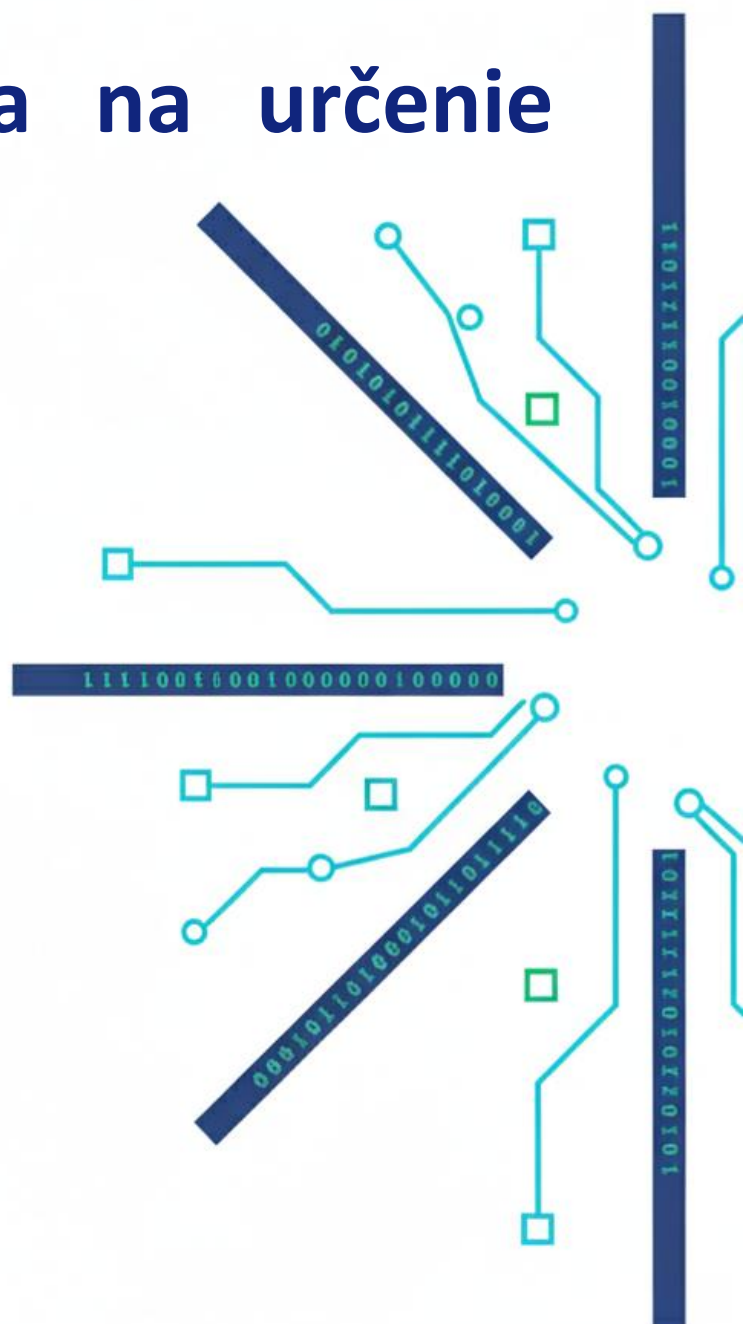


D21 – Metóda na určenie časového rámca a fáz útoku



Projekt Automatizácia digitálnej forenznej analýzy a odpovede na incident (ADFIR) financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079.

Obsah

1	Popis projektu.....	2
2	Úvod	3
3	Časové rady.....	4
4	Metóda na určenie časového rámca a fáz útoku	5
4.1	Vstupy a výstupy navrhovanej metódy	5
4.2	Kroky metódy.....	5
4.3	Vytvorenie časových radov z artefaktov operačného systému Windows	6
4.3.1	Voľba šírky okna	7
4.3.2	Chýbajúca hodnota nie je nula	7
4.4	Výber relevantných časových radov.....	8
4.4.1	Pokrytie	8
4.4.2	Aktivita	8
4.4.3	Variabilita	8
4.4.4	Duplicitné časové rady	9
4.5	Detekcia anomálií v jednotlivých časových radoch.....	10
4.5.1	Typy anomálií	10
4.5.2	Štatistické metódy	12
4.5.3	Metódy založené na modeli.....	13
4.5.4	Metódy nad úsekmi radu	13
4.5.5	Spektrálne metódy	14
4.5.6	Detekcia zmien režimu	14
4.5.7	Hlboké učenie.....	15
4.6	Agregácia anomálií naprieč časovými radmi.....	15
4.6.1	Časová tolerancia ϵ	15
4.6.2	Hlasovanie	16
4.6.3	Prah θ	16
4.6.4	Zlúčenie časových okien do fáz	16
4.7	Určenie časového rámca incidentu	16
4.8	Charakterizácia a interpretácia fáz incidentu	17
5	Záver.....	20
6	Bibliografia.....	21
7	Príloha.....	24
7.1	Popisy vybraných časových radov pre EVTX	24
7.2	Popisy vybraných časových radov pre MFT a journal.....	29
7.3	Popisy vybraných časových radov pre MFT	34
7.4	Popisy vybraných časových radov pre register	36
7.5	Popisy vybraných časových radov pre SRUM.....	37
7.5.1	AppResourceUseInfo.....	37
7.5.2	AppTimelineProvider	42

1 Popis projektu

Projekt **Automatizácia digitálnej forenznej analýzy a odpovede na incident** (ďalej len „ADFIR“) je financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079. Tento projekt sa zaoberá jednou z kľúčových výziev v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti – ako spracovať obrovské množstvo digitálnych dôkazov, ktoré vznikajú počas incidentov kybernetickej bezpečnosti alebo forenznych vyšetrovaní. V súčasnosti je tento proces veľmi náročný z hľadiska ľudských zdrojov a času. Automatizácia pomocou metód strojového učenia môže preto výrazne **zlepšiť kvalitu digitálnej forenznej analýzy** a skrátiť čas potrebný na jej vykonanie. Celkovo to umožňuje bezpečnostným tímom efektívnejšie reagovať na kybernetické hrozby. Hlavné prínosy tohto projektu sú:

- **Rýchlejšie riešenie incidentov v oblasti kybernetickej bezpečnosti.** Projekt ADFIR zavádza automatizované prístupy k zberu, spracovaniu a analýze digitálnych stôp. Vďaka tomu môžu bezpečnostné tímy rýchlejšie identifikovať príčiny incidentov a prijať účinné opatrenia na ich riešenie.
- **Zníženie pracovnej záťaže forenznych analytikov.** Rutinné a časovo náročné úlohy spojené so spracovaním digitálnych stôp budú nahradené automatizovanými metódami. To umožní analytikom sústrediť sa na zložitejšie prípady a strategické rozhodovanie.
- **Vyššia kvalita a konzistentnosť výstupov.** Použitie jednotných metodík a nástrojov zaručuje, že spracované digitálne stopy budú presnejšie, konzistentnejšie a ľahšie overiteľné. To výrazne znižuje riziko chýb spôsobených ľudskými faktormi.
- **Možné využitie v trestnom konaní.** Výstupy projektu budú vyvinuté v súlade s právnymi požiadavkami a normami, čo umožní, aby digitálne stopy boli akceptované ako relevantné dôkazy pre vyšetrovanie a súdne konania.

2 Úvod

V rámci tejto časti projektu ADFIR sa zameriame na vývoj metódy pre rekonštrukciu a analýzu digitálnych stôp prostredníctvom analýzy časových radov. Strategickým cieľom je posunúť forenznú analýzu od manuálneho prehliadania logov k (polo)automatizovanému určeniu časového rámca začiatku útoku a fáz útoku.

V prvej testovacej fáze sa ukázalo, že dáta z nástroja PLASO [1] (napr. údaje z prípadu The Stolen Szechuan Sauce [2], ktoré rozoberáme vo výstupe D14 - Syntetický dataset) obsahujú viacero časových rámcov bez údajov. To výrazne ovplyvňuje kvalitu a použiteľnosť časových radov.

V ďalšej fáze sa vybrala množina extrahovaných relevantných artefaktov z rôznorodých zdrojov, ako sú súbory EVTX (Windows event logs), MFTE (Master File Table), SRUM (System Resource Usage Monitor), či register operačného systému Windows, ktoré boli použité na vytvorenie časových radov z vybraných simulovaných incidentov (The Stolen Szechuan Sauce, Magnet_CTF_2019, Magnet_CTF_2020 a Magnet_CTF_2022 – bližšie informácie vo výstupe D14 - Syntetický dataset).

Vytvorené časové rady budú použité na analýzu, ktorej cieľom je nasledovné:

- a) **Determinácia „Time Zero“ (Začiatku incidentu)** - automatizované vytváranie časových radov môže umožniť identifikovať prvú anomálnu aktivitu. Namiesto odhadu, kedy mohlo dôjsť k prelomeniu, systém poskytne objektívny dátový základ pre definovanie časového okna útočnej fázy.
- b) **Podpora automatizovanej detekcie anomálií pomocou ML** - vizuálna a štatistická analýza časových radov bude slúžiť ako vstupná vrstva pre strojové učenie (ML). Cieľom je výber modelov, ktoré dokážu v reálnom čase alebo post-facto detegovať anomálie vo frekvencii volaní systémových funkcií, zmenách metadát súborov alebo aktivitách aplikácií. Tieto anomálie predstavujú signály pre začiatok zložitých útokov, ktoré uniknú tradičným pravidlám (rule-based) detekcii.
- c) **Zvýšenie efektivity Incident Response (IR)** - vytvorená metóda môže umožniť automaticky kontextualizovať incidenty. Namiesto zoznamu tisícov event logov systém vygeneruje zredukovanú časovú os („attack timeline“), ktorá prepojí súvislé udalosti z rôznych zdrojov (napr. spustenie procesu -> zápis do registrov -> sieťová komunikácia). To výrazne skracuje čas reakcie a uľahčuje prácu forezným analytikom.

3 Časové rady

Časový rad sa bežne definuje ako postupnosť dátových hodnôt zaznamenaných v po sebe nasledujúcich časových bodoch. Tieto hodnoty sú typicky usporiadané chronologicky a často majú rovnaký časový odstup, hoci v niektorých kontextoch je možný aj nepravidelný rozostup. Z matematického hľadiska je teória časových radov súčasťou teórie náhodných procesov [3]:

Nech $(\Omega, \mathcal{A}, P)$ je pravdepodobnostný priestor a nech množina T je nejaká podmnožina množiny reálnych čísel $\mathbb{R}$. Nech $X(t)$ je pre každé $t \in T$ náhodná veličina definovaná na tom istom pravdepodobnostnom priestore $(\Omega, \mathcal{A}, P)$. Množinu $X(\cdot) = \{X(t), t \in T\}$ náhodných premenných $X(t)$ nazývame náhodný proces.

Náhodný proces $X(\cdot) = \{X(t), t \in T\}$ nazývame náhodný proces so spojitým časom, ak množina T je interval na reálnej osi $\mathbb{R}$.

Náhodný proces $X(\cdot) = \{X(t), t \in T\}$ nazývame náhodný proces s diskretným časom, ak množina T je spočítateľná podmnožina $\mathbb{R}$. Náhodné procesy s diskretným časom sa nazývajú tiež **časové rady**.

Pre jednoduchosť použijeme zjednodušené značenie, kde miesto náhodných premenných budeme pracovať s číselnými hodnotami.

Časový rad môže byť reprezentovaný ako:

$$X = \{x_{t_j} \mid j \in \mathbb{N}\},$$

kde x_{t_j} je číselná hodnota zaznamenaná v čase t_j . Ako vyplýva z definície, umožňuje aj nerovnomerný časový rozostup medzi jednotlivými hodnotami. Pre podmienku rovnakého časového odstupu ho môžeme zapísať ako:

$$X = \{x_i \mid i \in \mathbb{N}\},$$

kde x_i je číselná hodnota zaznamenaná v čase i . Prípadne ešte jednoduchšie:

$$X = x_0, \dots, x_t,$$

kde x_i predstavujú hodnoty časového radu usporiadané podľa času s indexom $i \in \mathbb{N}$ a $t \in \mathbb{N}$ je posledný časový index.

Časové rady nachádzajú uplatnenie v mnohých odvetviach pri zbieraní a analýze kľúčových dát. Medzi nich patrí napríklad meteorológia (zber nameraných hodnôt ako teplota, vlhkosť, ...), finančníctvo (akcie), energetika a verejné služby (spotreba elektriny a vody), kybernetická bezpečnosť (počet neúspešných pokusov o prihlásenie na SSH server, atď.), doprava, zdravotníctvo, poľnohospodárstvo, šport a ďalšie.

