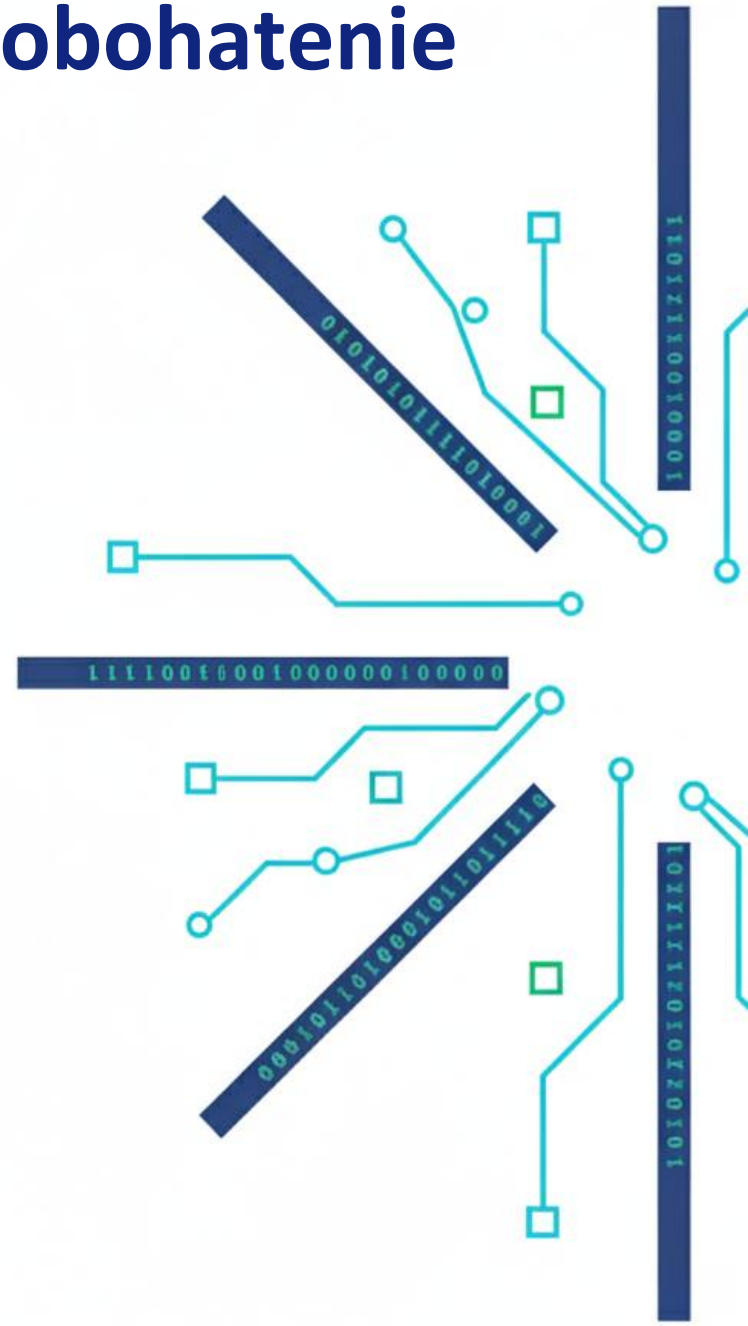
D18 – Model na obohatenie digitálnych stôp



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

Popis projektu *6*
1 Možnosti digitálneho obohatenia dôkazov *7*
2 Zložitosť obohacovania digitálneho artefaktu – predspracovanie *11*
3 Spôsoby, ako obohatiť digitálne stopy *12*
3.1 API kľúč / token **12**
3.1.1 Význam a použitie 12
3.1.2 Typické artefakty obsahujúce údaje 12
3.1.3 Spôsoby a nástroje na obohatenie 12
3.2 Cloud Resource ID **13**
3.2.1 Význam a použitie 13
3.2.2 Typické artefakty obsahujúce údaje 13
3.2.3 Spôsoby a nástroje na obohatenie 13
3.3 Podpis kódu **13**
3.3.1 Význam a použitie 14
3.3.2 Typické artefakty obsahujúce údaje 14
3.3.3 Spôsoby a nástroje na obohatenie 14
3.4 Adresy kryptomenových peňaženiek **14**
3.4.1 Význam a použitie 14
3.4.2 Typické artefakty obsahujúce údaje 15
3.4.3 Spôsoby a nástroje na obohatenie 15
3.5 CVE / Zraniteľnosť **15**
3.5.1 Význam a použitie 15
3.5.2 Typické artefakty obsahujúce údaje 16
3.5.3 Spôsoby a nástroje na obohatenie 16
3.6 Digitálny certifikát **16**
3.6.1 Význam a použitie 16
3.6.2 Typické artefakty obsahujúce údaje 16
3.6.3 Spôsoby a nástroje na obohatenie 17
3.7 DNS dopyty **17**
3.7.1 Význam a použitie 17
3.7.2 Typické artefakty obsahujúce údaje 17
3.7.3 Spôsoby a nástroje na obohatenie 17
3.8 E-mailová adresa **18**
3.8.1 Význam a použitie 18
3.8.2 Typické artefakty obsahujúce údaje 18
3.8.3 Spôsoby a nástroje na obohatenie 19
3.9 Hash súboru **19**
3.9.1 Význam a použitie 20

3.9.2 Typické artefakty obsahujúce údaje 20
3.9.3 Spôsoby a nástroje na obohatenie 21

3.10 FQDN / Doménové meno 21
3.10.1 Význam a použitie 21
3.10.2 Typické artefakty obsahujúce údaje 22
3.10.3 Spôsoby a nástroje na obohatenie 22

3.11 Geolokácia 23
3.11.1 Význam a použitie 23
3.11.2 Typické artefakty obsahujúce údaje 23
3.11.3 Spôsoby a nástroje na obohatenie 23

3.12 Zdroj logu 24
3.12.1 Význam a použitie 24
3.12.2 Typické artefakty obsahujúce údaje 24
3.12.3 Spôsoby a nástroje na obohatenie 24

3.13 MAC adresa 24
3.13.1 Význam a použitie 24
3.13.2 Typické artefakty obsahujúce údaje 25
3.13.3 Spôsoby a nástroje na obohatenie 25

3.14 MITRE ATT&CK ID 25
3.14.1 Význam a použitie 25
3.14.2 Typické artefakty obsahujúce údaje 25
3.14.3 Spôsoby a nástroje na obohatenie 26

3.15 Názov mutexu a named pipe 26
3.15.1 Význam a použitie 26
3.15.2 Typické artefakty obsahujúce údaje 26
3.15.3 Spôsoby a nástroje na obohatenie 26

3.16 Sieťový tok - Netflow 27
3.16.1 Význam a použitie 27
3.16.2 Typické artefakty obsahujúce údaje 27
3.16.3 Spôsoby a nástroje na obohatenie 27

3.17 Sieťový port / protokol 27
3.17.1 Význam a použitie 27
3.17.2 Typické artefakty obsahujúce údaje 28
3.17.3 Spôsoby a nástroje na obohatenie 28

3.18 Meno osoby 28
3.18.1 Význam a použitie 28
3.18.2 Typické artefakty obsahujúce údaje 29
3.18.3 Spôsoby a nástroje na obohatenie 29

3.19 Telefónne číslo 29
3.19.1 Význam a použitie 29

3.19.2 Typické artefakty obsahujúce údaje 29
3.19.3 Spôsoby a nástroje na obohatenie 30

3.20 Súkromná IP adresa 30
3.20.1 Význam a použitie 30
3.20.2 Typické artefakty obsahujúce údaje 30
3.20.3 Spôsoby a nástroje na obohatenie 31

3.21 Názov procesu 31
3.21.1 Význam a použitie 32
3.21.2 Typické artefakty obsahujúce údaje 32
3.21.3 Spôsoby a nástroje na obohatenie 32

3.22 Verejná IP adresa - externá 32
3.22.1 Význam a použitie 32
3.22.2 Typické artefakty obsahujúce údaje 33
3.22.3 Spôsoby a nástroje na obohatenie 33

3.23 Verejné IP, vlastnené samotnou organizáciou 34
3.23.1 Význam a použitie 34
3.23.2 Typické artefakty obsahujúce údaje 34
3.23.3 Spôsoby a nástroje na obohatenie 35

3.24 Kľúč/hodnota registra 35
3.24.1 Význam a použitie 35
3.24.2 Typické artefakty obsahujúce údaje 35
3.24.3 Spôsoby a nástroje na obohatenie 36

3.25 Plánovaná úloha / Cron 36
3.25.1 Význam a použitie 36
3.25.2 Typické artefakty obsahujúce údaje 36
3.25.3 Spôsoby a nástroje na obohatenie 36

3.26 URL 37
3.26.1 Význam a použitie 37
3.26.2 Typické artefakty obsahujúce údaje 37
3.26.3 Spôsoby a nástroje na obohatenie 38

3.27 Používateľský účet 38
3.27.1 Význam a použitie 38
3.27.2 Typické artefakty obsahujúce údaje 39
3.27.3 Spôsoby a nástroje na obohatenie 39

3.28 User-Agent reťazec 40
3.28.1 Význam a použitie 40
3.28.2 Typické artefakty obsahujúce údaje 40
3.28.3 Spôsoby a nástroje na obohatenie 41

3.29 WiFi SSID / BSSID 41
3.29.1 Význam a použitie 42

3.29.2 Typické artefakty obsahujúce údaje 42
3.29.3 Spôsoby a nástroje na obohatenie 42

3.30 Windows Event ID 42
3.30.1 Význam a použitie 42
3.30.2 Typické artefakty obsahujúce údaje 43
3.30.3 Spôsoby a nástroje na obohatenie 43

3.31 Windows služba 43
3.31.1 Význam a použitie 43
3.31.2 Typické artefakty obsahujúce údaje 43
3.31.3 Spôsoby a nástroje na obohatenie 44

3.32 YARA a Sigma pravidlá 44
3.32.1 Význam a použitie 44
3.32.2 Typické artefakty obsahujúce údaje 44
3.32.3 Spôsoby a nástroje na obohatenie 44

4 Schematický návrh modelu na obohacovanie digitálnych stôp 45

4.1 Vyťažovanie dát na obohatenie zo sparsovaných dát 45
4.1.2 1. úroveň obohatenia 52
4.1.3 2. až N-tá úroveň obohatenia 52
4.1.4 Schéma procesu spracovania a obohacovania stôp 52
4.1.5 Pseudokód 54

5 Záver 58

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. 09-I05-03-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 forenzných 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 forenzných 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 Možnosti obohatenia digitálnych stôp

Ako prvý krok je potrebné objasniť, aké informácie je možné získať z digitálnych dôkazov a ktoré z nich sú vhodné na ďalšie obohatenie. Pri výbere boli zohľadnené nasledujúce kritériá:

- Je to informácia, ktorú možno použiť ako indikátor kompromitácie?
  - Napríklad IP adresa, URL alebo hash súboru sú štandardné príklady údajov, s ktorými sa dá ďalej pracovať. Existuje viacero verejne dostupných dôveryhodných služieb, ktoré nám umožňujú získať o nich ďalšie informácie.
- Je zvyčajne možné tieto informácie získať z digitálnych stôp?
  - FQDN, MAC adresa, telefónne číslo alebo názov bežiaceho procesu sa vyskytujú, či už v úlohe dôležitej stopy alebo irelevantných údajov, na disku alebo v logoch udalostí mnohých zariadení, ktoré môžeme analyzovať.
- Existujú dostatočne overené externé zdroje, prostredníctvom ktorých je možné dáta obohatiť o poznatky z komunity?
  - Podobné obmedzenia ako pri dátach, ktoré môžeme použiť ako IOC.

Zhrnuli sme vybrané typy údajov a identifikovali možnosti ich obohatenia. Tabuľka č. 1 poskytuje prehľad o nich a ich význame pre forenznú analýzu, ako aj o najbežnejších artefaktoch, v ktorých sa daný typ údajov nachádza. Jednotlivé metódy obohacovania digitálnych artefaktov sú uvedené v rozšírenej tabuľke , ktorú prikladáme k dokumentu.

