tenable
Vulnerability Management

QUICK START DEPLOY FOR 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 Deploy 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 three (3) outcomes within the scope defined in this Brief:

(a) **Install and configure Tenable Vulnerability Management**. Tenable Vulnerability Management and Tenable Nessus will be installed and configured based on requirements captured during the solution design.

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

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

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 usernames and passwords for software applicable to this Brief

(c) Tenable port requirements have been 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 - standard for exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider.

CIS

The Center for Internet Security (CIS) 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

This Quick Start service is scoped by two categories: Installation and Configuration, and Operational.

Installation and Configuration

Engineer will perform the following installations and configurations:

(a) Install up to seven (7) combined Tenable Nessus sensors

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

Operational

Engineer will create and demonstrate the following in Tenable Vulnerability Management:

(a) Configure up to two (2) networks (within Tenable Vulnerability Management)

(b) Create up to four (4) tags

(c) Create up to four (4) users

(d) Create up to four (4) discovery scans for predetermined subnets

(e) Create up to four (4) Windows and/or Linux credentialed scans and policies for predetermined subnets

(f) Create one (1) CIS Compliance scan upon one (1) benchmark

(g) Create up to four (4) saved searches

(h) Create up to three (3) dashboard views using custom widgets or templates

(i) Up to one (1) custom report

(j) Create up to two (2) access groups

(k) Assigning custom groups to target groups

4. DELIVERABLES

A single master deliverable document containing three parts (shown below) will be completed as part of the engagement:

(a) Configuration document summarizing the configuration of Customer's installation with descriptions for each configuration

(b) Future recommendations

(c) 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 40,000 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