BEARCLAVE

Report z analýzy

Microsoft Sentinel — optimalizace nákladů a detekcí

Verze	1.0
Zpracoval	Bearclave s.r.o.
Klasifikace	Veřejné — vzorový dokument

Bearclave s.r.o., Třešňová 916/16, Přímětice, 669 04 Znojmo
IČO 30007534 · DIČ CZ30007534 · zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 153837
info@bearclave.cz · bearclave.cz

1. Manažerské shrnutí

374 000 Kč	170 000 Kč	71 %	19 dní
měsíční náklad dnes	měsíčně po úpravách	incidentů je planý poplach	bez záznamů z e-shopu

Zhruba polovinu nákladu na dohled tvoří data, ze kterých nečte žádná detekce ani analytik. Po úpravách klesne měsíční náklad přibližně o 204 000 Kč, aniž by se ztratila jediná použitelná detekce.

Nejnaléhavější ale není cena. Ze dvou serverů e-shopu 19 dní nechodí žádné záznamy a nikdo o tom neví. Šest pravidel navíc vytváří tři čtvrtiny všech incidentů a sedm z deseti incidentů je planý poplach.

Doporučujeme začít obnovou a hlídáním sběru, pak omezit zbytečná data a nakonec ladit pravidla.

Nálezy podle priority



2. Rozsah a metoda

Prostředí	Hodnota
Pracovní prostor	jeden, region West Europe
Objem dat	96 GB denně, platba průběžně podle objemu
Zdroje	Defender XDR, Entra ID, aktivita Azure a Microsoft 365, události Windows ze 180 serverů, 2 firewally FortiGate, Syslog
Pravidla a incidenty	64 aktivních pravidel, 3 710 incidentů za 90 dní
Licence	Microsoft 365 E5, 1 450 uživatelů

Analýza pokrývala náklady a objem dat podle tabulek, retenci a cenový model, analytická pravidla a klasifikaci incidentů, pokrytí technik útoku, zdraví konektorů a automatizaci. Pracovalo se jen se čtením.

2.1 Proti čemu se měřilo

- Objektivní metriky: účtovaný objem ze sloupce _BilledSize, nákladová data za tři měsíce, klasifikace uzavřených incidentů, mapování pravidel na MITRE ATT&CK.
- Posouzení v kontextu: která drahá data jsou potřeba pro vyšetřování nebo pro doložení regulátorovi, i když z nich dnes nečte žádné pravidlo.