#	Typ údajov	# Obohatenia	Kľúčové využitie vo forenzných vedách	Príklady zdrojov (forenzných artefaktov) typu údajov
1	API kľúč / token	5	Odhaľovanie krádeže prihlasovacích údajov, neoprávnené používanie API a únik API kľúčov.	Súborový systém, konfiguračné súbory, skripty, ...
2	Cloud Resource ID	7	Vyšetrovanie únikov v cloude, nesprávnych konfigurácií a neoprávneného prístupu.	AWS/Azure/GCP – pravdepodobne priama analýza v konzole, alebo inak získané dáta o cloudovej infraštruktúre.
3	Podpis kódu (code signing certificate)	6	Overenie legitímnosti softvéru, detekcia podpísaného malvéru.	Podpis spustiteľného súboru
4	Adresa kryptomenovej peňaženky	5	Sledovanie platby ransomvéru a finančná atribúcia.	Ransom notes, vzorky malvéru. Osobné kryptopeňaženky, história transakcií používateľa.
5	CVE / Zraniteľnosť	10	Určenie pravdepodobnosti zneužitia zraniteľnosti a prioritizácia záplat.	Vzorky malvéru
6	Digitálny certifikát	13	Identifikácia škodlivej infraštruktúry, detekcia zneužívania certifikátov.	Úložisko certifikátov, súborový systém (odlišujeme Machine, User certifikáty)
7	DNS dotaz	6	Detekcia C2 beaconov, DNS tunelovania a DGA domén.	DNS logy.

8	E-mailová adresa	10	Sledovanie phishingových kampaní, overenie legitimity odosielateľov, prepájanie persón.	Artefakty e-mailu: lokálna schránka, hlavičky e-mailov, logy a úložisko MS365/Exchange, história prehliadania (navštívené schránky).
9	Hash súboru	20	Identifikácia malvéru, mapovanie na rodiny malvéru, hodnotenie schopností a atribúcia.	Image disku/HDD/SSD – súborový systém, exportované dokumenty – hashe vypočítané z jeho obsahu; Amcache.
10	FQDN / Doménové meno	24	Sledovanie infraštruktúry C2, phishingových domén a vzorcov registrácie útočníkov.	História prehliadania, PowerShell logy/trace, vzorky malvéru, sieťové logy, najmä web proxy a podobne.
11	Geolokácia	4	Detekcia nemožného cestovania, pôvod neoprávneného prístupu.	Najpravdepodobnejšie sú cloudové dátové zdroje (MS365, Google účet - Google mapy, Apple účet, ...), WiFi kľúče v registri (niekedy je možné online vyhľadať MAC adresu routera alebo AP).
12	Zdroj logu	4	Zabezpečiť integritu logov a správnu rekonštrukciu časovej osi.	Log samotný, riadiace konzoly SIEM/EDR/XDR/SCCM a podobne.
13	MAC adresa	5	Sledovanie fyzického zariadenia, detekcia spoofingu a neautorizovaných zariadení.	Kľúče registra, JumpListy, LNK súbory. ARP tabuľky, DHCP logy, CAM tabuľky switchov
14	MITRE ATT&CK ID	6	Mapovanie správanie protivníka na framework, určovanie postupu pri detekcií a reakcií.	Rôzne artefakty.
15	Názov Mutexu	2	Identifikácia rodín malvéru a detekcia súbežnej infekcie	Obraz/obsah pamäte RAM, vzorka malvéru.
16	Named Pipe	2	Detekcie C2 frameworkov a techniky bočného pohybu.	Obraz pamäte RAM, vzorka malvéru, záznamy udalostí (ak sa používajú ako služba).
17	Sieťový tok (Network Flow)	7	Identifikácia úniku dát, laterálneho pohybu a komunikácie s C2.	Netflows, ak sú k dispozícii. Záznamy prevádzky zo sieťových sond či span portu.
18	Sieťový port / protokol	4	Detekcia protokolových anomálií, tunelovania a neautorizovaných služieb.	Firewall (pravidlá a logy), IDS/IPS, EDR. Netflows
19	Meno osoby	5	Atribúcia, vyšetrovanie hrozieb zvnútra, profilovanie cez OSINT.	Dokumenty, e-maily a podobné, s používateľom súvisiace údaje. Chatovacie aplikácie. Active Directory. Mobilné telefóny a cloudové dáta/kontakty.
20	Telefónne číslo	5	Vyšetrovanie vishingu, SMS phishingu a sociálneho inžinierstva.	Dokumenty, e-maily a podobné, používateľské údaje. Active Directory (ak sú kontaktné údaje uvedené vo vlastnostiach účtu). Forenzná analýza mobilných telefónov (kontakty). Uložené kontakty/vcf súbory. Cloudové účty – kontakty (Google, Apple ID a pod., uložené kontakty).

21	Súkromná IP adresa	17	Mapovanie rozsahu vnútornej kompromitácie, identifikácia postihnutých systémov a segmentov.	Logy prihlásenia (evtx a ďalšie), RDP logy, konfiguračné a logové súbory nástrojov na vzdialený prístup, vzorky malvéru. DHCP logy, DNS, Active Directory. Dokumentácia siete.
22	Názov procesu	9	Odhaľovanie zneužívania, maskovania a škodlivých procesov LOLBins.	EDR, SIEM, EVTX logy, obraz pamäte RAM.
23	Verejná IP adresa	33	Identifikácia infraštruktúry útočníka, hostingu, geolokácie a reputácie.	Logy prihlásenia (evtx a ďalšie), RDP logy, konfiguračné a logové súbory nástrojov na vzdialený prístup, vzorky malvéru. DHCP logy, DNS, Active Directory.
24	Kľúč/hodnota registra	5	Identifikácia mechanizmov perzistencie a zmien konfigurácie.	Windows Registry.
25	Plánovaná úloha / Cron	5	Identifikácia mechanizmov perzistencie a neoprávnenej automatizácie.	SchTasks kľúč registru, eventové záznamy, definačné súbory. Crontab. Poznámka: artefakt by už mal byť spracovaný v štandardnej fáze parsovania.
26	Sigma pravidlá	4	Overiť detekcie založené na logoch a mapovať na ATT&CK	Rôzne, Sigma pravidlá vytvorené na základe analýzy, známe IOC, spravodajské informácie a podobne.
27	URL	10	Analýza phishingu, doručenia payloadu a presmerovacích reťazcov.	História prehliadania, PowerShell logy/trace, vzorky malvéru, sieťové logy - webový proxy.
28	Používateľský účet	15	Odhaľovanie kompromitovaných účtov, hodnotenie eskalácie oprávnení, auditovanie prístupu.	Zoznam používateľských profilov, logy prihlásenia, Active Directory.
29	User-Agent reťazec	5	Detekcia škodlivých nástrojov, C2 frameworkov a anomálnych klientov.	História prehliadania, logy webservera.
30	WiFi SSID / BSSID	3	Detekcia neoprávnených bezdrôtových prístupových bodov (Wireless Access Points, AP) a sledovanie fyzickej blízkosti.	Kľúče registra súvisiace so sieťovými nastaveniami.
31	Windows Event ID	5	Budovanie časovej osi útokov, detekcia konkrétnych techník protivníka.	Windows Event Logs (evtx súbory).
32	Windows služba	6	Detekcia perzistencie a eskalácie privilégií na základe služieb.	Kľúče registra súvisiace so službami. Event logy (System.evtx, Security.evtx). Poznámka: mal by byť už spracovaný v štandardnej fáze spracovania!
33	YARA pravidlá	3	Rozsah infekcie malvérom a overenie pokrytia detekcie pravidlom.	Rôzne, pravidlá YARA vytvorené na základe analýzy,

				známych IOC, informácií a podobne.

Tabuľka 1

3 Zložitosť obohacovania digitálneho artefaktu – predspracovanie

Pri navrhovaní modelu je vhodné upresniť, ktoré informácie, ktoré budeme ďalej obohacovať, sú zvyčajne už dostupné v parsovaných dátach a ktoré vyžadujú určitú formu predspracovania (okrem už vykonaného spracovania digitálnych dôkazov). Pre účely tohto dokumentu sme rozdelili typy údajov na obohacovanie do troch kategórií:

1. **Spracované**: Dáta, ktoré sa zvyčajne nachádzajú vo výstupe pri spracovaní digitálneho dôkazu a môžu byť okamžite ďalej spracované. Patria sem napríklad IP adresy získané z logov udalostí, používateľské mená získané zo SAM a ProfileList, SHA1 hashe súborov z AmCache a podobne.

2. **Vypočítané**: Dáta ako hashe súborov na analyzovanom digitálnom zdroji: nemôžeme ich získať parsovaním štandardných artefaktov, je potrebné najprv vypočítať hash. Môžeme sem tiež zahrnúť dáta, ktoré môžeme extrahovať pomocou regulárnych výrazov, ako sú IP adresy alebo e-mailové adresy, ktoré sa nachádzajú mimo artefaktov, z ktorých ich získavame štandardným parsovaním. IP adresu možno ľahko nájsť v event ID 4624 v Security.evtx (Parsed Artifact), ale dá sa nájsť aj v konfiguračnom súbore, odkiaľ by sa dala získať len podrobnejším vyhľadávaním. IP adresy však budeme klasifikovať ako „Spracované“ či „Parsed“ artefakty, nie ako vypočítané artefakty, keďže primárne počítame s ich výskytom na bežných miestach, v parsovaných artefaktoch.

3. **Zložené:** Napríklad pravidlá YARA alebo Sigma. Aby sme ich mohli vytvoriť, zvyčajne musíme kombinovať niekoľko artefaktov, vyhodnotiť potrebné logické podmienky na funkčnosť výsledného pravidla, získať znalosti o jeho návrhu alebo získať potrebné existujúce pravidlá z externého zdroja prostredníctvom spravodajstva o hrozbách (Threat Intelligence).

4 Spôsoby, ako obohatiť digitálne stopy

V nasledujúcej časti predstavíme každý typ dát, ktoré navrhujeme obohatiť. Zahrnuli sme tiež informácie o artefaktoch, v ktorých sa každý z "obohacovateľných" dátových typov nachádzal. Nakoniec pre každý typ dát poskytujeme popis, ako by sa obohacovanie mohlo vykonať a aká kombinácia s ďalšími údajmi je potrebná na získanie najhodnotnejších a najpresvedčivejších výsledkov.

4.1 API kľúč / token

4.1.1 Význam a použitie

Odhaľujte krádež prihlásenia, neoprávnené používanie API a zverejňovanie kľúčov. Obohacovanie API kľúčov alebo tokenov nám môže pomôcť pochopiť, k čomu má prihlasovacie oprávnenie prístup a aké nebezpečné môže byť jeho odhalenie. Podľa skúseností nášho tímu sú najužitočnejšími prvkami súvisiaca služba, efektívny rozsah oprávnení, detaily vytvorenia, čas posledného použitia API kľúča a či sa kľúč objavil vo verejných repozitároch. Hlavnou výhradou voči výpovednej hodnote kľúča či tokenu je, že hodnota kľúča závisí od jeho skutočných oprávnení a aktuálnej platnosti, takže samotný identifikátor na posúdenie dopadov úniku nestačí.

4.1.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa API kľúče a tokeny často obnovujú zo skriptov, zdrojového kódu, konfiguračných súborov, premenných prostredia, artefaktov prehliadača, histórie cloud CLI, PowerShell logov, záznamov pamäte RAM, CI/CD súborov, poznámok vývojára a EDR telemetrie. API kľúče/tokeny v „surovom stave“ (nešifrované, uložené v rôznych skriptoch) môžu byť prítomné v artefaktoch zbieraných z koncových zariadení, ale rozsah oprávnení, tvorca, história používania a informácie o verejnej expozícií tokenu/kľúča zvyčajne pochádzajú z cloudových logov alebo nástrojov na vyhľadávanie v repozitároch, nie z samotného endpointu. V praxi spočíva najsilnejšia hodnota v jeho naviazaní kľúča na používateľa, proces, repozitár alebo cloudovú akciu.

4.1.3 Spôsoby a nástroje na obohatenie

Zvyčajne sa v prvom kroku služba identifikuje podľa formátu tokenu alebo pridruženej aplikácie. Potom môžeme pokračovať v kontrole IAM politík, OAuth rozsahov, auditných logov a záznamov používania, aby sme potvrdili oprávnenia, tvorcu a čas posledného použitia. Môžeme tiež skontrolovať nástroje na zviditeľnenie repozitárov a zdroje verejného kódu, aby sme zistili, či tajomstvo uniklo.

Obohatenie API kľúčov je najužitočnejšie, keď sa kombinuje s dôkazmi z analyzovaných koncových zariadení, cloudovými auditnými logmi a prehľadom histórie prístupu.

4.2 Cloud Resource ID

Vyšetrovanie únikov v cloude, nesprávnych konfigurácií a neoprávneného prístupu.

