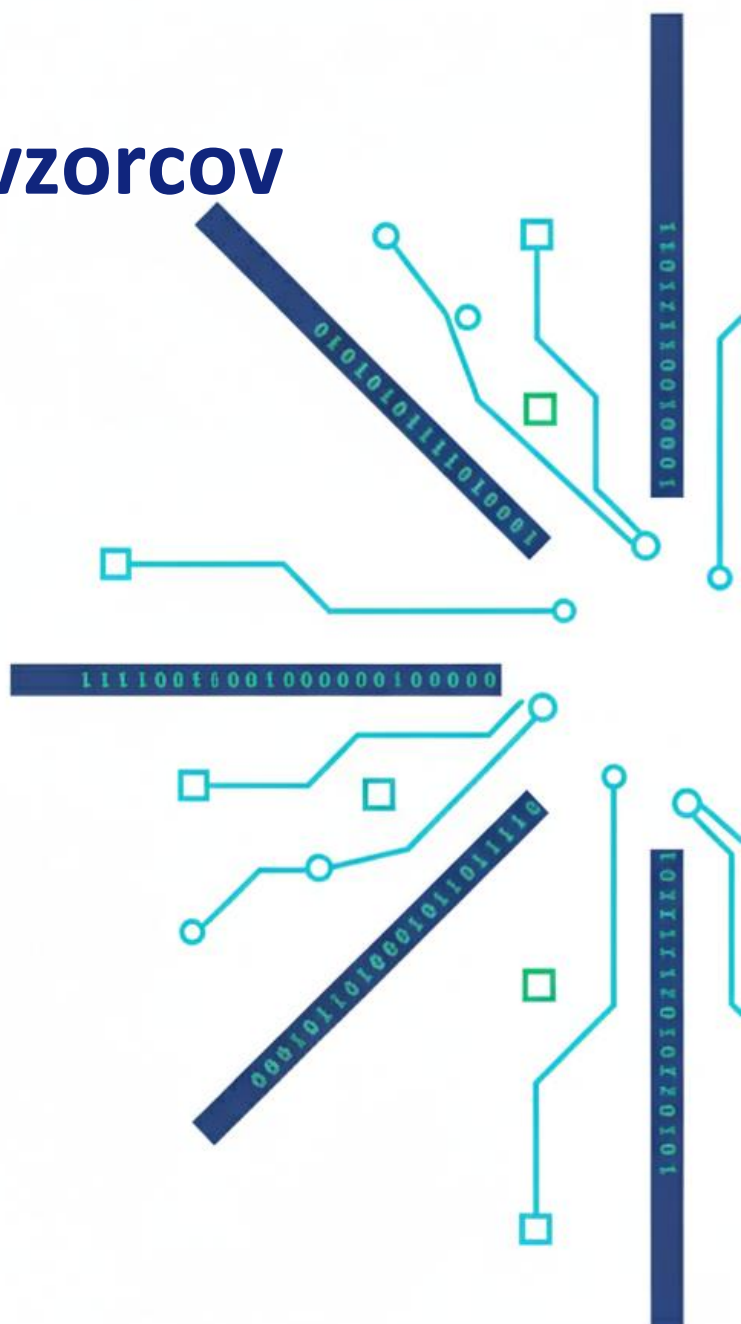


D22 – Databáza behaviorálnych vzorcov



Projekt Automatizácia digitálnej forenznej analýzy a reakcie 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	<i>Popis projektu</i>	3
2	<i>Úvod</i>	4
3	<i>Štruktúra databázy - popis stĺpcov.....</i>	5
3.1	MITRE	5
3.2	Event Type	6
3.3	Trigger Condition.....	6
3.4	Brief	7
3.5	Description.....	7
4	<i>Ako čítať pravidlá (ukážka)</i>	9
5	<i>Prečo je táto štruktúra podstatná pre nástroj automatizujúci forenznú analýzu 10</i>	
6	<i>Poznámky k údržbe a rozširovaniu katalógu</i>	11
7	<i>Príloha</i>	12

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

Databáza behaviorálnych vzorov predstavuje katalóg detekčných pravidiel. Každé pravidlo popisuje jednu konkrétnu, pozorovateľnú stopu útočnickej aktivity. Pravidlo je postavené nad jedným z troch typov telemetrie:

- **udalosti vytvorenia procesu** (ProcessCreate) - napr. spustenie podozrivého alebo zneužívateľného binárneho súboru - typicky Event ID 4688, Sysmon Event ID 1 alebo EDR telemetria.
- **záznamy v event logoch** (Windows Event Log / ETW) - napr. udalosti PowerShellu, bezpečnostného logu a pod.,
- **udalosti zmeny registrov** (Registry change) - napr. vytvorenie alebo úprava kľúča slúžiaceho na perzistenciu.

