tenable™
ProServe Optimize

Optimize Services Package

SERVICES OVERVIEW

Designed for enterprise organizations that are committed to developing a risk-based vulnerability management (RBVM) program, an Optimize Services Package from Tenable® delivers a comprehensive custom deployment of our Tenable.sc™ on-premises solution or Tenable.io® cloud-based solution for new deployments of up to 100,000 assets. We will enable you to discover and assess assets across your attack surface, prioritize the greatest risks to your organization, remediate vulnerabilities using integrated workflows and measure the success of your RBVM program to reduce your overall Cyber Exposure.

A Tenable Certified Security Consultant, or one of our qualified partners, will collaborate with your vulnerability management team to install, deploy, configure and validate your Tenable solution, following our industry-leading best practices to address your unique challenges and align with your objectives.

This service can be performed remotely or on site, and includes a Cyber Exposure Workshop, a Quick Start Optimize service, three training vouchers for the instructor-led virtual course applicable to your product, and a Health Check service.

SERVICES OUTCOME

- Comprehensive Risk-based Vulnerability Management solution, installed, deployed, configured and validated following Tenable's industry-leading best practices
- Cyber Exposure Workshop to plan, design and give guidance on adopting the Cyber Exposure Lifecycle and RBVM practices
- Design and Architecture Workshop providing documented Architectural Design to suit your environment
- Three student training vouchers for applicable instructor-led virtual training course
- Follow-up evaluation of the continued resilience and effectiveness of your RBVM capability
- Confidence in asset visibility and discovery with comprehensive data to report risk at organizational level

WORKING TOGETHER

In an Optimize Services Package from Tenable, you collaborate with a Tenable Certified Security Consultant or one of our qualified partners.

The service begins with a Cyber Exposure Workshop to analyze and identify steps to plan, design and guide you towards adopting the Cyber Exposure Lifecycle and our Role Based Vulnerability Management (RBVM) practices.

Our Tenable Design and Architecture workshop will evaluate visibility gaps and process improvements to plan a strategic vulnerability scanning approach. We will work with you to develop and deploy a solution that ensures all assets are visible to, and covered by, your vulnerability management program.

The session includes an in-depth dedicated enablement session focused on our industry leading RBVM practices to drive adoption of Cyber Exposure principles.

Services are typically delivered across eighteen days and can be performed remotely, on site or a combination of both for your convenience. Tenable's dedicated Project Coordination team will align activities to ensure smooth delivery and maximum benefit.

Upon completion, you will receive key documentation to assist you in maintaining your deployment and reducing your Cyber Exposure gap as new threats emerge. The instructor-led training courses with a hands-on lab environment will be available to schedule at your convenience.

SERVICE PACKAGE INCLUDES:

1. Cyber Exposure Workshop
2. Tenable.sc or Tenable.io Quick Start Optimize
3. Tenable.sc or Tenable.io Instructor-Led Training Course
4. Health Check

For more information, visit www.tenable.com/services

STEPS OF TENABLE OPTIMIZE PACKAGE

Phase 1: Tenable Cyber Exposure Workshop, Design & Planning Workshop & Readiness

Cyber Exposure Workshop	This workshop will assess the current Vulnerability Management program providing an executive report summarizing findings and recommendations.
Design and Architecture Workshop	This workshop will pre-plan, review and agree on Tenable's approach and the organization's prerequisites to ensure readiness for a smooth installation phase.
Installation Readiness Exercise	Tenable will review and validate the solution design, prerequisites and specifications before work begins.

Phase 2: Tenable Implementation, Configuration and RBVM Enablement

Install and Configure Tenable	Tenable.sc or Tenable.io and Nessus® will be installed and configured to business requirements and implemented following Tenable's best practices for enterprise deployment.
Validate Operational Capabilities	Tenable solution will validated end-to-end for scanning and other operational capabilities.
Enablement	This enablement session will guide you through Tenable's best practices for Vulnerability Management.

Phase 3: Documentation and Project Coordination

Tenable Deliverable Documentation	Documentation of your specific Tenable product configuration provided for future use, to include a Cyber Exposure Workshop Executive Report, High Level Design Document and Customer Solution documentation.
Project Coordination	Tenable will provide ongoing project coordination and updates throughout delivery.

Phase 4: Education

Instructor-Led Training	Live virtual classroom session with Tenable experts to enable users with best practices and up-to-date product knowledge.

Phase 5: Solution Maturity

Health Check	Experienced Tenable Consultants will provide guidance and direction in evaluating and ensuring the continued resilience and effectiveness of your Vulnerability Management capability.