Případovka

AUTOCONT

Bezpečnostní dohled
v Palivovém kombinátu Ústí, s. p.

PROFIL ZÁKAZNÍKA

Hlavním předmětem činnosti společnosti Palivový kombinát Ústí, s. p. je v současné době zejména zahlazování následků hornické činnosti, vypořádání restitučních nároků, správa majetku sloužícího k zajištění energetické bezpečnosti státu, sanace zbytkových jam podle plánů likvidace a jejich doplňků schválených Státní báňskou správou ČR.

PKÚ
PALIVOVÝ KOMBINÁT ÚSTÍ, s. p.

OBDOBÍ REALIZACE

2018

„AUTOCONT se pro nás stal spolehlivým partnerem. Nabídnuté řešení umožňuje v případě incidentu jeho rychlé odhalení a pohotovou reakci téměř v reálném čase.“

Jiří Borusík, IT správce

Výchozí situace a cíle projektu

Státní podnik hledal řešení, které by umožnilo sledování síťového provozu s cílem zvýšit bezpečnost prostředí a zajistit archivaci za účelem zpětného dohledávání v případě incidentu.

Popis řešení

Na začátku spolupráce jsme zjišťovali očekávání zákazníka, upřesňovali jeho požadavky na poskytované IT služby a mapovali aktuální stav IT infrastruktury.

PŘÍNOSY

- Zázemí kvalitního bezpečnostního týmu
- Přenesení rizik na poskytovatele IT služeb
- Garantovaná úroveň služeb, rychlé řešení IT požadavků
- Úspora nákladů a jejich rozložení do měsíčního poplatku za službu
- Úspora lidských zdrojů nutných pro obsluhu řešení, detekci a analýzu incidentů, znalých souvisejícíproblematiky a legislativy

Na základě zjištěných výsledků jsme předložili 3 varianty řešení:

- **LOG manager** - řešení primárně určené pro shromažďování logů, obsahuje tedy pouze základní analytické a korelační nástroje a vyžaduje kvalifikovanou obsluhu
- **SIEM** - komplexní On-Premise řešení postavené na produktu AlienVault, rovněž vyžadující kvalifikovanou, časově náročnou obsluhu a související nároky na lidské zdroje zákazníka.
- **Bezpečnostní dohled** - řešení, které je jako celek poskytováno formou služby, obsahující pronájem a údržbu souvisejícího HW/SW, zajištění kvalifikovaných zdrojů pro obsluhu, zaznamenávání, analýzu a asistenci při řešení vzniklých incidentů.

Po zvážení všech okolností se zákazník rozhodl pro variantu Bezpečnostního dohledu formou služby zejména z těchto důvodů:

- Výrazná úspora celkových nákladů v porovnání s On-Premise řešením
- Rozložení nákladů (poplatek za službu fakturován měsíčně)
- Absence vlastních kvalifikovaných zdrojů pro obsluhu řešení, detekci a analýzu incidentů, znalých souvisejícíproblematiky a legislativy
- Náklady na údržbu potřebného HW/SW, maintenance poplatky, záruky apod. jsou přeneseny na stranu poskytovatele
- Možnost ukončení služby (smlouvy) jednostrannou výpovědí bez udání důvodu

Od ledna 2019 má zákazník zajištěn stálý bezpečnostní dohled prostřednictvím týmu vysoce kvalifikovaných specialistů IT bezpečnosti, který využívá procesně i technologicky vyspělých vlastností tzv. AUTOCONT Security Operations Center (AC SOC). Smlouva je uzavřena na 3 roky.