4 Metóda na určenie časového rámca a fáz útoku

Táto kapitola predstavuje metódu, ktorá je predmetom tohto výstupu. Metóda vychádza z predpokladu, že aktivita útočníka sa v operačnom systéme Windows neprejaví v jedinom zdroji dát, ale zanechá súbežnú digitálnu stopu vo viacerých na sebe relatívne nezávislých artefaktoch, napr. v záznamoch udalostí, v metadátach súborového systému, v registri alebo v štatistikách využívania systémových prostriedkov. Jednotlivo môže byť takáto digitálna stopa nevýrazná a nerozlíšiteľná od bežnej prevádzky operačného systému, resp. bežného správania sa používateľa. Ak sa však rovnaký časový úsek javí ako anomálny súčasne vo viacerých nezávislých časových radoch, pravdepodobnosť, že ide o náhodnú fluktuáciu, výrazne klesá. Metóda preto nehľadá „najväčšiu anomáliu“, ale časovú zhodu anomálií naprieč zdrojmi.

4.1 Vstupy a výstupy navrhovanej metódy

Vstup: množina forenzných artefaktov získaných z jedného skúmaného systému (EVTX, MFT/\$J, register, SRUM) spracovaných do podoby časových radov podľa kapitoly 4.3 spolu s časom akvizície obrazu.

Výstup metódy má tri zložky:

- **Časový rámec incidentu** – odhad intervalu $[\hat{t}_0, \hat{t}_1]$, kde $\hat{t}_0$ je odhadovaný začiatok incidentu („Time Zero“) a $\hat{t}_1$ jeho koniec, spolu s vyjadrením neistoty oboch hraníc.
- **Množina kandidátskych fáz útoku** – usporiadaná postupnosť disjunktných časových okien $F_1 < F_2 < \dots < F_K$, v ktorých bola zaznamenaná súbežná anomálna aktivita vo viacerých časových radoch.
- **Charakterizácia fáz** – pre každú fázu zoznam časových radov, ktoré k nej najviac prispeli, mieru dôveryhodnosti a návrh interpretácie (napr. priradenie k taktike podľa MITRE ATT&CK [4]).

4.2 Kroky metódy

Metóda pozostáva zo šiestich krokov, ktorým sú venované nasledujúce podkapitoly:

- 1) **Krok 1 – Vytvorenie časových radov z artefaktov operačného systému Windows** – z forenzných artefaktov sa vytvorí množina časových radov na spoločnej časovej osi.
- 2) **Krok 2 – Výber relevantných časových radov** - z vytvorenej množiny sa odfiltrujú rady, ktoré neposkytujú využiteľnú informáciu a redundantné rady sa zhlukujú a preváhujú.

- 3) **Krok 3 – Detekcia anomálií v jednotlivých radoch** - na každý rad sa nezávisle aplikuje viacero metód detekcie anomálií; ich skóre sa normalizujú, prahujú a kombinujú.
- 4) **Krok 4 – Agregácia anomálií naprieč radmi** - anomálie sa rozšíria o ε -okolie a hlasovaním sa určia časové okná, v ktorých je anomálnych aspoň θ -podiel radov. Tieto okná predstavujú kandidátske fázy útoku.
- 5) **Krok 5 - Určenie časového rámca incidentu** - minimum a maximum množiny potvrdených anomálnych časov určuje začiatok a koniec kybernetického bezpečnostného incidentu.
- 6) **Krok 6 - Charakterizácia a interpretácia fáz incidentu** - každej fáze sa priradia dominantné rady a navrhne sa jej forenzný význam.

4.3 Vytvorenie časových radov z artefaktov operačného systému Windows

Záznamy v artefaktoch vznikajú v nepravidelných časoch τ , kedykoľvek v systéme niečo nastane. Takýto zdroj zodpovedá časovému radu s nepravidelným odstupom $\{x_{\{t_j\}}\}$. Väčšina metód detekcie anomálií a najmä porovnávanie viacerých radov však vyžaduje rovnaký odstup a spoločné časové indexy. Preto sa časová os rozdelí na okná šírky Δ a pre každé okno i sa vypočíta jedna hodnota x_i .

Každý časový rad je určený dvoma vlastnosťami:

- **filtr** – ktoré záznamy sa berú do úvahy (napr. „kanál = Application“),
- **agregáciou** – ako sa spracujú záznamy v jednom okne (napr. sa aplikuje súčet, priemer).

Hodnota x_i = výsledok agregácie všetkých záznamov, ktoré prešli filtrom a ich čas τ spadá do okna i .

Výsledkom je rad $X = x_0, \dots, x_t$ s rovnakým časovým odstupom Δ , presne v tvare podľa definície v kapitole 3. Označme $X^{(m)}$ ako m -tý časový rad z množiny nami vytvorených časových radov, takže $x^{(m)}_i$ bude hodnota m -tého časového radu v časovom okne i . Všetky rady majú rovnaké indexy $0, \dots, t$, takže hodnota $x^{(m)}_i$ v rôznych radoch sa vždy týka toho istého časového okna.

Používané agregácie:

- **počet** – koľko záznamov nastalo v danom časovom okne (najčastejšie pri forenzných artefaktoch EVT, MFT a registri operačného systému),
- **súčet** – súčet číselnej hodnoty, napr. počet prenesených bajtov v danom časovom okne (typicky forenzný artefakt SRUM),

- **počet rôznych hodnôt** – napr. koľko rôznych EventID alebo používateľov sa v časovom okne objavilo. Takýto rad zachytí, keď útočník „rozširuje záber“ (prieskum, laterálny pohyb),
- **maximum** – najväčšia hodnota jedného záznamu v časovom okne, napr. najväčší objem dát, ktorý v danom časovom okne prečítala alebo zapísala jedna aplikácia. Na rozdiel od súčtu táto agregácia nezávisí od počtu záznamov v časovom okne, preto zvýrazní jednorazovú objemnú operáciu (napr. hromadné čítanie súborov pred exfiltráciou) aj v čase, keď v systéme prebieha veľa drobnej bežnej aktivity, ktorá by v súčte takúto operáciu zakryla.

Napríklad `ts_{'Channel': 'Application'}.csv` je počet záznamov z kanála Application v každom okne. Súbor `ts_['{SidType': 'LogonId}', 'BackgroundBytesRead']_value_BackgroundBytesRead.csv` je súčet prečítaných bajtov na pozadí pre záznamy typu LogonId. Zoznam vybraných časových radov je uvedený v prílohe.

4.3.1 Voľba šírky okna

Príliš krátke okno vytvorí rad plný núl, z ktorého sa nedá nič spoľahlivo odhadnúť. Príliš dlhé okno rozmazá krátku aktivitu útočníka v bežnej prevádzke. Vhodná šírka závisí od množstva zozbieraných dát. Čím je časové okno menšie, tým dostáva forenzná analytika presnejšie určenie rámca útoku. Na druhej strane to môže spôsobiť pri rozsiahlom obraze disku (niekoľko mesačné dáta) veľké množstvo časových rámcov.

Odporúčame spustiť metódu pre tri šírky okna (10, 30 a 60 minút) vzhľadom na celkový časový rámec analyzovaných údajov.

4.3.2 Chýbajúca hodnota nie je nula

Nula ($x_i = 0$) znamená, že forenzný artefakt v časovom okne i záznamy zaznamenával, ale v systéme nenastala žiadna udalosť, ktorá by spôsobila zápis. Chýbajúca hodnota znamená, že o okne i nemáme informáciu, pretože forenzný artefakt za toto obdobie neobsahuje žiadne záznamy, napr. obdobie pred najstarším zachovaným záznamom po rotácii logu EVT-X alebo obdobie mimo doby uchovávanía údajov v databáze SRUM. Ak sa tieto dva prípady zamenia, môžu nastať dve chyby. Buď vznikne falošná anomália na hranici dostupnosti zdroja, t. j. v časovom okne, v ktorom sa záznamy forenzného artefaktu začínajú alebo končia, alebo sa prehliadne skutočný výpadok záznamov v logu (napr. po jeho vymazaní).

Preto sa pre každý rad eviduje **pokrytie $C^{(m)}$ pre časový rad $X^{(m)}$** , t. j. množina indexov časových okien, za ktoré má zdroj dáta: $C^{(m)} = \{i_{\text{prvý}}, \dots, i_{\text{posledný}}\}$, kde $i_{\text{prvý}}$ je okno s najstarším a $i_{\text{posledný}}$ okno s najnovším záznamom artefaktu. Pokrytie sa určuje podľa rozsahu celého

artefaktu, nie podľa toho, kde má rad nenulové hodnoty. Pre okná v pokrytí ($i \in C^{(m)}$) je hodnota x_i platná aj vtedy, keď je nulová; mimo pokrytia ($i \notin C^{(m)}$) sa označí ako chýbajúca.

$$C^{(m)} = \{ i : i_{\text{prvý}} \leq i \leq i_{\text{posledný}} \},$$

kde $i_{\text{prvý}}$ je index okna, do ktorého padne najstarší záznam artefaktu, a $i_{\text{posledný}}$ index časového okna s jeho najnovším záznamom. Pokrytie sa určuje podľa rozsahu celého forenzného artefaktu, z ktorého časový rad vznikol (napr. celého logu security), nie podľa toho, v ktorých oknách má samotný rad nenulové hodnoty.

Odporúčame vytvoriť časový rad „počet zdrojov s dátami v časovom okne i“. Náhly výpadok záznamov v inak aktívnom kanáli je sám silným indikátorom (napr. vymazanie logu, EventID 1102).

4.4 Výber relevantných časových radov

Výber radov má byť založený na jasných a opakovateľných pravidlách, nie len na úsudku bezpečnostného analytika. Výber vhodných časových radov pre vybrané forenzné artefakty operačného systému Windows je uvedený v prílohe tohto dokumentu.

4.4.1 Pokrytie

Rad musí mať dáta aspoň za určitú časť okien 0, ..., t (odporúčane aspoň 30 %). Rady s malým pokrytím sa nevyraďujú, ale v oknách, kde nemajú dáta, sa nezapočítavajú do hlasovania.

4.4.2 Aktivita

Rad s niekoľkými nenulovými hodnotami x_i neumožňuje odhadnúť, čo je normálne. Každá jeho nenulová hodnota by automaticky vyzerala ako anomália.

Veľmi riedke rady sa spracujú inak: každé ich nenulové okno sa priamo považuje za **udalosť záujmu**. Typickým príkladom sú zmeny v kľúčoch automatického spúšťania (ASEP), kde je forenzne významná už samotná zmena.

4.4.3 Variabilita

Časový rad, ktorého hodnoty sa takmer nemenia, nenesie informáciu, a preto sa vyraduje. Mierou premenlivosti je variačný koeficient, t. j. podiel smerodajnej odchýlky a priemeru hodnôt radu v jeho pokrytí $C^{(m)}$ (odporúčaný prah uvádza Tabuľka 1).

Užitočným ukazovateľom je aj pomer rozptylu k priemeru (index disperzie). Ak je približne 1, hodnoty časového radu sa správajú ako počty nezávislých, náhodne nastávajúcich udalostí, t. j. zodpovedajú Poissonovmu rozdeleniu, pre ktoré sa rozptyl rovná strednej hodnote. Ak je pomer oveľa väčší ako 1 (nadmerný rozptyl), udalosti prichádzajú v zhlukoch a časový rad je „nárazový“. Pre takýto časový rad je vhodnejší model s negatívne binomickým rozdelením (kap. 4.5.3) pred použitím štatistických metód [5].

4.4.4 Duplicitné časové rady

Z forenzných artefaktov operačného systému Windows je možné vytvoriť veľké množstvo časových radov, ktoré sú z pohľadu toto, čo reprezentujú, veľmi podobné a redundantné. Napríklad z forenzného artefaktu SRUM je možné vytvoriť rôzne kombinácie typu účtu a druhu prenesených bajtov.

Keďže všetky rady majú spoločné indexy 0, ..., t, dajú sa priamo porovnať hodnotu po hodnote. Riešenie pre duplicitné časové rady:

1. zistí sa, ktoré časové rady sa správajú takmer rovnako (vysoká korelácia napr. nad 0,8),
2. takéto časové rady sa zoskupia,
3. každá skupina takmer rovnakých časových radov má pri hlasovaní spolu váhu jedného hlasu. Buď sa v skupine ponechajú všetky časové rady a hlas sa medzi ne rovnomerne rozdelí ($w_m = 1/|G|$, kde $|G|$ je počet radov v skupine), alebo sa ponechá len jeden reprezentant, napr. rad s najväčším pokrytím, s váhou $w_m = 1$ a ostatné časové rady sa vyradia.

Po tejto úprave možno určiť **efektívny počet nezávislých časových radov** $N_{eff} = \sum_m w_m$, t. j. súčet váh všetkých radov. Keďže každá skupina takmer rovnakých radov má spolu váhu jedného hlasu, N_{eff} vyjadruje, koľko navzájom nezávislých hlasov má hlasovanie v skutočnosti k dispozícii. Voči N_{eff} sa v kroku 4 nastavuje prah, ktorý určuje, koľko nezávislých radov sa musí zhodnúť, aby sa okno považovalo za anomálne.