4.2.1 Význam a použitie

Z pohľadu forenzného analytika by nám obohacovanie cloud resource ID malo pomôcť pochopiť, o aký zdroj (resource) ide, kto ho vlastní, kde sa nachádza, k čomu má prístup a či je vystavený internetu. Najužitočnejšie prvky sú typ zdroja, vlastnícky účet alebo predplatné, región, priradená IAM rola, verejná expozícia, detaily vytvorenia a tagy. Musíme však mať na pamäti, že cloudové zdroje sa menia rýchlo, preto by sa vlastníctvo a expozícia mali vždy overovať na základe aktuálnych logov a metadát z riadiacich prvkov pre daný resource (napr. cloudová konzola).

4.2.2 Typické artefakty obsahujúce údaje

Na systémoch Windows je možné cloudové ID zdrojov obnoviť z histórie prehliadača, histórie cloudových CLI, PowerShell logov, skriptov, konfiguračných súborov, EDR telemetrie, záznamov z pamäte, screenshotov, poznámok vývojára a exportovaných cloudových logov. Nespracovaný identifikátor môže byť prítomný v artefaktoch koncových bodov, ale detaily ako IAM rola, verejná expozícia, tvorca a vlastníctvo účtu zvyčajne pochádzajú z telemetrie na strane cloudu. Najväčšia hodnota prichádza z naviazania ID zdroja na akciu používateľa, prihlasovacie údaje, skript alebo udalosť prístupu.

4.2.3 Spôsoby a nástroje na obohatenie

V navrhovanom workflow zvyčajne vyhľadávame zdroje v cloudovej konzole, auditné logy a metadáta IAM, aby sme potvrdili ich typ, vlastníctvo, región, oprávnenia, históriu vytvorenia a tagy. Tiež kontrolujeme tzv. security posture alebo bezpečnostné nástroje, aby sme zistili, či je zdroj (nedopatrením) verejne prístupný alebo inak nesprávne konfigurovaný.

Obohacovanie dát o cloudových zdrojoch je najužitočnejšie, keď sa kombinuje s artefaktami z koncových bodov, identitami a dôkazmi z auditných záznamov, a nespolieha sa iba na ich identifikáciu.

4.3 Podpis kódu

Overenie legitímnosti softvéru, detekcia podpísaného malvéru.

4.3.1 Význam a použitie

Z pohľadu forenzného analytika nám obohacovanie údajov podpisovania kódu pomáha posúdiť, či je podpísaný binárny súbor skutočne dôveryhodný, alebo sa len javí dôveryhodne. Polia ako meno podpisovateľa, platnosť reťazca certifikátov, časová pečiatka, stav zrušenia, znalosť zneužitie daného certifikáciu a odtlačok certifikátu sú užitočné na overovanie nárokov vydavateľa, odhaľovanie ukradnutých alebo zneužitých certifikátov a zhlukovanie súvisiacich vzoriek podpísaného malvéru. Podľa skúseností nášho tímu pomáha platný podpis s doplnením kontextu, ale sám o sebe nikdy nestačí, pretože útočníci bežne zneužívajú legitímne certifikáty.

4.3.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa detaily podpisovania kódu najčastejšie obnovujú priamo zo spustiteľného súboru, ale môžu sa objaviť aj v Amcache, EDR telemetrii, antimalware detekciách, artefaktoch PowerShell o vykonávaní skriptov, záznamoch o sťahovaní z webového prehliadača a súboroch z disku alebo pamäte. Mená signatárov a odtlačky môžu byť niekedy zachované v metadátach bezpečnostných nástrojov aj vtedy, keď pôvodný súbor už nie je dostupný. Externé detaily, ako je stav revokácie certifikátu alebo známe škodlivé použitie toho istého certifikátu, zvyčajne vyžadujú obohatenie nad rámec endpointu.

4.3.3 Spôsoby a nástroje na obohatenie

V našom pracovnom postupe zvyčajne kontrolujeme podpisy pomocou nástrojov ako sigcheck, PEStudio, OpenSSL a VirusTotal na overenie identity podpisovateľa, trust chainu, protipodpisu, odvolania (revocation status) a identifikátorov certifikátov. Potom sa zameriavame na odtlačok alebo sériové číslo v zdrojoch spravodajstva o hrozbách, ako sú VirusTotal, ReversingLabs alebo MISP, aby sme zistili, či bol ten istý podpisový certifikát použitý na známom malvére. Stopy súvisiace s podpisovaním kódu sú najužitočnejšie v kombinácii s analýzou hashov súborov, kontextom vykonávania a ďalšími artefaktmi koncových bodov.

4.4 Adresy kryptomenových peňaženiek

Sledovanie platby ransomvéru a finančná atribúcia.

4.4.1 Význam a použitie

Obohacovanie adries kryptomenových peňaženiek nám pomáha pochopiť, či je peňaženka len platobným koncovým bodom alebo súčasťou väčšieho kriminálneho či regulovaného ekosystému. Najužitočnejšími prvkami sú história transakcií, asociácia s ransomvérom, zhlukovanie súvisiacich peňaženiek, atribúcia burzy a screening sankcií. Hlavnou výhradou je, že viditeľnosť blockchainu automaticky neznamená atribúciu, preto by sa závery získané o

peňaženkách mali považovať za pravdepodobnostné, pokiaľ nie sú podložené silnejším externým dôkazom.

4.4.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa kryptomenové adresy často získavajú zo správ vydieračov (ransom notes), chatových záznamov, e-mailov, histórie prehliadača, artefaktov v schránke (clipboard), aplikácií peňaženiek, záznamov z pamäte RAM, skriptov, dokumentov a EDR telemetrie viazanej na vydieranie alebo podvodnú činnosť. Samotná adresa môže byť prítomná v artefaktoch na koncových zariadeniach, ale história stavu konta, zhlukovanie, priradenie k burze a prípadný kontext vydaných sankcií sú zvyčajne analyticky pridané vylepšenia získané z blockchainu a compliance zdrojov. Najsilnejšiu hodnotu pre vyšetrovanie prináša prepojenie adresy peňaženky s udalosťou vydierania, interakciou používateľa alebo platobným procesom.

4.4.3 Spôsoby a nástroje na obohatenie

V našom pracovnom postupe odporúčame začať s blockchainovým prieskumníkom (napríklad https://www.blockchain.com/explorer alebo mnohými ďalšími), ktorý prehliada zostatok a transakčnú aktivitu, potom je vhodné skontrolovať reportovanie ransomvéru, využiť služby zhlukovania peňaženiek (ak je takáto služba pre vyšetrovateľa dostupná), overiť zdroje atribúcie búrz a zoznamy sankcií. Tieto výsledky môžeme použiť na posúdenie, či je peňaženka prepojená so známymi kampaňami, súvisiacimi peňaženkami, burzami alebo sankcionovanými subjektmi.

Obohatenie kryptomenových adries je najužitočnejšie, keď sa kombinuje s dôkazmi z koncových bodov, komunikácie a časovej osi incidentov.

4.5 CVE / Zraniteľnosť

Určenie pravdepodobnosti zneužitia a uprednostnenie záplaty.

4.5.1 Význam a použitie

Z pohľadu forenzného analytika nám obohacovanie dát CVE pomáha posúdiť, nakoľko je zraniteľnosť relevantná pre vyšetrovanie a ako naliehavo by sa mala riešiť. Intuitívne sú najpoužiteľnejšie polia ako popis CVE, CVSS, postihnuté produkty, dostupnosť verejných exploitov, aktívne zneužitie, stav KEV, dostupnosť záplat, mapovanie ATT&CK, známe použitie útočníkmi a skóre EPSS. Hlavnou výhradou je, že samotná závažnosť nestačí: vysoký CVSS môže byť menej dôležitý ako aktívne využívanie alebo potvrdená expozícia v skúmanom prostredí.

4.5.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa samotný identifikátor CVE môže objaviť vo výsledkoch skenera zraniteľností, nálezoch EDR, nástrojoch na správu záplat, upozorneniach SIEM systémov, v ticketovacích systémoch, referenciách pre dodávateľov a poznámkach k incidentom. Je pochopiteľné, že detaily CVE sa nemajú vyskytovať v natívnych artefaktoch koncových bodov alebo v ich spracovanej verzii. Zvyčajne korelujeme údaje CVE s nainštalovaným softvérom, informáciami o verziách, stavom záplat a stopami zneužitia z logov, procesnej aktivity či z forenzných artefaktov na postihnutom systéme. Najväčšiu hodnotu prináša prepojenie CVE so skutočne zraniteľným aktívom a akékoľvek známkami zneužívania.

4.5.3 Spôsoby a nástroje na obohatenie

Pri získavaní ďalších údajov o CVE je vhodné začať s odporúčaniami NVD, CVE.org, MITRE a dodávateľmi na overenie popisu a hodnotenia zraniteľností, ovplyvnených verzií a usmernení k náprave. Potom môžeme skontrolovať zdroje ako ExploitDB, Metasploit, GitHub, KEV, platformy na reportovanie hrozieb a EPSS, aby sme pochopili zneužiteľnosť a reálne riziká.

Obohacovanie CVE je najužitočnejšie, keď sa kombinuje s inventárom aktív, riešeniami na správu záplat a dôkazmi z vyšetrovaných incidentov samotných.

4.6 Digitálny certifikát

Identifikovanie škodlivej infraštruktúry, odhalenie zneužívania certifikátov.

4.6.1 Význam a použitie

Obohacovanie certifikátov pomáha forenznému analytikovi pochopiť, do akej infraštruktúry certifikát patrí a či vyzerá rutinne, alebo je nastavený nesprávne alebo podozrivo. Polia ako predmet, SAN, vydavateľ, doba platnosti, sériové číslo, odtlačok, algoritmus podpisu, typ kľúča, stav zrušenia, prítomnosť CT logu, samopodpísaný stav (self-signing status), voľné CA použitie a opätovné použitie certifikátu na iných zariadeniach sú užitočné na zhlukovanie súvisiacich systémov, identifikáciu exponovaných služieb a odhaľovanie slabej dôveryhodnosti alebo opustenej infraštruktúry. Hlavným obmedzením je, že certifikáty sú silnými indikátormi infraštruktúry, ale samy o sebe nie dôkazom zámeru, najmä ak ide o zdieľaný hosting, CDN alebo automatizovane vydávané certifikáty.

4.6.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa detaily certifikátov môžu objavovať v artefaktoch prehliadača, v úložiskách certifikátov Windows, v logoch súvisiacich so SChannel/TLS, v telemetrii EDR, v logoch webových proxy, artefaktoch e-mailových klientov, pamäti RAM a v záznamoch sieťovej prevádzky (packet capture) obsahujúcich TLS handshake. Niekedy tiež obnovujeme subjekty certifikátov, SAN, odtlačky alebo mená vydavateľov z konfigurácií malvéru,

stiahnutých súborov, PowerShell skriptov a forenzných údajov o sieťových pripojeniach. Niektoré polia, ako napríklad história CT logov, stav odvolania alebo iné koncové zariadenia s rovnakým certifikátom, zvyčajne pochádzajú z externého obohacovania, nie z natívnych artefaktov koncových bodov.

4.6.3 Spôsoby a nástroje na obohatenie

Je bežné extrahovať metadáta certifikátov pomocou OpenSSL alebo podobných nástrojov a potom prejsť na zdroje ako crt.sh, Censys a Shodan pre históriu CT a opätovné použitie certifikátov naprieč infraštruktúrou. Prehodnocujeme vydavateľa, validitu, revokáciu, odtlačok prsta, algoritmus podpisu a kľúčové vlastnosti, potom tieto zistenia korelujeme s doménami, IP adresami a dôkazmi z koncových zariadení.

Na základe skúseností nášho tímu sú certifikáty najužitočnejšie, keď sa analyzujú spolu s príbuznými artefaktmi z endpointov, domény a siete - nie izolovane.

4.7 DNS dopyty

Detegovanie C2 beaconing, DNS tunneling a DGA domény.

4.7.1 Význam a použitie

Obohacovanie DNS dotazov používame, aby sme pomohli vyšetrovateľom rozhodnúť, či je aktivita pri name resolution rutinná, podozrivá alebo jasne spojená so správaním malvéru. Podľa skúseností nášho tímu sú najužitočnejšie prvky, o ktoré možno dopyty obohatiť, typ dotazu, reputácia a infraštruktúra dotazovanej domény, vrátená odpoveď, frekvencia dotazov, indikátory tunelovania a proces samotného vyžadovania. Hlavnou nevýhodou je, že jediný nezvyčajný dotaz zriedka stačí sám o sebe; vzor v priebehu času a proces, ktorý za ním stojí, zvyčajne zaváži najviac. Preto množstvo forenzných dôkazov potrebných na vytvorenie legitímneho záveru môže byť relatívne veľké a pochádzať z rôznych zdrojov.

