CASE STUDY

# IBM QRADAR

ENERGETIKA A DISTRIBUCE

SOITRON

## Velká firma kritické infrastruktury má kybernetická rizika pod kontrolou díky systému SIEM

„Úspěch projektu byl jednoznačně zásluhou lidí v realizačním týmu, a to jak na straně zákazníka, tak na naší straně jako dodavatele. Pomohla nám pečlivá příprava, zodpovědný přístup a součinnost zákazníka. V projektu jsme plně využili naše dlouhodobé zkušenosti s technologií IBM QRadar a potvrdili jsme naši kompetenci v oblasti zabezpečení IT i OT prostředí."

**Maroš Rajnoch**
Soitron, Architekt bezpečnostních řešení

## 1. POŽADAVKY

- Klient reaguje na rostoucí **hrozbu kybernetických útoků**, které by v krajním případě mohly způsobit i zastavení dodávek energií.
- Společnost **neměla k dispozici nástroj na shromažďování záznamů** z logů důležitých pro vyhodnocování bezpečnostních rizik a provozních problémů.
- **Chyběla možnost korelace** různých **událostí**, analytiky, zpětného vyšetřování incidentů nebo auditu.
- Komplikované bylo i **plnění nových legislativních požadavků**, které ukládá zákon o kybernetické bezpečnosti.

## 2. ŘEŠENÍ

- **Systém QRadar** pro záznam, vyhodnocování a správu bezpečnostních událostí (SIEM).
- **Analýza a integrace systému QRadar s infrastrukturou** IT a OT pro komplexní sběr záznamů z logů.
- **Vývoj a nastavení** desítek různých **bezpečnostních a provozních scénářů** specifických pro daného zákazníka, na které má systém SIEM reagovat.
- **Zavedení nadstavby s umělou inteligencí Watson** na podporu korelací a analýzy agregovaných dat.

## 3. PŘÍNOSY

- **Zvýšení ochrany proti kybernetickým rizikům** a **eliminace provozních problémů**, které můžou vést k výpadkům služeb.
- **Usnadnění práce** správců a bezpečnostních specialistů.
- **Automatická upozornění na rizika** odvozená z analýzy dat a událostí v infrastruktuře.
- **Bezpečné ukládání záznamů z logů** s možností zpětného vyhodnocování, auditu a vykazování.
- Vytvoření předpokladů pro **splnění legislativních požadavků.**

CASE STUDY

# IBM QRADAR

ENERGETIKA A DISTRIBUCE

SOITRON

Firma se vždy intenzivně zabývala vyhodnocováním a řízením všech typů rizik. V posledních letech věnuje zvýšenou pozornost také kybernetickým hrozbám, které by v krajním případě mohly vést k ohrožení dodávek energie zákazníkům.

Podobným černým scénářům se snaží předcházet i stát tím, že vybraným organizacím – tzv. provozovatelům základních služeb, mezi které patří i energetické společnosti – ukládá v souvislosti s kybernetickou bezpečností řadu povinností.

Jednou z nich je systematické zaznamenávání, vyhodnocování a hlášení kybernetických bezpečnostních incidentů do centrálního systému včasného varování.

## Východiska

V prostředí technologické infrastruktury zákazník dříve zaznamenával tzv. logy (auditní stopy činnosti informačních systémů). Data se ale shromažďovala v několika databázích a neexistoval nástroj s analytickými funkcemi, který by umožnil uvést jednoduchá hlášení do souvislostí a identifikovat tak relevantní bezpečnostní incidenty.

Vyšetřování podezřelých událostí a identifikace bezpečnostních i provozních rizik byly komplikované a společnost nedokázala účinně plnit nové legislativní požadavky.

Proto se jeho vedení rozhodlo nasadit technicky vyspělé řešení pro komplexní identifikaci a správu bezpečnostních informací a událostí (SIEM – Security Information and Event Management), které umožňuje shromažďovat vybrané záznamy logů z infrastruktury v reálném čase a následně je analyzovat, dávat do souvislostí a hlásit případné nesrovnalosti s bezpečnostními zásadami.

## Řešení

Volba padla na jeden z nejrozšířenějších systémů SIEM, QRadar od IBM, který analytici společnosti Gartner již podvanácté v řadě zařadili mezi lídry na trhu.

QRadar umožňuje zaznamenávat data nejen z IT infrastruktury, ale také z tzv. OT prostředí, tedy z průmyslových technologií. Díky nadstavbě Watson navíc může využívat prvky umělé inteligence, které pomáhají při vyšetřování a vyhodnocování událostí a automatizují řadu rutinních manuálních úkonů, čímž poskytují odborníkům podrobné podklady k rozhodování a uvolňují jim ruce pro sofistikovanější práci.

Kvalitní nástroj SIEM je sám o sobě důležitým předpokladem účinné kybernetické ochrany a splnění legislativních požadavků. Pro maximalizaci přínosů a přidané hodnoty je ale zásadní kvalitní implementace s detailním přizpůsobením celého řešení.

CASE STUDY

# IBM QRADAR

ENERGETIKA A DISTRIBUCE

SOITRON

## Nasazení

Firma se spolehla na integrační služby společnosti SOITRON s.r.o., která má rozsáhlé zkušenosti s budováním infrastruktur, propojováním různých systémů a zabezpečením technologií a dat proti kybernetickým rizikům. Subdodavatelem na tomto projektu byla společnost AXENTA s.r.o. Díky této spolupráci společnost SOITRON dokázala urychlit implementaci celého řešení.

