tenable

QUICK START REMOTE FOR TENABLE CLOUD SECURITY

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 Quick Start is a tailored remote service to streamline identification and remediation of cloud resource misconfigurations, workload vulnerabilities and excessive permissions via:

- Set up Single-Sign-On (SSO) to Tenable Cloud Security console
- Onboard your cloud accounts
- Integrate your Identity Provider (IdP)
- Add out-of-the-box third-party integrations
- Configure Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), Cloud Workload Protection (CWP) and Cloud Native Application Protection Platform (CNAPP) capabilities

This Quick Start Service is designed to provide six (6) 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 Cloud Security approach and Customer's prerequisites to ensure a smooth transition to Phase 2 activities.
2) **Provide Customer onboarding and familiarization.** Consultant will assist the Customer in configuring SSO, onboarding cloud accounts, integrating with the IdP.
3) **Integrate Tenable Cloud Security.** Integrate supported ticketing, notification, Security Information and Event Management (SIEM), and data security posture management (DSPM) tools with Tenable to create tickets and send push notifications to these tools when specific findings are created in Tenable Cloud Security.
4) **Configure Tenable Cloud Security.** Optionally, configure Tenable Cloud Security for use with supported continuous integration/continuous deployment (CI/CD) pipelines.
5) **Optimize Customer use and understanding of Tenable Cloud Security.** Consultant will provide overview of data provided in the Tenable Cloud Security console, interpretation of the data and generation of reports.
6) **Provide Deliverable Document.** Document will provide a summary of your deployment objectives and outcomes.

General Prerequisites

In order to receive the Tenable Cloud Security 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 2** below may have additional prerequisites, which are outlined in the **Quick Start Remote for Tenable Cloud Security Prerequisites Document**.

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

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

(c) Customer has identified cloud provider accounts and, optionally, 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.

(f) Access to Tenable Cloud Security online documentation will be available to those with access to the Tenable Cloud Security web interface.

3. SCOPE

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

Phase 1 - Pre-Call & Prerequisites

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** activities.

Phase 2 – Onboarding, Configuration, Integration and Operation

The Tenable consultant will assist the Customer in performing the following actions:

(a) Configuring one of the following SSO providers: (**NOTE:** Not required for Tenable One customers)

(i) Azure Active Directory (AAD)

(ii) Google

(iii) Okta

(iv) OneLogin

(v) Ping Identity

(vi) JumpCloud

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

(i) Amazon Web Services (AWS) accounts

(ii) Microsoft Azure subscriptions

(iii) Google Cloud Platform (GCP) projects

This activity will include implementing CWP for virtual machines and containers, if desired.

(c) Configuring one (1) of the following IdPs for a complete inventory of federated users and groups associated with your cloud accounts.

(i) Azure AD

(ii) Google Workspace

(iii) Okta Organization

(iv) OneLogin

(v) Ping Identity

(d) Configuring Infrastructure as Code (IaC) scanning for up to three (3) supported repositories.

(e) Configuring Tenable Cloud Security with one (1) Customer CI/CD pipeline, from any of the following:

(i) Azure Pipeline

(ii) GitHub Actions

(iii) GitLab CI/CD

(iv) Jenkins Pipeline

(v) Terraform Cloud

(f) Integrate Tenable Cloud Security for use with up to three (3) of the following supported third-party integrations:

(i) Jira (Ticketing)

(ii) Slack (Alerting)

(iii) Microsoft (MS) Teams (Alerting)

(iv) Datadog (SIEM)

(v) QRadar (SIEM)

(vi) Splunk (SIEM)

(vii) Dig Security (Data Security)

(viii) Sentra (Data Security)

(g) Configure Tenable Cloud Security for use with one of the following Kubernetes Services:

(i) Amazon Elastic Kubernetes Service (EKS) Cluster

(ii) Azure Kubernetes Service (AKS) Cluster

(iii) Google Kubernetes Engine (GKE) Cluster

(h) Consultant will provide overview of data provided in the Tenable Cloud Security console, interpretation of the data and generation of reports, to optimize Customer use and understanding of Tenable Cloud Security. This will include the following:

- Console navigation overview
- Create an account hierarchy with folders
- Perform permission queries
- Review permission analysis and risk levels
- Identity intelligence
- Excessive permissions
- AWS federated permissions
- View your asset inventory
- Drill down into resources
- Visualize permission mapping
- Activity log
- Anomaly detection
- Monitor cloud compliance
- Analyze IaC findings from scan results

(i) Consultant will provide overview and workflow for remediation for up to three (3) findings. This may include:

- Snoozing findings
- Manual remediation of findings
- Automatic remediation findings
- Marking findings as resolved

Phase 3 - Documentation

After installation, Tenable consultants will provide a summary of your specific configuration of Tenable products, 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:

(i) Configuration document summarizing Tenable Cloud Security deployment configuration and integration with cloud provider(s), Supply Chain Management (SCM) provider(s), CI/CD pipeline(s) and supported third-party applications.

(j) Future recommendations

(k) 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