tenable

PROFESSIONAL SERVICES

Tenable One Core Deployment

SERVICES BRIEF

Table of Contents

1. INTRODUCTION

The description of Professional Services in this Services Brief ("Brief" or "SOW") 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 SOW 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 One Core Deployment service is a structured engagement designed to help organizations strategically implement and adopt the Tenable One exposure management platform with up to three (3) Tenable products. The list of eligible products includes:

- Tenable Vulnerability Management
- Tenable Security Center
- Tenable Web App Scanning
- Tenable Cloud Security
- Tenable Identity Exposure
- Tenable Attack Surface Management

Tenable OT Security is not in scope for this service.

Through a phased approach, Tenable Professional Services will guide your team from initial design through planning, implementation, enablement, and optimization, ensuring a seamless and effective integration of Tenable's exposure management capabilities.

Service Phases

1. Phase 1: Planning
   The engagement begins with the Tenable One Planning Session, where Tenable Professional Services collaborates with your team to define a prioritized plan for adopting the Tenable One platform. This phase establishes a structured roadmap for exposure management implementation.
2. Phase 2: Implementation
   Once the planning deliverable is agreed upon, Tenable experts will lead a sequenced implementation plan, ensuring a smooth onboarding process. This phase includes deploying, configuring, and integrating up to three (3) Tenable and up to four (4) third-party products to establish a fully operational exposure management solution tailored to your environment.
3. Phase 3: Enablement
   This phase focuses on knowledge transfer and hands-on enablement to maximize the value of your investment.

Your team will gain the expertise needed to use the Tenable One platform effectively, enhancing visibility across the attack surface and enabling accurate cyber risk communication to support business objectives.

4. Phase 4: Optimization
   The final phase includes a series of Optimization Workshops, during which Tenable experts assess your existing implementation, review current capabilities, and provide recommendations based on industry best practices. This ensures that your exposure management solution operates at peak efficiency and aligns with evolving security needs.

Prerequisites

a) Tenable software covered by this Service Brief is downloaded and accessible to Consultant.

b) Customer has valid administrative credentials for software applicable to this Service Brief.

c) Tenable port requirements must be reviewed at https://community.tenable.com/s/article/What-ports-are-required-for-Tenable-products and the necessary ports must be opened.

d) Tenable Cloud Sensors must be reviewed at https://docs.tenable.com/vulnerability-management/Content/Settings/Sensors/CloudSensors.htm for Tenable Vulnerability Management and Tenable Web App Scanning and at https://docs.tenable.com/attack-surface-management/Content/Topics/CloudSensors.htm for Tenable Attack Surface Management. The necessary source IP ranges must be allowed.

e) Tenable sensors must be allow-listed (a.k.a. "whitelisted") in antivirus/Endpoint Detection and Response (EDR), host-based firewalls, Intrusion Detection System (IDS) or Web Application Firewalls (WAF).

f) Access to Tenable's Community Portal.

g) All necessary hardware and appliances are mounted and in place.

h) Customer desired Tenable One user list and permissions.

i) Customer Security Assertion Markup Language (SAML) configuration (if applicable).

j) For Tenable Vulnerability Management or Tenable Security Center:

   i) Customer network topology diagram and information.

   ii) List of Customer hosts that can be actively scanned.

   iii) Administrative credentials for Customer hosts to be scanned.

   iv) Lightweight Directory Access Protocol (LDAP) information (Tenable Security Center only).

   v) Simple Mail Transfer Protocol (SMTP) information (Tenable Security Center only).

k) For Tenable Web App Scanning:

   i) List of web applications to be scanned.

   ii) Customer must have legal authorization to scan the identified web applications.

   iii) Credentials for web applications to be scanned.

   iv) A customer representative with knowledge of the structure and makeup of the web applications (ideally a Developer).

   v) The web application is accessible from the Tenable cloud scanners or from the on-premises Tenable Web Application Scanner.

l) For Tenable Attack Surface Management:

   i) The customer's name must match the WHOIS DNS record (e.g., for sub-sub-domains the customer is the registered WHOIS owner).

   ii) Customer representative with knowledge of the structure and makeup of the external domain and address space must be available.

m) For Tenable Cloud Security:

   i) Customer has approval for and access to credentials needed for cloud provider integration, pipeline integration, Kubernetes Cluster integration, and third-party integrations.

   ii) Customer has identified cloud provider accounts and, optionally, pipelines to be scanned.