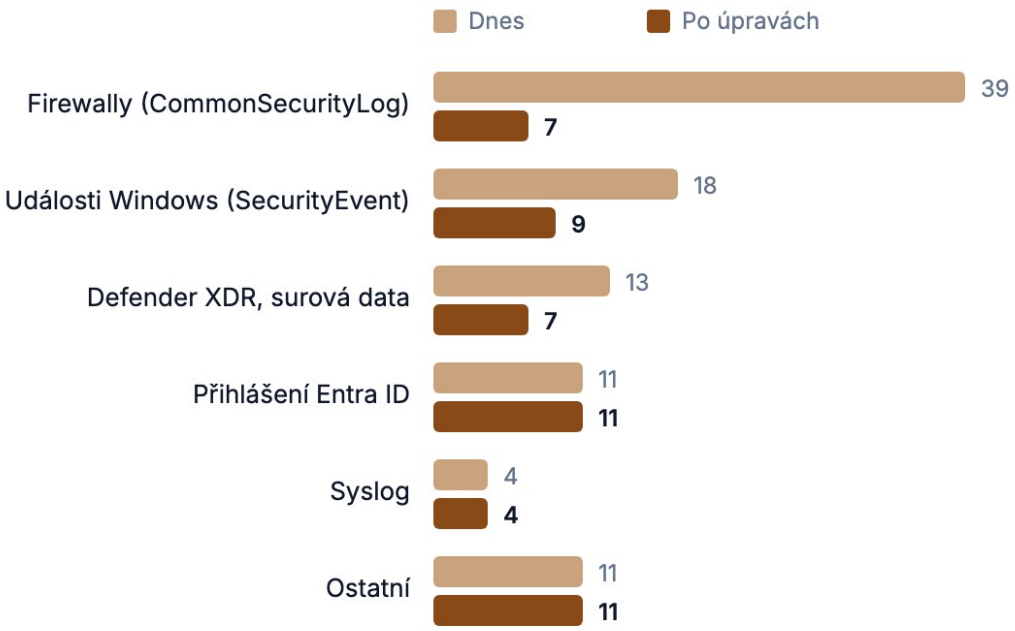
2.2 Co analýza není

- Nasazení nových konektorů ani psaní nových detekcí — návrhy jsou v reportu, implementace je navazující práce.
- Provoz dohledu a reakce na incidenty, kterou zajišťuje externí dohledové centrum.
- Audit souladu ani penetrační test.

3. Náklady

Nejvíc stojí data z firewallů, která z velké části popisují povolený provoz. Graf ukazuje denní objem v analytické úrovni podle zdroje dnes a po úpravách.

Denní objem v analytické úrovni (GB)



Položka	Dnes měsíčně	Po úpravách
Ingesce do analytické úrovně	348 000 Kč	164 000 Kč
Retence nad zahrnutých 90 dní	26 000 Kč	1 000 Kč
Data lake pro provoz firewallů	—	5 000 Kč
Celkem	374 000 Kč	170 000 Kč

> Dnešní stav je průměr posledních tří zúčtovacích období. Stav po úpravách je výpočet podle veřejného ceníku West Europe, kurzem 23 Kč/USD a bez smluvních slev. Datový grant licencí E5 (5 MB na uživatele a den) pokrývá 7 GB denně v obou případech. Částky jsou zaokrouhlené na tisíce.

4. Nálezy

Tři nálezy v plném znění. Všech deset je v registru nálezů v příloze.

4.1 N-001 — Firewally posílají celý povolený provoz, který nikdo nečte

Vlastnost	Hodnota
Oblast	Data, za která se platí zbytečně
Priorita	**Vysoká**
Pracnost	Střední
Úspora měsíčně	přibližně 120 000 Kč

4.1.1 Zjištěný stav

Tabulka CommonSecurityLog tvoří 41 % objemu (39 GB denně). 83 % řádků jsou povolená a ukončená spojení. Z 64 pravidel čtou tabulku dvě a obě pracují jen se zablokovaným provozem a s událostmi webového filtru a IPS.

Ověření: objem podle kategorie a akce za 30 dní

```
CommonSecurityLog
| where TimeGenerated > ago(30d)
| summarize GB = round(sum(_BilledSize) / 1e9, 1)
    by DeviceEventCategory, DeviceAction
| order by GB desc
```

4.1.2 Dopad

Přibližně 125 000 Kč měsíčně za data, ze kterých nevzniká žádný incident. Objem roste s každou pobočkou.

4.1.3 Doporučení

- Na pravidle sběru dat (DCR) nastavit transformaci, která do analytické úrovně pustí jen zablokovaný provoz a události mimo provoz.
- Povolená spojení odklonit druhým tokem do tabulky v úrovni data lake. Zůstanou dostupná pro vyšetřování za zlomek ceny.
- Obě dotčená pravidla týden provozovat souběžně a ověřit, že dostávají stejná data.

Transformace na pravidle sběru dat

```
source
| where not(DeviceEventCategory startswith "traffic"
    and DeviceAction in ("accept", "close", "timeout"))
```

