CASE STUDY

IBM QRADAR

ENERGETIKA A DISTRIBÚCIA

SOITRON

Veľká firma kritickej infraštruktúry má kybernetické riziká vďaka systému SIEM pod kontrolou

„ Za úspechom projektu stali jednoznačne ľudia v realizačnom tíme, ako na strane zákazníka, tak aj nás ako realizátora. Pomohla nám dôsledná príprava, zodpovedný prístup a súčinnosť zákazníka. V projekte sme tak naplno využili naše dlhodobé skúsenosti s technológiou IBM QRadar a potvrdili našu kompetenciu v oblasti zabezpečenie prostredí IT aj OT. “

Maroš Rajnoch
Soitron, Security Solutions Architect

1. POŽIADAVKY

- Zákazník reaguje na rastúce **hrozby kybernetických útokov**, ktoré môže v krajných prípadoch odstaviť aj dodávky energií.
- Spoločnosť **nemala nástroj na zhromažďovanie log záznamov** dôležitých pre vyhodnocovanie bezpečnostných rizík a prevádzkových problémov.
- **Chýbali možnosti korelácie** rozličných **udalostí**, analytiky a spätného vyšetrovania incidentov či auditu.
- Komplikované **naplnenie nových legislatívnych požiadaviek** uložených zákonom o kybernetickej bezpečnosti.

2. RIEŠENIE

- **Systém QRadar** pre evidenciu, vyhodnocovanie a manažment bezpečnostných udalostí (SIEM).
- **Analýza a integrácia QRadaru s IT a OT infraštruktúrou** pre komplexný zber log záznamov.
- **Vypracovanie a nastavenie** desiatok rozličných **bezpečnostných a prevádzkových scenárov** na mieru zákazníka, na ktoré má SIEM systém reagovať.
- **Zavedenie nadstavby s umelou inteligenciou Watson** pre podporu korelácií a analýz agregovaných dát.

3. VÝSLEDKY

- **Zvýšenie ochrany pred kybernetickými rizikami** a **eliminácia prevádzkových problémov**, ktoré môžu vyústiť do výpadkov služieb.
- **Uľahčenie práce** administrátorom a špecialistom na bezpečnosť.
- **Automatizované upozornenia na riziká** odvodené na základe analýz dát a udalostí z infraštruktúry.
- **Bezpečné uskladnenie log záznamov** s možnosťou spätného vyhodnocovania, auditovania a reportovania.
- Vytvorenie predpokladov pre **naplnenie požiadaviek legislatívy**.

CASE STUDY

IBM QRADAR

ENERGETIKA A DISTRIBÚCIA

SOITRON

Zákazník sa vždy intenzívne zaoberal hodnotením a riadením všetkých druhov rizík. V ostatných rokoch venuje zvýšenú pozornosť aj kybernetickým hrozbám, ktoré by v krajných prípadoch mohli vyústiť do ohrozenia dodávok energií zákazníkom.

Takýmto čiernym scenárom sa snaží predchádzať aj štát, ktorý ukladá vybraným organizáciám – takzvaným prevádzkovateľov základných služieb, ku ktorým patria aj energetické podniky – v súvislosti s kybernetickou bezpečnostou, viaceré povinnosti.

Jednou z nich je systematická evidencia, vyhodnocovanie a hlásenie kybernetických bezpečnostných incidentov do centrálneho systému včasného varovania.

Východiská

Zákazník už v minulosti zaznamenával takzvané logy (auditné záznamy o činnosti informačných systémov) v prostredí technologickej infraštruktúry. Údaje sa však zbierali do viacerých databáz a chýbal nástroj s analytickou funkcionalitou, ktorý by jednoduché hlásenia umožňoval dávať do súvislostí a identifikovať tak relevantné bezpečnostné incidenty.

Vyšetrovanie podozrivých udalostí a identifikácia bezpečnostných aj prevádzkových rizík boli preto komplikované a spoločnosť tak nevedela efektívne naplniť nové legislatívne požiadavky.

