Valutazione delle Vulnerabilità per VMware

DESCRIZIONE GENERALE DEI SERVIZI[1]

La Valutazione di Sicurezza VMware è un servizio di valutazione della sicurezza e della conformità di tipo consulenziale fornito da Park Place Technologies (PPT). Il servizio utilizza uno strumento di scansione VMware completamente automatizzato e gestito da PPT, insieme a un motore di analisi della sicurezza, per eseguire la raccolta dati di configurazione in modalità sola lettura e per generare e consegnare automaticamente report di valutazione della sicurezza. Tutte le attività di analisi, validazione e raccomandazione vengono effettuate da esperti di sicurezza di PPT.

Questo servizio fornisce una valutazione completa dell'ambiente di virtualizzazione VMware del Cliente, inclusi vCenter Server, host ESXi, cluster, rete virtuale, macchine virtuali e componenti di archiviazione.

L'analisi identifica configurazioni errate, lacune di sicurezza e deviazioni di conformità allineate a framework di riferimento come CIS Benchmarks, DISA STIGs, VMware Hardening Guidelines, NIST Cybersecurity Framework e SOC 2 Trust Services Criteria.

SERVIZI E CONSEGNE

PPT esegue identificazione delle vulnerabilità specifiche di VMware-, analisi delle configurazioni e valutazione della conformità ("Servizi"). Tutti i servizi vengono forniti da remoto.

Attività di Valutazione

PPT utilizza uno script di scansione VMware automatizzato in modalità sola lettura gestito da PPT- e un motore di analisi per:

- Raccogliere metadati di configurazione VMware senza usare credenziali archiviate e senza modifiche alla configurazione.
- Valutare le configurazioni rispetto a oltre 200 controlli di sicurezza allineati a VMware-.
- Rilevare configurazioni errate, impostazioni non sicure e deviazioni delle configurazioni.
- Mappare i risultati a più framework di conformità contemporaneamente.
- Identificare problemi in vCenter, host ESXi, cluster, macchine virtuali, reti, certificati, autenticazione e registrazione.
- Validare i risultati e rimuovere eventuali falsi positivi identificabili.

Consegne

Onboarding

- Implementazione e Valutazione Iniziale.
- Briefing Esecutivo che riassume il punteggio di sicurezza di base, le principali-conclusioni, lo stato di conformità e i passi successivi consigliati.

[1] Lo strumento di scansione ("Software") è un prodotto proprietario di Kalosys, concesso in licenza da PPT. Tutti i brevetti, diritti d'autore, segreti commerciali e altri diritti di proprietà intellettuale rimangono esclusivamente di proprietà di Kalosys e dei suoi licenziatari. Il Cliente acquisisce solo diritti limitati per utilizzare il Software, senza acquisirne la proprietà. Il Cliente non deve: (a) copiare, modificare o creare opere derivate; (b) effettuare reverse engineering, decompilare o disassemblare; (c) rimuovere avvisi o etichette di proprietà; (d) concedere sublicenze, affittare, noleggiare o trasferire; (e) utilizzare per fornire servizi a terzi; o (f) aggirare eventuali misure di protezione. L'Utente Finale comprende che questo Software è progettato per valutazioni di sicurezza e accetta di utilizzarlo esclusivamente su sistemi per i quali è autorizzato a effettuare test.

Report Automatizzati Ricorrenti

Consegna automatica con la frequenza scelta dal Cliente (mensile, trimestrale o settimanale):

- Risultati di conformità mappati a CIS, DISA STIG, VMware Hardening Guides, NIST CSF, SOC 2.
- Inventario delle vulnerabilità categorizzato per gravità.
- Classificazione delle vulnerabilità, inclusi CVE e punteggi di gravità CVSS.
- Guida alla correzione con azioni correttive consigliate.
- Piano di azione prioritizzato in base al rischio e all'impatto operativo.
- Report consegnati in vari formati supportati.

Ambito del Consulente

PPT fornisce solo analisi e raccomandazioni. Il Cliente è pienamente responsabile dell'implementazione delle correzioni, delle modifiche alla configurazione e delle azioni operative.