Výber časových radov teda prebieha v štyroch krokoch. Najprv sa pre každý rad overí pokrytie, aktivita a variabilita. Rady, ktoré kritériá spĺňajú, sa ponechajú a veľmi riedke rady sa zaradia medzi bodové indikátory. Potom sa takmer rovnaké rady zoskupia a rozdelia sa im váhy. Nakoniec sa obmedzí celkový vplyv jedného zdroja. Kritériá a ich odporúčané hodnoty sumarizuje Tabuľka 1.

Kritérium	Čo sa meria	Odporúčaná hodnota	Účel
Pokrytie	podiel okien s dátami	$\geq 30 \%$	časový rad pod prahom sa nevyraďuje, iba sa označí
Aktivita	počet nenulových okien	≥ 100	dostatok dát na odhad bežného správania, časový rad pod prahom sa spracuje ako bodový indikátor
Variabilita	miera premenlivosti	$> 0,05$	vyradiť takmer konštantné časové rady
Duplicita	korelácia	0,9	zoskupiť takmer rovnaké časové rady a zabrániť dominancii jedného zdroja

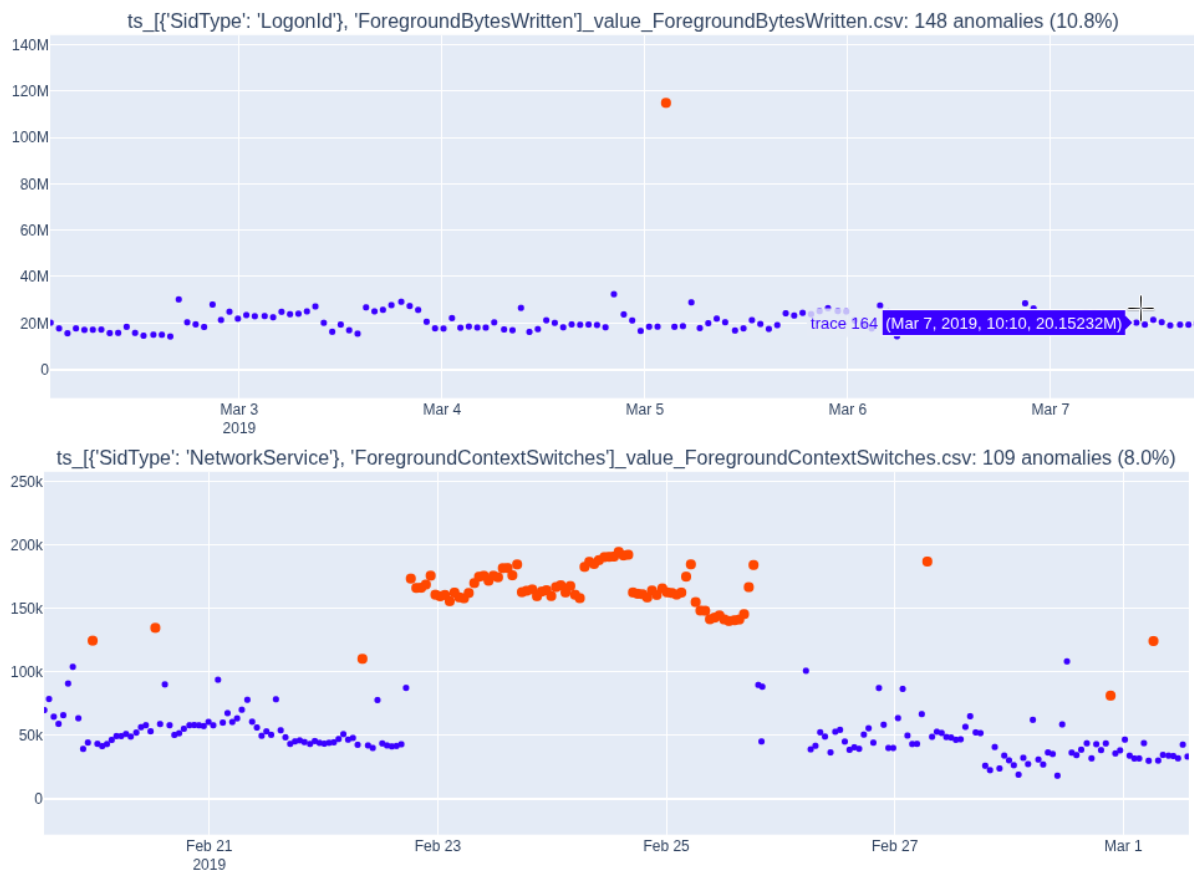
Tabuľka 1 - Kritériá výberu relevantných časových radov

4.5 Detekcia anomálií v jednotlivých časových radoch

4.5.1 Typy anomálií

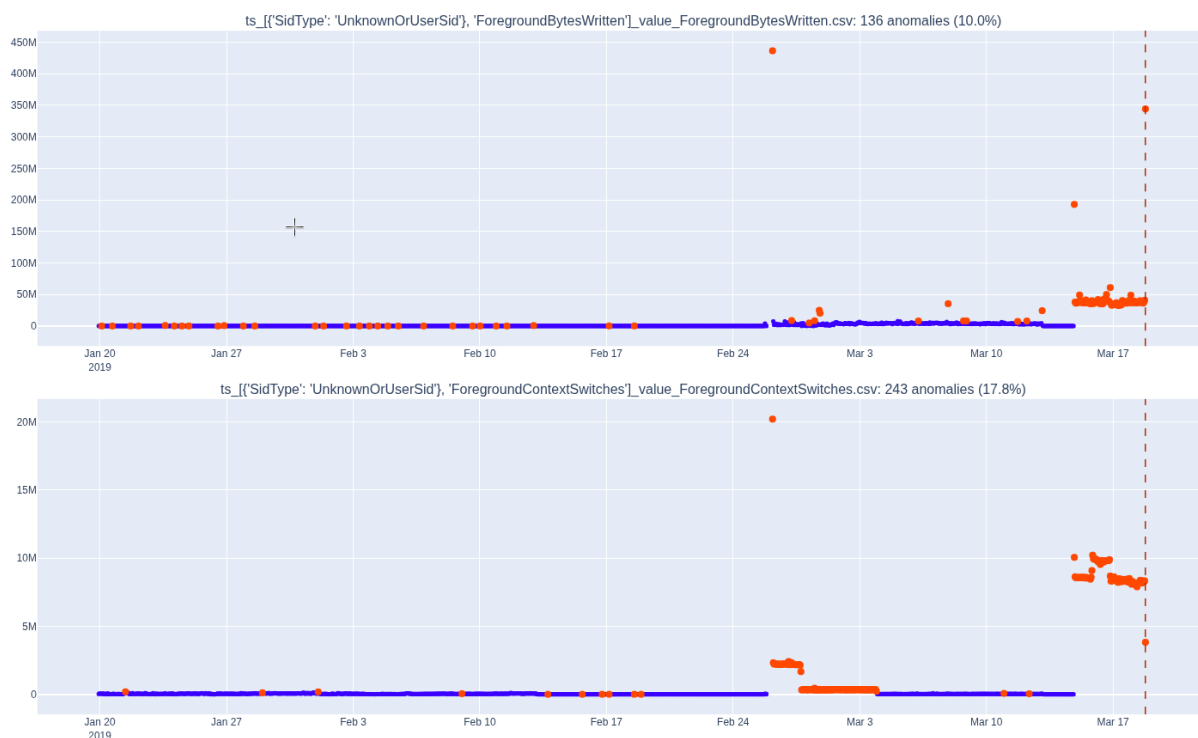
Rozlišujeme štyri typy anomálií [6,7], pričom každá zodpovedá inému správaniu útočníka a vyžaduje inú triedu metód:

- **Bodová anomália** – jediná hodnota výrazne mimo očakávaného rozsahu. Forenzne zodpovedá jednorazovej udalosti, a to napr. spusteniu nástroja, zápisu do kľúča automatického spúšťania, jednorazovému exportu dát. Obrázok č. 1 znázorňuje príklad bodovej anomálie.
- **Kontextová anomália** – hodnota, ktorá je sama osebe bežná, ale nezvyčajná vo svojom kontexte. Typickým prípadom je aktivita v čase, keď systém obvykle nepracuje (v noci, cez víkend). Bez modelovania dennej a týždennej sezónnosti sa tento typ anomálie nedá odhaliť. Z tohto dôvodu je tento typ je pri cielených útokoch najčastejší.
- **Kolektívna anomália (anomálna podpostupnosť)** – jednotlivé hodnoty sú v norme, ale ich postupnosť nie. Zodpovedá dlhšie trvajúcej aktivite, ako napr. exfiltrácii dát rozdelenej na menšie prenosy, pomalému skenovaniu, šifrovaniu súborov.
- **Zmena režimu (change point)** – trvalý posun strednej hodnoty, rozptylu alebo periodicity radu. Zodpovedá inštalácii perzistentného mechanizmu, zmene konfigurácie systému alebo vypnutiu bezpečnostnej služby. Fáza útoku je práve úsek medzi dvoma zmenami režimu. Na Obrázku č. 1 je ukážka tejto anomálie.



Obrázok 1 - Príklad bodovej anomálie (hore) a príklad zmeny režimu (dole).

Následne prechádzame k implementácii automatizovaných metód na detekciu anomálií. Testujeme viacero algoritmov s rôznou výpočtovou náročnosťou a citlivosťou [8], pričom ich presnosť, robustnosť a schopnosť lokalizovať počiatočný bod útoku, či rôzne podozrivé miesta sa vyhodnocuje ručne. Pri kvantitatívnom vyhodnotení na označených kybernetických bezpečnostných incidentoch treba použiť metriky pre intervaly [9], nie bodové metriky s úpravou point-adjust, ktorá výsledky nadhodnocuje [10]. Tento proces by mal umožniť vybrať najvhodnejšiu metódu pre oddelenie normálnej systémovej záťaže od útočníckej aktivity.



Obrázok. 2: Ukážka analýzy anomálií pre tabuľku Application Resource Usage forenzného artefaktu SRUM na viacerých časových radoch v rámci jedného incidentu.

Ďalší z prístupov bol založený na analýze nájdených anomálií na viacerých časových radoch v rámci jedného incidentu naraz. Táto analýza nám umožňuje sledovať potencionálnu činnosť útočníka z rôznych pohľadov (sieťová, disková, systémová, ... aktivita) a tak lepšie odhadnúť napríklad počiatkový bod útoku. Ukážku je možné vidieť na Obrázku č. 2. Tejto analýze sa viac venujeme v kroku 4.

Dôležitou súčasťou je manuálne porovnávanie časových radov a nájdených anomálií v rámci jedného typu časového radu naprieč rôznymi simulovanými incidentmi, čo môže umožniť identifikovať zaujímavé udalosti, na ktoré sa treba sústrediť všeobecne.

4.5.2 Štatistické metódy

Štatistické metódy sú rýchle a dobre vysvetliteľné, čo je vo forenznej praxi dôležité.

Prvým príkladom štatistickej metódy je **odolné z-skóre [11]**. Meria, o koľko typických odchýlok (MAD) je hodnota x_i vzdialená od mediánu radu. Hodnota je anomálna, ak je vzdialenosť väčšia ako zvolený prah (typicky 3 až 5). Ak je viac ako polovica hodnôt nulová, typická odchýlka je nula a metóda nefunguje. Takéto rady patria medzi bodové indikátory.

Ďalším príkladom je **medzikvartilové rozpätie (IQR)**. Hodnota je anomálna, ak leží príliš ďaleko nad horným alebo pod dolným kvartilom. Počtové dáta sú však nesúmerné (majú dlhý chvost smerom hore) a bežný IQR by tam hlásil veľa falošných nálezov. Preto sa používa **upravený boxplot [12]**, ktorý hranice posúva podľa miery nesúmernosti.

Iným príkladom štatistickým metód je **kľazové okno**. Každá hodnota x_i sa porovnáva s mediánom okolitých hodnôt. Dôležité: ak porovnávací úsek obsahuje aj samotnú hodnotu x_i , anomália ovplyvní vlastné porovnanie. Preto sa má x_i porovnávať **len s predchádzajúcimi hodnotami** $x_{i-1}, x_{i-2}, \dots$, čo zároveň zodpovedá priebežnému monitorovaniu.

Posledné uvedené príklady štatistických metód sú **GESD [13]** a **S-H-ESD [14]**. GESD opakovane nájde najextrémnejšiu hodnotu, otestuje ju a odstráni, a tak postupne určí, koľko anomálií rad obsahuje. Rieši tým problém, keď jedna anomália „skrýva“ druhú. S-H-ESD robí to isté, ale až po odstránení denného a týždenného rytmu.

4.5.3 Metódy založené na modeli

Pri tejto skupine detekcie anomálií model odhadne, aké hodnoty by náhodná veličina $X(i)$ mala nadobúdať pri bežnej prevádzke a **anomália je pozorovaná hodnota x_i , ktorá sa od tohto očakávania výrazne odchyľuje**.

Predpovedné modely (SARIMA [15], Holt-Winters [16], Prophet [17]) predpovedajú hodnotu v okne i z predchádzajúcich hodnôt a udávajú aj rozsah, v ktorom by mala ležať. Hodnota mimo rozsahu je anomálna. Výhodou je, že prirodzene zachytia trend aj rytmus; nevýhodou je potreba dlhšieho radu.

