tenable

QUICK START DEPLOY FOR TENABLE IDENTITY EXPOSURE

tenable Identity Exposure

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 Identity Exposure (formerly Tenable.ad) Quick Start Deploy services accelerate configuration and integration to a fully operational capability of Tenable Identity Exposure. The service allows your organization to realize several key benefits of Tenable Identity Exposure in a short period of time.

This 2-day Quick Start Service is designed to provide four (4) outcomes within the scope defined in this Brief:

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

(b) **Configure and customize IOEs**. Experienced Tenable Engineers will empower you to fine-tune Tenable Identity Exposure deviances detection to make it fit to your operational and regulation constraints.

(c) **Configure alerts**. Configure and demonstrate SMTP and SYSLOG alerts.

(d) **Configure dashboards and tools**. Tenable Engineers will provide turnkey dashboards and tools to facilitate monitoring the benefits of Tenable Identity Exposure on your Active Directory (AD) governance.

Prerequisites

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

(a) For SaaS customers only: VPN Tunnel configuration form filled and submitted.

(b) For On-Premises customers only:

  (i) Tenable software covered by the Brief is downloaded and accessible to Engineers.

  (ii) Customer has valid credentials applicable for installation (local administrative permissions on each component).

(c) Service account has read permissions on alternate containers (Recycle Bin and Password Settings Container).

(d) Ensure necessary ports are open according to the pre-call document.

(e) Access to Tenable's Community and/or Support portal.

(f) All necessary hardware and appliances are mounted and in place (On-Premises only).

(g) Customer desired AD domains and forests list.

(h) Administrative credentials for the IOA GPO deployment (if applicable).

(i) Customer desired Tenable Identity Exposure user list (if customer wants to use internal Tenable Identity Exposure authentication method).

(j) Customer SAML configuration file (if applicable).

(k) Customer LDAP authentication configuration information (if applicable).

(l) Customer desired Tenable Identity Exposure standard profile information.

(m) Customer SYSLOG information (if applicable).

(n) SMTP information.

Definitions

Active Directory (AD)

Microsoft technology, based on LDAP technology, used to manage computers and other devices on a network. It is a primary feature of Windows Server, an operating system that runs both local and Internet-based servers.

SAML

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

LDAP

Lightweight Directory Access Protocol – standard for communicating (authentication, access, modification) with directory services.

GPO

Group Policy Object – Virtual object containing policy settings applied to a scope of users, groups or computer objects in your Active Directory.

IOE

Indicator of Exposure – Indicator referencing one or more misconfigurations that expose your Active Directory forest(s) and domain(s) to external threats, categorized by criticality (from Low to Critical).

IOA

Indicator of Attack – Indicator indicating a cyberattack is happening in your environment using Active Directory breaches.

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 one (1) Directory Listener (DL), if applicable.

(b) Install one (1) Security Engine Node (SEN).

(c) Install one (1) Storage Manager (SM).

(d) Configure up to two (2) Active Directory domains to monitor with Tenable Identity Exposure.

(e) Assist customer during VPN tunnel configuration and implementation (SaaS only).

(f) Deploy one (1) IOA GPO with Customer (if applicable).

(g) Configure up to four (4) local accounts with access to the Tenable Identity Exposure solution.

(h) Configure one (1) SAML and/or LDAP authentication (if applicable).

Operational

Tenable's Engineers will create and demonstrate in Tenable Identity Exposure the following for up to one (1) security profile:

(a) Create one (1) new security profile.

(b) Deploy up to three (3) pre-configured dashboards.

(c) Demonstrate how to perform Trail Flow searches.

(d) Review, analyze and customize IOEs behavior (prioritizing Critical and High severity).

(e) Review and analyze IOAs (if applicable).

(f) Create one (1) new role (If applicable).

(g) Create up to two (2) SMTP Alerts (if applicable).

(h) Create up to two (2) Syslog Alerts (if applicable).

(i) Configure one (1) SMTP connection (if applicable).

(j) Provide Dashboard and Security Profile tool demonstrations (if applicable).

(k) Implement and demonstrate one (1) pre-configured dashboard in PowerBI (if applicable).

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

A spreadsheet document containing these three parts:

(a) Global metrics of the domain that was analyzed in the workshop.

(b) List of Indicators with deviant elements that need to be remediated, with expected workload and remediation step(s) suggested by Tenable Consultant.

(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 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