Pravidlá sú **statické** v tom zmysle, že nevyužívajú strojové učenie ani pravdepodobnostné skórovanie. Každé pravidlo má jednoznačne definovaný trigger, ktorý sa vyhodnotí ako pravdivý alebo nepravdivý. Vďaka tomu je každý zásah (hit) plne vysvetliteľný, auditovateľný a reprodukovateľný - analytik vždy presne vie, prečo pravidlo zareagovalo.

Každé pravidlo je zároveň namapované na techniku z frameworku **MITRE ATT&CK**, čo pravidlám dáva spoločnú taxonómiu a umožňuje merať pokrytie útočníckych techník.

3 Štruktúra databázy - popis stĺpcov

Nižšie je prehľad všetkých stĺpcov, po ktorom nasleduje detailný popis každého z nich.

Stĺpec	Čo obsahuje	Príklad hodnoty
MITRE	Identifikátor techniky MITRE ATT&CK, na ktorú je pravidlo namapované	T1113
Event Type	Typ telemetrie / spúšťacej udalosti pravidla	OnProcessCreate
Trigger Condition	Presná podmienka, pri ktorej pravidlo zareaguje	process.name == 'psr.exe'
Brief	Krátky, ľudske čitateľný názov pravidla	Zneužitie Psr.exe na zachytenie obrazovky
Description	Podrobný popis detegovanej aktivity a jej kontextu	(viď nižšie)

3.1 MITRE

Stĺpec **MITRE** obsahuje číslo (identifikátor) techniky z frameworku MITRE ATT&CK, na ktorú je dané pravidlo namapované, napr. T1113 (Screen Capture) alebo T1547 (Boot or Logon Autostart Execution). MITRE ATT&CK je verejne dostupná znalostná báza reálnych útočných taktík a techník, ktorá funguje ako spoločný, štandardizovaný slovník pre bezpečnostné tímy.

Mapovanie každého pravidla na konkrétnu techniku má niekoľko praktických prínosov:

- **Kontext pre analytika** - pri zásahu pravidla je okamžite zrejmé, o akú fázu útoku a aký typ správania ide, bez toho, aby analytik musel dohľadávať význam.
- **Analýza pokrytia (coverage)** - z namapovania sa dá vypočítať, ktoré techniky sada pravidiel pokrýva a kde sú medzery v detekcii.
- **Reporting a komunikácia** - umožňuje reportovať zistenia a schopnosti detekcie v jazyku, ktorému rozumejú aj iné tímy a zákazníci.
- **Prepojenie na threat intelligence** - zistenia sa dajú korelovať so správaním konkrétnych útočných skupín, ktoré sú v MITRE ATT&CK tiež popísané cez techniky.

3.2 Event Type

Stĺpec **Event Type** určuje, na akom type telemetrie je pravidlo postavené, a tým aj to, kedy sa jeho podmienka vyhodnocuje. Nadobúda jednu zo šiestich hodnôt:

- **OnProcessCreate** - pravidlo sa vyhodnocuje pri každom vytvorení nového procesu (typicky zdroj ako Sysmon Event ID 1 alebo Windows Security Event ID 4688). K dispozícii sú polia ako názov procesu, príkazový riadok, rodičovský proces, hash a pod. Vhodné na detekciu spúšťania podozrivých binárok, zneužívaných legitímnych nástrojov (LOLBins) či nezvyčajných reťazcov procesov.
- **OnEvent** - pravidlo sa vyhodnocuje pri výskyte konkrétneho záznamu v event logu / ETW (napr. operačný log PowerShellu, bezpečnostný log). Ide o najširší typ, ktorý pokrýva rôznorodé zdroje udalostí a ich polia (payload).
- **OnRegistryValueChange** - pravidlo sa vyhodnocuje pri vytvorení alebo úprave hodnoty v registri (typicky Sysmon Event ID 13). Vhodné na detekciu perzistencie, úprav konfigurácie a manipulácie s nastaveniami systému.
- **OnFileCreate** – pravidlo sa vyhodnocuje pri vytvorení, či existencii súboru v rámci súborového systému (napríklad SACL Event ID 4663, prípadne MFT). Vhodné napríklad na detekciu škodlivých súborov útočníka.
- **OnConnectionEstablished** – pravidlo sa vyhodnocuje pri vytvorení sieťového spojenia (typicky Sysmon Event ID 3). Umožňuje detegovať spojenia na škodlivú infraštruktúru útočníka, či legítimne - no zneužívané weby.
- **OnDnsRequest** - pravidlo sa vyhodnocuje pri DNS žiadosti (typicky Sysmon Event ID 22). Umožňuje detegovať preklady domén škodlivej infraštruktúry útočníka, či legítimných - no zneužívaných webov.

