VMware vSphere Security Configuration Posture Assessment

The Heart of the Matter

Your virtual infrastructure is the heart of your data center — and attackers know it. Misconfigured ESXi hosts, overly permissive access roles, and underutilized security features create silent exposure that can persist for years. HUME-IT's VMware vSphere Security Configuration Posture Assessment (VM-SCPA) uncovers these vulnerabilities and provides focused recommendations to secure your vSphere environment from the inside out.

This targeted security assessment focuses on core elements such as host configurations, vCenter access controls, network policies, and VM protection settings. It helps your organization leverage its existing platform investments to create a stronger, more defensible virtualization layer.

Assessment Focus & Methodology

HUME-IT's evaluation model for vSphere environments has been developed through extensive hands-on experience across enterprise and regulated environments. Our assessment includes alignment with platform-specific best practices, security hardening guides, and compliance-relevant controls. We analyze host and management plane configurations using both tooling and manual validation, and deliver clear, risk-prioritized reporting with actionable steps. Our approach ensures findings are accurate, license-aware, and realistically scoped for remediation.

Key Benefits

- Identifies misconfigurations that enable lateral movement or privilege escalation
- Assesses host and vCenter access controls against security best practices
- Reviews VM templates, isolation settings, and encrypted configuration
- Supports SIEM integration and audit logging for infrastructure visibility
- Provides remediation guidance tailored to your license level and deployment model

What We Evaluate

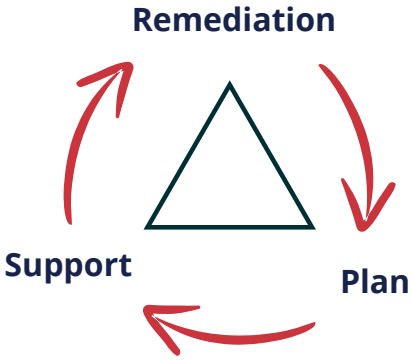
- Host-level configuration (including Secure Boot, lockdown mode, and SSH),
- vCenter role and permission design,
- nNetwork policy enforcement,
- Audit logging,
- VM template security, and
- VMX configuration settings.

We evaluate how vSphere features are deployed and where additional security value can be realized based on current entitlements.

Contact Us

info@humeit.com

www.humeit.com



Remediation Support and Validation

After an assessment, HUME-IT can support you with targeted remediation guidance, hands-on help where needed, and validation that changes were implemented securely.

Fortifying Modern Platforms with Human Understanding

Offering more than just assessments; we deliver expert insight into your platform's security posture. Our services are designed to uncover real risks, guide secure implementation, and validate remediation efforts through a flexible, research-driven model.

Our Process

At HUME-IT, our engagement process is structured, collaborative, and designed to minimize disruption while maximizing value.

Discover **Analyze** **Report** **Review**

We are dedicated to providing innovative, proactive cybersecurity solutions tailored to your organization's unique needs.

Our team of experts is ready to help secure your IT infrastructure, mitigate evolving threats, and ensure compliance with industry standards.

Get in touch with us today to learn how we can fortify your digital environment and support your ongoing security strategy.

Confidently Secure Your Environment

Schedule a VM-SCPA with HUME-IT to uncover critical risks in your vSphere deployment and begin building a stronger virtualization security posture.

Security Expertise Where it Matters Most

- Helping organizations identify vulnerabilities,
- Strengthen compliance, and
- Implement real-world security solutions for Microsoft, VMware, and cloud environments.

Why HUME-IT?

Our team has deep VMware security experience in high-scale environments — including telecom, finance, and federal data centers. We understand the challenges of securing production infrastructure while maintaining stability and performance. Our assessment is focused, evidence-based, and customized to your deployment.

Contact Us

info@humeit.com
www.humeit.com