4.2 N-006 — Šest pravidel tvoří 78 % incidentů, většina je planý poplach

Vlastnost	Hodnota
Oblast	Analytická pravidla
Priorita	**Vysoká**
Pracnost	Vysoká

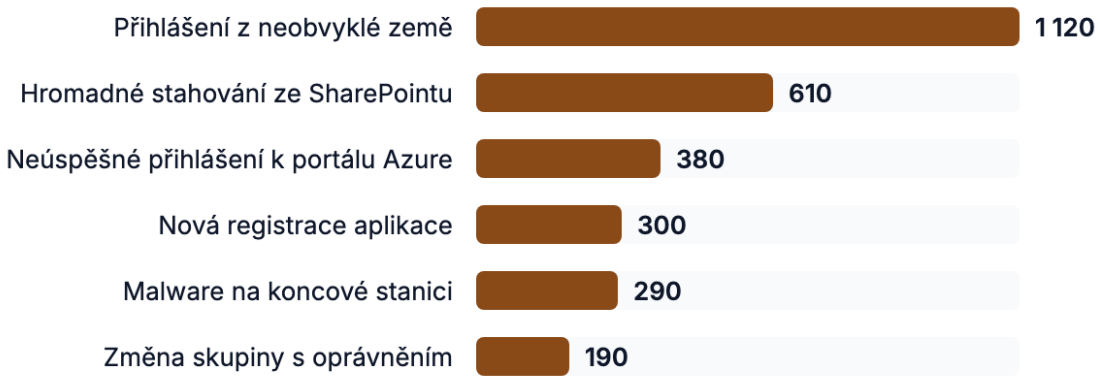
4.2.1 Zjištěný stav

Za 90 dní vzniklo 3 710 incidentů, přes 40 denně. Šest pravidel převzatých ze šablon bez úpravy tvoří 78 % z nich.

Klasifikace incidentů za 90 dní



Incidenty šesti nejhlučnějších pravidel za 90 dní



4.2.2 Dopad

Analytici zavírají incidenty těchto pravidel hromadně a skutečný nález od stejného pravidla zapadne. Za hluk se platí dvakrát — v datech a v hodinách dohledového centra.

4.2.3 Doporučení

- Výstupní adresy organizace a partnerů do watchlistu a vyloučit je z pravidel na neobvyklé přihlášení.
- U dvou pravidel sloučit výstrahy do jednoho incidentu podle uživatele a zvýšit práh.
- Pravidlo na malware vypnout — duplikuje incident, který přichází z Defender XDR.
- Úpravy nasazovat po jedné a po čtyřech týdnech znovu změřit podíl planých poplachů.

4.3 N-008 — Sběr ze dvou serverů e-shopu 19 dní nefunguje

Vlastnost	Hodnota
Oblast	Zdraví konektorů
Priorita	**Vysoká**
Pracnost	Nízká

4.3.1 Zjištěný stav

Ze dvou linuxových serverů s reverzní proxy e-shopu nepřišel 19 dní žádný záznam. Po aktualizaci systému přestal rsyslog předávat data agentovi. Monitorování zdraví Sentinelu není zapnuté.

Ověření: zdroje, které přestaly posílat data

```
Syslog
| where TimeGenerated > ago(30d)
| summarize Posledni = max(TimeGenerated) by Computer
| where Posledni < ago(24h)
```

4.3.2 Dopad

Tři týdny chybí záznamy z nejexponovanější části prostředí. Průnik přes e-shop by v tom období nešel vyšetřit.