Model pre počty (Poisson, negatívne binomický). Pre počty udalostí je najvhodnejší model, ktorý odhadne **očakávaný počet udalostí v okne i** podľa hodiny dňa, dňa v týždni a predchádzajúcej hodnoty x_{i-1} . Skóre anomálie potom vyjadruje, **aká je pravdepodobnosť, že by $X(i)$ pri bežnej prevádzke nadobudla aspoň takú vysokú hodnotu ako pozorované x_i** .

Výhody:

- výsledok je priamo pravdepodobnosť (p-hodnota), netreba ho ďalej upravovať,
- správne funguje aj pri nulách a malých počtoch,
- pri „názarových“ radoch stačí vymeniť Poissonov model za negatívne binomický.

4.5.4 Metódy nad úsekmi radu

Pri týchto metódach detekcie anomálií namiesto jednotlivých hodnôt x_i sa porovnávajú **krátke úseky** radu, napr. $x_i, x_{i+1}, \dots, x_{i+5}$. Vďaka tomu tieto metódy zachytia kolektívne anomálie.

- **Izolačný les [18]** – hľadá úseky, ktoré sa dajú ľahko „oddeliť“ od ostatných. Treba ho použiť na úseky, nie na jednotlivé hodnoty, inak nájde len to, čo zvládnu aj jednoduchšie metódy. Jeho parameter „očakávaný podiel anomálií“ priamo určuje počet nálezov, preto sa nemá voliť svojvoľne.
- **LOF [19] a kNN [20]** – porovnávajú, či je úsek v „riedkej“ oblasti v porovnaní s okolím. Vhodné, keď má rad viac režimov (pracovný a nepracovný čas).
- **Matrix Profile [21]** – pre každý úsek nájde najpodobnejší iný úsek v rade. Úsek, ktorý nemá žiadneho podobného, je najneobvyklejší (tzv. discord). Hlavným parametrom je dĺžka úseku, ktorá by mala zodpovedať očakávanej dĺžke útoku; odporúčame skúsiť viac dĺžok. Výpočtovo je náročnejší, existujú však rýchle varianty (STOMP [22], SCRIMP++ [23]).

4.5.5 Spektrálne metódy

Spectral Residual [24] rozloží rad na frekvencie, odstráni „očakávanú“ časť a spätne zvýrazní okná, ktoré do nej nezapadajú. Je rýchla, nepotrebuje tréningovanie a hodí sa na rady s ostrými vrcholmi. Slabinou je horšia presnosť na začiatku a konci radu (okolo x_0 a x_t), teda práve tam, kde hľadáme začiatok incidentu. Preto sa rad na okrajoch umelo predĺži.

4.5.6 Detekcia zmien režimu

Bodové metódy odpovedajú na otázku „ktorá hodnota x_i je nezvyčajná“. Detekcia zmien odpovedá na otázku „od ktorého indexu sa správanie procesu trvalo zmenilo“, čo priamo zodpovedá pojmu fáza útoku.

- **PELT [25], binárna segmentácia** – rozdelia rad $x_0, \dots, x_t$ na úseky s podobným správaním. Každá ďalšia hranica je „penalizovaná“, aby sa rad nerozdobil zbytočne. Výstupom sú priamo indexy kandidátskych hraníc fáz.
- **BOCPD [26]** – priebežne sleduje, ako dlho sa proces správa rovnako. Ak táto dĺžka náhle klesne, nastala zmena. Výstupom je pravdepodobnosť zmeny v každom okne.
- **CUSUM [27], Page-Hinkley, ADWIN** – jednoduché priebežné testy, ktoré zachytia aj pomalý posun úrovne, ktorý bodové metódy prehliadnu.
- **SAND [28]** – zoskupuje podobné úseky a priebežne sa prispôsobuje zmenám, spája tak hľadanie neobvyklých úsekov so sledovaním zmien.

Zmeny režimu majú vstupovať do hlasovania ako samostatný typ udalosti (hranica, nie úsek). Ak sa zmena objaví vo viacerých radoch v rovnakom alebo blízkom okne, je to veľmi silný indikátor prechodu medzi fázami.

4.5.7 Hlboké učenie

Neurónové siete (LSTM-AE [29], USAD [30], Anomaly Transformer) sa naučia normálne správanie radu a anomáliu určia podľa toho, ako zle vedia pozorovaný úsek „zrekonštruovať“.

Odborná literatúra však ukazuje, že pri jednotlivých radoch a bez označených dát spravidla **neprekonávajú jednoduché štatistické metódy**, ťažko sa nastavujú a ich výsledok sa ťažko vysvetľuje. Vo forenznom kontexte je vysvetliteľnosť nevyhnutná. Odporúčame ich preto ako doplnkovú, nie hlavnú vetvu. Ich prínos následne porovnať s jednoduchými metódami.

4.6 Agregácia anomálií naprieč časovými radmi

Kým predchádzajúca kapitola pracovala s každým radom izolovane, tento krok informáciu spája. Východisková myšlienka: ak sa ten istý časový úsek javí ako anomálny vo viacerých navzájom nezávislých radoch, ide s vysokou pravdepodobnosťou o skutočnú udalosť v systéme, nie o šum jedného zdroja. Takýto úsek označujeme ako kandidátsku fázu útoku.

Vstupom pre krok agregácie sú binárne indikátory $a^{(m)}_i \in \{0, 1\}$ z predchádzajúceho kroku 3, pričom $a^{(m)}_i = 1$, ak je časové okno i v rade m anomálne. Sú definované len pre okná $i \in C^{(m)}$, kde $C^{(m)}$ označuje množinu časových okien patriacich do časového radu m . Ďalej vstupujú váhy w_m z kroku 2 a bodové indikátory, ktorých každé nenulové okno má $a^{(m)}_i = 1$. Zmena režimu sa zapisuje ako $a^{(m)}_i = 1$ v okne detegovanej hranice.

Pre detailnejší popis agregácii je možné primerane použiť výstup D17 - Model na agregáciu a prepojenie digitálnych stôp.

4.6.1 Časová tolerancia ϵ

Tá istá činnosť útočníka sa v rôznych forenzných artefaktoch neprejaví v rovnakom časovom okne. Záznam EVTX vzniká takmer okamžite, forenzný artefakt SRUM ukladá agregované údaje približne raz za hodinu a zápis do žurnálu \$J\$ či zmena pečiatky v MFT môže nastať s oneskorením.

Nech $A^{(m)} = \{j \in C^{(m)} : a^{(m)}_j = 1\}$ je množina anomálnych časových okien radu m . Každá anomália sa rozšíri o ϵ_m časových okien na obe strany (ϵ -okolie):

$$\tilde{a}^{(m)}_i = 1, \text{ ak existuje } j \in A^{(m)} \text{ také, že } |i - j| \leq \epsilon_m; \text{ inak } \tilde{a}^{(m)}_i = 0.$$

Parameter $\epsilon_m \in \{0, 1, 2, \dots\}$ sa udáva v počte časových okien podľa časovej granularity zdroja radu m . Pre rady SRUM je $\epsilon_m = \lceil 60 \text{ min} / \Delta \rceil$ (pri $\Delta = 10 \text{ min}$ teda 6), pre ostatné zdroje $\epsilon_m = 1$. Príliš veľké ϵ zlieva susedné fázy do jednej.

4.6.2 Hlasovanie

Pre každé časové okno i sa vypočíta vážený podiel časových radov, ktoré ho označili za anomálne:

$$V_i = \sum_{m: i \in C^{(m)}} w_m \cdot \tilde{a}_i^{(m)} / \sum_{m: i \in C^{(m)}} w_m, V_i \in [0, 1].$$

Súčty zahŕňajú len rady, ktoré majú v časovom okne i dáta. Časový rad mimo svojho pokrytia teda nehlasuje ani za, ani proti.

4.6.3 Prah θ

Časové okno i je kandidátske, ak $V_i \geq \theta$, kde $\theta \in (0, 1]$. Súčin $\theta \cdot N_{\text{eff}}$ udáva, koľko nezávislých časových radov sa musí zhodnúť, aby sa časové okno považovalo za kandidátske.

Aj nezávislé rady sa občas náhodne zhodnú. Z tohto dôvodu sa pre každé časové okno určí p -hodnota. Ak detektory v kroku 3 poskytujú p -hodnoty $p_i^{(m)}$, skombinujú sa Fisherovou metódou [31] alebo váženou Stoufferovou metódou [32]:

4.6.4 Zlúčenie časových okien do fáz

Časové okná, ktoré spĺňajú $V_i \geq \theta$ a zostanú významné aj po korekcii, sa zlúčia do fáz. Významné časové okná vzdialené najviac g časových okien patria do tej istej fázy. Ekvivalentne možno použiť zhľukovanie DBSCAN [33] na indexoch okien s parametrom $\text{eps} = g$.

4.7 Určenie časového rámca incidentu

Časový rámec kybernetického bezpečnostného incidentu je určený minimom a maximom množiny anomálnych časov. Táto kapitola formalizuje uvedený postup a dopĺňa dve veci, ktoré sú pre forenzné použitie nevyhnutné: robustnú variantu a vyjadrenie neistoty.

- **Začiatok incidentu i_Z** = index prvého okna s **potvrdenou** anomáliou.
- **Koniec incidentu i_K** = index posledného okna s **potvrdenou** anomáliou.

Odhad začiatku incidentu je $\hat{t}_0 = \tau_0 + i_Z \cdot \Delta$ (začiatok prvého potvrdeného časového okna) a odhad konca $\hat{t}_1 = \tau_0 + (i_K + 1) \cdot \Delta$ (koniec posledného potvrdeného časového okna), kde τ_0 je začiatok časovej osi (kapitola 4.3).

Potvrdená anomália je taká, ktorá patrí do niektorej z významných fáz (s toleranciou ϵ). Použiť všetky surové anomálie by bola chyba: jediný falošný nález na začiatku radu (a pri mnohých radoch ich vznikajú desiatky) by posunul odhad začiatku o týždeň dozadu.

Súčasne sa má uvádzať aj odolnejší odhad: namiesto úplne prvého a posledného potvrdeného okna sa vynechá prvých a posledných 5 % potvrdených anomálií. Ak sa oba odhady výrazne líšia, rámec je určený len niekoľkými ojedinelými nálezmi a treba ho manuálne overiť.

4.8 Charakterizácia a interpretácia fáz incidentu

Posledný krok metódy prevádza časové okná na forenzne interpretovateľný výstup. Bez neho je výsledkom len zoznam intervalov, ktorý analytikovi nehovorí, čo sa v nich dialo.

Pre každú fázu sa zistí, **aký podiel jej anomálnych okien pochádza z jednotlivých časových radov** (s ohľadom na ich váhy). Zoradením získame zoznam časových radov, ktoré fázu najviac tvoria. Užitočný je aj **profil zdrojov**, teda koľko fázy pripadá na EVTX, MFT, register a SRUM, pretože význam fázy väčšinou určuje práve kombinácia zdrojov. Tabuľka 2 uvádza typické vzory, ktoré možno použiť ako východiskovú znalostnú bázu.