Nezbytnou součástí projektu byla rozsáhlá analýza, která byla zvlášť důležitá kvůli široké škále technologické infrastruktury, včetně softwarových systémů vyvinutých na zakázku. Následovala integrace systému QRadar se síťovými a bezpečnostními zařízeními, servery, operačními systémy, aplikacemi a dalšími (nejen) IT systémy.

Ačkoli má QRadar zabudovanou řadu předdefinovaných scénářů, každá organizace je specifická, takže je vždy nutné přizpůsobit SIEM individuálním potřebám a podmínkám. Pro zákazníka SOITRON s.r.o. rozšířil QRadar o desítky relevantních scénářů, na které systém reaguje. Reakce může spočívat v upozornění odpovědného zaměstnance na potenciální riziko, ale také v automatizovaném kroku, například v zablokování podezřelé komunikace. Právě kvůli detailnímu přizpůsobení a integraci většího množství systémů pracovali odborníci společnosti SOITRON s.r.o. na projektu více než rok. Technologické prostředí velkého distributora energií se neustále mění, takže ho asi nikdy nelze považovat za zcela dokončené. K naplnění poslání firmy i očekávání zákazníků to ale není vůbec nutné.

„Bezpečnostní odbor klienta správně vyhodnotil rizika v prostředí průmyslových řídicích systémů, a proto byl součástí projektu také sběr a vyhodnocení bezpečnostních událostí z tzv. OT prostředí. Samotné prostředí systémů ICT zákazníka je rozsáhlé a různorodé. Pokud projekt implementace technologie SIEM zahrnuje IT i OT, zvláště pokud jde o velkou organizaci, je třeba vzít v úvahu časovou náročnost a zapojení pracovníků z více oborů IT/OT.“


**Maroš Rajnoch**
Soitron, Architekt bezpečnostních řešení

CASE STUDY

# IBM QRADAR

ENERGETIKA A DISTRIBUCE

## Přínosy

Přesné nastavení sběru dat do systému QRadar z IT i OT prostředí, definice desítek scénářů, které můžou potenciálně vyústit v provozní nebo bezpečnostní problémy, a pomocná ruka umělé inteligence pozvedly úroveň kybernetické bezpečnosti na novou úroveň. Zároveň jí umožnily snadno plnit legislativní povinnosti, jako je například podrobné zaznamenávání a hlášení incidentů.

Klíčovou roli v projektu hrála integrace provedená Soitronem. Bez přidané hodnoty v podobě ladění a přizpůsobení prostředí organizace je totiž funkčnost jakéhokoli systému SIEM do značné míry omezena na pouhou agregaci záznamů z logů. To samo o sobě nemusí správcům a bezpečnostním specialistům usnadnit práci – naopak je to zahltí daty.

Dobře nasazený systém SIEM poskytuje týmům IT nástroj, díky kterému mají neocenitelný přehled o dění v celé technologické a průmyslové infrastruktuře. Můžou pak lépe identifikovat nejen bezpečnostní, ale také provozní rizika nebo chyby v konfiguraci, které by mohly vést ke zbytečným výpadkům služeb. QRadar se zároveň stal bezpečným centrálním úložištěm všech logů, což umožňuje zjednodušit vyšetřování předchozích incidentů a prevenci jejich opakování.

Projekt implementace řešení SIEM a jeho technologická a procesní integrace u zákazníka probíhaly ve vícero fázích. Tento způsob umožnil efektivně využít lidské zdroje a důsledně uzavřít jednotlivé funkční celky i v tak rozsáhlé a komplexní infrastruktuře, jakou zákazník provozuje. Již během implementace začal zákazník intenzivně využívat platformu IBM QRadar SIEM. Připojování dalších systémů IKT a zvýšení detailu auditních záznamů postupně narůstalo se zvýšeným rizikem kybernetických hrozeb na Slovensku v letech 2021/2022. Licenční rozšiřování v původním modelu se tak stalo finančně náročné, a proto zákazník využil migraci do nového licenčního programu IBM Cloud Pak for Security. V rámci řešení IBM QRadar SIEM jsme tak dokázali vyhodnocovat více než 10násobek původně navrhovaného počtu událostí a zároveň umožnili výkonnostně škálovat řešení bez licenčních omezení. IBM Cloud Pak for Security obsahuje stack bezpečnostních aplikací, které výrazně obohacují a rozšiřují působnost samotného řešení SIEM. Zásadní rozvoj jsme tak uskutečnili i následnou automatizací s využitím platformy IBM QRadar SOAR.

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

Společnost Soitron je středoevropský integrátor, který působí na IT trhu již od roku 1991. Filozofií společnosti je snaha o neustálý pokrok. I proto je Soitron lídrem v zavádění jedinečných technologií a inovativních řešení. Svým klientům nabízí produkty a služby v oblasti robotizace a automatizace procesů, kybernetické bezpečnosti, datových center, IoT řešení, IT outsourcingu, komunikačních a síťových řešení, IT supportu a poradenství. Do produktového portfolia společnosti patří také řešení pro chytrá policejní auta – Mosy a služby v oblasti kybernetické bezpečnosti – VOID Security Operations Center.
Soitron je členem skupiny Soitron Group, ve které pracuje přes 800 mezinárodních odborníků. Skupina sdružuje profesionální týmy na Slovensku, v České republice, Rumunsku, Turecku, Bulharsku, Polsku a Velké Británii.