UNIPROG
Unique is the new different

Case Study

MONETA Money Bank, a.s.

Zabezpečení systémů pomocí Microsoft Azure Sentinel

PROJEKT V KOSTCE

ODVĚTVÍ

Bankovnictví

O ZÁKAZNÍKOVI

- Nejlepší banka roku 2021 (dle HN)
- Na českém trhu od r. 1997
- Lídr v mobilním bankovnictví

VÝSTUP PROJEKTU

- Implementace Microsoft Azure Sentinel pro zabezpečení dat v cloudu i lokální firemní síti
- Vyškolení interního cyber security týmu
- Dokumentace a analýza nákladů na provoz

Microsoft
PARTNER PROJEKTU

KLÍČOVÉ BENEFITY

- Flexibilní propojení se Salesforce
- Jasné pracovní scénáře
- Workshopy o architektuře Microsoft Sentinel a předání dovedností

POZADÍ PROJEKTU

Interní tým pro kybernetickou bezpečnost banky MONETA Money Bank se rozhodl adoptovat novou generaci SIEM technologie pro analýzu a hlášení bezpečnostních hrozeb, Microsoft Azure Sentinel. Jednoznačnou výhodou cloudového řešení přímo od Microsoftu jsou jeho široké možnosti integrace a přirozená kompatibilita s prostředím Microsoft 365.

Microsoft Sentinel pomocí umělé inteligence v cloudu Azure vyhodnocuje podezřelé události dříve, než se z nich stanou bezpečnostní incidenty, a zároveň automatizuje návazné akce.

MONETA Money Bank se rozhodla nový nástroj nejprve opilotovat v rámci Proof of Concept (PoC) projektu a zjistit přínosy a potenciál produktu do budoucna.

ŘEŠENÍ UNIPROGU & MICROSOFTU

Tým UNIPROGu společně s týmem Microsoftu zahájil projekt úvodním workshopem s představením systému Azure Sentinel a analýzou požadavků a priorit zákazníka.

V další fázi byla připravena Azure subscripce a definice bezpečnostních přístupů. Poté už byl implementován pracovní prostor Azure Sentinel a připojeny lokální zdroje, Active Directory, syslogy a aplikace Salesforce. Byly definovány workbooky, analytika, dotazy do databáze (tzv. „hunting queries“) a parsery tak, aby bezpečnostní monitoring pokryl zvolené on-premise i cloudové systémy zákazníka.

Na závěr byla předána precizní dokumentace a vypočítány odhady budoucích nákladů. Microsoft Sentinel se osvědčil jako plnohodnotné SIEM řešení a je připravený na další využití.

BENEFITY SPOLUPRÁCE

Flexibilní propojení se Salesforce

V rámci přechodu na cloudovou platformu jsme napojili aplikaci, která nebyla součástí dosavadního systému zákazníka.

Jasné pracovní scénáře pro interní tým

Vytvořili jsme přehledné dashboardy s vizualizací dat a na míru napsali dotazy do databáze, např. sledování pokusů o přihlášení z podezřelých lokalit nebo nebo hlášení případů mazání obsahu jinému uživateli.

Workshopy a předání dovedností

Naučili jsme interní tým správně interpretovat bezpečnostní hlášky a samostatně si napsat dotaz do databáze. Seznámili jsme je také s potenciální rozšiřitelností Microsoft Sentinel do budoucna.

ZAJÍMAVÁ ČÍSLA

20 000

událostí za sekundu

Škálovatelnost Azure Sentinel v cloudu umožňuje analýzu velkého množství bezpečnostních událostí za krátký čas.

500 GB

dat denně

Integrované strojové učení prochází obrovské objemy dat efektivně a minimalizuje výskyt falešně pozitivních výsledků.

SLOVY ZÁKAZNÍKA

„UNIPROG se v tomto pilotním projektu prokázal jako odborník – implementace nástroje Microsoft Azure Sentinel v našem prostředí a následné napojování zdrojů logů probíhalo velmi hladce. Během workshopů jsme poté byly seznámeni s fungováním samotného nástroje tak, abychom jej mohli plnohodnotně využívat pro bezpečnostní monitoring ve skupině MONETA.“

ING. JAKUB PTÁČNÍK
MONETA Money Bank, a.s.