   iii) Customer must have internal approval to scan the identified cloud resources.

   iv) Customer representative with knowledge of the structure and makeup of identified cloud resources.

n) For Tenable Identity Exposure:

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

   ii) Customer desired Active Directory (AD) domains and forest list

   iii) Administrative credentials for the Indicator of Attack (IoA) Group Policy Object (GPO) deployment (if applicable)

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

   v) Customer LDAP authentication configuration information (if applicable)

   vi) Customer desired Tenable Identity Exposure standard profile information

   vii) Customer system logging protocol (syslog) information (if applicable)

   viii) SMTP information

o) For the Tenable One Platform:

   i) List of different stakeholders from the Tenable Vulnerability Management teams, Security teams and other stakeholders interested in Tenable One analytics data.

   ii) At least one (1) product ingesting data into Tenable One. At least two (2) products ingesting data into Tenable for Attack Path Analysis.

3. SCOPE

PHASE 1: PLANNING

This Service Brief defines the scope of activities delivered by Tenable Professional Services to support the customer in planning and preparing for the successful adoption of the Tenable One Exposure Management Platform.

The Tenable One Planning session is a structured, collaborative engagement to develop an implementation plan supporting the deployment phase.

Activity 1: Tenable One Preparation Call

Prior to the Planning Session, Tenable Consultant(s) will conduct a preparatory call to:

- Review the customer's purchased services for the Tenable One Exposure Management Platform and validate implementation priorities.
- Identify key internal stakeholders within the customer's organization for participation in the Planning session.
- Coordinate and schedule the planning session with the customer's project manager or lead contact, facilitated by Tenable's Professional Services Resource Management team.

Activity 2: Tenable One Planning Session

Tenable will conduct one (1) consecutive session for up to six (6) hours of consultant time. If the session needs to be modified, rescheduled or split, this must be coordinated with Tenable's Professional Services Resource Management team.

During this session, Tenable Consultant(s) will guide customer stakeholders through structured discussions to understand and validate their security priorities and Tenable product prerequisites and requirements for adopting the Tenable One platform.

This Planning Phase ensures a well-structured, customer-specific approach to implementing Tenable One, setting the foundation for a successful deployment and ongoing security optimization.

Activity Tasks
Tenable will review the Tenable One Platform Components and develop a structured deployment and optimization plan through targeted discussions during the planning session.

Introductions and Project Overview

- Discuss Planning Session overview, review executive goals and the rollout plan.

Tenable Vulnerability Management or Tenable Security Center

- Review network environment.
- Create a sensor deployment strategy for base Vulnerability Management implementation.

Tenable Attack Surface Management

- Review external address and domain space.

Tenable Web App Scanning

- Review Web App Scanning environment, technologies used and requirements for scanner deployment.

Tenable Cloud Security

- Review public cloud infrastructure, Infrastructure as Code (IaC) technology, code repositories, and Continuous Integration/Continuous Deployment (CI/CD) tools.

Tenable Identity Exposure

- Review AD infrastructure (AD Forest, Domains, number of users) and requirements to connect to Tenable One.

Tenable Exposure Management

- Clarify stakeholder access permissions and Tenable Exposure Management third-party connectors, analytics and reporting requirements.

Finalize the deliverable remotely with continued customer collaboration as needed.

This structured approach ensures an optimized and well-integrated Tenable One deployment, enhancing security visibility and operational efficiency.

Activity 3: Tenable One Planning Deliverable

Following the planning session, the Tenable Consultant will create the Tenable One Planning Deliverable based on a Tenable template, documenting the recommended platform deployment of the Tenable products (Tenable Vulnerability Management or Tenable Security Center, Tenable Web App Scanning, Tenable Cloud Security, Tenable Identity Exposure, and Tenable Attack Surface Management). It will also include future recommendations and best practices to support an optimal Implementation Phase.

Activity 4: Final Planning Review Call

Tenable will conduct a Planning Review Call before proceeding to the next phase. This review call concludes the Planning Phase, providing the client a clear roadmap for a seamless transition into the Implementation Phase.

Phase Closure:

The Tenable Consultant will formally confirm the completion of the Planning Phase (Phase 1), ensuring that all agreed-upon deliverables and objectives have been met.

