tenable
OT Security

QUICK START FOR TENABLE OT SECURITY

SERVICES BRIEF

Table of Contents

1. INTRODUCTION 3
2. SERVICE OVERVIEW 3
3. SCOPE 4
4. DELIVERABLES 6
5. ASSUMPTIONS AND CONSTRAINTS 7

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.

All services outlined in this brief will be delivered by a Tenable Certified Security Consultant, or by one of Tenable's qualified partners (hereinafter "Consultant").

2. SERVICE OVERVIEW

The QuickStart engagement is required for the setup of Tenable OT Security. The service allows your organization to realize several key benefits of Tenable OT Security in a short period of time.

This QuickStart Service is designed to:

- **Install and configure Tenable OT Security.** Tenable OT Security Appliance and up to three (3) sensors will be installed and configured based on requirements captured during the Planning phase.

Additionally, this QuickStart Service is designed to provide the following outcomes:

(a) Implement leading practices. Consultant will orient you to Tenable's leading practices to meet your goals.

(b) Validate operational capabilities. Tenable OT Security will be tested end to end for asset visibility and other operational capabilities.

(c) Integrate with Tenable Security Center (optional).

If the Customer has an operational Tenable Security Center, the Tenable OT Security Appliance can be configured to upload asset and vulnerability information.

If the Customer does not have Tenable Security Center but wants it, then a Tenable Security Center QuickStart and Tenable Security Center training are recommended prior to this engagement.

Tenable Security Center is not a prerequisite to installing and operating Tenable OT Security.

(d) Integrate with Tenable OT Security Enterprise Manager (optional).

If the Customer has an operational Tenable OT Security Enterprise Manager, the Tenable OT Security Appliance can be configured to upload asset and vulnerability information.

If the Customer does not have Tenable Security Center but wants it, then a Tenable Security Center Quick Start and Tenable Security Center training are recommended prior to this engagement.

Tenable Security Center is not a prerequisite to installing and operating Tenable OT Security.

The Tenable OT Security QuickStart does not include the setup or configuration of Tenable Security Center in support of optional Tenable Security Center activities identified in this Brief, and assumes the customer is already qualified in the Tenable Security Center product.

Prerequisites

In order to receive the QuickStart Services, the Customer must ensure before Consultant begins the setup and deployment that all of the following actions have been completed:

(e) Network SPAN ports have been configured and pcaps shared with Consultant for evaluation.

(f) Tenable OT Security Appliance and sensors have been received by the Customer and are ready to be staged, and all requirements for connectivity (rack space, power, network, etc.) are met. Customer verifies fans operate when the Appliance is powered on.

(g) After discussions in the planning meeting, the following actions have been completed:

Dataflow permission has been put in place in relevant internal and external firewalls. Refer to: https://community.tenable.com/s/article/What-ports-are-required-for-Tenable-products

Customer's high level network topology information provided.

Customer's OT subnets listed, specifics on controllers and inventory shared.

Optional - SMTP, syslog, and LDAP server information gathered.

3. SCOPE

This QuickStart Service is scoped by Planning, Installation, Configuration, Operational, Instructional and Tuning phases.

For remote engagements all sessions will be performed remotely through remote video conferencing sessions.

For on-site engagements the deployment, installation, configuration, operational and instructional phases and initial tuning will be performed over two (2) days. All planning, design, staging and follow-up tuning sessions will be performed remotely through remote video conferencing sessions.

(a) Planning

Consultant will assist the Customer with the following planning steps:

Discuss with OT team Customer OT requirements, business functions, project goals, and scope.

Discuss with OT team network topology, inventory, and types of controllers.

Discuss network requirements for Tenable OT Security.

Discuss project phases and timetable.

(b) Installation

Tenable Consultant will assist the Customer with the following installation steps:

Install one (1) instance of Tenable OT Security Appliance and upgrade to the latest version.

Install up to three (3) Tenable OT Security sensors on SPAN ports.

(c) Configuration

Consultant will assist the Customer with the following configuration steps:

Tenable OT Security:

(i) Evaluate the passive sniffing by the appliance and remote sensors to identify subnets, protocols, types of devices and traffic patterns.

(ii) Develop asset groups specifying OT subnets.

(iii) Allow the system time to capture an adequate sample of traffic.

(iv) Connect Tenable OT Security to the SMTP server, syslog and LDAP server.

Tenable Security Center: (optional)

(i) Set up an agent repository.

(ii) Integrate Tenable OT Security Appliance with the Tenable Security Center server.

(iii) Evaluate the assets and CVE information from Tenable OT Security Appliance.

(d) Operational

These steps benefit from having the network engineers that know the OT network and devices available during the engagement. Consultant will assist the Customer in setting up the following:

Tenable OT Security:

Evaluate events and policies:

For trusted traffic that is leaving and entering the OT network.

For traffic the Customer considers normal, which does not need alerting.

For activities needing review and possibly email alerts.

For evaluating network threats.

Identify controllers that can be actively queried and perform snapshots at the Customer's direction.

Customer prioritizes controllers.

Customer arranges best timing for testing query.

Closely collaborate with OT operations contacts.

Identify other devices that can be queried at the Customer's direction.

Customer determines which probes they want to include.

Evaluate network and configuration events.

Review events and customize relevant policies.

Tenable Security Center: (optional)

(i) Configure up to two (2) useful dashboards and/or reports according to customer requests.

Explain relevant plugins, asset lists and queries.

(e) Instructional

A key part of this engagement is the knowledge transfer and increasing the Customer's operational skills. Therefore, the following will be included in the engagement:

Customer will operate the keyboard for most activities to increase their familiarity with Tenable OT Security interface and routine activities.

Knowledge transfer between Consultant and Customer on valuable functional concepts and leading practices.

Customer's directions on key decision points like OT operational context, network information and corrections, active querying and useful tuning.

(f) Tuning

One (1) tuning session after initial setup.

Performed remotely through video conferencing sessions.

Activities will continue the work begun in the Operational phase as outlined in Section 3 above.

4. DELIVERABLES

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

(a) Summary of planning, configuration, and tuning activities

(b) Links to useful resources

In accordance with the Agreement upon completion of the final task, receipt of the final deliverable will be deemed as accepted unless otherwise notified by Customer via email within ten (10) business days after completion and delivery by Consultant.

Once the final deliverable is accepted all Professional Services will be complete and the engagement concluded.

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) Consultant may perform the service both remotely and on-site at a mutually agreed upon Customer location.

(c) Customer will provide Consultant access to key individuals, information and network resources that are required in order for Consultant 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 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 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