Manažment organizácie sa preto rozhodol nasadiť technicky pokročilé riešenie na komplexnú identifikáciu a správu bezpečnostných informácií a udalostí (SIEM – Security Information and Event Management), ktorý umožňuje v reálnom čase zbierať vybrané log záznamy z infraštruktúry, a tie následne analyzovať, dávať do súvislostí a reportovať prípadne nezrovnalosti s bezpečnostnými politikami.

Riešenia

Voľba padla na jeden z najpoužívanejších SIEM systémov, QRadar od IBM, ktorý sa už po 12-krát za sebou umiestnil v hodnotení analytikov Gartneru medzi lídrami trhu.

QRadar umožňuje zaznamenávať dáta nielen z IT infraštruktúry, ale aj z takzvaného OT prostredia, čiže z priemyselných technológií. Okrem toho dokáže vďaka nadstavbe Watson využívať prvky umelej inteligencie, ktorá vie pomôcť pri vyšetrovaní a vyhodnocovaní udalostí a automatizovať viaceré rutinné manuálne úlohy, čím odborníkom pripraví detailné podklady pre rozhodovanie a uvoľňuje ruky pre sofistikovanejšiu prácu.

Kvalitný SIEM nástroj je sám o sebe dôležitým predpokladom pre efektívnu kybernetickú ochranu a naplnenie legislatívnych požiadaviek.
Pre maximalizáciu prínosov a pridanej hodnoty je však kľúčová kvalitná implementácia s detailným prispôsobením celého riešenia na mieru.

CASE STUDY

IBM QRADAR

ENERGETIKA A DISTRIBÚCIA

SOITRON

Nasadenie

Zákazník sa spoľahol na integračné služby spoločnosti SOITRON, s.r.o., ktorá má rozsiahle skúsenosti s budovaním infraštruktúr, prepájaním rozličných systémov aj so zabezpečovaním technológií a dát voči kybernetickým rizikám. Subdodávateľom na tomto projekte bola spoločnosť AXENTA s.r.o. Vďaka tejto spolupráci spoločnosť SOITRON dokázala urýchliť implementáciu celého riešenia.

Nevyhnutnú súčasť projektu tvorila rozsiahla analýza, ktorá bola dôležitá hlavne pre veľkú rozmanitosť technologickej infraštruktúry, vrátane softvérových systémov vyvinutých na mieru. Po nej nasledovala integrácia QRadaru so sieťovými a bezpečnostnými zariadeniami, servermi, operačnými systémami, aplikáciami a inými (nielen) IT systémami.
Hoci QRadar má v sebe zabudovaných množstvo preddefinovaných scenárov, každá organizácia je špecifická, preto je vždy potrebné prispôsobiť SIEM individuálnym potrebám a podmienkam. SOITRON pre zákazníka obohatil QRadar o desiatky relevantných scenárov, na ktoré systém reaguje. Reakcia môže spočívať v upozornení zodpovedného pracovníka na potenciálne riziko, ale aj v automatizovanom kroku, napríklad zablokovaním podozrivej komunikácie. Práve pre detailné prispôsobovanie a integráciu viacerých systémov pracovali odborníci spoločnosti SOITRON na projekte viac ako rok. Technologické prostredie veľkej firmy kritickej infraštruktúry sa neustále mení, preto azda nikdy nebude môcť byť považovaný za úplne dokončený. Pre naplnenie svojho poslania a očakávaní zákazníka, to však ani nie je potrebné.

„Odbor bezpečnosti klienta správne vyhodnotil riziká v prostredí riadiacich priemyselných systémov, a preto súčasťou projektu bol aj zber a vyhodnocovanie bezpečnostných udalostí z tzv. prostredia OT. Už samotné prostredie systémov IKT zákazníka je rozsiahle a rozmanité. V prípade, keď projekt implementácie technológie SIEM pokrýva oblasť IT aj OT, obzvlášť ak ide o veľkú organizáciu, treba počítať s časovou náročnosťou a zapojením pracovníkov z viacerých IT/OT odborov,“

Maroš Rajnoch
Soitron, Security Solutions Architect

CASE STUDY

IBM QRADAR

ENERGETIKA A DISTRIBÚCIA

SOITRON

Prínosy

Precízne nastavenie zberu dát do QRadaru z IT aj OT prostredia, nadefinovanie desiatok scenárov, ktoré môžu potenciálne vyústiť do prevádzkových alebo bezpečnostných problémov, ako aj pomocná ruka umelej inteligencie, posunuli úroveň kybernetickej bezpečnosti na novú úroveň. Zároveň firme umožnili poľahky plniť legislatívne povinnosti, ako je podrobná evidencia a reportovanie incidentov.

