Professional Services for Security Posture Assessment

At a glance

Security assessment focused on evaluating over 140 technical security configurations for VMware vCenter Server and ESXi host infrastructure for the small and medium enterprise. The service provides a detailed findings report, actionable recommendations, and a roadmap to help prioritize remediation activities.

Key benefits

- Gain valuable insights into how security controls are implemented in your datacenter
- Aligned to NIST 800-52
- Identify gaps in current VMware vCenter and VMware ESXi configurations to VMware and industry best practices
- Prioritized roadmap and actionable recommendations to remediate gaps and achieve target state

SKU

Available in AMER only

PS-SEC-TECH-ASSMT-SM
VMware Small Scale Security Posture Assessment

PS-SEC-TECH-ASSMT-MID
VMware Mid Scale Security Posture Assessment

Service overview

VMware Professional Services security experts will perform a detailed security assessment for small and medium enterprise customers focused on evaluating Customers vCenter Server and ESXi environment to VMware and industry security best practices. The service utilizes a combination of workshops and technical configuration reviews to analyze the current state environment to desired target state. The service delivers a detailed findings report to provide the Customer with the assessment findings, actionable recommendations to achieve the target state, and a roadmap to help prioritize remediation activities

Project scope

This service is packaged for Customers with a small to medium sized VMware vSphere environment based on the following environment sizes:

- Small Environment
  - Up to two (2) vCenter Servers
  - Up to one hundred (100) ESXi Hosts
- Medium Environment
  - Up to four (4) vCenter Servers
  - Up to two hundred (200) ESXi Hosts

In-Scope VMware Technology

The service checks 141 individual technical configurations across the following VMware datacenter technologies:

- VMware vCenter: 81 configurations
- VMware ESXi Hosts: 60 configurations

Each of the configurations in the service are mapped to NIST 800-52 to assist the Customer in aligning technical configurations to industry standard security frameworks.

Four-Phased Approach

The service is delivered leveraging a four phased approach. During the Due Diligence phase VMware security consultants and Project Manager will work

with the Customer to identify a Single Point of Contact (SPOC) to ensure efficient communication between the Customer and VMware during the engagement. During this phase VMware will work with the Customer SPOC to identify key stakeholders and schedule the kickoff meeting.

In phase 2, Start-up and Planning, VMware will hold the project kickoff meeting, finalize the project schedule, document handling and access requirements, as well as identify Customer interviewees, contacts, and schedule technical workshops.

The Workshops and Reviews phase begins with the security consultant conducting the Security Strategy Workshop which is designed to review and align the Customer's security goals and objectives with the assessment. Next the security consultant will conduct an Access Validation Workshop to ensure the consultant has all required access and permissions to perform technical reviews. Once these workshops are completed the security consultant will work with Customer subject matter experts to review the current state environment. This is done via a series of technical workshops (up to four, four-hour workshops) and technical implementation reviews leveraging scripts and manual configuration reviews.

During the final phase, Document Findings and Recommendations, the security consultant will perform the gap analysis of the current state environment to the target state. A draft findings report will be provided to key Customer stakeholders for review and input. Once Customer feedback is received, the security consultant will conduct a findings presentation for Customer key stakeholders. The findings presentation will provide an overview of the engagement, technical findings, and prioritized recommendations/next steps.

Deliverables

At the conclusion of the security assessment, the Customer will be provided with the following deliverables:

- Detailed Findings Report: Highlights all findings and recommendations for in-scope products and evaluation criteria and is aligned to technical best practices
- Scan Result Workbook: Supplemental Excel Workbook documents all product findings and aids in remediation of settings identified in the Detailed Findings Report
- Findings Presentation: Consolidated presentation of prioritized recommendations that provides the customer with an executive-level overview of current state in relation to target state and highlights key gaps and recommendations as well as provides a prioritized roadmap to achieve target state

Engagement Timeline

The duration of the service is dependent on the SKU selected and is based on the size of the environment.

- Small Environment: 3 to 4 weeks
- Medium Environment: 4 to 6 weeks

The duration is also dependent on Customer availability as well as the time to ensure the security consultant has proper access to the environment.

Customer Requirements

This service is delivered utilizing an iterative model that requires the security consultant to work closely with Customer resources in order to properly assess the customers environment. It is expected that the Customer will participate in the following project activities:

- Kickoff Meeting – up to 2 hours
- Security Strategy Workshop – up to 4 hours
- Access Validation Workshop – up to 2 hours
- Technical Workshop(s) – up to 16 hours
- Draft findings report review – up to 4 hours
- Findings presentation – up to 2 hours

The activities outlined above may require multiple Customer stakeholders be in attendance. Based on the project, VMware recommends the following Customer stakeholders be available to support project activities (Note: this is not an exhaustive list and other stakeholders may be required based on Customer environment and operations):

- Security policy team leads
- Infrastructure architect
- Security technology team leads
- VMware operations team leads
- Security manager
- Infrastructure manager
- IT security manager
- Enterprise architect

Engagement Requirements

To perform the technical configuration reviews, the VMware security consultant has the following access requirements:

- Read-only access to all in-scope products and systems
- SSH and Root Access
- Ability to run PowerShell plus PowerCLI from a Linux machine

Completion Criteria

The project is deemed complete upon ONE of the following criteria – whichever comes first:

1. Completion of all service deliverables in the Deliverables section
2. After 12 months from purchase date
3. If the services were purchased using PSO credits, the services expire at the same time the credits expire unless a credit extension is requested and granted. Work with your Account Executive to determine a plan for all remaining credits on the account and to request an extension.

Out of Scope

1. A certified compliance outcome. VMware provides general guidance to the controls that are applicable to VMware Solutions and not general environmental configuration. Organizations should engage appropriate legal, business, technical, and audit knowledge within their specific organization for review of regulatory compliance requirements.
2. Evaluation of user access controls such as separation of duties, and least privilege with identity access management (LDAP/AD). These configurations are specific to the environment and not VMware products and technologies. This service assumes the required user access controls have been previously implemented.
3. Operational transformation of the organization. This service focuses on the technical implementation of security controls for the environment, not changes to people and process that may be required for full regulatory compliance.
4. Remediation activities are out of scope.

Service Assumptions

Customer Resources: Should the Customer request VMware to perform tasks that are dependent upon Customer resources or decisions, the Customer will make the required resources available or decisions final in a timely manner.

Hardware Procurement: Procurement and installation of hardware (if any) is the responsibility of the Customer. VMware will provide recommendations and assistance.

Learn more

Visit vmware.com/services.

Working Hours: VMware resources will only be actively available during Americas business hours (9 am to 5 pm EST) and for the time blocks decided upon between the customer and VMware.

Engagement Requirements: Items outlined in the Engagement Requirements section above must be provided before technical configuration reviews can be performed. If these requirements cannot be met, a change request may be required.

Project Management: VMware and the Customer's project management will work closely together to ensure that project scope remains consistent and to avoid any scope creep.

Deliverable Language: The event, challenge, documentation, and work product(s) will be delivered in English.

This service must be delivered and accepted within the first 12 months of purchase, or the service will be forfeited. Pricing for this service excludes travel and other expenses. For detailed pricing, contact your local VMware representative.