PHASE 2: IMPLEMENTATION

The Tenable One Core Deployment Implementation Service ensures a structured and efficient deployment of Tenable products, establishing a fully operational Exposure Management solution tailored to your environment. The process begins with a prerequisite validation to confirm all necessary conditions are met before proceeding with deployment, configuration, and integration. Tenable experts will lead a sequenced implementation plan, ensuring a smooth onboarding experience.

During the implementation phase, **you can select up to three (3) Tenable products** from our comprehensive Tenable One portfolio for deployment.

In the planning phase, your Tenable Consultant will collaborate with you to define a strategic implementation sequence for the selected products. While we follow a recommended methodology, the order of implementation is fully adaptable to align with your unique priorities and timelines.

The final implementation plan will be shaped by insights gathered during Phase 1 (Planning) to reflect your organization’s goals, resource availability, and success criteria.

Activity 1 – Prerequisites Validation Call

Before implementation begins, Tenable Consultant will conduct a readiness assessment, reviewing and validating all prerequisites to ensure a seamless transition into the Implementation Activities.

Activity 2 – Tenable Vulnerability Management Implementation

The Tenable Vulnerability Management Implementation Service accelerates the deployment and configuration of Tenable Vulnerability Management, enabling organizations to realize their benefits quickly. Consultant will create and demonstrate the following in Tenable Vulnerability Management:

- Install up to fourteen (14) Tenable sensors:
  - Sensors include Tenable Nessus Scanners, Tenable Nessus Agents, Tenable Nessus Network Monitor and Tenable Sensor Proxy.
- Configure up to four (4) Networks (within Tenable Vulnerability Management)
- Create up to eight (8) Tags
- Create up to eight (8) Users
- Create up to eight (8) Discovery Scans for predetermined subnets
- Create up to eight (8) Windows and/or Linux credentialed Scans for predetermined subnets
- Create up to two (2) CIS Compliance Scans based upon two (2) pre-existing benchmarks
- Create up to eight (8) Saved Searches throughout Assets and Findings pages
- Create up to eight (8) Dashboard views using custom widgets or templates
- Create up to one (1) custom Report
- Up to two (2) Out-of-the-box (OOTB) integrations from the following list: https://static.tenable.com/ps/DS_VM-SC_QS_Intgrtns.pdf
  - **Note:** The Service Now integration is out of scope for a Tenable One Core Deployment.
- Accept/Recast risk - basic understanding and operation
- Exclusions - basic understanding and operation
- Create up to two (2) Queries in Vulnerability Intelligence
- Create up to two (2) (one custom) Combinations in Exposure Response
- Create up to two (2) Initiatives in Exposure Response
- Create up to two (2) Report Cards in Exposure Response
- Create up to two (2) Remediation Goals or Remediation Projects

This structured implementation ensures a fully operational Tenable Vulnerability Management deployment, optimized for effective Tenable Vulnerability Management within your organization.

Activity 3 – Tenable Security Center Implementation

Install and configure Tenable Security Center and components. Tenable components will be installed and configured based on requirements captured during the solution design phase with collaborative activities to cover:

- Install one (1) instance of Tenable Security Center
- Install and configure up to fourteen (14) Tenable sensors:
  - Sensors include Tenable Nessus Scanners, Tenable Nessus Network Monitor, Tenable Nessus Agents, Web Application Scanners and Sensor Proxies.
- Configure one (1) Organization
- Configure up to six (6) Scan Zones
- Configure up to three (3) Repositories
- Connect Tenable Security Center to one (1) SMTP server
- Connect Tenable Security Center to one (1) LDAP server
- Configure one (1) Group
- Create up to six (6) users
- Create up to five (5) Discovery Scans for predetermined subnets
- Create up to five (5) Basic Network Scans with Policies and Credentials
- Create up to two (2) CIS Compliance Scans based upon pre-existing benchmarks
- Create up to eight (8) Dashboards from templates
- Use and creation of up to eight (8) Dashboard components, including a Matrix
- Up to eight (8) Reports - using templates and basic custom creation
- Use and creation of Report elements, including the Iterator
- Create up to twelve (12) Asset lists - basic custom creation of dynamic or static IP or combination
- Up to two (2) OOTB integrations from the following list: https://static.tenable.com/ps/DS_VM-SC_QS_Intgrtns.pdf
  - **Note:** Splunk and ServiceNow connectors are out of scope for a Tenable One Core Deployment.
- Create up to eight (8) Queries
- Up to two (2) custom Assurance Report Cards (ARCs) - basic custom creation and creation using templates
- Create up to eight (8) Alerts
- Create up to two (2) Queries in Vulnerability Intelligence
- Freeze Windows - basic understanding and operation
- Accept/Recast risk - basic understanding and operation

