓ Export Custom Rules
✓ Export Custom Searches
✓ Export Regex & QID Mapping

1.3 Verification
✓ Planning and Design Discussion
✓ Verifying the reediness of prerequisites
✓ Verifying the current HA Functionality & effectiveness

2- Installation and Migration

2.1 Installation (Offline)
✓ Install The Same Version of IBM QRadar SIEM that Installed on the old Appliances
✓ Initial Configuration Using the same old appliances info Like (Host Name , IP address, Gateway, email server , etc…)
✓ Apply The Same Patches that Installed on the old Appliances
✓ Perform the HA Configuration
✓ Verifying the HA Functionality And Effectiveness

2.2 Migration (Offline)
✓ Upload the old configuration backup to new Appliances
✓ Restore the old configuration backup
✓ Verify that the Restoring done successfully and all services are up and working well
✓ Restore the old Data
✓ Verify that the Restoring done successfully and All Data have been copied

2.3 Going Production (Live)
✓ Verify that the new Appliances are Installed , Powered on and ready to be connected To the network
✓ Disconnect \ Disable the network connection from the old Appliances
✓ Connect \ Enable the network connection on the new Appliances
✓ Test the Appliances connectivity
✓ Verify that the all configured services are up and running
✓ Verify that the old Users able to login with their old roles
✓ Verify that the Events are being received , parsed and stored (As the old state)
✓ Verify that the Flows are being received and stored (As the old state)
✓ Verify that the all Exported & Backup Components Restored Successfully
✓ Verify that the HA working well
✓ Test the fail over Scenarios

3- Creating Custom DSM

3.1 Creating Custom DSM Up to (5) Applicable Log Sources
✓ Get Sample of Logs for the unsupported Device
✓ Set Meeting / Conference with the specialized team to discuss and get the required
✓ Integrate with the Unsupported Device \ Application
✓ Create the required UDSM / Parsers
✓ Create the required QIDs
✓ Perform the required Mapping
✓ Verify that the Events are being received , parsed , mapped and stored

4- Fine Tuning and KT

4.1 Testing
✓ Verify that the all installed devices are up and running
✓ Verify that the all installed and configured services are up and effectively running
✓ Verify that the Events are received , parsed and stored
✓ Verify that the Flows are received and stored

4.2 Fine Tuning
✓ Verify that the Events for the unsupported devices are parsed and mapped correctly
✓ Analyze and review some events and traffic with ABK Team
✓ Perform some fine tuning for system performance
✓ Verify the management activities Like (Backup, Retention Period, Users & Permissions, etc...)

4.3 KT and Project Documentation
✓ Handover Workshop
✓ Project Documentation

Timeline Plan

Date	Required Days	Phase Completion
	3	Phase 1
	7	Phase 2
	17	Phase 3
	3	Phase 4

Prerequisites \ Assumption

- The Servers are racked \ Installed (Powered on)
- The connection between the primary and secondary HA host has a minimum bandwidth of 1 Gigabits per second (Gbps)
- The latency between the primary and secondary HA host is less than 2 milliseconds (ms)
- Provide suitable offboard storage for Data and configuration backup

Customer Responsibilities

- Provide the all mentioned requirements and prerequisites
- Ensuring the prospect has the proper accounts and passwords or have the Administrators Available to configure Log Sources, Flows, and Windows accounts
- Determine if any change control processes will need to be followed in getting the solution Installed and the Log / Flow data forwarded to QRadar
- Take into account various items that can be resolved prior to arriving on-site, e.g. log Sources already configured, firewall accesses opened, domain accounts for WinCollect, User accounts For FTP, etc.
- Syslog should be sent to the QRadar IP address over port 514. Firewalls will need to allow That information to get to the QRadar appliance
- Avail administrator to be the focal point for all Implementer communication relative to This project and will have the authority to act on your behalf in matters regarding this Project
- Provide suitable work space for the Implementer with Internet access during the installation

IT Valley Responsibilities

- Assign the Delivery Team for the required Service
- Provide qualified resources to perform the required Implementation
- Perform the all mentioned tasks in this SOW