4.7.2 Typické artefakty obsahujúce údaje

Detaily týkajúce sa DNS dotazov sa bežne získavajú z logov DNS klienta, Sysmon Event ID 22, EDR telemetrie, packet captures, proxy logov a niekedy aj zo záznamov v pamäti RAM. Názov dopytu, typ a odpoveď môžu byť natívne pre artefakt, zatiaľ čo hodnotenia reputácie domény a tunelovania sú analyticky pridané vylepšenia. Najsilnejšiu hodnotu prináša viazanie DNS aktivity na konkrétny proces, používateľskú reláciu a následné sieťové pripojenie.

4.7.3 Spôsoby a nástroje na obohatenie

Obohacovací workflow by mal začať preštudovaním typu dotazu a vrátených dát. Potom vyšetrovatelia alebo navrhovaný model obohacovania aplikujú plné obohatenie domény na

dopytované meno. Môžeme kontrolovať frekvenciu a objem v SIEM alebo DNS analytike, hľadať vzory typické pre tunelovanie, ako sú dlhé subdomény alebo subdomény s vysokou entropiou, nezvyčajné typy záznamov, a tam, kde je to možné, identifikovať požadovaný proces zo Sysmon alebo EDR.

Obohatenie DNS dotazov je najužitočnejšie, keď sa kombinuje s dôkazmi z procesov, sietí a časových línií.

4.8 E-mailová adresa

Sledovanie phishingových kampaní, overenie legitimity odosielateľa, referencia na persony.

4.8.1 Význam a použitie

Z pohľadu forenzného analytika nám obohatenie e-mailových adries pomáha prejsť od jednoduchého reťazca odosielateľa alebo príjemcu k úplnejšiemu pochopeniu legitímnosti, pôvodu, expozície a vyšetrovacej relevantnosti. Doménová časť adresy je často prvým a najcennejším pivotom, pretože aplikácia kompletného obohatenia domény môže odhaliť vlastníctvo, vek, e-mailovú infraštruktúru, reputáciu a spojenie s phishingom či malvérom. Overenie existencie poštovej schránky, prítomnosť v databáze o narušení, súvisiace účty alebo persony a asociácie z threat intelligence nám môžu pomôcť posúdiť, či je adresa skutočná, predtým exponovaná, dôležitá pre operácie (potenciálne záškodnícke) alebo či súvisí s podvodom či narušením. Výsledky založené na hlavičkách, ako sú SPF, DKIM, DMARC a extrakcia IP odosielateľov, sú obzvlášť dôležité pri vyšetrovaní e-mailov, pretože nám pomáhajú rozlíšiť medzi legitímnou infraštruktúrou na odosielanie správ, artefaktmi preposielania a pokusmi o falšovanie. Cenná je aj históriu phishingových hlásení, najmä keď sa tá istá adresa alebo doména opakovane objavuje v interných alebo verejných kanáloch hlásení o útokoch. Zároveň je potrebné tieto polia posudzovať opatrne: overenie schránky môže byť nemožné alebo zavádzajúce, prítomnosť kompromitovaného e-mailu (resp. schránky) sama o sebe neznamená zlý úmysel, asociovanie mailu s personou môže viesť k falošným poplachom a výsledky SPF, DKIM a DMARC musia byť interpretované v kontexte preposielania, tretích strán a poštových služieb, nie ako samostatný dôkaz.

4.8.2 Typické artefakty obsahujúce údaje

Keď skúmame Windows endpointy, najčastejšie obnovujeme e-mailové adresy z Outlook OST alebo PST súborov, artefaktov Windows Mail, exportov MBOX alebo EML, metadát príloh, úložísk kontaktov, údajov automatického dopĺňania do formulárov a údajov z hlavičiek správ zachovaných priamo v e-mailoch. Vidíme ich tiež v histórii prehliadača z prístupu k webmailu alebo autofill údajov, artefaktov Teams alebo iných kolaboratívnych nástrojov, exportov chatov, CRM exportov, stiahnutých CSV súborov, artefaktov v schránke a používateľských dokumentov ako tabuľky, adresáre a poznámky k prípadom.

V prípadoch phishingu a kompromitácie účtu sa e-mailové adresy často objavujú v hlavičkách SMTP, logoch bezpečnostných brán, SIEM upozorneniach, PowerShell skriptoch (falošné poplachy sa objavujú vo verejne dostupných moduloch a skriptoch), v databázach formulárov uložených v prehliadači, artefaktoch správcu hesiel a v EDR telemetrii viazanej na e-mail-klienta alebo procesy prehliadača. Polia odvodené z hlavičky ako SPF, DKIM, DMARC a IP odosielateľa sa získavajú zo surového zdroja správy, nie z jednoduchého zobrazenia schránky, preto je zachovanie plných hlavičiek počas zberu kľúčové. Prítomnosť v oblasti narušenia, prepojenie osôb a vzťahy medzi hrozbami a spravodajstvom musia byť pridané neskôr obohacovaním e-mailových adries získaných z týchto miestnych zdrojov. Najsilnejšia dôkazná hodnota spočíva v korelácii e-mailovej adresy s celými hlavičkami správ, artefaktmi používateľskej interakcie, akýmikoľvek vloženými URL alebo prílohami, a okolitým overovaním alebo sieťovou aktivitou.

4.8.3 Spôsoby a nástroje na obohatenie

Obohatenie e-mailových adries zvyčajne začína normalizáciou adresy a oddelením lokálnej časti od domény, aby sa všetky relevantné doménové a FQDN obohatenia mohli aplikovať na doménovú časť. Následne si prezeráme dostupné hlavičky e-mailov, aby sme vyhodnotili výsledky SPF, DKIM a DMARC, analyzujeme prijaté riadky na identifikáciu pravdepodobnej IP adresy odosielateľa alebo reťazca a porovnávame tieto zistenia s údajnou identitou odosielateľa. Kde je to vhodné, je možné otestovať existenciu poštovej schránky pomocou metód overovania SMTP alebo komerčných validačných služieb, hoci výsledky by sa mali používať opatrne, pretože mnohé poštové systémy zámerne obmedzujú alebo maskujú overovacie správanie. Pre kontext odhalenia a identity môžeme skontrolovať zdroje únikov, ako sú Have I Been Pwned alebo podobné dátové súbory, preskúmať nástroje OSINT pre súvisiace účty alebo persony a vyhľadávať platformy na analýzu hrozieb, ako sú MISP, OTX alebo VirusTotal, či neexistujú známe škodlivé asociácie. Ak sú dostupné v skúmanom prostredí, odporúča sa tiež preskúmať interné systémy na hlásenie phishingu a platformy na zabezpečenie e-mailov, aby ste zistili, či sa tá istá adresa odosielateľa neobjavila v predchádzajúcich incidentoch.

Najspoľahlivejším procesom je začať s pôvodnou správou a hlavičkami, obohatiť e-mailovú adresu aj jej doménu, overiť technické riadenie odosielania a potom interpretovať kombinované výsledky spolu s artefaktmi koncových bodov, aktivitou používateľov a akoukoľvek prepojenou infraštruktúrou, ako sú URL, domény, prílohy alebo IP adresy odosielateľov.

4.9 Hash súboru

Identifikácia malvéru, mapovanie na rodiny, zhodnotenie schopnosti a atribúcia.

4.9.1 Význam a použitie

Hash súboru je jedným z najpoužívanejších indikátorov kompromitácie (IOC). Ich obohatenie o dodatočné informácie nám pomáha premeniť jeden kryptografický identifikátor na širšie pochopenie toho, čo súbor je, ako sa správa, či je bežný a či je spojený so známou škodlivou aktivitou. Obohacovaním by sme mohli pridať dátové polia obsahujúce informácie ako miera detekcie antimalware riešeniami, klasifikácia rodiny malvéru, zhody s YARA pravidlami, správanie vzorky v sandboxe, sieťové IOC, mapovanie na ATT&CK, súvisiacich aktérov hrozieb alebo kampaní a prevalencia danej vzorky. Popísané polia sú obzvlášť cenné pri triáži a scopingu počas riešenia incidentu. Pomáhajú rozlíšiť komoditný malware, neškodný softvér a doteraz neznáme vzorky.

Statické atribúty ako typ súboru, veľkosť, časová pečiatka kompilácie, detekcia packera, digitálny podpis, tabuľka importov, reťazce extrahovateľné zo vzorky, fuzzy hashe a súvisiace rodičovské hashe nám pomáhajú overiť identitu vzorky a pochopiť jej pravdepodobné schopnosti (perzistencia, sieťová aktivita, prístup k prihlasovacím informáciám alebo injekcia kódu). Používame tiež pozorovania podľa názvov súborov, dátumy prvého a posledného videnia a údaje o prevalencii, aby sme pochopili, ako sa vzorka objavila vo voľnej prírode a či je v podniku zriedkavá. Napriek zrejmým výhodám je potrebné mať na pamäti limity obohacovania založeného na hashoch: hashe sú presné identifikátory a nepomôžu identifikovať súvisiace varianty, pomenovávanie antimalware riešenia je nekonzistentné medzi dodávateľmi, časy kompilácie môžu byť falšované, digitálne podpisy môžu byť ukradnuté alebo zneužité, výsledky sandboxu sa môžu líšiť podľa prostredia a atribučné polia by sa mali považovať skôr za analytické stopy než za definitívny dôkaz.

4.9.2 Typické artefakty obsahujúce údaje

Keď skúmame hashe súborov na Windows endpointoch, zvyčajne začíname s artefaktmi, ktoré uchovávajú spustené, stiahnuté, vytvorené alebo referencované súbory. Medzi bežné zdroje patrí najmä samotný súborový systém – čím myslíme obsah skúmaného disku alebo samotný obraz disku. Niektoré údaje môžu byť poskytované metadátami NTFS, $MFT, $LogFile, USN Journal, Amcache, Shimcache, Prefetch, SRUM, Jump Lists, LNK súbormi, históriou sťahovania prehliadača, cache prehliadača, prílohami Outlooku, stiahnutiami z Teams alebo spolupráce, záznamami v koši a karanténnymi lokalitami z antivírusových alebo EDR nástrojov. Hashe môžu byť tiež priamo prítomné v EDR telemetrii, logoch Windows Defender, karanténnych záznamoch AV, forenzných triediacich kolekciách, SIEM upozorneniach, Sysmon udalostiach, PowerShell logoch (vrátane logov PowerShell skriptových blokov) a artefaktoch odvodených z pamäte, keď sa súbory načítavajú alebo referencujú v execution chain. V prípadoch malvéru náš tím často koreluje primárny hash vzorky s rodičovskými alebo dropper hashmi, hashmi potomkov alebo dropped súborov a súvisiacimi sieťovými indikátormi získanými zo sandboxov, telemetrie koncových bodov alebo analýzy pamäte. Statické charakteristiky ako veľkosť súboru, údaje z podpisu, časové pečiatky kompilácie, importy a embedované reťazce sú odvodené priamo z obnoveného súboru - hoci stopy názvov súborov, ciest alebo

príkazových riadkov často pretrvávajú aj po zmiznutí pôvodného binárneho súboru, popísané údaje z nich nezískavame.

Najväčšia pridaná hodnota pochádza z viazania hashu na konkrétnu cestu súboru, udalosť vykonávania, používateľský kontext a okolitú sadu artefaktov.

4.9.3 Spôsoby a nástroje na obohatenie

V navrhovanom pracovnom postupe sa obohacovanie hashov zvyčajne začína dotazovaním na platformách združujúcich údaje z threat intelligence, ako sú VirusTotal, Hybrid Analysis, MetaDefender, MISP a OTX. Tak zozbierame názvy detekcie, klasifikácie rodín, dátumy prvého a posledného videnia, prevalencia, fuzzy-hash a známe asociácie. Okrem týchto automatizovaných úloh môžu analytici malvéru vykonávať statickú analýzu pomocou nástrojov ako file, ExifTool, PEStudio, sigcheck, Detect It Easy, PEiD, FLOSS, YARA a kde je to potrebné, disassemblerov ako IDA Pro, na určenie skutočného typu súboru, metadát, použitie packerov alebo obfuskácie, stavu podpisov, importov a významných reťazcov. Samozrejme, tieto obohatenia nie sú zahrnuté v automatizovanom rámci, zahrnujeme ich len kvôli úplnosti navrhovaných možností obohatenia.