Activity 4: Tenable Attack Surface Management Implementation

A Tenable Consultant will lead a Tenable Attack Surface Management workshop, focusing on inventory creation, configuration, and optimization. Key activities include:

- Inventory Creation and Configuration
  - Adding domains, subdomains, hostnames, IP addresses, Autonomous System Number (ASN), exclusion and automation rules.
  - Reviewing the Tenable Attack Surface Management Suggested Domains feature for asset verification.
- Platform Configuration
  - Optimizing the Tenable Attack Surface Management console to display relevant data types.
  - Using filters and metadata to analyze the attack surface.
  - Configuring asset tags for efficient management.
- Optimization and Monitoring
  - Assisting with up to three (3) subscriptions, including custom libraries and state-change notifications.
  - Setting risk prioritization, third-party integrations (email alerts), Tenable integration (to Tenable Vulnerability Management and Tenable Web App Scanning) and fine-tuning for potential vulnerabilities like expired certificates, Log4j, open ports/services, and exposed infrastructure.

Activity 5: Tenable Web App Scanning Implementation

Session 1: Initialization and Scanning

During a one-day session, a Tenable Consultant will ensure appropriate users can access Tenable Web App Scanning for scanning and result analysis. Role-Based Access Control (RBAC) will be configured, requiring administrative credentials. Key activities include:

- Reviewing security objectives from the Planning Workshop
- Install and configure up to three (3) Tenable sensors:
  - Sensors include Tenable Web App Scanning scanners and Sensor Proxies.
- Configuring and deploying quick scans on up to ten (10) URLs, for triaging new web applications
- Reviewing quick scan results and sitemap crawled data to refine scanning strategies
- Selecting three (3) URLs for in-depth scanning in Session 3 using sitemap analysis
- Creating and deploying optimized vulnerability scans for the selected URLs

Sessions 2 and 3: Tuning and Optimization

Over two half-day dedicated sessions, a Tenable Consultant will fine-tune the three (3) selected web applications (URLs), ensuring an optimized Tenable Web App Scanning configuration. Key activities include:

- Creating and deploying optimized vulnerability scans for detailed assessments
- Applying authentication methods and tuning scan configurations per Tenable best practices

- Guiding the customer in optimizing scans for efficiency and coverage
- Guiding the customer in using other scanning templates (e.g., Application Programming Interface [API] scan), if applicable
- Reviewing scan results and making further optimizations as needed

This structured onboarding approach ensures effective Tenable Vulnerability Management, improved attack surface visibility, and an optimized web application security strategy.

Activity 6: Tenable Cloud Security Implementation

Delivered over two dedicated sessions, the Tenable Cloud Security Implementation Service is a remote, structured engagement designed to enhance cloud security posture by identifying and remediating misconfigurations across the development lifecycle. This includes code scanning before commits, Source Control Management (SCM) scanning, risk detection in the CI/CD pipeline, and runtime risk assessment.

Session 1: Onboarding

Key Activities:

- Onboard a combination of up to four (4) public cloud providers from the following list (requires login): https://docs.ermetic.com/docs/cloud-onboarding
- Configure the required Identity Providers (IdPs) for a complete inventory of federated users and groups associated with your cloud accounts from the following list (requires login): https://docs.ermetic.com/docs/identity-providers
- Configuring IaC scanning for up to three (3) supported repositories from the following list (requires login): https://docs.ermetic.com/docs/connect-your-code-repository
- Configuring Tenable Cloud Security with one (1) supported Customer CI/CD pipeline from the following list (requires login): https://docs.ermetic.com/docs/connect-your-cicd-pipeline
- Connect up to two (2) Kubernetes clusters from the following list: https://docs.ermetic.com/docs/kubernetes
- Connect up to one (1) third-party container registry from the following list: https://docs.ermetic.com/docs/container-image-registry-scanning
- Integrate Tenable Cloud Security for use with up to three (3) supported third-party integrations from the following list (requires login): https://docs.ermetic.com/docs/integrations-and-automations

Session 2: Configuration, Tuning and Optimization

Consultant will provide overview of data 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 includes the following:

- Asset Inventory
  - Review asset inventory and discuss common inventory use cases
  - Demonstrate the generation of least privilege policies and roles
  - Visualize permission mapping

