tenable
Cloud Security

QUICK START REMOTE FOR TENABLE CLOUD SECURITY

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.

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 Tenable Cloud Security (formerly Tenable.cs) Quick Start is a tailored remote service to streamline identification and remediation of code misconfiguration via:

- Scanning of code prior to committing to Source Control Management (SCM)
- Scanning of code within SCM
- Identification of risk in the Continuous Integration/Continuous Delivery (CI/CD) pipeline
- Runtime configuration and risk assessment

This Quick Start Service is designed to provide seven (7) outcomes within the scope defined in this Brief:

1) **Plan and prepare the Customer.** An experienced Tenable Consultant ("Consultant") will pre-plan, review and validate the Tenable.cs Cloud Security approach and Customer's prerequisites to ensure a smooth transition to **Phase 2** activities.

2) **Create a Tenable.cs Cloud Security software as a service (SaaS) instance for the Customer.** The Customer will complete this following **Phase 1 - Pre-Call**. The Consultant will complete the Tenable.cs Cloud Security license upgrade from trial license to full license.

3) **Provide Customer Onboarding and Familiarization.** Consultant will assist the Customer in adding user accounts, downloading and installing the Tenable.cs Command Line Interface (CLI), and connecting to and scanning the chosen assets and repositories.

4) **Integrate Tenable.cs Cloud Security.** Perform integration of Tenable.cs into one (1) Customer CI/CD pipeline.

5) **Configure Tenable.cs Cloud Security.** Configure Tenable.cs for use with any of the supported third-party integrations (for example Splunk, JIRA or other supported applications) identified in **Phase 1 - Pre-Call**.

6) **Optimize Customer Use and Understanding of Tenable.cs Cloud Security.** Consultant will provide overview of data provided in the Tenable.cs console, interpretation of the data and generation of reports.

7) **Provide Deliverable Document.** Document will provide a summary of your deployment objectives and outcomes.

General Prerequisites

In order to receive the Tenable.cs Remote 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. Please note these are general prerequisites. Each service outlined in **Section 3, Phase 3** below may have additional prerequisites, which are outlined in the **Quick Start Remote for Tenable.cs Prerequisites Document**.

(a) Confirm Administrator access to Tenable.cs Cloud Security website.

(b) Customer has approval for and access to credentials needed for SCM integration, cloud provider integration, pipeline integration, Kubernetes Cluster integration, and third-party integrations identified in **Section 2, item 5**, above.

(c) Customer has identified locally cloned repositories, cloud provider projects/virtual private clouds (VPCs), SCM repositories and pipelines to be scanned.

(d) Customer must have internal approval to scan the identified resources listed in **Section 2**, above.

(e) Customer representative with knowledge of the structure and makeup of identified resources in **Section 2**, above must be available during all phases of the engagement (typically associated with DevOps).

(f) Confirm access to Tenable.cs online documentation.

3. SCOPE

Tenable's Quick Start implementation is scoped by three (3) phases, split into multiple categories: **Phase 1 – Pre-Call; Phase 2 – Prerequisites (optional); Phase 3 - Implementation; Phase 4 - Integration, Configuration and Optimization; Phase 5 – Documentation**.

Phase 1 - Pre-Call

Requirements around integration will be gathered during one (1) or more Pre-Call(s). Prerequisites for integration will be discussed to ensure that the customer environment and infrastructure is correctly prepared and configured for **Phase 2** and **Phase 3** activities.

The customer may require additional aid to meet all prerequisites for the services discussed during the Pre-Call. The consultant should aid the customer as needed to meet all requirements as noted in **Section 4 Prerequisites**.

Phase 2 - Prerequisites (optional)

The customer may require additional aid to meet all prerequisites for the services discussed during the Pre-Call. The consultant should aid the customer as needed to meet all requirements as noted in the Prerequisites document.

Phase 3 – Implementation

Consultant will assist the Customer in performing the following actions:

(a) Download, installation and use of Tenable.cs CLI to scan up to three (3) locally cloned repositories.

(b) Connection to and scanning of a combination of three (3) of the following cloud provider assets:

(i) Amazon Web Services (AWS) Virtual Private Cloud (VPC)

(ii) Microsoft Azure Project

(iii) Google Cloud Provider (GCP) Project

(c) Connection to and scanning of three (3) repositories from the following SCM providers:

(i) Bitbucket

(ii) GitHub

(iii) GitLab

(iv) Azure DevOps

(v) AWS Code Commit

Phase 4 - Integration, Configuration and Optimization

Integration

Consultant will perform integration of Tenable.cs into one (1) Customer CI/CD pipeline, from any of the following:

(a) Azure DevOps

(b) Jenkins

(c) CircleCI

(d) AWS CodeCommit

(e) GitHub Workflows and/or Actions

(f) GitLab CI/CD

Configuration

Assist in configuring Tenable.cs for use with up to three (3) of the following supported third-party integrations identified in **Phase 1 - Pre-Call:**

(a) Jira (Ticketing)

(b) Slack (Alerting)

(c) AWS Simple Notification Service (SNS) (Alerting)

(d) Microsoft (MS) Teams (Alerting)

Optimization

Consultant will provide overview of data provided in the Tenable.cs Cloud Security console, interpretation of the data and generation of reports, to optimize Customer use and understanding of Tenable.cs Cloud Security.

Phase 5 - 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 Tenable.cs deployment configuration and integration with cloud provider(s), SCM provider(s), CI/CD pipeline(s) and supported third-party applications.

(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