tenable

QUICK START OPTIMIZE FOR TENABLE SECURITY CENTER

tenable Security Center

SERVICES BRIEF

Table of Contents

1. INTRODUCTION

This Services Brief ("Brief") incorporates and is governed by the Master Agreement located at http://static.tenable.com/prod_docs/tenable_slas.html, or any negotiated agreement between the parties that covers Professional Services ("Agreement"). Any capitalized terms used herein but not defined will have the definitions ascribed to them in the Agreement.

Any installation, configuration, knowledge transfer, or instruction not specifically referenced in this Brief is considered out of scope for this engagement. This includes, but is not limited to, any integrations related to third party products.

2. SERVICE OVERVIEW

Tenable Security Center (formerly Tenable.sc) Quick Start Optimize services is a tailored service beginning with a Design and Planning Workshop to plan, design and guide towards adopting the Cyber Exposure Lifecycle and Risk-Based Vulnerability Management (RBVM) practices through the configuration and integration of a fully operational capability of Tenable Security Center.

This Quick Start service develops an organizational RBVM approach, leveraging Tenable's enterprise platforms and services to reduce overall Cyber Exposure risk.

This Quick Start Optimize Implementation is designed across three (3) key phases within the scope defined in this Brief:

Phase 1: Tenable Design & Planning, and Readiness

- **Design and Planning.** Experienced Tenable Consultants ("Consultant") will perform a one-day design and architecture workshop with Customer to agree on a solution design according to Tenable Best Practice and recommendations
- **Readiness Exercise.** Experienced Tenable Consultants ("Consultant") will review and validate the solution design, prerequisites and specifications before Phase 2 - Implementation and Enablement commences.

Phase 2: Tenable Security Center Implementation, Configuration and Enablement

- **Install and configure Tenable Security Center**. Tenable Security Center and Tenable Nessus will be installed and configured based on requirements and will implement following Tenable's best practices for enterprise deployment captured during Phase 1 - Design and Planning.
- **Validate operational capabilities**. Tenable Security Center will be validated end-to-end for scanning and other operational capabilities
- **Enablement**. Experienced Tenable Consultants ("Consultant") will provide a Tenable Security Center Enablement session guiding you through Tenable's best practices for Vulnerability Management

Phase 3: Documentation and Project Coordination

- **Tenable Deliverable Documents**. Include Design and Architecture Workshop deliverable and Tenable Security Center documentation of your specific configuration of Tenable products post Installation provided for your future use.

- **Project Coordination**. Experienced Tenable Consultants ("Consultant") will provide ongoing Project Coordination and updates throughout the project.

Prerequisites

In order to receive the Quick Start Services, the Customer must ensure before Tenable begins work that all of the following actions have been performed, is available or is accessible as applicable:

(a) Tenable software covered by this Brief is downloaded and accessible to Engineer

(b) Customer has valid activations and licenses for software applicable to this Brief

(c) Tenable port requirements must be reviewed at https://community.tenable.com/s/article/What-ports-are-required-for-Tenable-products and the necessary ports are open

(d) Access to Tenable's Community and/or Support Portal

(e) All necessary hardware and appliances are mounted and in place

(f) Customer network topology diagram and information

(g) List of Customer hosts that can be actively scanned

(h) Administrative credentials for Customer hosts to be scanned

(i) Customer SMTP server information (if applicable)

(j) Customer LDAP server information (if applicable)

(k) Customer desired Tenable Security Center user list

(l) Customer SAML configuration file (if applicable)

Definitions

SMTP

Simple Mail Transfer Protocol - an internet standard communication protocol for electronic mail transmission.

LDAP

Lightweight Directory Access Protocol - an industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

SAML

Security Assertion Markup Language - standard for exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider.

3. SCOPE

Tenable's Quick Start Optimize Implementation is scoped across three (3) key phases organized by activities. Engineer will create and demonstrate the following in Tenable Security Center:

Phase 1: Activity 1 – Design and Architecture Workshop (Combination of Remote and Onsite delivery to be agreed)

(a) Tenable will perform a one-day Design and Architecture workshop with Customer to agree on a solution design according to Tenable best practice and recommendations.

(b) Review vulnerability scanning in a strategic manner to develop a deployment solution ensuring all assets to be covered.

(c) Review, discuss and agree on solution requirements to identify and define elements required for implementing Tenable solutions such as scan zones, scan repositories and reporting requirements.

  (i) Review solution analysis and preparation

  (ii) Document integration requirements for the defined list of systems in scope

  (iii) Agree on a deployment schedule and plan with Customer Project Lead

  (iv) Agree on an approach for Customer deployment roadmap and activities

(d) Design and Planning Workshop Deliverable(s):

  (i) High-Level Architecture and Design (Tenable Solution) including specific integration points

Phase 1: Activity 2 – Remote Design and Readiness Review:

(a) Pre-planning call to conduct a high-level review of the Design Document deliverable created from Activity 1 following the Design Workshop.