- Findings
  - Review Findings and discuss sample end-to-end Findings workflow.
  - Discuss prioritization of Findings.
  - Manage Findings using actions such as ignore, remediate, close and reopen.
- IAM Governance
  - Permissions Query - Perform flexible and granular queries across all identities to quickly surface problems of interest.
  - Identity Intelligence - View a breakdown of identities by severity level to map identities and their associated permissions to potential risks in your environment.
  - Excessive Permissions - View a breakdown of identities that have been assigned more permissions than what they need, to help minimize the risk that such identities pose to your organization.
- Data Protection
  - Review discovered sensitive data and data types, which are grouped into different categories such as Personally Identifiable Information (PII), Protected Health Information (PHI) and Digital Identity identifiers. This helps both to understand the data's sensitivity level and context, as well as to help ensure compliance with industry standards.
- Workload Protection
  - Analyze findings from diverse workloads: virtual machines, containers, Kubernetes, and CI/CD pipelines.
- Kubernetes
  - Examine Kubernetes cluster configuration, admission controller policies findings, and admission controller logs.
- IaC Security
  - Review IaC findings and trace findings back to code.
  - Analyze IaC scan results for misconfigurations, understanding their impact.
- Policies
  - Review the use and configuration of default policies.
  - Demonstrate the creation of up to three (3) custom policies.
- Compliance
  - Explain Tenable Cloud Security policy map to compliance controls and required configurations.
  - Generate reports for stakeholders on compliance, audits, and security.
  - Create up to three (3) custom standards to monitor policies aligned with organizational goals.
- Reports
  - Generate reports of findings by exporting filtered data.

  - Export inventory data for specific resource types in CSV format.
  - Export compliance data for specific standards in CSV format, supplementing PDF reports.
- Just-In-Time (JIT) Access
  - Manage eligibility that define the parameters of valid access requests.
  - Review access requests, and either approve or deny them.
  - View audit trail information about JIT-related activity, including access requests, eligibility changes, and the activities users performed with JIT permissions.

Activity 7: Tenable Identity Exposure Implementation

Delivered over two dedicated sessions, this service accelerates the configuration and integration of AD security monitoring to enhance threat detection and response.

Session 1: Deployment and Configuration

A Tenable Consultant will:

- Deploy a Tenable Identity Exposure Software-as-a-Service (SaaS) instance and configure Secure Relay and VPN (if applicable).
- Configure up to two (2) Active Directory domains for monitoring.
- Deploy one (1) IoA GPO (if applicable).
- Enable Tenable One integration.

Session 2: Security Monitoring and Optimization

The consultant will then configure and demonstrate Tenable Identity Exposure's monitoring capabilities, including:

- Creating one (1) new security profile and deploying three (3) pre-configured dashboards.
- Deploy up to three (3) pre-configured dashboards.
- Demonstrate how to perform Trail Flow searches.
- Review, analyze and customize Indicator of Exposure (IoE) behavior (prioritizing Critical and High severity).
- Review and analyze IoAs (if applicable).
- Create one (1) new role (If applicable).
- Create up to two (2) SMTP Alerts (if applicable).
- Create up to two (2) Syslog Alerts (if applicable).
- Configure one (1) SMTP connection (if applicable).
- Provide Dashboard and Security Profile tool demonstrations (if applicable).
- Implement and demonstrate one (1) pre-configured dashboard in Microsoft Power BI (if applicable).
- Demonstrating ID360 (if applicable).

This structured onboarding ensures proactive identity security, risk assessment, and optimized AD monitoring, helping organizations strengthen their exposure management strategy.

Activity 8: Tenable Exposure Management Third-Party Connectors

The Tenable Consultant will configure third-party connectors over a session lasting up to four (4) hours.

- Adding up to four (4) third-party connectors from the following list: https://docs.tenable.com/exposure-management/Content/connectors/connectors-and-supported-integrations.htm
- Validating data ingestion from connector(s) into Tenable Exposure Management.

Activity 9: Tenable One Implementation Deliverable

Following the implementation activities, the Tenable Consultant will independently create the Tenable One Implementation Deliverable based on a Tenable template, documenting the Tenable One solution documentation, future recommendations, and links to appropriate documentation.

