tenable one
Exposure Management Platform

DESIGN & ARCHITECTURE WORKSHOP FOR TENABLE ONE

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

A Tenable One Design & Architecture Workshop ("Services") by Tenable Professional Services approaches exposure management and vulnerability scanning in a strategic manner, by developing a prioritized strategic plan for the implementation and adoption of our unified exposure management platform.

The Tenable One Design & Architecture workshop will be conducted with the key stakeholders in your business together with Tenable's experts to map together your business and security objectives in a collaborative approach. The Tenable One Design & Architecture deliverable will outline an effective pathway for the adoption of Tenable One.

The Services include the following activities:

(a) **Tenable One Preparation Call**. Tenable will review purchased services and validate priorities, identify required stakeholders for the workshops and draft a detailed agenda for the workshops.

(b) **Tenable One Design & Architecture Workshops**. Tenable will guide the client through a series of assessment workshops together with key customer stakeholders to ensure the client's business and security objectives are prioritized and mapped together into a strategic Tenable One Platform deployment and enablement plan.

(c) **Tenable One Design & Architecture Deliverable**. Tenable will create and provide an endorsed Tenable One High-Level Architecture & Design deliverable including architecture for each sensor, high-level network topology, links to appropriate Tenable documentation and future recommendations.

3. SCOPE

This Service Brief sets out the activities in scope to be provided by Tenable Professional Services to the Customer.

The Tenable One Design and Architecture workshop is designed to be constructive, leading to development of an architecture design to support the deployment phase. The workshop will also provide knowledge transfer in both security best practices and the Tenable One platform and products.

Activity 1: Tenable One Preparation Call

Prior to the Design & Architecture (D&A) workshop, Tenable Consultant(s) will cover the following tasks during a scheduled call:

Activity Tasks

(a) Review the client's Tenable One Exposure Management Platform purchased services and validate priorities

(b) Identify the key internal stakeholders within the Customer organization to schedule the D&A workshops.

(c) Tenable's Professional Services Project Coordination team will schedule the assessment workshops in agreement with the client's project manager/lead contact.

Activity 2: Tenable One Design & Architecture Workshops

Tenable will perform two (2) consecutive Design and Architecture sessions with the customer stakeholders, with each session providing up to six (6) hours of consultant time. Should the sessions be reduced or split, this will need to be coordinated and agreed with the Tenable Professional Services Project Coordination team.

During the workshops, experienced Tenable Consultant(s) will carefully guide the client stakeholders through a series of discussion points to understand and validate the client's priorities for the Tenable One Platform adoption.

The Tenable Consultant(s) will discuss various topics, including access requirements and permissions required to perform users' responsibilities aligned with customer policies.

The Tenable Consultant(s) will gain a deep understanding of the client's environment, network topology, asset types, visibility points, sensor requirements, and availability and map together the key workflows.

The Tenable Consultant(s) will discuss networking requirements, desired scan locations and targets, review credential requirements, and suggest scanner deployment locations.

A scan strategy will be discussed and will involve reviewing any existing Target Operating Model (TOM) and exposure management objectives.

The Tenable Consultant(s) will pre-plan, review and validate Tenable's approach during the workshop sessions to familiarize the client with the different types of Tenable sensors and platform components to be adopted, to enable a comprehensive view of the client's attack surface.

Activity Tasks

(a) **Review Tenable One Platform Components**. Tenable One Exposure Management Platform components are determined by the license type purchased.

  (i) **Tenable Vulnerability Management**:

    (A) Plan Tenable Nessus and Tenable Nessus Network Monitor sensor placement and capacity planning

    (B) Plan Tenable Nessus Agent use and deployment

    (C) Evaluate sensor proxy use and placement (optional)

    (D) Discuss scan strategy, RBAC, tagging and other options

  (ii) **Tenable Security Center Plus or Director, where licensed:**

    (A) Plan Tenable Nessus and Tenable Nessus Network Monitor sensor placement and conduct capacity

planning.

(B) Plan Tenable Nessus Agent use and deployment.

(C) Plan Tenable Nessus Manager placement and conduct capacity planning.

(D) Discuss system configuration (e.g., scan zones and repository design).

(E) Discuss scan strategy, permissions, assets and other options.

(iii) **Tenable Cloud Security:**

(A) Review Cloud Service Provider (CSP) connectors requirements.

(B) Review Cloud Connectors for Amazon Web Services (AWS), Azure and Google Cloud Platform (GCP).

(C) Discuss Infrastructure as Code (IaC) code scanning requirements to achieve correct scanner placement.

(D) Review Continuous Integration/Continuous Delivery (CI/CD) pipeline requirements to ensure the maximum benefits of CI/CD are realized.

(E) Discuss requirements for using Agentless Assessment so that the full capabilities of Tenable Cloud Security vulnerability detection can be achieved.

(iv) **Tenable Web App Scanning:**

(A) Review web applications technology and scope.

(B) Plan usage of Tenable hosted cloud scanners and on-premises Web App Scanning scanner placement, and conduct capacity planning.

(v) **Tenable Identity Exposure:**

(A) Review scope of Active Directory Infrastructure to be monitored (forests, domains and a number of users).

(B) Review Tenable Identity Exposure operational needs and expectations (authentication methods, Syslog and Simple Mail Transfer Protocol [SMTP] alerting needs, identified user profiles).

(vi) **Tenable Attack Surface Management (with Tenable One Enterprise License Only):**

(A) Identify domain targets for later perimeter and web application scanning.

(B) Discuss current domain inventory to ensure the attack surface is properly assessed.

Integration with other systems reduces the need for time-consuming manual export/import of data, adding efficiency, accuracy and standardized, repeatable processes. This frees the analyst's and practitioner's time to focus on analysis, prioritization and remediation activities.

During the workshops, Tenable will discuss out-of-the-box integrations with Tenable Technology Partner products for the ingestion of data into Tenable One, and the enrichment of data on partner products.

The results of the workshops will be documented and included in the Tenable One Design & Architecture deliverable following each session. The deliverable will be completed remotely following the workshop sessions. Further customer collaboration may continue offline with input and guidance led by the Tenable Consultant(s) to arrange the client's agreement of Tenable One Design & Architecture deliverable and agreed deployment plan.

4. DELIVERABLES

Tenable One High-Level Design Deliverable. A single deliverable document containing the two (2) parts listed below will be completed as part of the engagement:

(a) Tenable One High-Level Architecture & Design document summarizing the recommended Customer platform deployment with a description of each component. Deliverable includes:

  (i) Introduction

  (ii) Executive priorities

  (iii) Tenable system components

  (iv) Tenable hardware design

  (v) Tenable scan strategy

  (vi) Recommended approach

  (vii) Operational responsibilities

  (viii) Data flow requirements

  (ix) Tenable One data security

  (x) Capacity planning

  (xi) Appendices containing other relevant information

(b) Future recommendations and 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 may 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