Integrácia zo strany Soitronu zohrala v projekte kľúčovú rolu. Bez pridanej hodnoty v podobe vyladenia a prispôsobenia prostrediu organizácie je totiž funkcionalita každého SIEM systému obmedzená prevažne na agregáciu log záznamov. To samo o sebe nemusí administrátorom a špecialistom zodpovedným za bezpečnosť uľahčovať prácu, ale naopak ich zahlcovať dátami.
Dobre nasadený SIEM systém vyzbrojuje IT tímy nástrojom, ktorý im dáva neoceniteľný pohľad „zhora“ na dianie v celej technologickej aj priemyselnej infraštruktúre. Vďaka tomu dokážu lepšie identifikovať nielen bezpečnostné, ale aj prevádzkové riziká či konfiguračné chyby, ktoré môžu viesť k zbytočným výpadkom služieb. QRadar sa stal zároveň bezpečným centrálnym úložiskom všetkých logov,čo im umožňuje ľahšie vyšetrovať minulé incidenty a predchádzať ich opakovaniu.

Projekt implementácie riešenia SIEM a jeho technologická a procesná integrácia u zákazníka prebiehali vo viacerých fázach. Týmto spôsobom sa umožnilo efektívne využiť ľudské zdroje a dôsledne uzavrieť jednotlivé funkčné celky aj v takej rozsiahlej a komplexnej infraštruktúre, akú zákazník prevádzkuje.

Už v priebehu implementácie začal zákazník intenzívne využívať platformu IBM QRadar SIEM. Pripájanie ďalších systémov IKT a zvýšenie detailu auditných záznamov postupne narastalo so zvýšeným rizikom kybernetických hrozieb na Slovensku v rokoch 2021/2022. Licenčné rozširovanie v pôvodnom modeli sa tak stalo finančne náročné, a preto zákazník využil migráciu do nového licenčné programu IBM Cloud Pak for Security. V rámci riešenia IBM QRadar SIEM sme tak dokázali vyhodnocovať viac ako 10-násobok pôvodne navrhovaného počtu udalostí, a zároveň umožňujeme výkonnostne škálovať riešenie bez licenčných obmedzení. IBM Cloud Pak for Security obsahuje stack bezpečnostných aplikácií, ktoré výrazne obohacujú a rozširujú pôsobnosť samotného riešenia SIEM. Zásadný rozvoj sme tak uskutočnili aj následnou automatizáciou s využitím platformy IBM QRadar SOAR.

SOITRON, s.r.o., člen skupiny SOITRON Group

Spoločnosť Soitron je stredoeurópsky integrátor, ktorý pôsobí na IT trhu od roku 1991. Filozofiou spoločnosti je snaha neustále napredovať, a aj preto je lídrom v zavádzaní unikátnych technológií a inovatívnych riešení. Svojim klientom ponúka produkty a služby v oblasti robotizácie a automatizácie procesov, kybernetickej bezpečnosť, dátových centier, IoT riešení, IT outsourcingu, komunikačných a sieťových riešení, IT supportu a poradenstva. Do portfólia spoločnosti patrí aj riešenie pre inteligentné policajné autá – Mosy a služby v oblasti kybernetickej bezpečnosti – VOID Security Operations Center.
Soitron je členom skupiny Soitron Group, v ktorej pracuje viac ako 800 medzinárodných odborníkov. Skupina združuje profesionálne tímy na Slovensku, v Českej republike, Rumunsku, Turecku, Bulharsku, Poľsku a Veľkej Británii.