LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Případová studie - Dr.Max

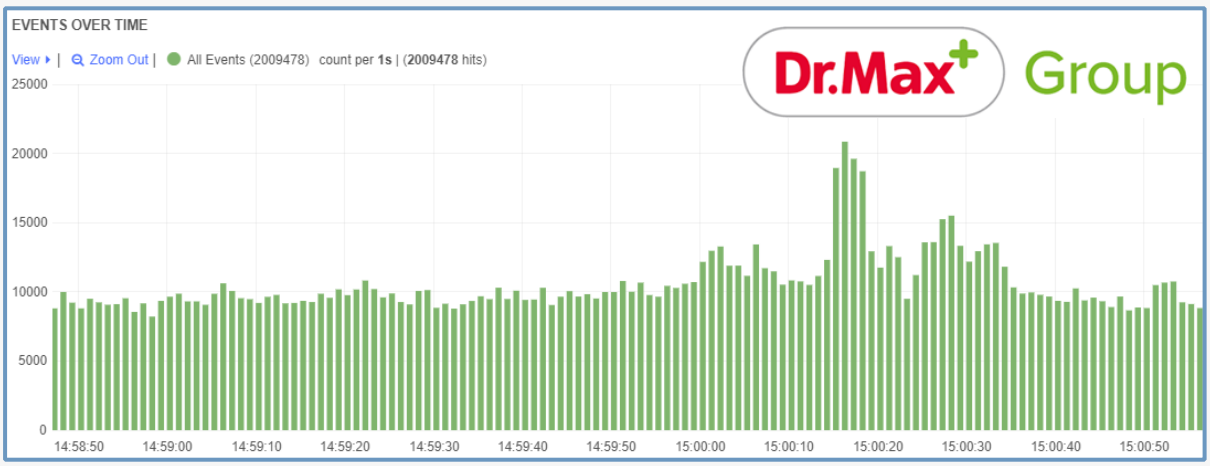
O zákazníkovi

Nejdostupnější lékárenskou péči v ČR poskytují lékárny Dr.Max. V České republice se jedná o síť více jak 400 lékáren s více než 3000 zaměstnanci. Dr. Max Group působí i v dalších 7 evropských zemích.

Co zákazník řešil a proč?

Skupina Dr.Max provozuje a spravuje velmi různorodé IT systémy určené pro chod nejen lékáren, ale i skladů, distribuce léčiv, jejich vývoj a výrobu. To vše vyžaduje řadu databázových systémů a velmi rozsáhlou počítačovou síť. Každý ze systémů generuje velké množství důležitých strojových dat o své činnosti, stavu a činnosti administrátorů/uživatelů. V případě výskytu problémů znamenala předchozí decentralizace ukládání logů velmi složitou identifikaci a významné prodloužení doby nutné k jejich vyřešení. A to i při podezření na bezpečnostní incidenty.

Cílem zákazníka bylo sjednocení ukládání logů na externím zabezpečeném systému a získání uceleného přehledu o bezpečnosti a provozu informačních systémů. Požadavkem bylo, aby úložiště logů zajišťovalo dlouhodobé uchovávání informací v nezměnitelné podobě pro získání přehledu o stavu provozovaných systémů, přístupech k jednotlivým aplikacím nebo přesně zmapované činnosti privilegovaných účtů. Úložiště muselo být zabezpečené tak, aby nemohlo dojít k mazání či jiné úpravě nasbíraných dat. Zvolené řešení nemělo být licenčně omezeno maximálním počtem zpracovávaných událostí za časovou jednotku ani maximálním počtem sledovaných zařízení a mělo umožnit zpracování velkého počtu událostí za vteřinu. *Poznámka: tento předpoklad byl správný, ve špičkovém výkonu LOGmanager-XL zpracuje více než 20 tisíc EPS— viz snímek obrazovky celkového počtu událostí.*



Rozsah a popis projektu

I. Fáze

Cílem této fáze bylo ověření technických možností řešení a přizpůsobení prostředí pro analýzu dat. Byla dodána testovací appliance LOGmanager-M s kapacitou úložiště 12 TB. V rámci úvodní instalace došlo k napojení autentizace uživatelů LOGmanageru přes Active Directory. Pro sběr událostí byla vytipována referenční zařízení, která měla prověřit výkon systému, schopnost zpracování a analýzy uložených dat.