Activity 10: Tenable One Architect Calls

At the beginning of the implementation phase, the Tenable Security Architect will schedule up to two (2) status calls with the client's project team stakeholders. These calls will review progress, provide guidance, and ensure the implementation remains on track, facilitating a seamless onboarding experience and a smooth transition to the Enablement phase.

Phase Closure

The Tenable Consultant will formally confirm the completion of the Implementation Phase (Phase 2), ensuring that all agreed-upon deliverables and objectives have been met.

PHASE 3: ENABLEMENT

The Tenable One Platform Enablement service will equip your teams with the knowledge and skills to use the Tenable One Exposure Management Platform effectively. It will provide visibility across the modern attack surface and enable clear communication of cyber risk to support business objectives.

Activity 1: Enablement Preparation Call

A one-hour remote session with a Tenable Consultant to:

- Review the deployed Tenable One Platform components and tailor priorities for enablement
- Validate the deployed Tenable One Platform components and tailor priorities for enablement
- Identify key internal stakeholders for the Enablement Session

Activity 2: Tenable One Platform Enablement Session

Across one (1) day, a Tenable Consultant will lead an interactive session, during which they will:

- Review Tenable One scoring
  - Cyber Exposure Score (CES)
  - Asset Exposure Score (AES)
  - Vulnerability Priority Rating (VPR)
- Review Tenable One third-party connector data ingestion
- Review and discuss built-in global and category Exposure View cards and create up to two (2) custom Exposure Cards
- Review built-in Exposure Signals and create one (1) custom Exposure Signals
- Discuss the advantages of the Tenable One Inventory and Tagging. Provide an overview of Inventory and create up to two (2) Tenable One tags.
- Discuss the advantages of Attack Path Analysis. Provide an overview of Attack Paths, Attack Techniques and the ATT&CK Heatmap.
- Create up to two (2) custom dashboards

Activity 3: Tenable One Platform Enablement Deliverable

Following the session, the Tenable Consultant will independently create and provide a detailed documentation deliverable based on a Tenable template covering the following:

- Tenable One solution details: Tenable One Scoring, Exposure Signals, Inventory (Assets, Weaknesses, Findings and Software), Analytics (Exposure View and Dashboards), Attack Path Analysis, Tagging and Connectors.

This enablement ensures your team can optimize security posture, analyze exposure risk, and take informed action within the Tenable One Platform.

Phase Closure

The Tenable Consultant will formally confirm the completion of the Enablement Phase (Phase 3), ensuring that all agreed-upon deliverables and objectives have been met.

PHASE 4: OPTIMIZATION

In the final phase, Tenable ensures your Exposure Management solution is fine-tuned for peak efficiency and aligned with evolving security needs.

Activity 1: Optimization Solution Review, Best Practices and Recommendations

The Tenable One Optimization Workshop is designed to maximize the value of your Exposure Management solution, ensuring efficiency, accuracy, and resilience in an evolving cybersecurity landscape.

Tenable will conduct up to one (1) workshop spanning two (2) consecutive days with up to eight (8) hours of consultation. The session will be with a Tenable Consultant who will lead a preparation call to tailor the agenda based on your Tenable One Platform requirements, ensuring optimal use of Tenable's expertise.

Key Focus Areas:

- Continuous performance validation and improvement
  - Assess applied optimizations to confirm operational improvements. Fine-tune configurations based on real-world security events and business objectives.
  - Provide long-term recommendations to sustain and enhance security resilience
  - Offer guidance on continuous improvement and optimization of Tenable One

Deliverable Documentation

After each Optimization Solution Review, Tenable will provide a detailed deliverable based on a Tenable template including:

- Tenable One solution documentation
- Future recommendations and links to relevant resources

This structured approach ensures organizations successfully deploy, adopt, and optimize the Tenable One Exposure Management Platform, strengthening security posture and risk management capabilities.

Phase Closure

The Tenable Consultant will formally confirm the Optimization Phase (Phase 4) completion, ensuring that all agreed-upon deliverables and objectives have been met.

ONGOING: PROJECT COORDINATION

To support the adoption of Tenable One, Tenable will collaborate closely with the designated consultant(s) from the Tenable delivery team. This role is instrumental in orchestrating all project-related activities—ensuring seamless scheduling, coordination, and communication—while aligning closely with your organization's assigned Project Manager (PM).

While your internal Project Manager retains responsibility for customer-side tasks and activities, the Tenable Project Coordination team will act as a strategic partner, facilitating engagement and alignment between your team and Tenable's delivery consultants to drive a smooth implementation.