Pre pochopenie správania sa vzorky je možné skontrolovať výstupy sandboxu z platforiem ako Any.Run, Joe Sandbox, Hybrid Analysis alebo Cuckoo. Tak je možné identifikovať vytvorené procesy, zmeny v súboroch, zmeny registra, spôsoby perzistencie, sieťovú aktivitu a techniky z ATT&CK frameworku. Súvisiace hashe sa potom používajú na budovanie execution chainov a klastrov vzoriek do širších súborov malvéru.

Základným spôsobom obohatenia hash dát je obnoviť súbor alebo jeho hash z dôkazov z koncových bodov, overiť lokálny kontext vzorky (vlastník, časové pečiatky MFT, dôkazy o vykonaní, ...), obohatiť ho naprieč statickými aj dynamickými zdrojmi a následne interpretovať kombinovaný výsledok spolu s artefaktmi hostiteľa, líniou procesov a akoukoľvek súvisiacou sieťovou aktivitou.

4.10 FQDN / Doménové meno

Sledovanie C2 infraštruktúry, phishingových domén a spôsobov registrácie domén útočníkov.

4.10.1 Význam a použitie

Z pohľadu forenzného analytika môžeme použiť obohatenia domény a FQDN na prechod od jednoduchého hostname alebo URL k úplnejšiemu obrazu vlastníctva, infraštruktúry, zámeru a rizika. Polia súvisiace s registráciou, ako sú údaje o WHOIS registrantovi, registrátor, dátumy registrácie a exspirácie, vek domény a stav ochrany súkromia alebo cenzúry, sú často užitočné na odhalenie podozrivej infraštruktúry. Podozrivé je najmä ak sa doména javí ako novo registrovaná, krátkodobá alebo zámerne skrytá. Polia súvisiace s DNS, ako sú name servery,

záznamy A/AAAA, MX, TXT, CNAME, pasívna DNS história a objavené subdomény, nám pomáhajú pochopiť, ako je doména hostovaná, či podporuje e-mail, či má anti-spoofing kontroly a ako sa jej infraštruktúra v priebehu času menila. Veľkú hodnotu prikladáme aj obohateniam orientovaným na hrozby, ako sú reputácia, asociácie s malvérom a phishingom, certifikátové dáta, CT logy, snímky obrazovky, skórovanie DGA (Domain Generation Algorithm), podobnosť s typosquattingom a či nejde o doménu použitú na sinkhole či parking. Tieto nám často pomáhajú rozlíšiť legitímnu infraštruktúru od phishingovej, stagingovej alebo riadiacej infraštruktúry. Zároveň však naša skúsenosť ukazuje, že žiadne z týchto polí by sa nemalo riešiť izolovane: WHOIS môže byť cenzurovaný alebo zastaraný, DNS sa rýchlo mení, zdieľaný hosting môže znemožňovať presnejšiu atribúciu a snímky obrazovky alebo reputácia odrážajú len určitý časový bod.

4.10.2 Typické artefakty obsahujúce údaje

Keď zbierame dáta o doménach na Windows endpointoch, bežne ich obnovujeme z histórie prehliadača, cache, cookies, záznamov o sťahovaní, session súborov (záznamy browserových relácií) a artefaktov TypedURLs. Domény vidíme aj v artefaktoch DNS cache, logoch DNS klientov Windows, logoch firewallu, sieťových udalostiach Sysmon, EDR telemetrii, proxy záznamoch, logoch VPN klientov a záznamoch pamäte. Tieto nám môžu pomôcť ukázať, že doména bola dotazovaná, resolvovaná alebo kontaktovaná z konkrétneho hostiteľa. V prípadoch phishingu a narušenia náš tím často nachádza stopy po doménach v súboroch Outlook OST alebo PST, hlavičkách e-mailov, vložených odkazoch, metadátach príloh, artefaktoch Teams alebo podobných nástrojov, LNK súboroch, JumpListoch, Office RecentDocs, histórii PowerShellu, definíciách plánovaných úloh, skriptoch a konfiguračných dátach malvéru. Domény súvisiace s certifikátmi sa môžu objavovať aj v úložiskách certifikátov prehliadača, v úložisku certifikátov Windows, artefaktoch súvisiacich s Schannel a v pamäti RAM počas TLS relácií. Niektoré z najcennejších korelácií vznikajú pri prepojení domény získanej z dôkazov koncových bodov s konkrétnou akciou používateľa, vykonaním procesu alebo sieťovým pripojením v konkrétnom čase. Naopak, polia ako informácie o registrátorovi, pasívna história DNS, história CT, DGA scoring alebo kategorizácia domén sa zvyčajne neukladajú lokálne na koncovom bode, ale musia byť pridané neskôr prostredníctvom obohatenia.

4.10.3 Spôsoby a nástroje na obohatenie

V bežnom pracovnom postupe sa obohatenie vykonáva kombináciou údajov registrátora, DNS, certifikátov, webového prehliadania a threat intelligence. Analytici zvyčajne začínajú vyhľadávaním WHOIS a registrátora, aby identifikovali údaje o registrantoch, časovanie registrácie, expiráciu a stav ochrany súkromia. Následne dotazujeme aktuálne DNS záznamy pomocou nástrojov ako dig alebo nslookup na zber NS, A, AAAA, MX, TXT a CNAME dát, a prechádzame na pasívne DNS zdroje ako DNSDB, PassiveTotal alebo SecurityTrails, aby sme pochopili historické zmeny hostingu a IP adresy. Pre širšie objavovanie infraštruktúry používame zdroje transparentnosti certifikátov a enumerovania subdomén, ako sú crt.sh,

Censys, Amass a Subfinder. Reputácia a kontext zneužitia sú pridané zo zdrojov ako VirusTotal, OTX, IBM X-Force, ThreatFox, URLhaus, PhishTank, OpenPhish a Google Safe Browsing. Keď je to potrebné, môžeme tiež skontrolovať detaily o SSL/TLS, webových technológiách a vykreslených screenshotoch stránok pomocou platforiem ako Shodan, SSL Labs, Wappalyzer, BuiltWith a urlscan.io. Pri podozrení na podvod môžeme pridať DGA skórovanie a typosquatting analýzu pomocou nástrojov ako dnstwist alebo URLCrazy.

Najobhájiteľnejšie výsledky by mali prísť najprv z extrakcie domény z artefaktov koncových bodov, potom jej obohatením naprieč viacerými nezávislými zdrojmi a interpretáciou ich kombinácie.

4.11 Geolokácia

Detekcia nemožného cestovania, geografický pôvod neoprávneného prístupu.

4.11.1 Význam a použitie

Geolokačné obohatenie nám pomáha rozhodnúť, či je lokalita očakávaná, podozrivá alebo podvrhutá/skrytá. Podľa skúseností nášho tímu sú najužitočnejšími prvkami krajina pôvodu, región a mesto, či poloha zodpovedá známemu VPN alebo proxy exitnodu, či vytvára nemožný cestovný vzorec a či je krajina považovaná (v zmysle internej politiky) za vysoko rizikovú. Hlavným nedostatkom je, že geolokácia je približná a často odráža sieťovú infraštruktúru, nie však skutočnú fyzickú polohu používateľa.

4.11.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa lokalizačné stopy často získavajú z prihlasovacích záznamov, VPN záznamov, artefaktov prehliadača, hlavičiek e-mailov, záloh mobilných zariadení, profilov bezdrôtových sieté, aplikačnej telemetrie, EDR dát a cloudových logov, nie len z klasických lokálnych artefaktov. Surová IP adresa alebo súradnice môžu byť v týchto záznamoch prítomné, ale identifikácia výstupov VPN, logika nemožného cestovania a klasifikácia rizika krajiny sú zvyčajne obohatené analyticky (napr pomocou EDR či SIEM). V praxi najsilnejšia hodnota pramení z prepojenia lokality s konkrétnym účtom, zariadením, reláciou a pozíciou na časovej osi.

4.11.3 Spôsoby a nástroje na obohatenie

GeoIP alebo GPS údaje o polohe sú dobrým východiskovým bodom pre obohacovacie snahy. Potom by sme mohli skontrolovať, či koncový bod zodpovedá známej VPN alebo proxy infraštruktúre. Porovnávame lokalitu s predchádzajúcimi prihláseniami, aby sme preverili nemožné cesty, a potom hodnotíme krajinu podľa internej (klientskej) politiky rizika alebo pokynov súvisiacich so sankciami. Geolokačné obohatenie by malo byť kombinované s autentifikáciou, dôkazmi zo zariadení a siete, a nie interpretované len z údajov o polohe.

4.12 Zdroj logu

Zabezpečte integritu logov a správnu rekonštrukciu časovej osi.

4.12.1 Význam a použitie

Obohatenie zdrojov záznamov (Log Source) nám pomáha pochopiť, čo vytvorilo záznam a koľko dôvery vkladať do jeho časových pečiatok a polí. Podľa skúseností nášho tímu sú najdôležitejšími prvkami typ logu, typ zariadenia/softvéru a jeho dodávateľ, metóda parsera alebo normalizácie, doba uchovávania (retention period) a časové pásmo. Tieto určujú, ako interpretujeme dáta, či mohli byť dôležité polia transformované, ako ďaleko do minulosti môžeme skúmať a či je potrebné upraviť časové pečiatky pre prácu s časovou osou.

4.12.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa tieto informácie zvyčajne neukladajú priamo do artefaktu koncového bodu, pokiaľ zdrojom nie je lokálny Windows Event Log. Častejšie pochádza z SIEM onboarding záznamov, definícií parserov, nastavení kolektora, konfigurácie zariadení a dokumentácie správy logov. Často ho korelujeme s metadátami EVTX, časovými pečiatkami kolektora, nastaveniami NTP a oneskoreniami pri ingeste (príjme) dát, aby sme vysvetlili medzery alebo časové posuny počas analýzy. Je pochopiteľné, že tento typ obohacovania je pomerne ťažké všeobecne automatizovať.

4.12.3 Spôsoby a nástroje na obohatenie

Počas forenznej analýzy zvyčajne potvrdzujeme typ zdroja a dodávateľa zo SIEMu alebo konfigurácie logovania, kontrolujeme, ktorý parser alebo normalizačný pipeline spravoval záznamy, kontrolujeme politiku uchovávania a overujeme časové pásmo zdroja alebo konfiguráciu NTP. Na základe skúseností nášho tímu je toto obohatenie nevyhnutné pre obhájiteľnosť zostavenej časovej osi a na zabránenie nesprávnej interpretácii spôsobenej problémami s parserom alebo časovými posunmi.

4.13 MAC adresa

Sledovanie fyzického zariadenia, detekcia spoofingu a neautorizovaných zariadení.

4.13.1 Význam a použitie

Z pohľadu forenzného analytika nám obohacovanie MAC adries pomáha identifikovať, s akým zariadením máme do činenia a kde sa v sieti objavilo. Najužitočnejšími prvkami sú vyhľadávanie dodávateľa OUI, pridružené IP adresy, inferencia typu zariadenia, asociovaný port prepínača (switchu) a VLAN, a či adresa vyzerá náhodne. Hlavnou nevýhodou je, že identifikácia založená na OUI je len približná a náhodné alebo falšované MAC adresy môžu znížiť jej dôveryhodnosť.

4.13.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa MAC adresy bežne objavujú v dátach registra sieťových rozhraní, artefaktoch ARP cache, výstupoch ipconfig /all, artefaktoch súvisiacich s DHCP, EDR telemetrii, zachytávaní pamäte a zachytávaní paketov. MAC adresa sa tiež zaznamenáva v artefakte JumpList, čo je ľahko pozorovateľné, najmä ak artefakt obsahuje dôkazy o prístupe k súboru alebo inej aktivite spojenej so vzdialenými zariadeniami, okrem prístupu k lokálnym zdrojom. Súvisiace IP adresy sa často lepšie rekonštruujú z DHCP, ARP a záznamov prepínača než len z koncového bodu, zatiaľ čo detaily portov prepínača a VLAN zvyčajne pochádzajú z infraštruktúry siete, nie z natívnych artefaktov hosta. Najsilnejšia hodnota prichádza z naviazania MAC na konkrétneho hosta, časové obdobie a sieťový segment.

