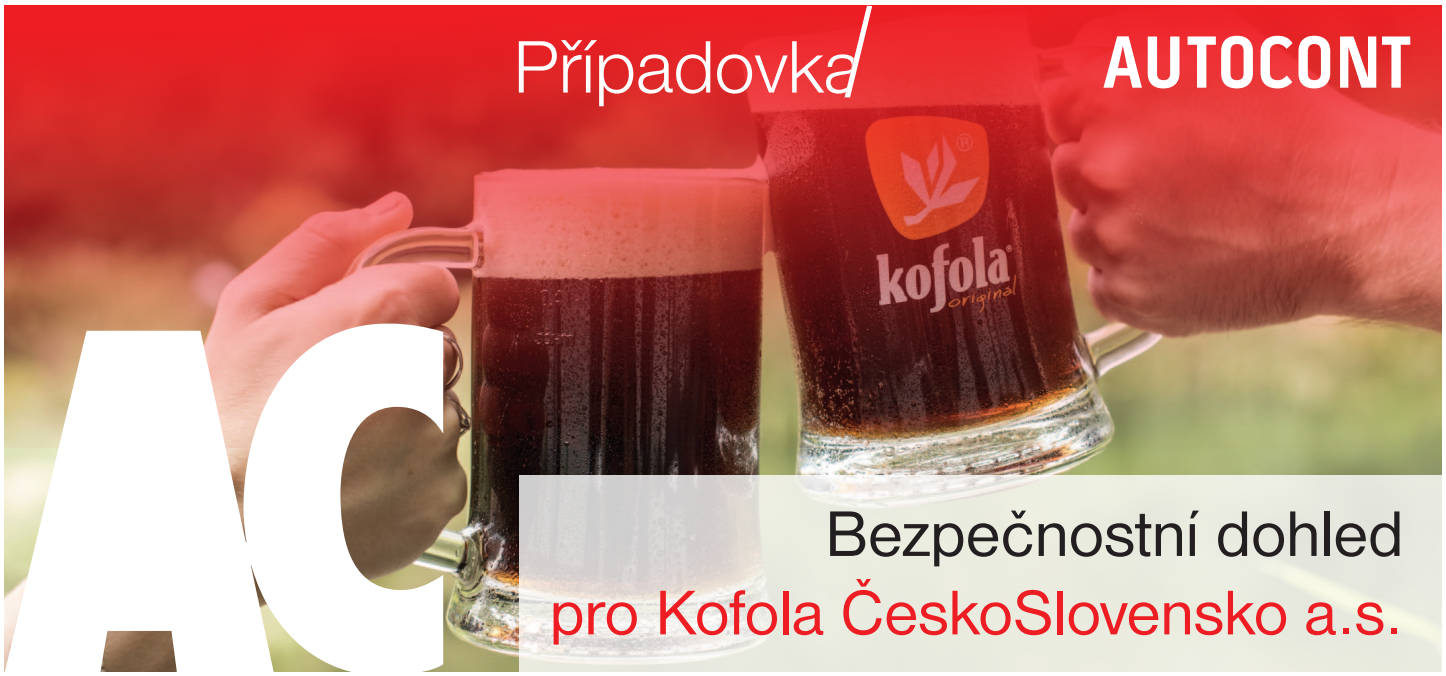
Případovka

AUTOCONT



Bezpečnostní dohled pro Kofola ČeskoSlovensko a.s.

ZÁKAZNÍK STRUČNĚ

Kofola ČeskoSlovensko a.s. vyrábí nealkoholické nápoje s péčí a láskou, a to hned v devíti závodech na pěti trzích střední a východní Evropy. Pod křídla Kofoly patří kromě stejnojmenného nápoje i pramenitá voda Rajec, sirupy Jupí a dětské nápoje Jupík, hroznová Vinea, čerstvé ovocné a zeleninové šťávy UGO, bylinné čaje LEROS, energetický nápoj Semtex a další tradiční československé i zahraniční značky.

www.kofola.cz

OBDOBÍ REALIZACE

10/2018

„Našli jsme řešení pro dohled nad kybernetickou bezpečností bez nároku na nové lidské zdroje.“

Milan Zmarzlák, Head of ICT ve společnosti Kofola ČeskoSlovensko a.s.

Výchozí situace a cíle projektu

V kybernetickém prostoru je dnes mnoho různě nebezpečných útočníků, kteří jsou většinou absolutně neznámí náhodně nebo cíleně útočící na méně či více chráněné informační a komunikační systémy. Služby „Bezpečnostního dohledu“ jsou založeny na co nejrychlejší detekci případného průlomu do informačního systému a zjištění jeho původu, cesty, rozsahu zasažení a pojmenování dopadu a následné správně řízené reakci a rychlé nápravě.

I když společnost Kofola provozuje ve výrobních jednotkách v Česku, Slovensku, Polsku, Slovinsku a Chorvatsku řadu informačních systémů a některé z nich pro všechny lokality i centrálně, nebyla z počátku přesvědčena o tom, že je pro ni kontinuální bezpečnostní dohled nutný.