Tento stĺpec zároveň slúži ako **abstrakcia nad zdrojom dát**: umožňuje, aby ten istý vyhodnocovací engine spracoval rôzne typy telemetrie jednotným spôsobom.

3.3 Trigger Condition

Stĺpec **Trigger Condition** obsahuje presnú podmienku, ktorej splnenie spôsobí, že pravidlo zareaguje. Ide o logický (booleovský) výraz, ktorý sa vyhodnotí voči konkrétnej udalosti a vráti pravda / nepravda. Je to jadro pravidla - definuje jeho detekčnú logiku.

Podmienka sa skladá z troch základných častí:

1. Odkazy na polia (podľa typu udalosti), napríklad:

- process.name, process.cmd, process.parent.name, process.hash - pre OnProcessCreate,
- etw.id, etw.fields.<názov>, etw.fields.payload - pre OnEvent,
- registry.path, registry.value_name, registry.value_data - pre OnRegistryValueChange.

2. Operátory na porovnanie hodnôt, napríklad:

- == (rovná sa), != (nerovná sa),
- Contains (obsahuje podreťazec),
- Starts with / Not starts with (začína / končí na),
- matches (zhoda s regulárnym výrazom).

3. Logické spojky na kombinovanie viacerých podmienok: AND, OR, NOT a zátvorky na určenie priority.

Príklady:

- process.name == 'psr.exe' - pravidlo zareaguje pri spustení procesu s názvom psr.exe.
- etw.id == 'Microsoft-Windows-PowerShell.4103' A etw.fields.payload contains 'CopyFromScreen' - pravidlo zareaguje, keď sa v operačnom logu PowerShellu vyskytne udalosť 4103 a jej payload zároveň obsahuje reťazec CopyFromScreen.

Podmienka je zámerne strojovo čitateľná a jednoznačná, aby ju bolo možné automaticky vyhodnotiť, verzionovať, testovať a v prípade potreby ladiť (napr. zúžením kvôli falošným poplachom).

3.4 Brief

Stĺpec **Brief** obsahuje krátky, ľudsky čitateľný názov pravidla - v podstate výstižnú „nálepku“, ktorá zhrnie, čo pravidlo deteguje. Slúži na rýchlu orientáciu: v zozname detekcií alebo v dashboarde analytik na prvý pohľad vidí, o čo ide, bez toho, aby musel čítať celú podmienku alebo detailný popis. Dobré formulovaný Brief výrazne zrýchľuje triedenie a prioritizáciu výstupov.

3.5 Description

Stĺpec **Description** obsahuje podrobnejší popis pravidla. Vysvetľuje, čo presne pravidlo deteguje, prečo je dané správanie podozrivé alebo relevantné z pohľadu útočníka, do akého kontextu (taktiky, techniky) zapadá, a podľa potreby aj možné legitímne výskyty (falošné poplachy) a odporúčania pre ďalšie vyšetrovanie. Tento stĺpec dáva analytikovi kontext priamo

v momente vyšetrovania konkrétnej detekcie a znižuje potrebu prepínať sa medzi nástrojmi a dohľadávať informácie inde.

4 Ako čítať pravidlá (ukážka)

Pre ilustráciu, ako jednotlivé stĺpce spolu tvoria jedno kompletne pravidlo, uvádzame dva príklady zamerané na zachytávanie obrazovky (screen capture).

Príklad A - zneužitie Psr.exe

Stĺpec	Hodnota
MITRE	T1113 (Screen Capture)
Event Type	OnProcessCreate
Trigger Condition	process.name == 'psr.exe'
Brief	Spustenie Psr.exe (Problem Steps Recorder)
Description	Deteguje spustenie legitímneho nástroja Windows „Problem Steps Recorder“ (Psr.exe), ktorý dokáže automaticky zachytávať snímky obrazovky pri akciách používateľa. Útočníci ho môžu zneužiť ako nástroj „living-off-the-land“ na zaznamenávanie činnosti obete bez potreby vlastného malvéru.

Čítanie pravidla: pri vytvorení akéhokoľvek procesu (OnProcessCreate) systém porovná názov procesu s hodnotou psr.exe. Ak sa zhodujú, pravidlo zareaguje, zásah sa označí ako technika T1113 a analytici sa zobrazia Brief a Description ako kontext.