Dominantné časové rady vo fáze	Konkrétne časové rady v agregácii	Návrh interpretácie	Taktika z MITRE ATT&CK rámca
EVTX Security: nárast neúspešných prihlásení, následne úspešné prihlásenie	ts_{'EventId_audit_logon_logoff'} (4625 → 4624); ts_{'EventId_audit_account_logon'} (4768, 4769, 4770/4771); ts_{'Channel': 'Security'}; ts_{'Channel': 'Microsoft-Windows-RemoteDesktopServices-RdpCoreTS-Operational'}; ts_{'Channel': 'Microsoft-Windows-TerminalServices-RemoteConnectionManager-Operational'}	útok hrubou silou alebo credential stuffing; pri RDP kanáloch vzdialený prístup	Credential Access, Initial Access
EVTX: nárast vytvárania procesov, WMI aktivita register OS: zmeny v Services	ts_{'EventId_audit_detailed_tracking'} (4688, 4689); ts_{'ProcessId': N} (nové PID rady); ts_{'Channel': 'Microsoft-Windows-WMI-Activity-Operational'}; ts_{'Category': 'Services'}; ts_{'Description': 'Services'}; ts_{'HiveType': 'System'} (MC_Output)	spustenie nástrojov a zriadenie perzistencie	Execution, Persistence
Register ASEP: zmeny mimo obvyklého času EVTX: nové služby, plánované úlohy SRUM: aktivita pod SYSTEM	ts_{'HiveType': 'Software'}; ts_{'HiveType': 'System'} (ASEPs); ts_{'Category': 'Services'}; ts_{'Channel': 'System'} (7045); ts_{'Channel': 'Microsoft-Windows-TaskScheduler-Maintenance'}; ts_{'EventId_audit_privilege_usage'} (4673, 4674); ts_['{'SidType': 'LocalSystem'}, 'BackgroundBytesWritten']; ts_{'SidType': 'LocalSystem'} (AppTimelineProvider)	zriadenie automatického spúšťania s vyššími oprávneniami	Persistence, Privilege Escalation

• EVTX: bezpečnostné mitigácie, AppContainer • SRUM: aplikácie mimo bežného SidType	ts_{'Channel': 'Microsoft-Windows-Security-Mitigations-KernelMode'}; ts_{'Channel': 'Microsoft-Windows-Security-LessPrivilegeAppContainer-Operational'}; ts_{'Channel': 'Microsoft-Windows-AppModel-Runtime-Admin'}; ts_{'SidType': 'UnknownOrUserSid'}, 'ForegroundContextSwitches']	pokus o zneužitie zraniteľnosti, obchádzanie ochrán	Privilege Escalation, Defense Evasion
• EVTX: enumerácia účtov, AD objektov, WMI dotazy	ts_{'Channel': 'Microsoft-Windows-WMI-Activity-Operational'}; ts_{'EventId_audit_ds_access'} (4661, 4662); ts_{'EventId_audit_account_management'} (4720, 4722, 4728, 4732); ts_{'EventId_audit_object_access'} (5140); ts_{'Channel': 'Microsoft-Windows-GroupPolicy-Operational'}	prieskum systému, účtov a siete	Discovery
• EVTX: vzdialené prihlásenia, RDP relácie, prístup k admin zdieľaniam	ts_{'EventId_audit_logon_logoff'} (4624 typ 3/10, 4648); ts_{'Channel': 'Microsoft-Windows-TerminalServices-RemoteConnectionManager-Operational'}; ts_{'Channel': 'Microsoft-Windows-RemoteDesktopServices-RdpCoreTS-Operational'}; ts_{'Channel': 'Microsoft-Windows-Winlogon-Operational'}; ts_{'EventId_audit_object_access'} (5140, 5145)	laterálny pohyb v počítačovej sieti	Lateral Movement
• MFT/USN: hromadné vytváranie súborov v dočasných a používateľských adresároch	ts_{'UpdateReasons': 'FileCreate'}; 'FileCreate-Close'; 'DataExtend-FileCreate'; 'DataExtend-FileCreate-Close'; ts_{'FileAttributes': 'Archive-Temporary'}; 'Hidden-Archive-Temporary'; ts_Created0x10_{'SiFlags': 'Archive'}	prenos nástrojov na systém, príprava dát	Command and Control, Collection
• SRUM: prudký nárast prečítaných bajtov v popredí/na pozadí • MFT: hromadný prístup • EVTX: prístup k zdieľaným prostriedkom	ts_{'Appld': N}, 'ForegroundBytesRead'; 'BackgroundBytesRead'; ts_{'SidType': 'LogonId'}, 'BackgroundBytesRead'; ts_{'SidType': 'UnknownOrUserSid'}, 'BackgroundBytesRead'; ts_{'Appld': N} (AppTimelineProvider); ts_LastAccess0x10_{'SiFlags': 'Archive'}; ts_{'UpdateReasons': 'DataExtend-Close'} (rast archívu); ts_{'EventId_audit_object_access'} (5140, 5145)	zber dát, ich odosielanie mimo systém	Collection, Exfiltration
• MFT/USN: hromadná modifikácia, prepis, premenovanie a mazanie súborov • SRUM: vysoké zápisy a context switches	ts_{'UpdateReasons': 'DataOverwrite'}; 'DataOverwrite-Close'; 'DataOverwrite-DataExtend-DataTruncation'; 'DataTruncation'; 'RenameNewName'; 'RenameOldName'; 'FileDelete-Close'; ts_LastModified0x10_{'SiFlags': 'Archive'}; ts_{'Appld': N}, 'ForegroundBytesWritten'; 'ForegroundContextSwitches'; ts_{'Channel': 'Microsoft-Windows-Storage-Storport-Operational'}	šifrovanie alebo poškodenie dát (ransomware)	Impact

EVTX: výpadok záznamov, vymazanie logu, zmena auditu, pokles aktivity Defenderu	ts_{'EventId_audit_non_audit'} (1100, 1102, 1104); ts_{'EventId_audit_policy_change'} (4715, 4719); ts_{'Channel': 'Microsoft-Windows-Windows Defender-Operational'} (pokles / 5001, 5010); ts_{'Channel': 'Security'} (diera v rade); ts_{'UpdateReasons': 'SecurityChange'}; 'FileDelete-Close' (mazanie nástrojov)	zahľadzovanie digitálnych stôp, vypnutie bezpečnostnej ochrany	Defense Evasion
--	---	--	------------------------

Tabuľka 2 – Vzory pre interpretáciu fáz útoku

5 Záver

Tento výstup predstavuje metódu na (polo)automatizované určenie časového rámca a fáz kybernetického bezpečnostného incidentu v operačnom systéme Windows pomocou analýzy časových radov. Metóda vychádza z predpokladu, že činnosť útočníka zanecháva súbežnú digitálnu stopu vo viacerých navzájom relatívne nezávislých artefaktoch, najmä v záznamoch udalostí (EVTX), v metadátach súborového systému (MFT, \$J), v registri a v databáze SRUM. Namiesto hľadania jedinej najvýraznejšej anomálie sa preto zameriava na časovú zhodu anomálií naprieč zdrojmi.

Navrhnutý postup pozostáva zo šiestich krokov, a to vytvorenia časových radov s rovnakým časovým odstupom z nepravidielných záznamov artefaktov, výberu relevantných radov a potlačenie vplyvu duplicitných radov, detekcie anomálií osobitne v každom rade, hlasovanie naprieč radmi s časovou toleranciou, určenie začiatku a konca incidentu a interpretácia jednotlivých fáz vrátane ich priradenia k taktikám MITRE ATT&CK. Dôraz je kladený na vlastnosti dôležité pre forenzné využitie, a to najmä na kontrolu miery falošných nálezov, overenie, či zhoda anomálií nie je náhodná, vyjadrenie neistoty odhadu a dohľadateľnosť každej fázy až k pôvodným záznamom.

Výstupom metódy je zredukovaná časová os incidentu, ktorá analytikovi umožňuje sústrediť sa na niekoľko podozrivých časových úsekov namiesto tisícov záznamov. Výsledky metódy treba chápať ako hypotézu určenú na overenie klasickou forenznou analýzou, nie ako samostatný záver. Metóda má známe obmedzenia, najmä citlivosť na manipuláciu časových pečiatok, obmedzenú históriu artefaktov a ťažšie odhaliteľné pomalé útoky.

6 Bibliografia

- [1] log2timeline. (n.d.). *Plaso (log2timeline)* [Computer software]. GitHub. <https://github.com/log2timeline/plaso>
- [2] DFIR Madness. (2020). *The stolen Szechuan sauce* [Data set]. <https://dfirmadness.com/the-stolen-szechuan-sauce/>
- [3] Brockwell, P. J., & Davis, R. A. (2016). *Introduction to time series and forecasting* (3rd ed.). Springer. <https://doi.org/10.1007/978-3-319-29854-2>
- [4] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). *MITRE ATT&CK: Design and philosophy* (Technical report). The MITRE Corporation.
- [5] Anscombe, F. J. (1948). The transformation of Poisson, binomial and negative-binomial data. *Biometrika*, 35(3/4), 246–254. <https://doi.org/10.2307/2332343>
- [6] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), Article 15. <https://doi.org/10.1145/1541880.1541882>
- [7] Blázquez-García, A., Conde, A., Mori, U., & Lozano, J. A. (2021). A review on outlier/anomaly detection in time series data. *ACM Computing Surveys*, 54(3), Article 56. <https://doi.org/10.1145/3444690>
- [8] Schmidl, S., Wenig, P., & Papenbrock, T. (2022). Anomaly detection in time series: A comprehensive evaluation. *Proceedings of the VLDB Endowment*, 15(9), 1779–1797. <https://doi.org/10.14778/3538598.3538602>
- [9] Tatbul, N., Lee, T. J., Zdonik, S., Alam, M., & Gottschlich, J. (2018). Precision and recall for time series. In *Advances in Neural Information Processing Systems 31* (pp. 1920–1930). Curran Associates.
- [10] Kim, S., Choi, K., Choi, H.-S., Lee, B., & Yoon, S. (2022). Towards a rigorous evaluation of time-series anomaly detection. *Proceedings of the AAAI Conference on Artificial Intelligence*, 36(7), 7194–7201. <https://doi.org/10.1609/aaai.v36i7.20680>
- [11] Iglewicz, B., & Hoaglin, D. C. (1993). *How to detect and handle outliers*. ASQC Quality Press.
- [12] Hubert, M., & Vandervieren, E. (2008). An adjusted boxplot for skewed distributions. *Computational Statistics & Data Analysis*, 52(12), 5186–5201. <https://doi.org/10.1016/j.csda.2007.11.008>
- [13] Rosner, B. (1983). Percentage points for a generalized ESD many-outlier procedure. *Technometrics*, 25(2), 165–172. <https://doi.org/10.1080/00401706.1983.10487848>
- [14] Hochenbaum, J., Vallis, O. S., & Kejariwal, A. (2017). *Automatic anomaly detection in the cloud via statistical learning* (arXiv:1704.07706). arXiv. <https://doi.org/10.48550/arXiv.1704.07706>
- [15] Kumari, S., & Muthulakshmi, P. (2024). SARIMA model: an efficient machine learning technique for weather forecasting. *Procedia Computer Science*, 235, 656–670.

- [16] Winters, P. R. (1960). Forecasting sales by exponentially weighted moving averages. *Management Science*, 6(3), 324–342. <https://doi.org/10.1287/mnsc.6.3.324>
- [17] Rafferty, G. (2023). *Forecasting Time Series Data with Prophet*. Packt Publishing.
- [18] Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining* (pp. 413–422). IEEE. <https://doi.org/10.1109/ICDM.2008.17>
- [19] Breunig, M. M., Kriegel, H.-P., Ng, R. T., & Sander, J. (2000). LOF: Identifying density-based local outliers. In *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data* (pp. 93–104). ACM. <https://doi.org/10.1145/342009.335388>
- [20] Martínez, F., Frías, M. P., Pérez, M. D., & Rivera, A. J. (2019). A methodology for applying k-nearest neighbor to time series forecasting. *Artificial Intelligence Review*, 52(3), 2019–2037.
- [21] Yeh, C.-C. M., Zhu, Y., Ulanova, L., Begum, N., Ding, Y., Dau, H. A., Silva, D. F., Mueen, A., & Keogh, E. (2016). Matrix profile I: All pairs similarity joins for time series: A unifying view that includes motifs, discords and shapelets. In *2016 IEEE 16th International Conference on Data Mining* (pp. 1317–1322). IEEE. <https://doi.org/10.1109/ICDM.2016.0179>
- [22] Zhu, Y., Zimmerman, Z., Senobari, N. S., Yeh, C.-C. M., Funning, G., Mueen, A., Brisk, P., & Keogh, E. (2016). Matrix profile II: Exploiting a novel algorithm and GPUs to break the one hundred million barrier for time series motifs and joins. In *2016 IEEE 16th International Conference on Data Mining* (pp. 739–748). IEEE. <https://doi.org/10.1109/ICDM.2016.0085>
- [23] Zhu, Y., Yeh, C.-C. M., Zimmerman, Z., Kamgar, K., & Keogh, E. (2018). Matrix profile XI: SCRIMP++: Time series motif discovery at interactive speeds. In *2018 IEEE International Conference on Data Mining* (pp. 837–846). IEEE. <https://doi.org/10.1109/ICDM.2018.00099>
- [24] Ren, H., Xu, B., Wang, Y., Yi, C., Huang, C., Kou, X., Xing, T., Yang, M., Tong, J., & Zhang, Q. (2019). Time-series anomaly detection service at Microsoft. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (pp. 3009–3017). ACM. <https://doi.org/10.1145/3292500.3330680>
- [25] Killick, R., Fearnhead, P., & Eckley, I. A. (2012). Optimal detection of changepoints with a linear computational cost. *Journal of the American Statistical Association*, 107(500), 1590–1598. <https://doi.org/10.1080/01621459.2012.737745>
- [26] Adams, R. P., & MacKay, D. J. C. (2007). *Bayesian online changepoint detection* (arXiv:0710.3742). arXiv. <https://doi.org/10.48550/arXiv.0710.3742>
- [27] Page, E. S. (1954). Continuous inspection schemes. *Biometrika*, 41(1/2), 100–115. <https://doi.org/10.2307/2333009>

- [28] Boniol, P., Paparrizos, J., Palpanas, T., & Franklin, M. J. (2021). SAND: Streaming subsequence anomaly detection. *Proceedings of the VLDB Endowment*, 14(10), 1717–1729. <https://doi.org/10.14778/3467861.3467863>
- [29] Malhotra, P., Ramakrishnan, A., Anand, G., Vig, L., Agarwal, P., & Shroff, G. (2016). *LSTM-based encoder-decoder for multi-sensor anomaly detection* (arXiv:1607.00148). arXiv. <https://doi.org/10.48550/arXiv.1607.00148>
- [30] Audibert, J., Michiardi, P., Guyard, F., Marti, S., & Zuluaga, M. A. (2020). USAD: Unsupervised anomaly detection on multivariate time series. In *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (pp. 3395–3404). ACM. <https://doi.org/10.1145/3394486.3403392>
- [31] Fisher, R. A. (1925). *Statistical methods for research workers*. Oliver and Boyd
- [32] Stouffer, S. A., Suchman, E. A., DeVinney, L. C., Star, S. A., & Williams, R. M., Jr. (1949). *The American soldier: Adjustment during army life* (Vol. 1). Princeton University Press.
- [33] Hahsler, M., Piekenbrock, M., & Doran, D. (2019). dbscan: Fast density-based clustering with R. *Journal of Statistical Software*, 91, 1-30.

