Evaluación de Vulnerabilidades para VMware

DESCRIPCIÓN GENERAL DE LOS SERVICIOS[1]

La Evaluación de Seguridad para VMware es un servicio de evaluación de seguridad y cumplimiento de carácter consultivo, ofrecido por Park Place Technologies (PPT). El servicio utiliza una herramienta de escaneo para VMware completamente automatizada y gestionada por PPT, junto con un motor de análisis de seguridad, para llevar a cabo recolecciones de datos de configuración en modo de solo lectura y generar automáticamente informes de evaluación de seguridad. Todas las actividades de análisis, validación y recomendaciones son realizadas por expertos en seguridad de PPT.

Este servicio proporciona una evaluación integral del entorno de virtualización VMware del Cliente, incluyendo vCenter Server, hosts ESXi, clústeres, redes virtuales, máquinas virtuales y componentes de almacenamiento.

La evaluación identifica configuraciones incorrectas, brechas de seguridad y desviaciones de cumplimiento, alineadas con marcos líderes como los Benchmarks CIS, DISA STIGs, las Guías de Fortalecimiento de VMware, el Marco de Ciberseguridad de NIST y los Criterios de Servicios de Confianza SOC 2.

SERVICIOS Y ENTREGABLES

PPT realiza la identificación de vulnerabilidades específicas de VMware-, análisis de configuración y evaluación de cumplimiento ("Servicios"). Todos los servicios se realizan de forma remota.

Actividades de Evaluación

PPT utiliza un script de escaneo automatizado y administrado por PPT- para VMware, configurado en modo de lectura-únicamente, junto con un motor de análisis para:

- Recolectar metadatos de configuración de VMware sin almacenamiento de credenciales ni cambios en la configuración.
- Evaluar configuraciones frente a más de 200 controles de seguridad alineados con VMware-.
- Detectar configuraciones incorrectas, ajustes inseguros y desvíos de configuración.
- Mapear los hallazgos a múltiples marcos de cumplimiento simultáneamente.
- Identificar problemas en vCenter, hosts ESXi, clústeres, máquinas virtuales, redes, certificados, autenticación y registros.
- Validar resultados y eliminar falsos positivos identificables.

Entregables

Onboarding

- Implementación y Evaluación Inicial.
- Informe Ejecutivo que resume la puntuación de seguridad inicial, hallazgos a nivel alto, estado de cumplimiento y los siguientes pasos recomendados.

Informe Automático Recurrente

Entregado automáticamente con la periodicidad elegida por el Cliente (mensual, trimestral o semanal):

- Resultados de cumplimiento mapeados a CIS, DISA STIG, Guías de Fortalecimiento VMware, NIST CSF, SOC 2.
- Inventario de hallazgos de seguridad categorizados por gravedad.

[1] La herramienta de escaneo ("Software") es un producto propietario de Kalosys, licenciado por PPT. Todas las patentes, derechos de autor, secretos comerciales y otros derechos de propiedad intelectual permanecen exclusivamente con Kalosys y sus licenciantes. El Cliente solo adquiere derechos limitados para usar el Software, no su propiedad. El Cliente no deberá (a) copiar, modificar o crear trabajos derivados; (b) realizar ingeniería inversa, descompilar o desensamblar; (c) eliminar avisos o etiquetas de propiedad; (d) sublicenciar, alquilar, arrendar o transferir; (e) usarlo para proporcionar servicios a terceros; o (f) eludir cualquier medida de protección. El Usuario Final entiende que este Software está diseñado para evaluaciones de seguridad y acepta usarlo únicamente en sistemas que esté autorizado a analizar.

- Clasificación de vulnerabilidades, incluidos CVEs y puntuaciones de severidad CVSS.
- Guía de Remediación con acciones correctivas recomendadas.
- Plan de Acción Priorizado alineado al riesgo y al impacto operacional.
- Informes entregados en varios formatos compatibles.

