tenable

QUICK START ADOPT FOR TENABLE VULNERABILITY MANAGEMENT

tenable Vulnerability Management

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 Vulnerability Management (formerly Tenable.io) Quick Start Adopt services accelerate configuration and integration to a fully operational capability of Tenable Vulnerability Management. The service allows your organization to realize several key benefits of Tenable Vulnerability Management in a short period of time.

This Quick Start Service is designed to provide five (5) outcomes within the scope defined in this Brief:

(a) **Plan and prepare the Customer**. Experienced Tenable Consultants ("Consultant") will pre-plan, review and validate Tenable's approach and customer's prerequisites to ensure a smooth transition to the Installation phase.

(b) **Configure Tenable Vulnerability Management.** Tenable Vulnerability Management and Nessus® sensors will be installed and configured based on requirements captured during Phase 1 - Planning and Validation.

(c) **Implement best practices**. Experienced Tenable Engineers ("Engineer") will implement and orient you to Tenable's best practices for enterprise deployment.

(d) **Validate operational capabilities**. Tenable Vulnerability Management will be validated end-to-end for scanning and other operational capabilities.

(e) **Provide Tenable Deliverable Document**. A summary of your specific configuration of Tenable products will be provided post-installation for your future use.

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, are available or are accessible, as applicable:

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

(b) Customer has valid administrative user names and passwords 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 desired Tenable Vulnerability Management user list

(j) Customer SAML configuration file (if applicable)

(k) Connector information to cloud environment

Definitions

SAML

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

CIS

Center for Internet Security - publishes the CIS Critical Security Controls (CSC) to help organizations better defend against known attacks by distilling key security concepts into actionable controls.

3. SCOPE

Tenable's Quick Start Adopt implementation is scoped by three (3) phases, split into multiple categories: Phase 1 – Planning and Validation; Phase 2 – Implementation and Enablement; Phase 3 – Documentation. Engineer will create and demonstrate the following in Tenable Vulnerability Management:

(a) **Phase 1 – Planning and Validation**

Consultant will perform the following high-level planning and validation activities:

(i) Pre-planning workshop to review resources, prepare a delivery schedule, review the installation approach and identify prerequisites and specifications.

(ii) Create a sensor deployment strategy for up to fourteen (14) sensors.

(iii) Prerequisites validation to verify all is in place and ensure Customer is ready for Phase 2 - Implementation

(b) **Phase 2 – Implementation and Enablement**

Implementation

Consultant will create and demonstrate in Tenable Vulnerability Management:

(i) Install up to fourteen (14) combined Nessus sensors

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

(ii) Configure up to four (4) networks (within Tenable Vulnerability Management)

(iii) Create up to eight (8) tags

(iv) Create up to eight (8) users

(v) Create up to eight (8) discovery scans for predetermined subnets

(vi) Create up to eight (8) Windows and/or Linux credentialed scans for predetermined subnets

(vii) Create two (2) CIS compliance scans based upon two (2) benchmarks

(viii) Create up to eight (8) saved searches

(ix) Create up to eight (8) dashboard views using custom widgets or templates

(x) Create up to four (4) access groups

(xi) Assigning custom groups to target groups

(xii) Up to two (2) out-of-the-box (OOTB) integrations from the following list: https://static.tenable.com/ps/DS_VM-SC_QS_Intgrtns.pdf

(A) **NOTE:** Splunk connectors are out of scope for an Adopt Quick Start.

(xiii) Set up and review Lumin

(xiv) Accept/recast risk – basic understanding and operation

(xv) Blackout windows – basic understanding and operation

(xvi) SAML implementation – Engineer will provide consultation on basic principles and operation

Enablement

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

- Vulnerability Lifecycle
    - Vulnerability Risk Management
        - What are your remediation SLAs?
        - How to determine time to remediate
        - Prioritization and VPR
- Scan Strategy
    - What is your corporate scanning policy?

        - Frequency
        - Coverage
    - Overview of credentialed scans vs. non-credentialed scans
    - Overview of asset classification (i.e., OS discovery)
        - Targeted scanning (e.g., scan assets by classification or just per subnet)
    - What is passive scanning and why use it?
- Reporting to Stakeholders
    - Identify stakeholders
    - Reporting to service providers and remediation teams (only report relevant data)
    - Understand who needs what and when

(c) Phase 3 – Documentation

Tenable consultants will provide a summary of your specific configuration of Tenable products, post-installation, for your future use (see Section 4 Deliverables).

4. DELIVERABLES

A single master deliverable document containing the following will be completed as part of the engagement:

(a) Configuration document summarizing a high-level network topology with Tenable products, scan groups, access groups and tags, in addition to details and specifications of configured setup

(b) Sensor deployment document for up to fourteen (14) sensors

(c) Future recommendations

(d) 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