7 Príloha

7.1 Popisy vybraných časových radov pre EVT X

- Channel - Application

Kanál **Application** obsahuje udalosti generované používateľskými aplikáciami a vybranými systémovými komponentmi prostredníctvom služby Windows Event Log. Zaznamenáva informácie o vykonávaní aplikácií, ich zlyhaniach, upozorneniach a ďalších prevádzkových udalostiach.

- Channel - Microsoft-Windows-AppModel-Runtime/Admin

Kanál **Microsoft-Windows-AppModel-Runtime/Admin** zaznamenáva administratívne udalosti súvisiace s prostredím Windows AppModel Runtime, ktoré zabezpečuje správu životného cyklu aplikácií typu Universal Windows Platform (UWP). Obsahuje informácie o inicializácii, spustení, ukončení a chybových stavoch týchto aplikácií.

- Channel - Microsoft-Windows-AppReadiness/Admin

Kanál **Microsoft-Windows-AppReadiness/Admin** obsahuje udalosti vytvárané službou App Readiness počas prípravy aplikácií po inštalácii používateľského profilu alebo aktualizácii operačného systému. Zaznamenané udalosti dokumentujú priebeh inicializácie aplikácií pred ich prvým použitím.

- Channel - Microsoft-Windows-AppXDeployment/Operational

Kanál **Microsoft-Windows-AppXDeployment/Operational** zaznamenáva udalosti súvisiace s nasadzovaním aplikácií distribuovaných vo formáte AppX alebo MSIX. Obsahuje informácie o inštalácii, aktualizácii, registrácii a odstránení aplikačných balíkov.

- Channel - Microsoft-Windows-AppXDeploymentServer/Operational

Kanál **Microsoft-Windows-AppXDeploymentServer** obsahuje udalosti vytvárané službou zabezpečujúcou spracovanie požiadaviek na nasadenie AppX balíkov. Zaznamenáva jednotlivé fázy procesu inštalácie vrátane identifikácie vzniknutých chýb.

- Channel - Microsoft-Windows-AppxPackaging/Operational

Kanál **Microsoft-Windows-AppxPackaging/Operational** zaznamenáva udalosti súvisiace so spracovaním aplikačných balíkov vo formáte AppX. Obsahuje informácie o overovaní integrity balíkov, ich podpisov a metadát počas procesu inštalácie.

- Channel - Microsoft-Windows-Diagnosis-DPS/Operational

Kanál **Microsoft-Windows-Diagnosis-DPS/Operational** obsahuje udalosti generované službou Diagnostic Policy Service. Zaznamenáva diagnostické operácie, detekciu systémových problémov a vykonané automatizované opravné mechanizmy.

- Channel - Microsoft-Windows-GroupPolicy/Operational

Kanál **Microsoft-Windows-GroupPolicy/Operational** zaznamenáva priebeh spracovania objektov skupinových politík (Group Policy Objects – GPO). Obsahuje informácie o načítaní, aplikovaní a prípadných chybách pri spracovaní bezpečnostných a konfiguračných politík.

- Channel - Microsoft-Windows-PushNotification-Platform/Operational

Kanál **Microsoft-Windows-PushNotification-Platform/Operational** obsahuje udalosti súvisiace s infraštruktúrou systémových notifikácií. Zaznamenáva prijatie, spracovanie a doručovanie push oznámení používateľským aplikáciám.

- Channel - Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational

Kanál **Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational** zaznamenáva udalosti vytvárané službami Remote Desktop Services (RDS). Obsahuje informácie o vytváraní, autentifikácii, správe a ukončovaní vzdialených používateľských relácií.

- Channel - Microsoft-Windows-Security-LessPrivilegeAppContainer/Operational

Kanál **Microsoft-Windows-Security-LessPrivilegeAppContainer/Operational** obsahuje udalosti súvisiace s mechanizmami obmedzovania používateľských oprávnení pri vykonávaní procesov. Zaznamenáva udalosti spojené s aplikáciou princípu najmenších privilégií (Principle of Least Privilege).

- Channel - Microsoft-Windows-Security-Mitigations/KernelMode

Kanál **Microsoft-Windows-Security-Mitigations** zaznamenáva udalosti bezpečnostných mechanizmov implementovaných na zmiernenie dôsledkov zneužitia softvérových zraniteľností. Obsahuje informácie o aktivácii ochranných mechanizmov, ako sú DEP, ASLR alebo Control Flow Guard.

- Channel - Microsoft-Windows-SettingSync/Debug

Kanál **Microsoft-Windows-SettingSync/Debug** obsahuje diagnostické udalosti súvisiace so synchronizáciou používateľských nastavení medzi zariadeniami. Zaznamenáva priebeh synchronizácie a vzniknuté chyby pri prenose konfiguračných údajov.

- Channel - Microsoft-Windows-Shell-Core/Operational

Kanál **Microsoft-Windows-Shell-Core/Operational** obsahuje udalosti vytvárané komponentom Windows Shell, ktorý zabezpečuje používateľské grafické rozhranie operačného systému. Zaznamenáva udalosti súvisiace s inicializáciou pracovného prostredia, správou okien a interakciou používateľa so systémom.

- Channel - Microsoft-Windows-StateRepository/Operational

Kanál **Microsoft-Windows-StateRepository/Operational** obsahuje udalosti databázy State Repository, ktorá uchováva stav moderných aplikácií systému Windows. Zaznamenáva operácie vykonávané nad databázou a zmeny stavu registrovaných aplikácií.

- Channel - Microsoft-Windows-Storage-Storport-Operational

Kanál **Microsoft-Windows-Storage-Storport/Operational** zaznamenáva udalosti vytvárané ovládačom Storport zabezpečujúcim komunikáciu s diskovými zariadeniami. Obsahuje informácie o vstupno-výstupných operáciách, stave úložiska a chybách diskového subsystému.

- Channel - Microsoft-Windows-Store-Operational

Kanál **Microsoft-Windows-Store/Operational** obsahuje udalosti vytvárané aplikáciou Microsoft Store. Zaznamenáva sťahovanie, inštaláciu, aktualizáciu a správu aplikácií distribuovaných prostredníctvom obchodu Microsoft Store.

- Channel - Microsoft-Windows-TaskScheduler-Maintenance

Kanál **Microsoft-Windows-TaskScheduler/Maintenance** zaznamenáva udalosti vytvárané plánovačom úloh počas vykonávania úloh údržby systému. Obsahuje informácie o plánovanom spustení, priebehu a výsledku jednotlivých úloh.

- Channel - Microsoft-Windows-TerminalServices-RemoteConnectionManager-Operational

Kanál **Microsoft-Windows-TerminalServices** obsahuje udalosti súvisiace so správou terminálových relácií. Zaznamenáva vytváranie, správu a ukončovanie používateľských relácií prostredníctvom terminálových služieb.

- Channel - Microsoft-Windows-UniversalTelemetryClient-Operational

Kanál **Microsoft-Windows-UniversalTelemetryClient** zaznamenáva udalosti vytvárané telemetrickým klientom operačného systému Windows. Obsahuje informácie o zhromažďovaní diagnostických údajov a ich spracovaní pred odoslaním.

- Channel - Microsoft-Windows-WMI-Activity-Operational

Kanál **Microsoft-Windows-WMI-Activity/Operational** obsahuje udalosti generované službou Windows Management Instrumentation (WMI). Zaznamenáva vykonávanie WMI dotazov, správu objektov a aktivitu administrátorských skriptov využívajúcich WMI.

- Channel - Microsoft-Windows-Windows Defender-Operational

Kanál **Microsoft-Windows-Windows Defender/Operational** zaznamenáva udalosti vytvárané antivírusovým riešením Microsoft Defender. Obsahuje informácie o detekcii škodlivého kódu, vykonaných kontrolách a aplikovaných bezpečnostných opatreniach.

- Channel- Microsoft-Windows-WindowsUpdateClient-Operational

Kanál **Microsoft-Windows-WindowsUpdateClient** obsahuje udalosti súvisiace s činnosťou služby Windows Update. Zaznamenáva vyhľadávanie, sťahovanie, inštaláciu a výsledok aktualizácií operačného systému.

- Channel - Microsoft-Windows-Winlogon-Operational

Kanál **Microsoft-Windows-Winlogon/Operational** zaznamenáva udalosti vytvárané procesom Winlogon počas prihlasovania, odhlasovania a uzamykania používateľských relácií. Obsahuje informácie o autentifikácii používateľov a správe prihlasovacích relácií.

- Channel - Security

Kanál **Security** obsahuje bezpečnostné udalosti generované auditovacím mechanizmom operačného systému Windows. Zaznamenáva autentifikáciu používateľov, prístup k objektom, zmeny oprávnení a ďalšie udalosti významné z hľadiska bezpečnosti.

- Channel - System

Kanál **System** obsahuje udalosti vytvárané jadrom operačného systému, ovládačmi zariadení a systémovými službami. Zaznamenáva spustenie a ukončenie systému, stav hardvéru, načítanie ovládačov a ďalšie systémové udalosti.

- EventId_audit_account_logon - 4768, 4769, 4770

Kategória **Audit Account Logon** obsahuje udalosti súvisiace s overovaním identity používateľských účtov počas procesu autentifikácie. Zaznamenáva úspešné aj neúspešné pokusy o overenie lokálnych alebo doménových účtov.

- EventId_audit_account_management - 4720, 4722

Kategória **Audit Account Management** zaznamenáva operácie správy používateľských účtov, skupín a bezpečnostných identifikátorov. Obsahuje udalosti vytvorenia, odstránenia, úpravy alebo zmeny oprávnení používateľských objektov.

- EventId_audit_detailed_tracking - 4688, 4689

Kategória **Audit Detailed Tracking** obsahuje detailné udalosti opisujúce vykonávanie procesov a ďalších systémových operácií. Poskytuje podrobné informácie o vytváraní procesov, ich ukončení a ďalších aktivitách operačného systému.

- EventId_audit_ds_access - 4661, 4662, 4928

Kategória **Audit Directory Service Access** zaznamenáva prístup k objektom adresárovej služby Active Directory. Obsahuje udalosti týkajúce sa čítania, úpravy alebo správy adresárových objektov v doménovom prostredí.

- EventId_audit_logon_logoff - 4624, 4625, 4626

Kategória **Audit Logon/Logoff** zaznamenáva úspešné aj neúspešné prihlásenia, odhlásenia a ďalšie udalosti súvisiace s používateľskými reláciami. Poskytuje informácie potrebné na rekonštrukciu aktivity používateľov v systéme.

- EventId_audit_non_audit - 1100, 1101, 1102

Kategória **Audit Non-Audit** obsahuje udalosti súvisiace so správou samotného auditovacieho mechanizmu operačného systému. Zahŕňa napríklad spustenie alebo zastavenie auditovacej služby a manipuláciu s bezpečnostnými logmi.

- EventId_audit_object_access - 5145, 5140, 5142

Kategória **Audit Object Access** zaznamenáva prístupy používateľov alebo procesov k objektom chráneným bezpečnostným mechanizmom Windows. Obsahuje udalosti prístupu k súborom, registrovým kľúčom, zdieľaným prostriedkom a ďalším systémovým objektom.

- EventId_audit_policy_change - 4715, 4719, 4817

Kategória **Audit Policy Change** obsahuje udalosti dokumentujúce zmeny bezpečnostných politík a auditovacích nastavení operačného systému. Umožňuje identifikovať zásahy do konfigurácie zabezpečenia systému.

- EventId_audit_privilege_usage - 4673, 4674

Kategória **Audit Privilege Usage** zaznamenáva využívanie špeciálnych systémových oprávnení procesmi alebo používateľmi. Poskytuje informácie o operáciách vyžadujúcich zvýšené bezpečnostné oprávnenia.

- EventId_audit_system - 5024, 5025, 5027, 5028

Kategória **Audit System** obsahuje bezpečnostné udalosti týkajúce sa činnosti samotného operačného systému. Zaznamenáva udalosti súvisiace so štartom systému, zmenami bezpečnostného stavu a činnosťou bezpečnostných služieb.

