IBM Security
Guardium

IBM Security Guardium je komplexní řešení, které je určeno k ochraně těch nejcitlivějších dat v rámci celé organizace, ať už se jedná o strukturovaná či nestrukturovaná data.

Data jsou jedním z nejcennějších majetků firem. Je tedy potřeba data chránit, ovšem tak, aby to neomezilo zaměstnance v jejich práci.

Díky široké podpoře podporovaných systémů, které je schopno Guardium chránit, lze řešit ochranu dat, audit, dodržování shody a vyhledávání zranitelností na jednom centrálním místě a v jedné konzoli. Tím lze ušetřit prostředky a zjednodušit celou bezpečnostní administraci.

Centrální ochrana strukturovaných i nestrukturovaných dat v celé organizaci z jedné konzole včetně možnosti blokování a maskování

Monitoring i lokálně připojených privilegovaných uživatelů, včetně záznamu celého SQL příkazu

Behaviorální analýza a korelace historických dat s odhalením nekalých činností uživatelů

Snadná implementace bez nutnosti změn architektury sítě a datové struktury

Snižování rizika pokut, dodržováním vládních a průmyslových nařízení (GDPR, PCI DSS, SOX, HIPAA)

IBM

Modul ochrany databází

- Díky nainstalovaným agentům přímo na DB serverech je možné zaznamenávat co se děje v databázi bez toho, aby to výrazně ovlivnilo výkon databáze. Díky tomuto přístupu je možné monitorovat a blokovat akce lokálně připojených privilegovaných uživatelů.
- Zaznamenané informace jsou poté v reálném čase analyzovány. Pokud dojde k podezřelé události, je zasláno upozornění na příslušná místa, případně dojde k blokaci akce, která může vést k úniku dat.
- Guardium sbírá informace typu: „kdo, co, kde, kdy a jak“.
- Guardium umožňuje dynamicky maskovat data v odpovědi DB serveru na základě politik, tímto způsobem lze vytvářet i sady testovacích dat bez citlivých údajů.
- Guardium umožňuje vyhledávat a klasifikovat citlivá data v databázích a dále s nimi pracovat jako s objekty.
- Připravené příklady politik pro GDPR, PCI DSS, SOX, HIPAA atd.
- Ochrana dat i v cloudových prostředích, data warehousech či big data prostředích.
- Jednoduché nasazení s možnostmi vysoké dostupnosti a loadbalancingu, včetně vysoké škálovatelnosti.
- Možnost integrace se systémy QRadar či PIM pro pokročilé schopnosti detekce a reakce na hrozby v síti.

Modul ochrany souborů

- Monitoring nestrukturovaných dat jako například MS Office souborů, PDF, zdrojových kódů, konfiguračních souborů a dalších.
- Možnost blokace smazání či úpravy souboru dle nastavitelných politik.
- Automatická detekce a klasifikace citlivých údajů v souborech dle GDPR, PCI DSS, SOX, HIPAA atd.
- Možnost zasílání alertů do SIEM systému při porušení politik.

Modul vyhledávání zranitelností

- Pravidelné skenování DB serverů a vyhledávání chybějících aktualizací, slabá hesla, známé chyby v nastavení a další bezpečnostní rizika.
- Jednotná konzole pro kontrolu a správu všech zranitelností v databázích, big data a data warehousech.
- Výsledkem je přehledný report, spolu s doporučenými best – practices, jak nalezené zranitelnosti opravit. Report je možné exportovat do PDF, CSV nebo Syslogu.
- Guardium podporuje integrované podepisovací workflow s eskalací a odesíláním reportů o nalezených zranitelnostech pro účely auditingu.
- Skenery Guardium jsou nastavené tak, aby minimálně zatěžovaly databázové systémy a nedocházelo k ohrožení dostupnosti.
- Výsledky testů lze odesílat pro další zpracování do SIEM QRadar nebo Data Risk Manageru.