Ambito VMware Supportato

- VMware vSphere 6.7 e successivi
- Servizi vCenter Server, autenticazione, permessi, registrazione
- Rinforzo della sicurezza per host ESXi (servizi, firewall, certificati, NTP, politiche di password/blocco)
- Servizi per cluster (HA, DRS, EVC, vSAN)
- Configurazioni vSwitch/vDS e sicurezza dei gruppi di porte
- Impostazioni di configurazione delle macchine virtuali, VMware Tools, politiche di isolamento
- Configurazione dei datastore e vSAN

PROCESSO E SLA

Valutazione Iniziale e Implementazione

- Distribuzione dello script di scansione nel sistema-designato dal Cliente.
- Convalida dei prerequisiti dello strumento.
- Verifica della connettività e delle autorizzazioni di vCenter.
- Esecuzione della valutazione VMware di base.
- Configurazione della consegna automatica dei report.

Briefing Esecutivo e Tecnico

- Panoramica sui risultati di base.
- Sintesi dello stato di conformità.
- Raccomandazioni per la correzione prioritarie (solo consulenziali).

Valutazioni Continuative

- Scansioni automatizzate eseguite con la frequenza definita dal Cliente-.
- Rilevamento di nuove vulnerabilità e regressioni.
- Monitoraggio delle deviazioni di configurazione.

Report sullo Stato di Avanzamento

- Tendenze nel livello di sicurezza di VMware.
- Rilevamento ricorrente delle problematiche.
- Visibilità sui progressi delle attività di correzione.

LIMITAZIONI DEL SERVIZIO

Questo servizio non include:

- Monitoraggio in tempo reale, SIEM/SOC o risposta agli incidenti.-
- Indagini su violazioni o analisi forense.
- Applicazione di patch, aggiornamenti o operazioni di ciclo di vita VMware.
- Esecuzione di correzioni o modifiche alla configurazione.
- Risoluzione di problemi di prestazioni (computazione, archiviazione o rete).
- Progettazione dell'architettura, ingegneria o pianificazione della capacità.
- Automazione personalizzata, scripting o integrazioni.
- Preparazione per certificazioni di conformità (ISO, PCI, SOC 2).
- Supporto ITSM (ticket, workflow, CAB).
- Gestione delle licenze o approvvigionamento dei diritti d'uso.
- Servizi di ingegneria o hardware in loco.

RESPONSABILITÀ DEL CLIENTE

Il Cliente deve:

- Assegnare personale VMware e di sicurezza per supportare l'attività.
- Fornire credenziali di sola lettura-e autorizzazioni per i target di valutazione.
- Garantire l'accessibilità di tutti i sistemi VMware durante le finestre di scansione.
- Assumersi la responsabilità di tutte le attività di correzione e operative.
- Gestire la classificazione, la gestione e la conservazione dei dati della valutazione.
- Riconoscere il carico temporaneo sulle risorse durante la valutazione.
- Mantenere la governance e il controllo delle modifiche per tutte le configurazioni VMware.

SICUREZZA DELLO STRUMENTO DI SCANSIONE, PROTEZIONE DEI DATI E AMBITO DI RACCOLTA

PPT garantisce l'operazione sicura e controllata dello strumento di scansione. Gli elementi chiave includono:

- Raccolta dati in modalità sola lettura- e non invasiva-.
- Nessun agente installato; nessuna modifica alla configurazione effettuata.
- Le credenziali vengono utilizzate solo durante la sessione attiva e non vengono mai archiviate.
- Vengono raccolti solo metadati di configurazione VMware (vCenter, ESXi, cluster, archiviazione, rete, autenticazione, certificati, registrazione, NTP e dettagli di licenza mascherati).
- Non vengono raccolti contenuti dei sistemi operativi guest delle VM, dati applicativi, dati utente, password o chiavi di licenza complete.
- Tutta la comunicazione è crittografata tramite HTTPS (porta 443).
- I file della valutazione sono crittografati sia durante il trasferimento che in fase di archiviazione.
- L'accesso è limitato al personale autorizzato di PPT e del Cliente.