II. Fáze

Byla dodána appliance LOGmanager-XL s kapacitou úložiště 100 TB. Tato appliance byla nainstalována v datovém centru společnosti. Byla provedena konfigurace do clusteru se zařízením dodaném ve fázi první. Po přenesení konfigurace a replikaci všech dat byla odpojena appliance LOGmanager-M a zařízení umístěné v datovém centru bylo převedeno do produkčního režimu.

III. Fáze

Byly nakonfigurovány vybrané aplikace a servery tak, aby zasílaly logy do LOGmanageru, který je kontinuálně sbírá a ukládá. V okamžiku, kdy byly v LOGmanageru logy dostupné, došlo k vytvoření specifických „parserů“. Vzhledem k velmi vysokému počtu událostí, generovaných zejména interními bezpečnostními prvky, byla provedena optimalizace zpracovaní dat. Bylo tak dosaženo stavu, kdy LOGmanager trvale přijímá a vyhodnocuje 10 000 událostí za vteřinu a v době špičky, která trvá mnohdy i několik hodin, je schopen zpracovávat až 25 000 událostí za vteřinu. Denně je tak zpracováváno 250 - 350 GB dat.

IV. Fáze

Bylo provedeno školení administrátorů, techniků IT podpory a bezpečnostních pracovníků pro práci s nástrojem LOGmanager a pro tvorbu „parserů“. Proběhlo také několik workshopů zaměřených na řešení specifických potřeb jednotlivých oddělení.

PŘÍNOS PRO ZÁKAZNÍKA A OCEŇOVANÉ VLASTNOSTI

LOGmanager svým sjednocením ukládání logů a jejich zabezpečením zcela splnil všechny očekávané cíle zákazníka. Spolu s profesionálním nasazením a následnou podporou certifikovaného partnera BIT SERVIS došlo k jednoduchému a rychlému nasazení z testovacího režimu přímo do produkčního prostředí.

Systém slouží především bezpečnostnímu managementu pro dohled. Provozní zkušenosti ukázaly, že řešení může být také velmi efektivním nástrojem pro práci techniků IT podpory i administrátorů jednotlivých aplikací či systémů. Mezi nejčastější operace patří kompletní vyčítání a zpracování logů o přihlášení a přístupech uživatelů do systému, rychlé dohledání a filtrace potřebných informací z obrovského množství logů, používání automatických upozornění na nestandardní stavy a vyčítání logů z provozované síťové infrastruktury včetně bezpečnostních zařízení.

Přínosem jsou dále možnosti průběžného rozšiřování díky otevřenosti systému LOGmanager, která umožňuje snadné vytváření přehledných zobrazení potřebných informací, činností nebo situací formou vlastních dashboardů. Zaujalo i zpracování logů ze zákaznických aplikací pomocí snadné tvorby vlastních „parserů“.

Zákazník nejvíce oceňuje:

⇒ Rychlé nasazení včetně iniciálního ověření vlastností během testů před koupí a možnost okamžitého využívání,
⇒ Korelaci logon/logoff operací napříč celou síťovou infrastrukturou,
⇒ Vyhodnocování přístupu uživatelů k souborům a systémovým prostředkům,
⇒ Sledování konfiguračních změn prováděných administrátory a operátory systému,
⇒ Rychlou diagnostiku a řešení bezpečnostních incidentů,
⇒ Podklady pro forenzní analýzu při vyšetřování bezpečnostních incidentů,
⇒ Zrychlení při odstraňování technických problémů systémů,
⇒ Možnost postupného škálování v rámci zemí z centrálního na distribuované řešení,
⇒ Otevřené řešení pro snadnou integraci systémů, které nejsou podporovány přímo výrobcem,
⇒ Unifikované a snadné vyhledávání napříč všemi typy dat a zařízení,
⇒ Přehlednost a minimální nároky na operativu, vysoký výkon,
⇒ Jemné nastavení přístupových práv k ukládaným datům i systémovým oprávněním.

INFORMACE O VÝROBCI A DALŠÍ REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Do vydání tohoto referenčního listu nalezl LOGmanager více jak 160 spokojených zákazníků a na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Certifikovaným partnerem realizujícím tento projekt byla firma BIT SERVIS s.r.o.