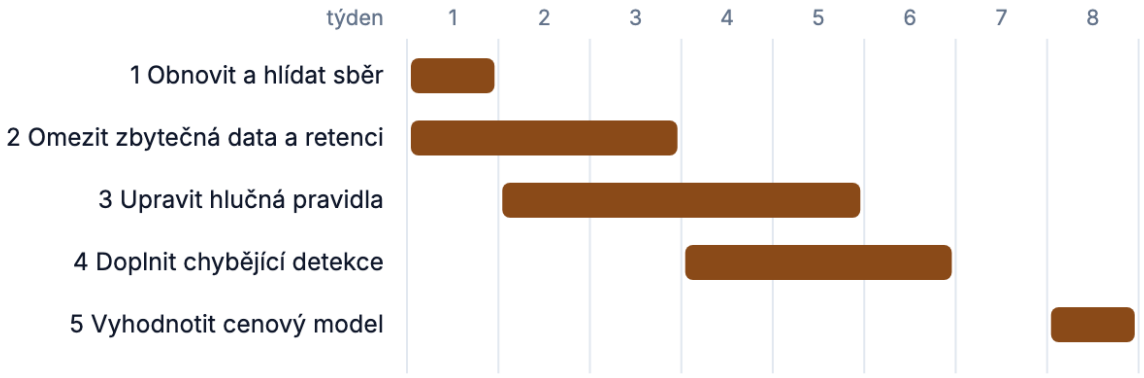
4.3.3 Doporučení

- Obnovit konfiguraci rsyslog a ověřit příjem.
- Zapnout monitorování zdraví (tabulka SentinelHealth).
- Přidat pravidlo, které vytvoří incident, když kritický zdroj mlčí déle než dvě hodiny. Seznam kritických zdrojů vést ve watchlistu.

5. Roadmapa

Pořadí stojí na závislostech. Cenový model se posuzuje až nakonec, protože úroveň závazku se dá snížit nejvýš jednou za 31 dní a musí vycházet z objemu po úpravách.

Harmonogram (týdny)



Krok	Obsah	Nálezy	Pracnost
1	Obnovit sběr a hlídat výpadky zdrojů	N-008	Nízká
2	Omezit data z firewallů a událostí Windows, zrušit duplicitní sběr, zkrátit analytickou retenci	N-001, N-003, N-004, N-009	Střední
3	Upravit šest nejhlučnějších pravidel, automatizovat opakované uzavírání	N-006, N-010	Vysoká
4	Doplnit detekce nad daty, která se už platí	N-005, N-007	Střední
5	Po měsíci stabilního objemu vyhodnotit cenový model	N-002	Nízká

> Kdyby se kroky 2 a 3 odložily o víc než měsíc, vyplatí se mezitím přejít na úroveň závazku 100 GB denně. Při dnešních 89 účtovaných GB denně ušetří sama o sobě kolem 80 000 Kč měsíčně.

6. Přílohy

6.1 Registr nálezů

ID	Nález	Priorita	Pracnost	Úspora/měs.
N-001	Firewally posílají celý povolený provoz	Vysoká	Střední	120 000 Kč
N-002	Úroveň závazku se po úpravách nevyplatí, zůstat na průběžné platbě	Nízká	Nízká	—
N-003	Události Windows v režimu všech událostí, 44 % objemu tvoří povolená spojení	Střední	Nízká	31 000 Kč
N-004	Retence 180 dní v analytické úrovni, přitom zahrnuto je 90 dní	Střední	Nízká	25 000 Kč
N-005	Tři pravidla čtou tabulky, do kterých nic neteče	Střední	Střední	—
N-006	Šest pravidel tvoří 78 % incidentů	Vysoká	Vysoká	—
N-007	Surová data z koncových stanic, ze kterých čtou tři pravidla	Nízká	Nízká	23 000 Kč
N-008	Sběr ze dvou serverů e-shopu 19 dní nefunguje	Vysoká	Nízká	—
N-009	Dvě pravidla sběru dat posílají tytéž události dvakrát	Střední	Nízká	4 000 Kč
N-010	38 % incidentů se zavírá ručně se stejným komentářem	Nízká	Nízká	—

6.2 Revize pravidel — výřez

Úplná revize obsahuje všech 64 pravidel. Tady je šest, která tvoří většinu incidentů.

Pravidlo	Incidenty 90 dní	Plané	Návrh
Přihlášení z neobvyklé země	1 120	96 %	Vyloučit výstupní adresy z watchlistu
Hromadné stahování ze SharePointu	610	88 %	Práh podle role, vyloučit zálohovací účet
Neúspěšné přihlášení k portálu Azure	380	91 %	Sloučit do incidentu podle uživatele
Nová registrace aplikace	300	74 %	Vyloučit automatizační účet správy
Malware na koncové stanici	290	63 %	Vypnout, duplikuje Defender XDR
Změna skupiny s oprávněním	190	58 %	Ponechat, doplnit mapování entit