4.13.3 Spôsoby a nástroje na obohatenie

V našom pracovnom postupe zvyčajne začíname vyhľadávaním v OUI, aby sme identifikovali pravdepodobného dodávateľa, potom korelujeme MAC adresu s údajmi DHCP lease, ARP tabuľkami a tabuľkami prepínačov, aby sme obnovili pridružené IP adresy a fyzické umiestnenie v sieti. Tiež kontrolujeme, či nastavenie bitu „locally administrated“ naznačuje náhodný MAC a to použijeme pri hodnotení dôvery atribúcie. Na základe skúseností nášho tímu je obohatenie MAC najužitočnejšie, keď sa kombinuje s dôkazmi z DHCP, koncových zariadení a switchov, nie keď je interpretované samostatne.

4.14 MITRE ATT&CK ID

Namapovanie správania útočníka na framework, prispôsobenie detekcie a reakcie.

4.14.1 Význam a použitie

Obohatenie ATT&CK ID nám pomáha premeniť referenčnú techniku na niečo použiteľné pre vyšetrovanie a detekciu. Najužitočnejšie prvky sú oficiálny popis techník MITRE, taktika, príklady reálnych postupov, odporúčané zdroje dát, súvisiace Sigma alebo YARA pravidlá a opatrenia na zmiernenie situácií. Hlavným obmedzením je, že ATT&CK je analytický rámec, nie samostatný dôkaz, takže by mal „len“ usmerňovať a dopĺňať štandardné vyšetrovanie. Určite to nenahrádza nálezy založené na artefaktoch.

4.14.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa samotné ATT&CK ID nenachádza v artefaktoch koncových bodov, pokiaľ nebolo pridané bezpečnostným produktom, varovaním, detekčným pravidlom, poznámkou analytika k prípadu alebo reportom. Analytik dokáže identifikovať základné správanie v logoch a artefaktoch, ako je vytváranie procesov, zmeny registra, plánované úlohy, služby, aktivita PowerShell, sieťové pripojenia, autentifikačné udalosti a aktivita súborov. Skutočná hodnota spočíva v mapovaní pozorovaných artefaktov na techniku ATT&CK, na štruktúrovanú analýzu a vysvetlenie, čo aktivita môže predstavovať.

4.14.3 Spôsoby a nástroje na obohatenie

Začínať by sme mali záznamom MITRE ATT&CK, aby sme potvrdili názov techniky, popis, taktiku, zdroje dát a opatrenia, potom je vhodné prejsť známe príklady postupov a súvisiaci detekčný obsah, ako sú pravidlá Sigma, Elastic alebo YARA. Toto mapovanie by sme mohli použiť na rozhodnutie, ktoré dáta z parsovaných artefaktov a ktoré súvisiace udalosti korelovať. Obohacovanie ATT&CK by bolo spoľahlivé a užitočné, ak podporuje analýzu a detekciu založenú na dôkazoch, nemožno ho používať izolovane.

4.15 Názov mutexu a named pipe

Identifikácia rodín malvéru a detekcia súbežných infekcií.

4.15.1 Význam a použitie

Obohacovanie mien mutexov a named pipes pomáhajú rozhodnúť, či je prítomnosť objektu rutinným správaním aplikácie, alebo znakom malvéru, nástrojov či aktivity po zneužití. Podľa skúseností nášho tímu je kľúčová hodnota v kontrole, či má mutex alebo pipe známu asociáciu s malvérom, mapuje sa na známy C2 framework, alebo či je bežne vytváraný legitímnym softvérom či štandardnými Windows službami. Hlavnou nevýhodou je, že mená môžu byť opakovane použité, náhodné alebo zámerne vybrané tak, aby vyzerali neškodne, takže samotné meno je len stopou a nie dôkazom škodlivosti.

4.15.2 Typické artefakty obsahujúce údaje

Mutex a named pipe sa najčastejšie získavajú z pamäte RAM, EDR telemetrie, sandboxových správ, Sysmonu (ak je nakonfigurovaný), enumerácie a analýzy procesov a reverzného inžinierstva malvéru. Niekedy ich nachádzame aj v dátach zozbieraných pre forenznú triáž, reťazcoch extrahovaných z binárnych súborov, stopách debuggerov a špecifických logoch pre (bezpečnostné) nástroje. Named pipes sa niekedy dajú nájsť v System.evtx, pretože môžu byť "nainštalované" ako služba. Najsilnejšia hodnota vychádza z prepojenia mutexu alebo pipe s procesom ktorý ju vytvoril, časom vykonávania, načítanými modulmi a akýmikoľvek súvisiacimi sieťovými alebo perzistentnými artefaktmi.

4.15.3 Spôsoby a nástroje na obohatenie

Pozorované meno mutexu alebo named pipe by sa malo porovnať so správami o škodlivom softvéri, VirusTotal, výsledkami sandboxov, obsahom Sigma a Yara pravidiel, referenciami na threat intelligence, dokumentáciou C2 frameworku a dokumentáciou Microsoftu alebo dodávateľa pre legitímny softvér. Potom skontrolujeme, či je objekt známym artefaktom Windows alebo aplikácie, alebo či lepšie zodpovedá bežným vzorom pomenovania malvéru či C2. Vo všeobecnosti je obohacovanie informáciami o mutexoch a named pipes najužitočnejšie, keď sa kombinuje so stopami o procese, pamäti a súbore, nie len na základe názvu objektu.

4.16 Sieťový tok - Netflow

Identifikácia exfiltrácie dát, laterálny pohyb a komunikácie s C2.

4.16.1 Význam a použitie

Obohatenie netflow nám pomáha pochopiť, kto s kým komunikoval, ako dlho, koľko dát sa presunulo a či vzor sieťovej prevádzky vyzerá rutinne alebo podozrivo. Prvky ako zdrojová a cieľová IP adresa, bajty na vstupe a výstupe, trvanie relácie, beaconing, fingerprints JA3 alebo JA3S a geolokácia sú najužitočnejšie vo forenzných vyšetrovaniach (napríklad na detekciu úniku dát). Hlavnou nevýhodou je, že jediný tok sám o sebe je zriedkakedy jednoznačný, takže najsilnejšie závery vychádzajú zo vzorcov z dlhšieho časového obdobia a z korelácie s dôkazmi hostiteľa.

4.16.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa tieto údaje bežne obnovujú z logov firewallu, EDR telemetrie, Sysmon sieťových udalostí, proxy logov, zachytených paketov, NetFlow záznamov, Zeek dát a niekedy aj z pamäte RAM. Niektoré polia, ako zdrojové a cieľové IP, časovanie a objem dát, sú natívne pre artefakty toku, zatiaľ čo analýza beaconingu, geolokácia a interpretácia TLS odtlačkov sú zvyčajne analyticky pridané vylepšenia. V praxi najsilnejšia hodnota prichádza z prepojenia toku s konkrétnym procesom, používateľskou reláciou a súvisiacou DNS alebo autentifikačnou aktivitou.

4.16.3 Spôsoby a nástroje na obohatenie

Zdrojové a cieľové IP adresy by mali byť najprv obohatené použitím metód popísaných v tomto dokumente. Potom je potrebné skontrolovať objem prenesených bajtov, trvanie spojenia a či načasovanie naznačuje beaconing. Ak sú dostupné, porovnávame fingerprinty JA3 alebo JA3S so známymi nástrojmi alebo malvérom a overujeme, či sa cieľová geografická lokalita očakáva pre aktívum alebo používateľa. Na základe skúseností nášho tímu je obohatenie sieťového toku najužitočnejšie, keď sa kombinuje s dôkazmi z koncových bodov, DNS a časovej osi.

4.17 Sieťový port / protokol

Detegujte protokolové anomálie, tunelovanie a neautorizované služby.

4.17.1 Význam a použitie

Obohacovanie portov a protokolov nám pomáha rozhodnúť, či je pozorovaná sieťová aktivita rutinná, podozrivá alebo jasne v rozpore s jej deklarovaným účelom. Najužitočnejšie prvky sú štandardné priradenie služby pre port, známe použitie tohto portu malvérom, či pozorovaný

protokol zodpovedá tomu, čo by tam normálne malo bežať, a či je port povolený politikou. Hlavným problémom, na ktorý si treba dávať pozor, je, že samotné čísla portov sú slabé indikátory, pretože útočníci rutinne tunelujú neočakávané protokoly cez spoločné povolené porty.

4.17.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa detaily portov a protokolov bežne obnovujú z logov firewallu, Sysmon Event ID 3, EDR telemetrie, zachytení paketov, proxy logov, výstupu netstatu, zachytení pamäte a aplikačných logov. Číslo portu je často natívne pre artefakt, zatiaľ čo mapovanie služieb, asociácie s malvérom a kontext politiky firewallu sú obohatenia pridané analytikom. V praxi najsilnejšia hodnota pre vyšetrovanie spočíva v prepojení prístavu s konkrétnym procesom, cieľom a pozorovaným dopravným vzorom.

4.17.3 Spôsoby a nástroje na obohatenie

V našom pracovnom postupe zvyčajne začíname mapovaním portu na jeho štandardnú IANA službu a potom to porovnávame so skutočným pozorovaným protokolom pomocou paketovej inšpekcie, Wiresharku, IDS/IPS alebo podobnej telemetrie. Tiež kontrolujeme známe použitie malvéru na porte z hrozbových zdrojov a kontrolujeme pravidlá firewallu alebo bezpečnostné politiky, aby sme zistili, či mala byť prevádzka povolená. Výsledky obohatenia portov sú najužitočnejšie v kombinácii s kontextom procesu, hostiteľa a siete.

4.18 Meno osoby

Atribúcia, vyšetrovanie vnútorných hrozieb, OSINT profilovanie.

4.18.1 Význam a použitie

Obohacovanie mena osôb nám pomáha posúdiť, či je možné meno spojiť s reálnymi účtami, kontaktnými bodmi, verejnými záznamami, doménami alebo interným prístupom. Podľa skúseností nášho tímu sú najužitočnejšími prvkami sociálne profily, prepojené e-mailové adresy, verejné záznamy, registrácie domén a organizačná úloha alebo prístup. Hlavnou výhradou je, že mená sú nejednoznačné (koľko "Ján Novák" je na Slovensku?) a môžu viesť k falošným zhodám, preto by sa vysudzovanie identity malo zakladať na viacerých potvrdzujúcich údajoch, nie len na názve.

4.18.2 Typické artefakty obsahujúce údaje

Mená osôb sa často obnovujú z e-mailov, chatovacích záznamov, dokumentov, histórie prehliadača, zoznamov kontaktov, exportov HR, profilov účtov, artefaktov Teams, tabuliek, screenshotov a rôznych poznámok k prípadom (napríklad rozhovory so zainteresovanými stranami počas IR). Interné údaje o rolách a prístupe sa môžu objaviť aj v exportoch adresárov, IAM reportoch a artefaktoch endpointov viazaných na používateľské profily alebo prihlasovacie aktivity. Väčšina OSINT-štýlových obohatení, ako sú sociálne profily, verejné záznamy, prepojené e-maily a výsledky reverzného WHOIS, sa zvyčajne pridávajú po zbere, nie sú natívne uložené na koncovom bode.

4.18.3 Spôsoby a nástroje na obohatenie

Bežné je začať s nástrojmi OSINT a zdrojmi verejných záznamov, aby sa identifikovali pravdepodobné sociálne účty, prepojené e-maily, verejné záznamy a registrácie domén, a potom tieto zistenia porovnávate s internými HR, IAM a Active Directory údajmi, ak sú relevantné. Hľadáme prekryvy v mene, e-maile, zamestnávateľovi, pozícii alebo iných identifikátoroch, aby sme znížili falošné poplachy. Obohatenie mena osôb je najužitočnejšie, keď sa kombinuje s dôkazmi o účtoch, komunikácii a organizácii.

4.19 Telefónne číslo

Preskúmajte Vishing, SMS phishing a sociálne inžinierstvo.

4.19.1 Význam a použitie

Z pohľadu forenzného analytika nám obohacovanie telefónnych čísel pomáha posúdiť, či číslo vyzerá štandardne, ako jednorazové, sfalšovateľné číslo alebo či už je známa súvislosť s podvodom. Najužitočnejšie parametre telefónneho čísla, ktoré by sme pridávali do obohacovacieho fondu, patria operátor, typ čísla, krajina alebo región, história nahlásení spamu a akékoľvek asociácie s verejnou identitou. Hlavnou nevýhodou je, že telefónne čísla sa dajú ľahko sfalšovať, preradiť alebo dočasne prenajať, takže sú síce užitočnými stopami, ale samy o sebe nepostačujú na silnú atribúciu.