- EventId_audit_uncategorized - 4960, 4961, 4962

Kategória **Audit Uncategorized** obsahuje bezpečnostné udalosti, ktoré nie sú zaradené do žiadnej zo štandardných auditných kategórií. Predstavuje doplnkovú skupinu udalostí využiteľnú pri podrobnej forenznej analýze.

- ProcessId: 0
- ProcessId: 1016
- ProcessId: 1152
- ProcessId: 1924
- ProcessId: 2592
- ProcessId: 2716
- ProcessId: 2748
- ProcessId: 3156
- ProcessId: 316
- ProcessId: 332
- ProcessId: 4332
- ProcessId: 4504
- ProcessId: 4696
- ProcessId: 4
- ProcessId: 5112
- ProcessId: 552
- ProcessId: 5908
- ProcessId: 612

7.2 Popisy vybraných časových radov pre MFT a journal

- FileAttributes: 'Archive'

Atribút **Archive** označuje súbor určený na zálohovanie alebo archiváciu. Príznak je štandardne nastavený pri vytvorení alebo zmene súboru a môže byť využitý zálohovacím softvérom.

- FileAttributes - Archive-Compressed'

Atribút **Archive-Compressed** označuje súbor, ktorý je komprimovaný pomocou mechanizmu NTFS a zároveň je označený na archiváciu. Záznam umožňuje identifikovať komprimované súbory, ktorých obsah bol vytvorený alebo upravený.

- FileAttributes - Archive-NotContentIndexed'

Atribút **Archive-NotContentIndexed** označuje súbor určený na archiváciu, ktorý je vylúčený z indexovania služby Windows Search. Používa sa na súboroch, ktorých obsah nemá byť zahrnutý do fulltextového vyhľadávania.

- FileAttributes - Archive-Temporary'

Atribút **Archive-Temporary** označuje dočasný súbor určený na krátkodobé uchovávanie údajov. Takéto súbory sú typicky vytvárané aplikáciami počas spracovania dát.

- FileAttributes - Directory'

Atribút **Directory** identifikuje objekt súborového systému ako adresár. Záznamy s týmto atribútom predstavujú kontajnery určené na organizáciu súborov a ďalších adresárov.

- FileAttributes': 'Hidden-Archive'

Atribút **Hidden-Archive** označuje skrytý súbor určený na archiváciu. Takéto súbory nie sú štandardne zobrazované používateľovi, pričom zostávajú súčasťou zálohovacieho procesu.

- FileAttributes - Hidden-Archive-Temporary'

Atribút **Hidden-Archive-Temporary** označuje skrytý dočasný súbor určený na archiváciu. Tento typ súborov je najčastejšie vytváraný systémom alebo aplikáciami počas dočasného spracovania údajov.

- FileAttributes - Hidden-System-Archive'

Atribút **Hidden-System-Archive** označuje systémový súbor, ktorý je skrytý pred používateľom a zároveň označený na archiváciu. Takéto súbory sú nevyhnutné pre správnu funkčnosť operačného systému.

- FileAttributes - Normal'

Atribút **Normal** označuje štandardný súbor bez špeciálnych atribútov. Predstavuje najbežnejší typ objektu uloženého v súborovom systéme NTFS.

- FileAttributes - NotContentIndexed'

Atribút **NotContentIndexed** označuje súbor alebo adresár, ktorého obsah nie je zahrnutý do indexovania služby Windows Search. Jeho využitie znižuje záťaž indexovacej služby alebo chráni citlivé údaje pred indexovaním.

- FileAttributes - System-Archive-NotContentIndexed'.csv.csv

Atribút **System-Archive-NotContentIndexed** označuje systémový súbor určený na archiváciu, ktorý je zároveň vylúčený z obsahového indexovania. Ide prevažne o systémové objekty využívané operačným systémom.

- UpdateReasons - 16777472'

Hodnota 16777472 predstavuje číselnú bitovú masku dôvodov aktualizácie záznamu v USN Journale alebo MFT. Kombinuje viacero príznakov zmien, ktoré je potrebné interpretovať podľa definície príznakov NTFS.

- UpdateReasons': '2164261120'

Hodnota 2164261120 predstavuje kombináciu viacerých bitových príznakov určujúcich dôvod aktualizácie záznamu súborového systému. Jej význam závisí od konkrétnej kombinácie nastavených príznakov definovaných implementáciou NTFS.

- UpdateReasons': 'BasicInfoChange'

Dôvod BasicInfoChange označuje zmenu základných metadát súboru alebo adresára. Môže zahŕňať úpravu časových značiek, atribútov alebo vlastníctva objektu.

- UpdateReasons - BasicInfoChange-Close'

Záznam označuje zmenu základných metadát, po ktorej nasledovalo uzavretie súboru. Indikuje ukončenie operácie meniacej základné vlastnosti objektu.

- UpdateReasons - Close'

Dôvod Close označuje uzavretie otvoreného deskriptora súboru aplikáciou alebo systémovým procesom. Nevypovedá o zmene obsahu súboru, ale o ukončení práce s objektom.

- UpdateReasons - DataExtend'

Dôvod DataExtend označuje zväčšenie veľkosti súboru zápisom nových dát. Typicky vzniká pri ukladaní alebo dopĺňaní obsahu súboru.

- UpdateReasons - DataExtend-Close'

Označuje rozšírenie obsahu súboru, po ktorom nasledovalo jeho uzavretie. Indikuje úspešné dokončenie operácie zápisu.

- UpdateReasons - DataExtend-DataTruncation'

Záznam obsahuje kombináciu rozšírenia a následného skrátenia súboru počas jednej operácie. Takéto správanie sa vyskytuje napríklad pri prepise alebo optimalizácii obsahu súboru.

- UpdateReasons - DataExtend-DataTruncation-Close'

Označuje kombinovanú operáciu rozšírenia a skrátenia súboru ukončenú uzavretím objektu. Predstavuje ukončenie komplexnej operácie nad obsahom súboru.

- UpdateReasons - DataExtend-FileCreate'

Dôvod označuje vytvorenie nového súboru, počas ktorého došlo k zápisu dát. Ide o typický priebeh vytvorenia nového súboru s obsahom.

- UpdateReasons - DataExtend-FileCreate-BasicInfoChange'

Záznam označuje vytvorenie súboru, zápis dát a následnú úpravu jeho základných metadát. Predstavuje bežný priebeh vytvorenia súboru aplikáciou.

- UpdateReasons - DataExtend-FileCreate-Close'

Označuje vytvorenie súboru, zápis obsahu a ukončenie práce so súborom jeho uzavretím. Predstavuje kompletný životný cyklus operácie vytvorenia súboru.

- UpdateReasons - DataOverwrite'

Dôvod DataOverwrite označuje prepísanie existujúcich dát bez zmeny veľkosti súboru. Obsah súboru sa zmení, pričom jeho alokovaný priestor zostáva zachovaný.

- UpdateReasons - DataOverwrite-Close'

Označuje prepísanie obsahu súboru ukončené uzavretím objektu. Signalizuje dokončenie operácie modifikácie dát.

- UpdateReasons - DataOverwrite-DataExtend-DataTruncation'

Záznam predstavuje kombináciu prepísania dát, rozšírenia aj skrátenia súboru počas jednej operácie. Ide o komplexnú úpravu obsahu súboru vykonanú aplikáciou alebo systémom.

- UpdateReasons - DataOverwrite-DataExtend-FileCreate'

Označuje vytvorenie súboru spojené so zápisom nových aj prepísaných dát. Takýto priebeh je typický pri vytváraní alebo kopírovaní súborov.

- UpdateReasons - DataTruncation'

Dôvod DataTruncation označuje zmenšenie veľkosti súboru odstránením jeho časti. Vyskytuje sa napríklad pri skracovaní logov alebo úprave dokumentov.

- UpdateReasons - FileCreate'

Dôvod FileCreate označuje vytvorenie nového záznamu súboru v súborovom systéme NTFS. Predstavuje začiatok životného cyklu nového objektu.

- UpdateReasons - FileCreate-Close'

Označuje vytvorenie nového súboru ukončené jeho uzavretím. Indikuje úspešne dokončenú operáciu vytvorenia objektu.

- UpdateReasons - FileDelete-Close'

Dôvod FileDelete-Close označuje odstránenie súboru potvrdené uzavretím objektu. Záznam indikuje ukončenie operácie mazania súboru.

- UpdateReasons - FileDelete-TransactedChange-Close'

Záznam označuje odstránenie súboru vykonané v rámci transakčného mechanizmu NTFS a následné uzavretie objektu. Takéto operácie sú menej časté a využívajú transakčné rozhranie súborového systému.

- UpdateReasons - HardLinkChange-Close'

Dôvod označuje zmenu hard linku existujúceho súboru ukončenú uzavretím objektu. Indikuje vytvorenie alebo odstránenie odkazu na existujúce dáta.

- UpdateReasons - HardLinkChange-TransactedChange'

Záznam predstavuje zmenu hard linku vykonanú prostredníctvom transakcie NTFS. Umožňuje identifikovať transakčné operácie nad odkazmi súborového systému.

- UpdateReasons - IndexableChange-BasicInfoChange'

Dôvod označuje zmenu nastavenia indexovania súboru spolu so zmenou jeho základných metadát. Takéto operácie vznikajú napríklad pri zmene atribútov súboru.

- UpdateReasons - RenameNewName'

Dôvod RenameNewName označuje vytvorenie nového názvu súboru alebo adresára počas operácie premenovania. Umožňuje identifikovať cieľový názov objektu po vykonaní operácie.

- UpdateReasons - RenameNewName-BasicInfoChange'

Záznam označuje premenovanie objektu spojené so zmenou jeho základných metadát. Indikuje súčasnú zmenu názvu aj atribútov objektu.

- UpdateReasons - RenameNewName-BasicInfoChange-Close'

Označuje premenovanie objektu, úpravu jeho metadát a ukončenie operácie uzavretím objektu. Predstavuje kompletný priebeh operácie premenovania.

- UpdateReasons - RenameNewName-Close'

Dôvod označuje úspešné dokončenie operácie premenovania nového názvu súboru alebo adresára. Záznam vzniká po uzavretí objektu aplikáciou.

- UpdateReasons - RenameOldName'

Dôvod RenameOldName zaznamenáva pôvodný názov objektu pred vykonaním operácie premenovania. Umožňuje rekonštruovať pôvodnú identitu súboru alebo adresára.

- UpdateReasons - RenameOldName-BasicInfoChange'

Záznam obsahuje informáciu o pôvodnom názve objektu a súčasnej zmene jeho základných metadát. Je využiteľný pri rekonštrukcii priebehu operácie premenovania.

- UpdateReasons - SecurityChange'

Dôvod SecurityChange označuje zmenu bezpečnostného deskriptora súboru alebo adresára. Zahŕňa zmeny vlastníka, prístupových práv alebo auditovacích pravidiel.

- UpdateReasons - SecurityChange-Close'}.csv

Záznam označuje ukončenie operácie zmeny bezpečnostných atribútov objektu uzavretím súboru. Potvrdzuje úspešné dokončenie úpravy bezpečnostného deskriptora.

7.3 Popisy vybraných časových radov pre MFT

Časový rad **Created0x10** vychádza z časovej značky vytvorenia objektu uloženej v atribúte **\$STANDARD_INFORMATION (0x10)** záznamu MFT. Zaznamenáva čas vytvorenia súboru alebo adresára spolu s príslušnými atribútmi objektu. Časový rad **LastAccess0x10** vychádza z časovej značky posledného prístupu k objektu uloženej v atribúte **\$STANDARD_INFORMATION (0x10)**. Poskytuje informácie o poslednom zaznamenanom otvorení alebo použití súboru či adresára. Časový rad **LastModified0x10** vychádza z časovej značky poslednej zmeny obsahu objektu uloženej v atribúte **\$STANDARD_INFORMATION (0x10)**. Umožňuje identifikovať čas poslednej modifikácie dát uložených v súbore. Časový rad **LastRecordChange0x10** vychádza z

časovej značky poslednej zmeny záznamu MFT uloženej v atribúte **\$STANDARD_INFORMATION (0x10)**. Zaznamenáva zmeny metadát objektu, ako sú atribúty, oprávnenia alebo názov súboru. Príznak **Archive** označuje objekt určený na archiváciu alebo zálohovanie. Nastavuje sa pri vytvorení alebo zmene súboru a využíva sa najmä zálohovacími aplikáciami. Príznak **Archive-NotContentIndexed** označuje objekt určený na archiváciu, ktorý je zároveň vylúčený z obsahového indexovania službou Windows Search. Používa sa pri súboroch, ktorých obsah nemá byť zahrnutý do indexu vyhľadávania. Príznak **Archive-RecallOnOpen** označuje objekt určený na archiváciu, ktorého obsah je možné načítať zo vzdialeného alebo hierarchického úložiska pri jeho otvorení. Vyskytuje sa najmä pri mechanizmoch Hierarchical Storage Management alebo cloudových riešeniach, ako je OneDrive Files On-Demand. Príznak **Hidden-System-NotContentIndexed** označuje systémový objekt, ktorý je skrytý pred používateľom a zároveň vylúčený z obsahového indexovania. Takéto súbory tvoria súčasť operačného systému alebo jeho interných mechanizmov.