(b) Review current resources, prepare an agreed delivery schedule, review the approach and list of prerequisites and specifications before Phase 2 - Implementation begins.

(c) Review, discuss and agree on solution requirements to update the Pre-Deployment Readiness Document.

(d) Remote design and readiness deliverable(s):

  (i) Pre-Deployment Readiness Document that includes prerequisites preparation steps and required specifications. To be revisited during Phase 1: Activity 3 - Validation.

Phase 1: Activity 3 – Prerequisites Validation delivered remotely prior to installation:

(a) Verify hardware/software prerequisites for Tenable components

(b) Verify firewall ports and required connectivity

(c) Verify access to licenses and support portal

(d) Resolve identified challenges

(e) Ensure "Readiness Document" identified preparations are made:

  (i) Naming convention of scanners

  (ii) Means of recording login credentials for Tenable components (applications/appliances)

  (iii) Configuration settings (NTP, gateways, proxies, LDAP, NS etc.)

(f) Verify IP ranges of environments/sites/subnets are known and will be available during deployment

Phase 2: Activity 1 – Implementation and Configuration for Tenable Security Center

Install and configure Tenable Security Center and components. Tenable components will be installed and configured based on requirements captured during the solution design phase with collaborative activities to cover:

Installation:

(a) Identify locations for Tenable Security Center server/appliance

(b) Install and configure up to twenty-seven (27) Tenable Nessus sensors

  (i) Sensors include Tenable Nessus Agents, Tenable Nessus Scanners, Tenable Nessus Manager, and Tenable Nessus Network Monitor.

(c) Configure scan zones

(d) Configure repositories

(e) Connect one (1) SMTP server

(f) Connect up to two (2) LDAP servers

(g) Connect up to three (3) out-of-the-box (OOTB) integrations the following list: https://static.tenable.com/ps/DS_VM-SC_QS_Intgrtns.pdf

  (i) **NOTE:** Splunk connectors are in scope for an Optimize Quick Start (only SIEM option).

(h) Accept/recast risk - basic understanding and operation

(i) Blackout windows - basic understanding and operation

(j) SAML implementation - Engineer will provide consultation on basic principles and operation

(k) Validate connectivity, confirm proper solution function and license installation and download all up-to-date plugins

(l) Create asset list for use in initial scans

(m) Configure Tenable Management Vulnerability Lumin integration (if licensed)

Scan Policies:

(n) Create up to ten (10) standard scan policies, including:

(i) Discovery scan (non-credentialed)

(ii) Credentialed Security Checks scan

(iii) Perimeter scan from Tenable Cloud scanner (if part of license)

(iv) Audit or compliance scan selected from the CIS group of audit files

(v) Agent scan

(o) Add credentials for Credentialed Security and "Audit and Compliance" scans

(p) Create and launch initial scans using the five (5) standard policies

(q) Review scan results

(r) Show how to use Vulnerability Priority Rating (VPR) score to prioritize remediation

(s) Create dynamic and combination assets for use in reporting and dashboards

Reporting:

(t) Creation of up to eight (8) basic custom report layouts

(u) Create up to eight (8) dashboard or Assurance Report Card views using templates or custom components

(v) Creation of up to eight (8) templates

Phase 2: Activity 2 – Implementation Validation exercise:

(a) Validate successful software and plugins update

(b) Validate successful scan results

(c) Optimize reports and dashboards

(d) End-to-end testing of solution function

(e) Tenable Security Center backup/restore and Disaster Recovery (DR)

(f) Implementation Validation Deliverables:

(i) One (1) Tenable Security Center

(ii) Up to twenty-seven (27) Tenable Nessus sensors

(A) Sensors include Tenable Nessus Agents, Tenable Nessus Scanners, Tenable Nessus Manager, and Tenable Nessus Network Monitor

(iii) Connection for up to four (4) OOTB Tenable Security Center integrations from https://docs.tenable.com/Integrations.htm

(A) **NOTE:** ServiceNow (SNOW) connectors (Tenable-developed or ServiceNow-developed) are out of scope for a Quick Start.