Vzájemná dohoda společnosti Kofola a AUTOCONT vedla k Proof of Concept řešení Pokročilého bezpečnostního dohledu a až poté dle výsledku a prokazatelných přínosů řešení se Kofola chtěla sama rozhodnout zda je pro ni služba tohoto typu užitečná nebo není.

Zkušební provoz Pokročilého bezpečnostního dohledu probíhal po dobu jednoho měsíce. Poté se společnost Kofola rozhodla využít této služby na delší období.

PŘÍNOSY

- Přehled nad konkrétními bezpečnostními hrozbami s pohotovou reakcí v téměř reálném čase
- Vysoká míra zabezpečení
- Analýza účinnosti organizačních a technických opatření
- Usnadnění činnosti při změnách ve společnosti
- Efektivní řízení investice do budování kybernetické bezpečnosti, realizace formou průběžně placených služeb
- Vysoká odbornost, zkušenost i přehled v oblasti kybernetických hrozeb díky externímu, vysoce kvalifikovanému týmu specialistů

POUŽITÉ TECHNOLOGIE

AT&T Cybersecurity, USM appliance

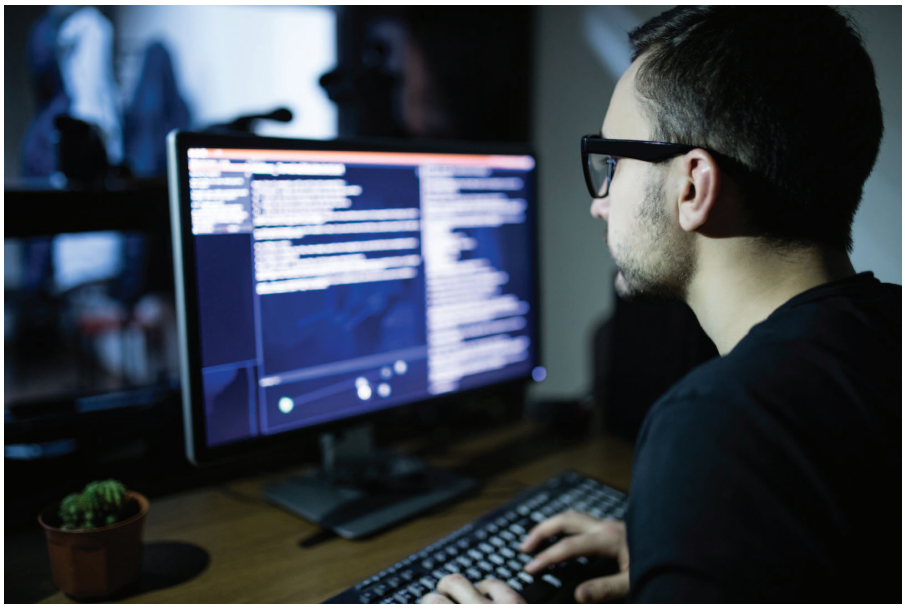
Dell EMC PowerEdge server

Virtualizace Microsoft Hyper-V

Popis řešení

Primárním cílem bylo zvýšení účinnosti boje s kybernetickými hrozbami pomocí sběru „provozně-bezpečnostních“ informací z informačních systémů a jejich následná korelace a analýza.

Pomocí vstupních auditů a analýz byla určena „Technická aktiva“, ze kterých jsou následně získávány informace v podobě logů a flow. To je pro kvalitní Bezpečnostní dohled zásadní.



Díky strategickému partnerství se společností AT&T Cybersecurity (dříve AlienVault) a výběrem dohledového systému založeného na produktu Unified Security Management (USM) je využito rozšířených detekčních mechanismů, které pracují i s informacemi z dalších oblastí bezpečnosti, které USM má. Jedná se především o informace z oblasti „správy aktiv“ (Asset Managementu), tzv. „správy zranitelností“ (Vulnerability Assessmentu) a také „monitoringu chování“ (Behavioral Monitoring).

Každý zákazník využívající služby Bezpečnostní dohled od firmy AUTOCONT je napojen na „federační server“ umístěný v prostředí AUTOCONT Security Operations Center (AC SOC). Všechny lokálně generované Kybernetické bezpečnostní události, alerty a incidenty každého zákazníka jsou na tento server bezpečnou cestou replikovány. Bezpečnostní team AUTOCONT tak má celkový přehled o všech dohledovaných zákaznících a dokáže tak včas a cíleně reagovat.

Díky tomu i společnost KOFOLA ČeskoSlovensko a.s. významně zvýšila svoji bezpečnost, aniž by musela investovat do implementace robustních softwarových systémů, hledat či vychovávat security specialisty a řešit jejich zastupitelnost. Dynamicky se vyvíjející bezpečnostní problematiku má spolehlivě zabezpečenu formou průběžně placených služeb.