Zákazník

kofola
drinks. life. emotion.

Obor činnosti

Výroba nealkoholických nápojů

Výzvy

- Rozsáhlá počítačová síť čítající více než 3 tisíce koncových IP zařízení, 100+ nezávislých LAN sítí a dvě datové centra
- Stávající monitoring nebyl schopen poskytnout dostatečně kvalitně a efektivně potřebné informace pro správu sítě a síťovou bezpečnost
- Z provozně-bezpečnostního pohledu bylo zapotřebí dodat monitorovací řešení, poskytující informace o provozu v síti, jeho struktuře a vývoji v čase

Přínosy řešení

- Viditelnost do sítě včetně detailního přehledu o chování uživatelů a zařízení na síti
- Zvýšení bezpečnosti počítačové sítě a s tím související kontrola přístupu k ICT prostředkům.
- Efektivnější správa a dohled sítě, zjišťování chybných konfigurací a řešení problémů na síti.

Nasazené produkty

- Flowmon kolektor
- Flowmon sondy
- Flowmon ADS

Flowmon
Driving Network Visibility

Kofola ČeskoSlovensko a.s.

Společnost Kofola je jedním z nejvýznamějších výrobců nealkoholických nápojů v Evropě. Skupina Kofola disponuje sedmi výrobními závody na čtyřech trzích střední a východní Evropy. Celkově v Evropě zaměstnává přes dva tisíce zaměstnanců.

Situace

IT oddělení společnosti denně řeší desítky úkonů týkajících se běžné správy ICT systémů. Vzhledem k vysokému vytížení stávajících pracovníků běžnou operativou v dynamicky se rozrůstajícím prostředí a vzhledem k limitovaným IT personálním zdrojům ve výrobních závodech bylo zapotřebí implementovat kvalitnější monitoring datové komunikace splňující následující požadavky:

- kompletní monitoring WAN jak pro výrobní, tak i obchodní pobočky,
- detailní monitoring LAN výrobních závodů, datových center a centrály,
- efektivnější správa a dohled sítě, zjišťování chybných konfigurací a řešení problémů na síti,
- potřeba jednoznačné dohledatelnosti identity původce provozně-bezpečnostních událostí a anomálií.

Řešení

Požadavky společnosti byly vyřešeny díky distribuovanému Flow Mon řešení sestávajícího se z:

- centrálního 3TB Flowmon kolektoru,
- 1, 2 a 4portových Flowmon sond implementovaných v klíčových lokalitách pro zajištění detailního monitoringu LAN,
- dalších 10+ aktivních prvků zasílajících NetFlow export data na centrální kolektor.

Výše uvedené řešení bylo dále integrováno s DDI (DNS, DHCP, IP address management) řešením třetí strany za účelem zajištění maximální konzistence záznamů (IP adresa vůči doménovému jménu), čímž se dosáhlo:

- jednoznačného identifikování původců provozně-bezpečnostních událostí v čase s možností zjistit MAC adresu původce a jeho místo připojení (lokalita, aktivní prvek, fyzický port),
- jednoznačného sledování komunikačních trendů systémů, které jsou dynamicky adresovány pomocí DHCP.

Přínosy

Nasazení řešení Flowmon hodnotí Milan Zmarzlák, IT ředitel společnosti Kofola:

Doposud byli naši ICT specialisti zaměstnáni z podstatné části běžnou operativou s omezenými možnostmi analýzy systémových, provozních a bezpečnostních logů a statistik. Tyto úkony jsou mnohdy předmětem nákladných SIEM systémů a jim dedikovaných lidských zdrojů. Kofola prozatím SIEM řešení takového rozsahu nevyžaduje, přesto implementace výše popsaného distribuovaného Flowmon řešení poskytuje pro každodenní správu ICT prostředí významný přínos, a to jak v efektivnějším řešení problémů, tak v proaktivních činnostech týkajících se ladění, plánování a redesignu ICT.