4.19.2 Typické artefakty obsahujúce údaje

Na systémoch s Windows sa telefónne čísla často obnovujú z e-mailov, chatov, histórie prehliadača, kontaktných súborov, záloh z mobilných zariadení, CRM exportov, Office dokumentov, snímkov obrazovky, artefaktov zo schránky a rozličných nástrojov na spoluprácu. Samotné číslo môže byť prítomné v artefaktoch koncových bodov, ale údaje o operátoroch, VoIP klasifikácii, podvodných hláseniach a OSINT musí pridať analytik. V praxi

najsilnejšia hodnota prichádza z prepojenia čísla so správou, záznamom hovoru, účtom alebo interakciou používateľa.

4.19.3 Spôsoby a nástroje na obohatenie

Proces obohacovania môže začať vyhľadávaním operátora a HLR (skratka HLR znamená Home Location Register) na identifikáciu poskytovateľa a typu čísla, potom použiť odkazy na číslovacie plány na potvrdenie krajiny a regiónu. Tiež kontrolujeme zdroje komunitných podvodných hlásení a verejné záznamy alebo OSINT na akékoľvek prepojené identity alebo účty. Ako sme pozorovali u predchádzajúcich artefaktov a obohatených údajov, obohatenie telefónnych čísel je najužitočnejšie v kombinácii s inými komunikačnými artefaktmi, informáciami o miestnych a doménových účtoch a v kontexte časovej osi.

4.20 Súkromná IP adresa

Zmapovanie rozsahu vnútornej kompromitácie, identifikácia postihnutých systémov a segmentov.

4.20.1 Význam a použitie

Obohacovanie privátnej IP použijeme na prevod IP adresy na konkrétne interné aktívum za ňou: aké zariadenie to je, kde v sieti sa nachádza, kto ho používa, ako sa autentifikuje, aké je kritické a kto je zaň zodpovedný. Na identifikáciu koncového bodu a jeho správne umiestnenie v rámci internej siete sú nevyhnutné polia (s informáciami z enrichmentu) ako je hostname, MAC adresa, história DHCP, podsieť, brána, VLAN a priradenie statickej IP vs. použitie DHCP. Úloha zariadenia, operačný systém, členstvo v AD doméne, prihlásení používatelia, nainštalované bezpečnostné riešenia a typ autentifikácie pomáhajú určiť, ako sa systém používa a či zapadá do očakávaných podnikových vzorcov. Kritickosť aktíva, výsledok posledného skenovania zraniteľností, , to, či je zariadenie fyzický alebo virtuálny a kto je zodpovedný vlastník sú informácie obzvlášť cenné pre určenie rozsahu incidentov a prioritizáciu, pretože naznačujú business impact a spôsob reakcie na incident.
Nevýhodou je, že súkromné IP adresy sa opätovne používajú, priraďujú a sú viditeľné len v internom kontexte. Súkromná IP je preto len zriedkakedy dostatočným dôkazom, pokiaľ nie je viazaná na časovo obmedzené DHCP, autentifikáciu a telemetriu koncových bodov. Aj CMDB a inventáre aktív môžu byť zastarané a NAT, VPN a multi-homed hosty môžu atribúciu komplikovať ešte viac.

4.20.2 Typické artefakty obsahujúce údaje

Na Windows endpointoch je možné IP adresy (verejné či privátne) často nájsť v rôznych forenzných artefaktoch. Hostname, doménové členstvo a verzia OS sa bežne objavujú v registri SYSTEM (presnejšie v SYSTEM\CurrentControlSet\Control\ComputerName, SYSTEM\CurrentControlSet\Control\Services\Tcpip\Parameters), v inštalačných a

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD PODPREDSEDU VLÁDY SLOVENSKEJ REPUBLIKY PRE PLÁN OBNOVY A ZNALOSTNÚ EKONOMIKU
VAIA VÝSKUMNÁ A INOVAČNÁ AUTORITA
VÝSKUMNÁ AGENTÚRA

aktualizačných logoch, EDR metadátach a výstupoch WMI repozitára. Sieťové detaily ako súkromná IP, gateway, maska podsiete, DHCP lease a DNS prípony môžu byť prítomné v registroch pod kľúčmi sieťového rozhrania, výstupmi z príkazu ipconfig /all (ak je zariadenie aktívne, zapnuté), prevádzkovými logmi DHCP klienta, firewallovými logmi, v RAMke a v EDR telemetrií. MAC adresy môžu byť obnoviteľné z artefaktov ARP cache, konfigurácie rozhrania, sieťových kľúčov registra a z volatilnej pamäte, pričom história leasov DHCP je často lepšie zachovaná na DHCP serveroch než na samotnom koncovom bode. Prihlásení používatelia a typ autentifikácie je možné rekonštruovať z logov Windows Security, ako napríklad z eventov s ID 4624 a ďalších, ďalej z logov Terminal Services, Sysmon, z RDP logov a artefaktov. Cacheované prihlasovacie údaje, adresáre používateľských profilov a časové osi EDR sú zdrojmi ďalších informácií. Nainštalovaní bezpečnostní agenti sa môžu objaviť v kľúčoch registra (Uninstalled, Installer), službách (Services), plánovaných úlohách (Scheduled tasks), medzi drivermi, v Program Files, záznamoch SCCM či EDR inventároch.

Sieťové informácie ako VLAN, info zo switcha, ďalej ohodnotenie kritickosti zariadenia, výsledok posledného skenu zraniteľnosti a zodpovedný vlastník zvyčajne nie sú natívne prítomné medzi štandardnými artefaktami na endpointe a musia byť korelované s inými dostupnými artefaktmi, ako sú CMDB, SIEM, konzoly skenerov, CAM tabuľky prepínačov, IPAM, ServiceNow a či Active Directory.

4.20.3 Spôsoby a nástroje na obohatenie

Obohacovanie sa vykonáva koreláciou dát z endpointu, Active Directory, zo sieťových stôp a zo správcovských interfacov. Identita a pomenovanie sa zvyčajne určujú z DHCP logov, interného DNS, Active Directory, LDAP a CMDB záznamov. Detaily adresovania a umiestnenia v sieti pochádzajú z IPAM, dát DHCP servera, konfigurácie prepínačov, ARP a CAM tabuliek, dokumentácie routingu a gateways, a niekedy aj z registra koncových bodov alebo EDR. Stav hosta po stránke bezpečnosti je obohatený pomocou EDR platforiem, SCCM, MDM, skenerov zraniteľností ako Nessus, Qualys alebo Rapid7 a inventára aktív, ktoré zaznamenávajú OS, nasadenie agentov a stav záplat. Používateľský a autentifikačný kontext je odvodený z Windows Event Logs, AD logov, RADIUS-u alebo iných autentifikačných systémov, SIEM korelácie a telemetrie vzdialeného prístupu. Nakoniec vlastníctvo a kritickosť systému sú potvrdené prostredníctvom CMDB, registrov rizík (risk register), virtualizačných platforiem, cloudových konzol a ticketovacích systémov ako ServiceNow. V praxi by najsilnejší výsledok mal prísť z vytvorenia mapovania z privátnej IP na DHCP lease, MAC, hostname, používateľa a položku z asset inventory, a následné overenie tohto mapovania oproti artefaktom koncových bodov a logom sieťovej infraštruktúry.

4.21 Názov procesu

Odhalenie zneužívania, maskovania a škodlivého vykonávania LOLBin procesov.

4.21.1 Význam a použitie

Z pohľadu forenzného analytika nám obohatenie názvov procesov pomáha rozhodnúť, či je bežiaci alebo zaznamenaný proces normálny, podozrivý alebo potenciálne maskovaný ako niečo legitímne. Najužitočnejšie polia na pridanie počas obohacovania sú známa zhoda s legitímnou aplikáciou, očakávaná cesta, očakávaný rodič, klasifikácia LOLBin, príkazový riadok, stav digitálneho podpisu, hash spustiteľného súboru, sieťová aktivita a rozšírenosť v prostredí. Známy názov procesu sám o sebe znamená veľmi málo. Skutočná výpovedná hodnota spočíva v kontrole, či proces bežal zo správneho miesta, so správnym rodičom, s očakávanými argumentmi a spôsobom, ktorý je bežný pre dané prostredie.

4.21.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa detaily vykonávania procesov bežne obnovujú zo Sysmonu, bezpečnostných logov, ak je nakonfigurované auditovanie procesov (Event ID 4688), z EDR telemetrie, Prefetch, Amcache, Shimcache, SRUM, z image RAM a samotného súborového systému. Príkazové riadky a vzťahy rodič-dieťa sú obzvlášť dobre zachované v Sysmon Event ID 1 a mnohých EDR platformách, zatiaľ čo sieťové pripojenia sú často dostupné v Sysmon Event ID 3, telemetrii firewallu alebo EDR záznamoch. Stav podpisu a hashe zvyčajne pochádzajú z binárneho súboru na disku alebo z metadát bezpečnostných nástrojov, takisto prevalencia je zvyčajne obohatením z EDR alebo SIEM – nie natívnym artefaktom koncového bodu.

4.21.3 Spôsoby a nástroje na obohatenie

V obohacovacom modeli by sme mohli začať overením, či názov procesu zodpovedá známej legitímnej aplikácii pomocou referencií ako Microsoft dokumentácia, NSRL alebo EchoTrail. Potom porovnáme pozorovanú cestu k súboru, rodičovský proces a príkazový riadok s očakávanými vzormi, overíme, či je binárny súbor známy LOLBin, overíme jeho podpis a hash a preskúmame všetky sieťové pripojenia, ktoré skúmaný proces inicioval. Na základe skúseností nášho tímu je obohacovanie názvov procesov najspoľahlivejšie, keď je viazané na kontext procesného stromu, metadáta súborov a okolité aktivity na pracovnej stanici.

4.22 Verejná IP adresa - externá

Identifikácia útočníckej infraštruktúry, hostingu, geolokácie a reputácie.

4.22.1 Význam a použitie

Tieto obohacovacie polia sa používajú na premenu surovej IP adresy na dáta, na základe ktorých sa dá vykonať ďalšia aktivita. DNS a passive DNS obohatenia, ako reverzné DNS,

forward DNS a historické preklady (DNS resolutions), pomáhajú identifikovať hostname, co-hostované domény a zmeny infraštruktúry v priebehu času. Obohatenia registrácie a routingu, vrátane WHOIS, CIDR, ASN, ASN organizácie a BGP histórie, ukazujú, kto ovláda daný adresný priestor, do ktorej siete patrí a či je správanie routingu normálne alebo podozrivé. Obohatenia infraštruktúry a služieb, ako geolokácia, typ hostingu, otvorené porty, HTTP bannery a SSL/TLS certifikáty, pomáhajú profilovať systém – jeho úlohu a expozíciu. Napokon, bezpečnostné obohatenia ako Tor/VPN flagy, reputačné skóre, prítomnosť na blacklistoch, známe prepojenia na malvér, asociácie s útočníckymi skupinami, časové pečiatky a referencie z OSINT-u podporujú atribúciu, prioritizáciu a adekvátnu reakciu na incidenty.

4.22.2 Typické artefakty obsahujúce údaje

Na Windows pracovnej stanici je často možné obnoviť verejné IP adresy, ktoré sa stanú kandidátmi na tento typ obohatenia, zo štandardných forenzných artefaktov, ako sú história a cache prehliadača, DNS cache, logy Windows Firewallu, sieťové udalosti v Sysmon, logy bezpečnostných udalostí (Security.evtx, najme event ID 4624), PowerShell logy, EDR telemetria, obsah pamäte RAM, Prefetch. Ďalšími zdrojmi sú artefakty e-mailových klientov, RDP artefakty a aplikačne špecifické logy z prehliadačov, VPN klienti, nástroje na synchronizáciu do cloudu a softvér na vzdialenú správu.

