TECHNICKÁ DOKUMENTACE

Technická specifikace zadavatele k VZ

Bezpečnostní SW pro detekci konfiguračních závad MS Windows

Všeobecné požadavky

- Řešení musí umět detekci konfiguračních závad a nabízet možnost automatické realizace nápravných opatření
- Řešení musí formou agenta podporovat operační systémy Windows, Windows Server
- Řešení podporuje prostředí AD a GPO
- Správa řešení prostřednictvím webové konzole
- Řešení umožňuje unifikovaný náhled na nálezy z pracovních stanic, serverů a doménových kontrolorů
- Řešení lze integrovat s libovolným SIEM

Servis a podpora

- Výrobce garantuje přístup k novým verzím produktu a zákaznické podpoře výrobce na 3 roky

Požadavky na funkcionalitu

Konfigurační bezpečnost

- Řešení umožňuje detekovat konfigurační zranitelnosti a provozní konfigurační chyby na základě srovnání stavu konfigurací AD/GPO z doménového kontroleru se stavem vyčteným agentem na koncovém bodu (server / workstation)
- Řešení umožňuje detekci rizikových defaultních (výchozích) konfigurací
- Řešení umožňuje upozornění na změny konfigurací na úrovni doménového řadiče
- Řešení umožní detekci lokálních administrátorských účtů
- Řešení umožňuje detekci lokálních konfigurací v rozporu s centrálně prosazenou podobou politik
- Řešení umožňuje detekci a odstranění zastaralých konfigurací nevyhovujících dnešním standardům
- Řešení umožňuje detekci nesouladu daných konfigurací s Best Practices
- Řešení umožňuje vyhledat neaktuální lokální konfigurace se zaniklou vazbou na doménový řadič (tzv. Orphaned / Unlinked politiky)
- Řešení umožňuje detekovat a napravit problémy v nasazení SCCM

Kontrola stavu obrany koncových bodů

- Řešení umožňuje kontrolu aktivity Bitlockeru
- Řešení umožňuje prověření aktivity antiviru
- Řešení umožňuje kontrolu aktualizací bezpečnostních mechanismů
- Řešení umožňuje detekovat více aktivních antimalware řešení

Kontrola aktualizací a prosazení konfigurací a politik

- Řešení umožňuje kontrolovat stav provádění aktualizací OS

- Řešení umožňuje kontrolovat provedení aktualizací AD/GPO konfigurací na jednotlivých koncových bodech
- Řešení umožňuje detekovat absenci aktuálních konfigurací zapříčiněnou nekorektní aplikací politik
- Řešení umožňuje detekovat konflikty všech skupinových politik a konfigurací
- Řešení umožňuje detekovat nekompatibilitu prosazovaných politik a konfigurací s cílovým OS

Compliance & Audit

- Řešení umožňuje kontrolovat soulad skupinových politik s ISO 27 001
- Řešení umožňuje definici vlastních požadavků pro kontrolu souladu

Pokročilé bezpečnostní a monitorovací funkcionality

- Řešení umožňuje kontrolovat oprávnění k adresáři / souborům Sysvol
- Řešení umožňuje detekovat tzv. Shadow Admins / Šedé administrátory, resp. uživatele, kteří nejsou v administrátorských skupinách, ale byly jim přímo udělena vyšší úroveň oprávnění
- Řešení umožňuje detekovat tzv. Shadow SID / šedé Security Identifiery
- Řešení umožňuje kontrolu členství v důležitých skupinách dle uživatelského nastavení
- Řešení umožňuje analýzu a kontrolu FSMO rolí
- Řešení umožňuje detekci útoků hádáním hesel
- Řešení umožňuje detekci útoků typu Kerberoasting
- Řešení umožňuje detekci nezabezpečené komunikace s využitím protokolu LDAP a vzdálené plochy
- Řešení umožňuje vyhodnocení rizikovosti uživatelů
- Řešení umožňuje sledování spuštění powershelu v reálném čase
- Řešení umožnuje detekci škodlivých příkazů spuštěných v powershellu
- Řešení umožňuje vyhledání dočasně uložených hesel (cached credentials)
- Řešení umožňuje detekci hesel uložených v cleartextu
- Řešení umožňuje detekci hesel uložených IIS v cleartextu
- Řešení umožňuje detekci nechráněných hesel uložených v prohlížečích
- Řešení umožňuje kontrolu oprávnění na úrovni Kernelu
- Řešení umožňuje detekci využívání zastaralého protokolu NTLM
- Řešení umožňuje detekci využívání zranitelného protokolu SMBv1
- Řešení umožňuje kontrolu neautorizovaných záznamů v souboru hosts
- Řešení umožňuje detekci nestandardních otevřených portů
- Řešení umožňuje detekci podezřelých nebo zastaralých prohlížečů
- Řešení umožňuje detekci podezřelého nebo zastaralého software
- Řešení umožňuje kontrolu zabezpečení Wi-Fi sítí, ke kterým se připojují vzdálená zařízení
- Řešení umožňuje kontrolu konfigurace LAPS
- Řešení umožňuje sledování startovacích časů jednotlivých koncových bodů a času přihlášení jednotlivých uživatelů
- Řešení umožňuje detekovat problémy v SPNs (Service Principal Names)
- Řešení umožňuje detekci nepoužívaných účtů a prázdných skupin AD

Nápravné procesy

- Řešení umožňuje whitelisting nerelevatních nálezů / false-positives
- Řešení umožňuje automatizovanou nápravu relevantních nálezů prostřednictvím GUI

- Řešení umožňuje konfiguraci automatické nápravy v případě opětovné detekce historicky napraveného nálezu
- Řešení poskytuje postupy pro řešení nálezů, které není technicky možné napravit automatizovaně z GUI
- Řešení poskytuje možnost opětovného otestování pro ověření nápravného procesu

Součástí dodávky

- Licence SW včetně definované podpory na 3 roky
- Dokumentace k instalaci, provozu a údržbě minimálně v anglickém jazyce

Výše uvedené vlastnosti splňuje např. SW řešení Gytpol Validator