Phase 2: Activity 3 – Dedicated Tenable Enablement Session:

Tenable consultants will provide an Enablement session guiding you through Tenable's best practices for vulnerability management. This includes:

- (a) Vulnerability Lifecycle
  - (i) Vulnerability Risk Management
    - (A) What are your remediation SLAs?
    - (B) How to determine time to remediate
    - (C) Prioritization and VPR
- (b) Scan Strategy
  - (i) What is your corporate scanning policy?
    - (A) Frequency
    - (B) Coverage
  - (ii) Overview of credentialed scans vs. non-credentialed
  - (iii) Overview of asset classification (i.e., OS discovery)
  - (iv) Targeted scanning (e.g., scan assets by classification or just per subnet)
  - (v) What is passive scanning and why use it?
- (c) Data Management and Scan Coverage
  - (i) Repositories (types, needs, going forward)
  - (ii) Scan zones (Why needed, network segregation, DMZs, discreet vs. overlapping)
- (d) Users Groups and Roles (Access Controls)
  - (i) Determine access needed to Tenable Security Center
  - (ii) Roles and responsibilities
    - (A) Identify the Admin
    - (B) Identify the Security Manager
    - (C) Identify who will run scans
    - (D) Identify who will be allowed to scan
    - (E) Identify who will own credentials
- (e) Responding to environmental changes (e.g., network changes, scanner deployment)

(i) Building VM design into network design (where and when to add additional scanners)

(ii) Understand the Change Management process

(iii) Understand the network/firewall review process

(iv) Backup, restore and DR

(f) Meeting Compliance and Policy Requirements

(i) Understand corporate compliance/hardening policies and requirements

(ii) Identify compliance standards

(g) Reporting to Stakeholders

(i) Identify stakeholders

(ii) Reporting to service providers and remediation teams (only report relevant data)

(iii) Understand who needs what and when

(h) Automation Requirements/Opportunities

(i) Agent Distributor

(ii) Asset Lists

(iii) Credential Management

(iv) Data Export

(v) Directory Based User Management

(vi) Risk Rules

(vii) Tenable Scan Bridge

(viii) Ticketing

Phase 3 – Documentation and Project Coordination – Completion of all Tenable documentation

Following the completion of Phase 2, the Tenable resource will finalize and present the following deliverables:

(a) Finalized Customer High-Level Design

(b) Tenable Security Center Solution Design Documentation

(i) Architecture diagram, including a high-level network topology with Tenable products, scan zones and repositories

(ii) Configuration design specific to the deployment

Ongoing throughout – Project Coordination and Reporting:

(a) Prerequisites:

(i) Customer to assign the main Project Manager or contact and authorize project management activities, including ownership of the agreed plan and associated activities to be performed by Tenable

(b) Tenable Tasks:

(i) Coordination of Tenable activities and tasks with Customer project manager/contact

(ii) Tenable activity progress reporting to be agreed, but no more than weekly in frequency

4. DELIVERABLES

Deliverable documentation will be completed and provided across the lifecycle of the project; those deliverables include:

(a) High-Level Architecture & Design (Tenable Solution) including specific integration points

(b) Pre-Deployment Readiness Document

(c) Customer Readiness Documentation

(d) Implementation:

(i) One (1) Tenable Security Center

(ii) Up to twenty-seven (27) Tenable Nessus sensors

(A) Sensors include Tenable Nessus Agents, Tenable Nessus Scanners, Tenable Nessus Manager, and Tenable Nessus Network Monitor.

(iii) Connection for up to four (4) OOTB Tenable Security Center integrations from https://docs.tenable.com/Integrations.htm

(A) **NOTE:** ServiceNow (SNOW) connectors (Tenable-developed or ServiceNow-developed) are out of scope for a Quick Start.

(e) Tenable Security Center Solution Documentation including architecture diagram, including a high-level network topology with Tenable products, scan zones and repositories

(f) Future recommendations

(g) Links to appropriate documentation

5. ASSUMPTIONS AND CONSTRAINTS

Tenable will rely on the following assumptions, together with those stated elsewhere in this Brief, in performing the service in this Brief. Should any of these assumptions prove incorrect or incomplete, or should Customer fail to comply with any of the responsibilities set forth in this Brief, Tenable reserves the right to modify the price, scope, level of effort, or schedule for the service in this Brief.

(a) Customer has valid licenses for all Tenable software covered by this Brief.

(b) Tenable will perform the service both remotely and on-site at a mutually agreed upon Customer location.

(c) Customer will provide Tenable access to key individuals, information and network resources at Customer site that are required in order for Tenable to perform the required tasks and deliverables of this Brief. Timely access to these key Customer individuals is required during the duration of this Brief, either onsite or remotely.

(d) When at a Customer facility, the Customer will provide Tenable Consultant with a professional workspace such as a conference room and access to personnel with sufficient privileges to the relevant hardware and software required to perform the engagement.

(e) Customer shall provide the Tenable Consultant with reasonable and safe access to Customer's facilities and ensure that its facilities constitute a safe working environment.

(f) The Customer systems meet or exceed the specifications found in the Tenable General Requirements document, available at https://docs.tenable.com/generalrequirements/.

(g) All workdays under this Brief are based upon an eight (8) hour workday and all work will be completed during normal working hours defined as Monday through Friday.

(h) Tenable personnel will not be exposed to hazardous environments. Customer will provide any safety equipment needed. Customer personnel will mount the hardware in the appropriate locations.

(i) Tenable is not responsible for any impact caused by Active Querying or any other network communication.

ABOUT TENABLE

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at tenable.com.

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com