Všetky nasledujúce časové rady predstavujú filtrovanie príslušnej časovej značky podľa hodnoty atribútu **SiFlags**:

- **Created0x10 + Archive** – obsahuje časy vytvorenia objektov označených atribútom *Archive*.
- **Created0x10 + Archive-NotContentIndexed** – obsahuje časy vytvorenia objektov určených na archiváciu, ktoré nie sú indexované.
- **Created0x10 + Archive-RecallOnOpen** – obsahuje časy vytvorenia objektov využívajúcich mechanizmus Recall-on-Open.
- **Created0x10 + Hidden-System-NotContentIndexed** – obsahuje časy vytvorenia systémových skrytých objektov bez obsahového indexovania.
- **LastAccess0x10 + Archive** – obsahuje časy posledného prístupu k objektom s atribútom *Archive*.
- **LastAccess0x10 + Archive-NotContentIndexed** – obsahuje časy posledného prístupu k neindexovaným archivovaným objektom.
- **LastAccess0x10 + Archive-RecallOnOpen** – obsahuje časy posledného prístupu k objektom využívajúcim Recall-on-Open.
- **LastAccess0x10 + Hidden-System-NotContentIndexed** – obsahuje časy posledného prístupu k systémovým skrytým objektom.
- **LastModified0x10 + Archive** – obsahuje časy poslednej modifikácie objektov označených atribútom *Archive*.
- **LastModified0x10 + Archive-NotContentIndexed** – obsahuje časy poslednej modifikácie archivovaných objektov bez indexovania.
- **LastModified0x10 + Archive-RecallOnOpen** – obsahuje časy poslednej modifikácie objektov využívajúcich Recall-on-Open.

- **LastModified0x10 + Hidden-System-NotContentIndexed** – obsahuje časy poslednej modifikácie systémových skrytých objektov.
- **LastRecordChange0x10 + Archive** – obsahuje časy poslednej zmeny metadát objektov označených atribútom *Archive*.
- **LastRecordChange0x10 + Archive-NotContentIndexed** – obsahuje časy poslednej zmeny metadát archivovaných neindexovaných objektov.
- **LastRecordChange0x10 + Archive-RecallOnOpen** – obsahuje časy poslednej zmeny metadát objektov využívajúcich Recall-on-Open.
- **LastRecordChange0x10 + Hidden-System-NotContentIndexed** – obsahuje časy poslednej zmeny metadát systémových skrytých objektov.

mtfeMFT:

- ts_Created0x10_{'SiFlags': 'Archive'}
- ts_Created0x10_{'SiFlags': 'Archive-NotContentIndexed'}
- ts_Created0x10_{'SiFlags': 'Archive-RecallOnOpen'}
- ts_Created0x10_{'SiFlags': 'Hidden-System-NotContentIndexed'}
- ts_LastAccess0x10_{'SiFlags': 'Archive'}
- ts_LastAccess0x10_{'SiFlags': 'Archive-NotContentIndexed'}
- ts_LastAccess0x10_{'SiFlags': 'Archive-RecallOnOpen'}
- ts_LastAccess0x10_{'SiFlags': 'Hidden-System-NotContentIndexed'}
- ts_LastModified0x10_{'SiFlags': 'Archive'}
- ts_LastModified0x10_{'SiFlags': 'Archive-NotContentIndexed'}
- ts_LastModified0x10_{'SiFlags': 'Archive-RecallOnOpen'}
- ts_LastModified0x10_{'SiFlags': 'Hidden-System-NotContentIndexed'}
- ts_LastRecordChange0x10_{'SiFlags': 'Archive'}
- ts_LastRecordChange0x10_{'SiFlags': 'Archive-NotContentIndexed'}
- ts_LastRecordChange0x10_{'SiFlags': 'Archive-RecallOnOpen'}
- ts_LastRecordChange0x10_{'SiFlags': 'Hidden-System-NotContentIndexed'}.csv

7.4 Popisy vybraných časových radov pre register

registry_MC_Output:

- Category': 'Services'

Kategória Services obsahuje záznamy registra súvisiace so systémovými službami a ovládačmi evidovanými operačným systémom Windows. Tieto záznamy definujú spôsob spúšťania služby, jej typ, závislosti a ďalšie parametre potrebné na jej vykonávanie.

- Description': 'Services'

Hodnota Description: Services identifikuje artefakty, ktorých význam sa viaže na konfiguráciu a správu služieb operačného systému. Z forenzného hľadiska umožňuje sledovať existenciu, zmeny a spôsob spúšťania legitímnych aj potenciálne škodlivých služieb.

- HiveType': 'System'

HiveType: System označuje údaje pochádzajúce z registra SYSTEM, ktorý obsahuje konfiguráciu hardvéru, ovládačov, služieb a vybraných systémových parametrov. Ide o jeden z najdôležitejších registrových hive súborov pri rekonštrukcii konfigurácie a správania operačného systému.

registry_registry_ASEPs_Output

- HiveType': 'Software'

HiveType: Software označuje záznamy získané z registra **SOFTWARE**, ktorý obsahuje konfiguráciu operačného systému, nainštalovaných aplikácií a mechanizmov automatického spúšťania. Pri analýze ASEPs umožňuje identifikovať aplikácie alebo komponenty, ktoré sa automaticky spúšťajú po prihlásení používateľa alebo počas štartu systému.

- HiveType': 'System'}).csv

HiveType: System označuje záznamy pochádzajúce z registra **SYSTEM**, ktorý obsahuje konfiguráciu systémových služieb, ovládačov a mechanizmov spúšťaných pri štarte operačného systému. Pri analýze ASEPs poskytuje informácie o komponentoch zabezpečujúcich automatické spustenie ešte pred prihlásením používateľa a umožňuje identifikovať zmeny ovplyvňujúce inicializáciu systému.

7.5 Popisy vybraných časových radov pre SRUM

7.5.1 AppResourceUseInfo

Artefakty **SRUM (System Resource Usage Monitor)** uchovávajú historické informácie o využívaní systémových prostriedkov jednotlivými aplikáciami a bezpečnostnými identitami. Časové rady vytvorené z tabuľky AppResourceUseInfo opisujú diskovú a procesorovú aktivitu aplikácií v popredí a na pozadí.

AppId predstavuje interný identifikátor aplikácie v databáze SRUM. Jednotlivé hodnoty, napríklad 252, 255, 383, 409, 410, 411, 413, 422, 423 alebo 451, iba odlišujú konkrétne aplikácie, pričom samotné číslo bez ďalšieho mapovania neurčuje názov programu. Metrika **BackgroundBytesRead** vyjadruje množstvo dát, ktoré aplikácia prečítala počas vykonávania na pozadí. Zvýšené hodnoty môžu indikovať automatické načítavanie súborov, cache, databáz alebo inú činnosť vykonávanú bez priamej interakcie používateľa. Metrika **BackgroundBytesWritten** predstavuje množstvo dát zapísaných aplikáciou počas činnosti na pozadí. Nárast môže súvisieť s ukladaním logov, cache, aktualizáciami, databázovou činnosťou alebo inými automatickými operáciami. Metrika **BackgroundContextSwitches** zaznamenáva počet prepnutí kontextu procesora počas vykonávania aplikácie na pozadí. Vyšší počet znamená intenzívnejšie plánovanie jej vlákien operačným systémom, pričom nemusí ísť o aktivitu používateľa. Metrika **ForegroundBytesRead** vyjadruje množstvo dát prečítaných aplikáciou počas jej aktívneho vykonávania v popredí. Zvýšené hodnoty môžu súvisieť s načítaním dokumentov, databáz alebo iných dát počas práce používateľa s aplikáciou. Metrika **ForegroundBytesWritten** predstavuje množstvo dát zapísaných aplikáciou počas jej vykonávania v popredí. Nárast môže indikovať ukladanie alebo modifikáciu dát pri aktívnej práci s aplikáciou. Metrika **ForegroundContextSwitches** udáva počet prepnutí kontextu procesora počas vykonávania aplikácie v popredí. Vyššie hodnoty v kombinácii s foreground čítaním a zápisom môžu indikovať intenzívnu aktivitu aplikácie v používateľskom kontexte. **SidType** označuje typ bezpečnostnej identity, pod ktorou bola aktivita zaznamenaná. Hodnoty ako Administrator, LocalSystem, LocalService, NetworkService, LogonId alebo UnknownOrUserSid umožňujú rozlíšiť systémovú, servisnú a používateľskú aktivitu.

- ts_['AppId': 252], 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 252], 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 252], 'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 252], 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 252], 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 252], 'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['AppId': 255], 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 255], 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 255], 'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 255], 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 255], 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 255], 'ForegroundContextSwit_value_ForegroundContextSwitches
- ts_['AppId': 383], 'BackgroundBytesRead']_value_BackgroundBytesRead.csv

- ts_['AppId': 383], 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 383},
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 383], 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 383], 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 383},
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['AppId': 409], 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 409], 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 409},
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 409], 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 409], 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 409},
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['AppId': 410], 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 410], 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 410},
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 410], 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 410], 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 410},
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['AppId': 411], 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 411], 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 411},
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 411], 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 411], 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 411},
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['AppId': 413], 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 413], 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 413},
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 413], 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 413], 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv

- ts_['AppId': 413},
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['AppId': 422}, 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 422}, 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 422},
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 422}, 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 422}, 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 422},
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['AppId': 423}, 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 423}, 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 423},
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 423}, 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 423}, 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 423},
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['AppId': 451}, 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['AppId': 451}, 'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['AppId': 451},
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['AppId': 451}, 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['AppId': 451}, 'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['AppId': 451},
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['SidType': 'Administrator'],
'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['SidType': 'Administrator'],
'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['SidType': 'Administrator'],
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['SidType': 'Administrator'],
'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['SidType': 'Administrator'],
'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['SidType': 'Administrator'],
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv

- ts_['SidType': 'LocalService'],
'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['SidType': 'LocalService'],
'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['SidType': 'LocalService'],
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['SidType': 'LocalService'],
'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['SidType': 'LocalService'],
'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['SidType': 'LocalService'],
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['SidType': 'LocalSystem'],
'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['SidType': 'LocalSystem'],
'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['SidType': 'LocalSystem'],
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['SidType': 'LocalSystem'],
'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['SidType': 'LocalSystem'],
'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['SidType': 'LocalSystem'],
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['SidType': 'LogonId'], 'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['SidType': 'LogonId'],
'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['SidType': 'LogonId'],
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['SidType': 'LogonId'], 'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['SidType': 'LogonId'],
'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['SidType': 'LogonId'],
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['SidType': 'NetworkService'],
'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['SidType': 'NetworkService'],
'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv

- ts_['SidType': 'NetworkService'],
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['SidType': 'NetworkService'],
'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['SidType': 'NetworkService'],
'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['SidType': 'NetworkService'],
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv
- ts_['SidType': 'UnknownOrUserSid'],
'BackgroundBytesRead']_value_BackgroundBytesRead.csv
- ts_['SidType': 'UnknownOrUserSid'],
'BackgroundBytesWritten']_value_BackgroundBytesWritten.csv
- ts_['SidType': 'UnknownOrUserSid'],
'BackgroundContextSwitches']_value_BackgroundContextSwitches.csv
- ts_['SidType': 'UnknownOrUserSid'],
'ForegroundBytesRead']_value_ForegroundBytesRead.csv
- ts_['SidType': 'UnknownOrUserSid'],
'ForegroundBytesWritten']_value_ForegroundBytesWritten.csv
- ts_['SidType': 'UnknownOrUserSid'],
'ForegroundContextSwitches']_value_ForegroundContextSwitches.csv

7.5.2 AppTimelineProvider

AppTimelineProvider je súčasť artefaktu SRUM, ktorá zaznamenáva časovú aktivitu aplikácií v operačnom systéme Windows. Umožňuje sledovať, kedy bola určitá aplikácia aktívna a s akým používateľským alebo systémovým kontextom bola jej aktivita spojená.

Hodnota **AppId** predstavuje interný identifikátor aplikácie v databáze SRUM, pričom jednotlivé číselné hodnoty rozlišujú rôzne aplikácie alebo systémové komponenty. **SidType** určuje typ bezpečnostnej identity, napríklad používateľa, LocalSystem, LocalService alebo NetworkService, zatiaľ čo **UserName** umožňuje aktivitu priradiť ku konkrétnemu používateľskému alebo systémovému účtu.

- AppId': 111
- AppId': 17
- AppId': 2243
- AppId': 2249
- AppId': 2276
- AppId': 2286

- Appld': 2288
- Appld': 3472
- Appld': 3
- Appld': 99
- SidType': 'Administrator'
- SidType': 'LocalService'
- SidType': 'LocalSystem'
- SidType': 'NetworkService'
- SidType': 'UnknownOrUserSid'
- UserName': 'Administrator'
- UserName': 'LocalService'
- UserName': 'NetworkService'
- UserName': 'SelmaBouvier'
- UserName': 'systemprofile'