Alcance Consultivo

PPT solo proporciona análisis y recomendaciones. El Cliente es completamente responsable de la implementación de todas las acciones de remediación, cambios de configuración y operaciones.

Alcance Compatible con VMware

- VMware vSphere 6.7 y posteriores
- Servicios de vCenter Server, autenticación, permisos, registros
- Fortalecimiento de hosts ESXi (servicios, firewall, certificados, NTP, políticas de contraseñas/restricción)
- Servicios de clúster (HA, DRS, EVC, vSAN)
- Configuración de vSwitch/vDS y seguridad de grupos de puertos
- Configuración de máquinas virtuales, VMware Tools, políticas de aislamiento
- Configuración de almacenes de datos y vSAN

PROCESO Y SLA

Evaluación Inicial e Implementación

- Despliegue del script de escaneo en el sistema designado por el Cliente-.
- Validación de requisitos previos de la herramienta.
- Verificación de conectividad y permisos de vCenter.
- Ejecución de la evaluación inicial de VMware.
- Configuración de la entrega automática de informes.

Informe Ejecutivo y Técnico

- Resumen de hallazgos iniciales.
- Estado de cumplimiento.
- Recomendaciones de remediación priorizadas (solo consultivas).

Evaluaciones Continuas

- Escaneos automatizados realizados con la periodicidad definida por el Cliente-.
- Detección de nuevas vulnerabilidades y regresiones.
- Monitoreo de desvíos de configuración.

Informes de Progreso

- Tendencias en la postura de seguridad de VMware.
- Detección recurrente de problemas.
- Visibilidad del progreso en la remediación.

LIMITACIONES DEL SERVICIO

Este servicio no incluye:

- Monitoreo en tiempo real, SIEM/SOC o respuesta a incidentes.-
- Investigación de brechas o análisis forense.
- Actualización, parches o operaciones del ciclo de vida de VMware.
- Ejecución de remediaciones o cambios de configuración.
- Resolución de problemas de rendimiento (computación, almacenamiento o red).
- Diseño de arquitectura, ingeniería o planificación de capacidad.
- Automatización personalizada, scripting o integraciones.

- Preparación para certificaciones de cumplimiento (ISO, PCI, SOC 2).
- Soporte de ITSM (tickets, flujos de trabajo, CAB).
- Gestión de licenciamiento o entitlements.
- Servicios de hardware o ingeniería en sitio.

RESPONSABILIDADES DEL CLIENTE

El Cliente debe:

- Asignar personal de VMware y seguridad para apoyar la colaboración.
- Proporcionar credenciales de solo lectura- y autorización para los objetivos de la evaluación.
- Asegurarse de que todos los sistemas VMware sean accesibles durante las ventanas de escaneo.
- Asumir todas las actividades de remediación y operacionales.
- Gestionar la clasificación, manejo y retención de los datos de la evaluación.
- Reconocer una carga temporal de recursos durante la evaluación.
- Mantener la gobernanza y el control de cambios para todas las configuraciones de VMware.

HERRAMIENTA DE ESCANEO: SEGURIDAD, PROTECCIÓN DE DATOS Y ALCANCE DE RECOLECCIÓN

PPT garantiza una operación segura y controlada de la herramienta de escaneo. Los elementos clave incluyen:

- Recolección de datos en modo de solo lectura-, no invasiva-.
- Sin instalación de agentes; no se realizan cambios en la configuración.
- Las credenciales se utilizan solo durante la sesión activa y nunca se almacenan.
- Solo se recolectan metadatos de configuración de VMware (vCenter, ESXi, clúster, almacenamiento, redes, autenticación, certificados, registros, NTP y detalles de licencias enmascarados).
- No se recolecta contenido del sistema operativo invitado de las máquinas virtuales, datos de aplicaciones, datos de usuario, contraseñas ni claves de licencia completas.
- Toda la comunicación está cifrada mediante HTTPS (443).
- Los artefactos de la evaluación están cifrados tanto en tránsito como en reposo.
- El acceso está restringido al personal autorizado de PPT y del Cliente.