GYTPOL

Misconfigurations Cause Cyberattacks

gytpol Validator

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. Unikátní technologie Validator od izraelské cybersecurity společnosti gytpol přináší možnost identifikace konfiguračních zranitelností, které jsou přehlíženy antiviry, EDR technologiemi, Vulnerability Managementy a mnohdy i penetračním testováním.

Kde gytpol Validator pomáhá

Active Directory je centrálním bodem všech organizačních činností, a to od menších firem po enterprise organizace.

Tento stěžejní systém vyžaduje zkušené administrátory, dokonce však i ti mohou mít problémy s bezchybnou správou bezpečnostních politik v AD prostředí s rozšířenou strukturou.

I v případě, kdy je prostředí spravováno bezchybně, stále hrozí, že se politika na koncový bod nedostane, což způsobí díru v bezpečnostním plášti celé organizace.

Validator s využitím pokročilých algoritmů porovnává data sesbíraná lightweight agenty z koncových bodů s informacemi z doménových serverů. Nálezy agreguje, kategorizuje dle postižených aktiv, závažnosti a po jejich srovnání s Best practices a požadavky široké škály norem uceleně interpretuje v GUI s možností exportu dat do SIEM.

Klíčové výhody:

- **Jednoduché nasazení**
- Dohledání kritických konfiguračních zranitelností **až na 90% endpointů**
- Detekce **nesrovnalostí a konfliktů v Intune a Group Policy**
- Identifikace hrozeb v **on-premise i Azure AD**
- Obsáhlá databáze konfiguračních **Best Practices**
- **Vylepšení výkonnosti** koncových zařízení
- Verifikace provedení **bezpečnostních updatů**

Funkcionality gytpol Validator

Endpoint Configuration Risks

Vyhledává kritická konfigurační rizika na koncových bodech. Identifikuje nechráněné přihlašovací údaje a cleartexrtová hesla. Upozorňuje na výskyt lokálních administrátorských účtů, neautorizovaně otevřených portů či neaktivitu bezpečnostních mechanismů.

Compliance & Audit

Slouží pro srovnání aktuálně prosazených politik se širokou škálou standardů - ISO 27001, CIS, GDPR, NIST, SOX, PCI, DSS, HIPAA. Nad rámec připravených Compliance šablon umožňuje tvorbu vlastního schématu odvozeného z politik dané organizace.

Policy Validation

Identifikuje hrozby v Active Directory a nesoulad reálného stavu s centrálně definovanými politikami. Detekuje Orphaned Policies a nežádoucí lokální politiky.

Remote Workfoce Analytics

Díky E2E šifrovanému propojení endpointů s gytpol Serverem obstarává skenování stanic mimo podnikovou síť bez potřeby VPN. Umožňuje prověření zabezpečení domácích sítí a datum posledního updatu politik.

Remediation

Opatřuje nálezy ostatních komponent nápravnými procesy s možností jejich provedení jedním klikem z GUI. Pro manuální nápravu připraví step-by-step doporučení postupu.

Endpoint Performance Optimization

V korelaci s informacemi o HW vyhledává koncové body a uživatelské účty s neadekvátně dlouhou dobou spouštění a identifikuje příčinu zpomalení.

COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz