IBM Security

Secret Server (ISSS)

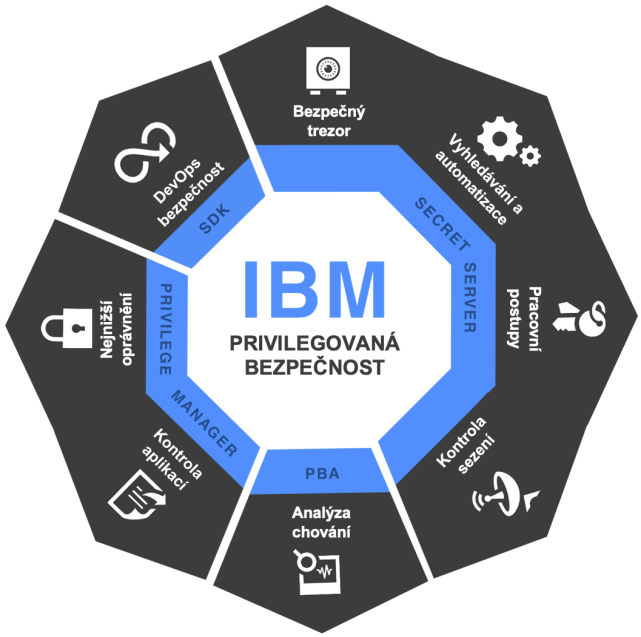
Privilegovaná hesla a pověření pro doménové administrátory, kořenové účty a super–uživatelské účty jsou preferované cíle pro hackery. Využívají zranitelnosti mezi koncovými body a uživateli, útočníci se snaží ohrozit pověření a zvýšit si tak oprávnění k získání "klíčů k firemním tajemstvím". To jim umožňuje vydávat se za důvěryhodného uživatele a získat přístup k vašim nejcitlivějším a nejdůležitějším informacím, a to často bez možnosti detekce tohoto útoku až v řádu měsíců.

Společnost IBM dodává komplexní bezpečnostní řešení, které chrání Vaše nejcennější informace před kybernetickými útoky a interními hrozbami.

Kombinuje osvědčenou ochranu privilegovaných účtů koncových stanic s kontrolou aplikací pro Windows, Mac a Unix.

Dramaticky snižuje riziko tím, že zabraňuje postupu útoků založených na malware na koncových bodech a na serverech, čímž omezuje schopnost útočníka překročit počáteční bod vstupu zabraňuje instalaci nástrojů vzdáleného přístupu (RAT).

Zajišťuje ochranu privilegovaných účtů, zatímco brání eskalaci oprávnění odstraněním a / nebo omezením oprávnění pro firemní uživatele a IT administrátory bez vlivu na produktivitu.



IBM Security Secret Server

Na té nejzákladnější úrovni je IBM Secret Server trezor pro bezpečné uložení a sdílení přístupu k přihlašovacím údajům privilegovaných účtů.

Řešení umožňuje řízení privilegovaných účtů, automatizaci změn hesel, vyhledávání používaných privilegovaných účtů, poskytnutí portálu pro uživatele, kde si mohou žádat o přístupy k jednotlivým tajemstvím. Dále také umožňuje monitorování a zaznamenávání sezení, SSH a RDP proxy, pořizování a archivování auditních záznamů, přehledné reportování a mnoho dalšího.

Spravovaná oprávnění jsou uložena v šifrované databázi MS SQL. IBM Secret server zpracovává přístup k těmto tajemstvím prostřednictvím struktury složek v kombinaci s řízením přístupu založeným na rolích a integrací se službou Active Directory.

IBM Security Privilege Manager

Poskytuje pokročilé zabezpečení pomocí implementace a vynucování principů nejnižších oprávnění, aniž by byla narušena produktivita. Agenti na koncových stanicích nebo serverech kontrolují nainstalované a spouštěné aplikace, které je možné i zablokovat pomocí nastavených politik.
Politiky kontroly aplikací zahrnují whitelisty, blacklisty a greylisty pro koncové body doménových a ne-doménových systémů Mac a Windows. Zároveň agenti umožňují prohledávání a zabezpečení lokálních účtů.

IBM Security Privileged Behaviour Analytics

Nástroj Privileged Behaviour Analytics sleduje chování privilegovaných uživatelů a v jejich aktivitě vyhledává anomálie v chování a odhaluje tak rizikové uživatele, kteří by mohli představovat hrozbu pro celou organizaci. Privileged Behaviour Analytics dále umožňuje analyzovat distribuci privilegovaných účtů a přístupů skrze celou organizaci

IBM Security Secret Server SDK

Nástroj IBM Secret Server SDK odstraňuje nutnost používat „hardcoded“ hesla ve zdrojových kódech aplikací, chrání tak privilegované účty a pomáhá splňovat požadavky na dodržování předpisů – bez ovlivnění pracovního postupu DevOps. Nástroj umožňuje nalézt a odstranit „hardcoded“ hesla v kódu, poskytuje unikátní účty a přihlašovací údaje do jednotlivých kontejnerů a služeb. Dále snižuje riziko pomocí nahrazení nebezpečných uložišť hesel, která mohou být napadena a zneužita. Nástroj umožňuje integraci s PAM pro každý nástroj v DevOps inventáři, včetně dynamického a rychlého přizpůsobení dle velikosti prostředí.