ENDPOINT CONFIGURATION SECURITY

IDENTIFIKUJTE A OPRAVTE KONFIGURAČNÍ RIZIKA

Komplexita správy koncových bodů v posledních letech výrazně narůstá a nedostatek kontrolních mechanismů pro efektivní prověření reálného stavu celoplošné propagace aktuálních bezpečnostních politik otevírá útočníkům dveře i do vaší infrastruktury. Přinášíme možnost identifikace konfiguračních zranitelností, které jsou přehlíženy antiviry, EDR technologiemi, Vulnerability Managementy a mnohdy i penetračním testováním.

KLÍČOVÉ FUNKCIONALITY

- Komplexně adresuje oblast konfiguračních zranitelností.
- Data o reálném stavu politik zpropagovaných na koncové body porovnává se žádoucím stavem dle informací z doménových serverů.
- Na základě reálného stavu koncových bodů identifikuje hrozby spočívající v:
  - Nesouladu daných konfigurací s Best Practices.
  - Absenci klíčových konfigurací.
  - Konfliktu politik, který zamezí zpropagování nových konfigurací díky starším politikám s vyšší prioritou.
  - Lokálních administrátorských účtech a jimi definovaných politikách.
- Dále detekuje:
  - Neautorizovaně otevřené porty.
  - Nechráněná cleartxtová hesla, credentials v cache.
  - Neaktivní antimalware či šifrování.
  - Zpomalení jednotlivých koncových bodů vlivem chybné konfigurace či SW s ohledem na HW.
  - Hrozby vázané k uživatelům mimo podnikovou síť bez závislosti na VPN – Slabé zabezpečení domácí WiFi, absence aktuálních politik.
- Detekované zranitelnosti a hrozby poté:
  - Kategorizuje dle assetů a závažnosti.
  - Doplní popisem zranitelnosti / vysvětlením rizika z ní plynoucího.
  - Opatřuje nápravnými procesy
    - 90 % lze napravit jedním kliknutím z GUI.
    - 10 % vyžaduje nápravu nikoliv na endpointu, ale na úrovni doménových serverů. Zde má gytpol read-only oprávnění. V tomto případě nález opatří step-by-step návodem k nápravě.
  - Údaje o nálezech umí exportovat do SIEM.

Endpoint Configuration Risks

Vyhledává kritické konfigurační zranitelnosti na koncových bodech. Detekuje lokální administrátorské účty, neautorizovaně otevřené porty či neaktivní bezpečnostní mechanismy.

Policy Validation

Identifikuje hrozby v rámci AD, zranitelnosti a nesoulady v Group Policy a Intune. Prověřuje stav bezpečnostních updatů a plošnou propagaci politik na koncové body.

Endpoint Performace Optimization

S ohledem na výkon HW daného koncového bodu vyhledává stanice / uživatelské účty s dlouhým spouštěcím časem. Identifikuje důvod zpomalení a umožní nápravu.

Remediation

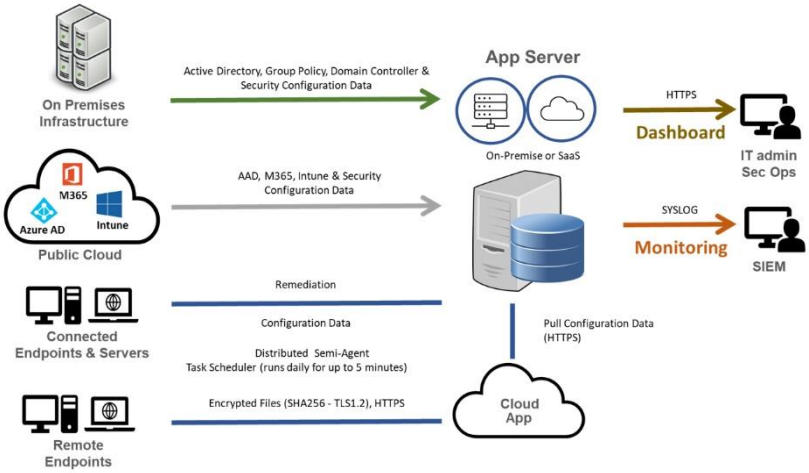
Díky široké knowledgebase automaticky navrhuje nápravné procesy k jednotlivým rizikovým nálezům.

Compliance & Audit

Srovnává aktuálně prosazené politiky s požadavky GDPR, ISO 27001, NIST, CIS, SOX, PCI DSS, HIPAA. Umožňuje tvorbu vlastních Compliance šablon.

Remote Workfoce Analytics

Udržuje přehled o zaměstnancích pracujících z domova bez potřeby připojení VPN.



Jednoduché a velice rychlé nasazení.
1 hodina a je hotovo!