Príklad B - zachytenie obrazovky cez PowerShell

Stĺpec	Hodnota
MITRE	T1113 (Screen Capture)
Event Type	OnEvent
Trigger Condition	etw.id == 'Microsoft-Windows-PowerShell.4103' AND etw.fields.payload contains 'CopyFromScreen'
Brief	Zachytenie obrazovky pomocou PowerShellu
Description	Deteguje záznam v operačnom logu PowerShellu (udalosť 4103 - logovanie modulov/pipeline), ktorého payload obsahuje volanie metódy CopyFromScreen. Táto .NET metóda sa používa na skopírovanie obsahu obrazovky do obrázka, čo je typický znak skriptu vykonávajúceho zachytávanie obrazovky.

Čítanie pravidla: pri výskyte udalosti v event logu (OnEvent) engine overí, že ide o PowerShell udalosť s ID 4103 **a zároveň** že jej payload obsahuje reťazec CopyFromScreen. Obe podmienky musia byť splnené (AND), aby pravidlo zareagovalo.

5 Prečo je táto štruktúra podstatná pre nástroj automatizujúci forenznú analýzu

Sada takto navrhnutých pravidiel je pre automatizovanú forenznú analýzu kľúčová z niekoľkých dôvodov:

Škálovateľnosť a konzistencia. Statické, deterministické pravidlá umožňujú spracovať veľké objemy telemetrie z mnohých systémov opakovateľne a jednotne. Nástroj aplikuje rovnakú logiku zakaždým rovnako, bez závislosti od skúseností či únavy konkrétneho analytika.

Zakódovanie znalostí do strojovo čitateľnej podoby. Každé pravidlo predstavuje jeden kus inštitucionálneho know-how o známej útočnickej technike, prevedený do formy, ktorú vie nástroj automaticky vyhodnotiť. Znalosť o tom, „ako útočník robí X“, tak nezostáva len v hlave experta, ale je zachytená, verzionovateľná a znovupoužiteľná.

Vysvetliteľnosť a auditovateľnosť. Na rozdiel od čiernej skrinky (napr. čisto štatistických modelov) má každý zásah jednoznačnú príčinu - konkrétnu splnenú podmienku. To je pri forenznej analýze zásadné, pretože zistenia musia byť obhájiteľné a doložiteľné, prípadne aj použiteľné ako dôkazný materiál.

Presnosť a laditeľnosť. Stĺpec Trigger Condition definuje presnú, testovateľnú logiku. Pravidlá sa dajú cielene zužovať alebo rozširovať podľa prostredia, čím sa riadi pomer medzi zachytením skutočných hrozieb a mierou falošných poplachov.

Jednotné spracovanie rôznych zdrojov dát. Stĺpec Event Type abstrahuje typ telemetrie (proces, event log, register), takže ten istý engine dokáže naprieč rôznymi zdrojmi aplikovať pravidlá rovnakým spôsobom. Pridanie nového pravidla nevyžaduje zmenu nástroja, len doplnenie riadku do katalógu.

Rýchlejšia forenzná analýza. Stĺpce Brief a Description dodávajú kontext priamo v momente zásahu, takže analytik netrávi čas dohľadávaním významu a môže sa sústrediť na triedenie a rozhodovanie. Namapovanie na MITRE ATT&CK pritom výsledky štruktúruje a umožňuje merať pokrytie techník. To všetko skracuje čas od výskytu aktivity po jej odhalenie a reakciu.

Rozšíriteľnosť. Katalóg pravidiel je živý dokument. S objavovaním nových techník či zneužití legitímnych nástrojov stačí pridávať ďalšie pravidlá, čím sa schopnosti nástroja priebežne rozširujú bez potreby prepracovania jeho jadra.

6 Poznámky k údržbe a rozširovaniu katalógu

Aby si sada pravidiel udržala hodnotu, odporúča sa:

- **konzistentné mapovanie na MITRE ATT&CK** - každé nové pravidlo priradiť k technike (prípadne subtechnike), aby zostala platná analýza pokrytia,
- **jasné a stručné Brief názvy** - aby zostali použiteľné pre rýchlu triáž,
- **dokumentované falošné poplchy** - v Description uvádzať známe legitímne výskyty a spôsob ich odlíšenia,
- **verzionovanie a testovanie podmienok** - zmeny v Trigger Condition testovať oproti známym vzorkám, aby sa predišlo neúmyselnému zúženiu alebo rozšíreniu detekcie,
- **periodické revízie** - pravidlá priebežne aktualizovať podľa nových poznatkov a zmien v telemetrii (napr. zmeny formátu event logov).

7 Príloha

ADFIR-D22-KPB4-04-Appendix.xlsx