Roles and Responsibilities of the Tenable Project Coordinator

1. Project Initiation
   - Collaborate with the customer's Project Manager to formally initiate the project
   - Deliver and review a detailed Tenable One Implementation Activity List
   - Introduce Tenable's delivery approach and scheduling plan
   - Assist in defining a preliminary project timeline, including major phases and milestones

2. Communication Management
    - Serve as the primary point of contact for all Tenable-side project communications
    - Maintain clear and consistent communication between all stakeholders throughout the project lifecycle
3. Project Activity Scheduling and Coordination
    - Lead the coordination and scheduling of all Tenable-related project tasks and sessions
    - Facilitate collaboration between Tenable consultants and customer stakeholders
    - Issue calendar invitations and share key documentation to ensure alignment and transparency
4. Monitoring and Control
    - Provide project updates summarizing progress, upcoming tasks, risks, and mitigation plans
    - Track ongoing activities to ensure adherence to the project plan and objectives
5. Scope and Change Management
    - Work closely with the delivery team to manage scope and ensure on-time, high-quality outcomes
    - If scope adjustments are needed, engage Tenable's Services Account Manager to initiate a formal change request process, securing documented agreement from the customer's Project Manager

4. ASSUMPTIONS AND CONSTRAINTS

Tenable has relied upon the following assumptions and constraints in performing the Professional Services in this SOW. If Customer or Reseller fails to comply with any of the following assumptions, constraints or responsibilities, Tenable reserves the right to modify the price, scope, level of effort, or schedule for the Professional Services in this SOW.

In the event Customer fails to meet the requirements under this **Assumptions and Constraints** section, resulting in a material delay preventing Tenable personnel from performing the Professional Services in the **Scope** section in accordance with any agreed Milestones, Tenable reserves the right to charge Customer for any additional costs, including travel and expenses, incurred.

a) Customer has valid licenses for all Tenable Products necessary to complete the Professional Services in the **Scope** section.

b) Customer and Tenable will each identify a designated account contact in advance of the Professional Services commencing.

c) Tenable may perform services either remotely or on-site at a mutually agreed upon Customer location.

d) For onsite engagements, estimated travel and expenses shall be included as a separate line item on the Quote and Purchase Order.

e) This SOW represents Tenable's commercially reasonable technical judgment based upon information made available by Customer or Reseller. Reseller acknowledges that any failure to provide accurate information in respect to Customer's environment may require Tenable to issue a change control notice.

f) If during the performance of this SOW Customer or Reseller requests a change to the **Scope** section, this will be documented using the change control notice process defined herein.

g) Customer or Reseller will provide Tenable access to key individuals, information and system resources at Customer site required for Tenable to provide the required deliverables set out in this SOW.

h) When at Customer's or Reseller's facility, Customer or Reseller will provide the 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 Professional Services.

i) Customer or Reseller shall provide the Consultant with reasonable and safe access to Customer's facilities and ensure that its facilities constitute a safe working environment.

j) The Customer's systems must meet or exceed the specifications found in the Tenable General Requirements document, available at https://docs.tenable.com/generalrequirements/.

k) All workdays under this SOW are based upon an eight (8) hour workday and all work will be completed during normal working hours defined by local custom.

l) Tenable personnel will not be exposed to physically hazardous environments without prior risk assessment and agreement by Tenable. Customer or Reseller will provide any safety equipment needed. If applicable, Customer or Reseller personnel will mount hardware and conduct configuration in appropriate locations where necessary.

m) Tenable is not responsible for any impact caused by querying, network communication or system interaction within Customer's environment. Customer understands that assessing Customer's network or infrastructure is a complex procedure, and Tenable does not guarantee that the results of the Professional Services will be error-free. Customer acknowledges that the Professional Services may result in loss of service or have other impacts to networks, infrastructure, assets or computers. Customer agrees not to pursue any claims against Tenable as a result of any Professional Services unless such a claim is based on the gross negligence or willful misconduct of Tenable.

n) Other than the work defined in the **Scope** section, ongoing support and maintenance of Tenable deliverables or scripts beyond the warranty period detailed in the Agreement is not within the scope of this SOW.

o) Additional maintenance of Tenable deliverables or scripts delivered under this SOW shall be contracted under a new Statement of Work through a change control notice.

5. ABOUT TENABLE

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. Learn more at tenable.com.

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com