4.22.3 Spôsoby a nástroje na obohatenie

Obohacovanie by malo byť vykonané kombinovaním viacerých kategórií zdrojov, nie spoliehania sa na jedno vyhľadávanie. Základné informácie o vlastníctve a alokácii pochádzajú z registrov a smerovacích zdrojov, ako sú ARIN, RIPE, APNIC, BGPView, Team Cymru a ipinfo.io. Kontext zameraný na DNS sa získava prostredníctvom priamych nástrojov ako dig a nslookup a pasívnych DNS platforiem ako PassiveTotal, SecurityTrails a DNSDB. Expozícia a odtlačok služieb vychádzajú z internetových platforiem na skenovanie a pozorovanie, ako sú Shodan, Censys, Nmap, crt.sh, a z nástrojov na zber HTTP hlavičiek ako curl. Kontext hrozieb a zneužitia je pridávaný z repozitárov spravodajských informácií a reputačných kanálov vrátane AbuseIPDB, VirusTotal, OTX, IBM X-Force, ThreatFox, Spamhaus a MISP, zatiaľ čo širšie verejné odkazy sa nachádzajú vo výsledkoch vyhľadávania, blogoch dodávateľov a publikovaných správach o hrozbách. V praxi koncových bodov môže skúšajúci extrahovať verejnú IP z artefaktov, ako je cache Windows DNS klienta, záznamy Event ID 3 zo Sysmonu, záznamy firewallu v pfirewall.log, databázy SQLite prehliadača, metadáta Outlooku, dôkazy z RDP cache a jump listu, alebo reťazce a štruktúry socketov v RAM, a potom túto IP pivotovať cez zdroje obohacovania na určenie vlastníctva, Známosť, reputácia a historické väzby.

Tieto obohatenia spolu poskytujú vrstvený pohľad na verejnú IP adresu naprieč vlastníctvom, infraštruktúrou, správaním, expozíciou a relevantnosťou hrozieb. Pomáhajú výskumníkovi rozlíšiť neškodné zdieľané hostovanie od infraštruktúry ovládanej útočníkmi, pripojiť IP adresu k doručovaniu malvéru alebo aktivite príkazov a kontroly, detegovať anonymizáciu alebo používanie relé a identifikovať eskalačné cesty, ako je hlásenie zneužívania alebo notifikácia poskytovateľa. Windows artefakty poskytujú dôležité dôkazy, pretože ukazujú, kde a kedy

koncový bod skutočne pozoroval alebo komunikoval s touto verejnou IP, čo môže podporovať tvorbu časovej osi, rekonštrukciu používateľských aktivít a koreláciu s externou inteligenciou. Zároveň však existujú dôležité výhrady: geolokácia je približná, pasívne DNS a skenovacie dáta sú časovo citlivé, reputačné skóre môžu byť šumové a cloudová alebo CDN infraštruktúra môže slúžiť legitímnej aj škodlivej prevádzke. Forenzné závery sú najsilnejšie, keď je verejné duševné vlastníctvo potvrdené naprieč viacerými miestnymi artefaktmi a viacerými kategóriami obohacovania.

4.23 Verejné IP, vlastnené samotnou organizáciou

4.23.1 Význam a použitie

Tieto obohacovacie polia sa používajú na pochopenie verejnej IP adresy, ktorá patrí samotnej organizácii, s cieľom zistiť, čo organizácia zámerne vystavuje internetu, kto za ňu nesie prevádzkovú zodpovednosť a či predstavuje bezpečnostné alebo súladové riziko. Polia súvisiace so službami, ako sú publikované internetové služby, súvisiace FQDN, detaily SSL certifikátov, súhrny pravidiel firewallu a stav ochrany WAF alebo DDoS, pomáhajú definovať vonkajší útočný povrch systému a spôsob jeho ochrany. Oblasti vlastníctva a správy, vrátane pridelených obchodných jednotiek alebo oddelení a histórie riadenia zmien, poskytujú internú zodpovednosť a prevádzkový kontext. Polia bezpečnostnej pozície, ako sú zistenia zraniteľností, stav záplat a súladu, ako aj stav čiernej listiny alebo reputácie, pomáhajú posúdiť, či je organizačné duševné vlastníctvo správne udržiavané, zbytočne vystavené alebo už priťahuje pozornosť súvisiacu so zneužitím.
Obohatenia poskytujú vyšetrovateľom kompletný obraz o verejnej duševnej svojine organizácie naprieč expozíciou, vlastníctvom, ochranou, hygienou a prevádzkovými zmenami. Sú obzvlášť užitočné pri reakcii na incidenty, prehliadkach povrchu útoku a scopingu narušenia, pretože pomáhajú určiť, či je zraniteľná alebo zneužitá IP súčasťou schválenej služby, či je dostatočne chránená, ktorý tím musí reagovať a či nedávne zmeny môžu vysvetliť nové správanie. Pomáhajú tiež identifikovať medzery medzi plánovaným a skutočným vystavením, ako sú nedokumentované služby, exspirované certifikáty, príliš široké pravidlá firewallu, chýbajúce záplaty alebo zoznamy na čiernych listinách, ktoré ovplyvňujú reputáciu. Hlavnou výhradou je, že žiadny jeden zdroj nestačí: interné zásoby môžu byť zastarané, externé skeny môžu byť neúplné alebo časovo citlivé a bezpečnostné zistenia musia byť interpretované s ohľadom na podnikateľský účel a nedávnu históriu zmien.

4.23.2 Typické artefakty obsahujúce údaje

Na Windows pracovnej stanici je často možné získať verejné IP adresy, ktoré sa stanú kandidátmi na tento typ obohatenia, z forenzných artefaktov, ako sú história prehliadača a cache, DNS cache, logy Windows Firewallu, udalosti pripojenia k Sysmon sieti, logy bezpečnostných udalostí, PowerShell logy, EDR telemetria, zachytenia pamäte, kontext vykonávania prepojený s prednačítaním, artefakty e-mailových klientov, RDP artefakty a

aplikačne špecifické logy z prehliadačov, VPN klienti, nástroje na synchronizáciu do cloudu a softvér na vzdialenú správu.

4.23.3 Spôsoby a nástroje na obohatenie

Obohacovanie sa zvyčajne vykonáva kombinovaním interných záznamov o aktívach a správe s externými pozorovacími údajmi. Interné zdroje ako CMDB, IPAM, inventár aktív, platformy na správu firewallu, PKI systémy, SCCM, BigFix, Tanium, ServiceNow, Jira a databázy riadenia zmien poskytujú autoritatívne informácie o vlastníctve, zámere konfigurácie, stave záplat a schválených zmenách. Externé a hybridné zdroje ako Shodan, Nmap, skenery zraniteľností, externé DNS, záznamy transparentnosti certifikátov, Qualys SSL Labs, MXToolbox, Spamhaus, AbuseIPDB, Cloudflare, Akamai a AWS Shield pomáhajú overiť, čo je viditeľné z internetu a či kontroly organizácie fungujú podľa očakávaní. V praxi analýza porovnáva, čo by malo byť odkryté podľa interných záznamov, s tým, čo je odkryté a pozorovateľné zvonku.

4.24 Kľúč/hodnota registra

Identifikácia mechanizmov perzistencie a zmien konfigurácie.

4.24.1 Význam a použitie

Obohacovanie registrových kľúčov môže analytikovi pomôcť určiť, či je kľúč štandardný pre Windows, alebo či môže byť bodom perzistencie alebo podozrivou zmenou konfigurácie. Podľa skúseností nášho tímu sú najužitočnejšie kontext doplňujúce polia napríklad: legitímny účel kľúča, či ide o známe miesto automatického štartu, či aktuálna hodnota zodpovedá očakávanej predvolenej hodnote, kedy bol kľúč naposledy upravený a ku ktorému používateľskému SIDu patrí. Hlavnou nevýhodou je, že i mnohé legitímne aplikácie používajú na ukladanie svojich nastavení miesta, ktoré využívajú i útočníci na perzistenciu. Hodnota a kontext sú preto dôležitejšie než samotná cesta ku kľúču.

4.24.2 Typické artefakty obsahujúce údaje

Podrobnosti o kľúčoch a hodnotách registra pochádzajú priamo z registrových hivov, ako je NTUSER.DAT, USRCLASS.DAT, SYSTEM, SOFTWARE a súvisiace transakčné logy. Časy posledného zápisu sú zachované v metadátach kľúčov a príslušný SID je zvyčajne možné odvodiť z cesty ku kľúču alebo z mapovania profilu (pokiaľ ide o hivy v registri používateľa NTUSER. DAT a USRCLASS. DAT). Je možné korelovať zistenia registra s Prefetchom, Amcache, naplánovanými úlohami, službami, LNK súbormi a EDR telemetriou, aby sa potvrdilo, či podozrivá hodnota registra skutočne viedla k vykonaniu nejakého procesu.

4.24.3 Spôsoby a nástroje na obohatenie

Je možné porovnať cestu ku kľúču a jeho hodnotu s dokumentáciou Microsoftu, referenciami z forenzných zdrojov/literatúry, so známymi Autoruns a s baseline systémami (napríklad golden image pracovnej stanice v organizácií), aby sme určili očakávané správanie. Potom môžeme klasifikovať, či je kľúč súčasťou známeho mechanizmu perzistencie, skontrolovať čas jeho poslednej úpravy a namapovať ho na používateľa alebo vlastníka systému. Na základe skúseností nášho tímu je obohatenie registra najspoľahlivejšie, keď je kľúč analyzovaný spolu s artefaktmi vykonania a v kontexte udalostí na časovej osi, ktoré s ním časovo alebo predmetne súvisia.

4.25 Plánovaná úloha / Cron

Identifikácia mechanizmov perzistencie a neoprávnenej automatizácie.

4.25.1 Význam a použitie

Obohatenie naplánovanej úlohy o dodatočné informácie nám pomáha rozhodnúť, či je úloha bežnou súčasťou systému alebo mechanizmom perzistencie. Podľa skúseností nášho tímu sú najužitočnejšie parametre názov úlohy, príkaz, ktorý úloha spúšťa, autor tasku, jej trigger (spúšťač) a účet, pod ktorým úloha beží, pretože rýchlo ukazujú zámer a privilégiá. Hlavnou výhradou je, že mnohé legitímne nástroje tiež používajú plánované úlohy, takže príkaz a kontext sú dôležitejšie než samotný názov úlohy.

4.25.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa podrobnosti zvyčajne obnovujú zo záznamov Task Scheduler, XML súborov úloh, priečinka Tasks, referencií v registri (kľúč registra TaskCache), z výstupu Autoruns, Symmonu a súvisiacich záznamov udalostí (nielen z Tasch Scheduler event logov). Zistenia ohľadne naplánovaných úloh často korelujeme s Prefetchom, Amcache, logmi tvorby procesov (Security.evtx - ID 4688, či Sysmon), spustenými skriptami (o.i. artefakt PSReadline, Windows PowerShell.evtx a Microsoft-Windows-Powershell Operational.evtx) a artefaktmi súborového systému, aby sme potvrdili, či sa úloha naozaj vykonala a čo spustila. V praxi vyplýva najsilnejšia hodnota z naviazania úlohy na jej autora, payload a časovú os vykonávania.

4.25.3 Spôsoby a nástroje na obohatenie

Preštudujte si definíciu úlohy, aby ste identifikovali spustiteľný súbor alebo skript, čas vytvorenia, autora, podmienky a kontext spustenia úlohy, potom porovnajte tieto úlohy s známymi správnymi vzormi (opäť napríklad pomocou baseline image). Tiež kontrolujeme, či úloha beží ako SYSTEM alebo iný privilegovaný účet a či príkaz ukazuje na podozrivé cesty alebo skripty. Na základe skúseností nášho tímu by sa analýza plánovaných úloh a obohacovanie mali kombinovať s artefaktmi vykonávania programov/procesov (Execution) a persencie, aby sa dosiahli čo najpresnejšie a najpresvedčivejšie výsledky.

4.26 URL

Analýza phishingu, doručovania payloadov a presmerovanie (redirection).

4.26.1 Význam a použitie

Z pohľadu forenzného analytika nám obohacovanie URL pomáha posunúť sa od jednoduchého záznamu o URL a pochopiť, na čo bol používateľ alebo proces smerovaný, či bol cieľ neškodný alebo škodlivý a ako sa obsah navštívený používateľom správal v čase jeho prístupu. Obohacovacie polia môžu obsahovať reputáciu URL, HTTP kód odpovede, konečný cieľ presmerovania, typ obsahu, názov stránky, vložené objekty, rozšírenie na celú URL v prípade použitia URL shortenera, archívne snímky (napr Archive.org) a vyrenderované snímky obrazovky. Tieto by boli obzvlášť užitočné pri phishingu, doručovaní škodlivého softvéru a vyšetrovaní používateľskej aktivity. Pomáhajú nám určiť, či bola URL aktívna, či prechádzala viacerými vrstvami, či nakoniec viedla k stránke na získavanie prihlasovacích údajov alebo stiahnutiu súboru, a či viditeľná stránka zodpovedala zdanlivému zámeru odkazu. Extrakcia domén je obzvlášť dôležitá, pretože mnohé pivoty vyšetrovania sú z úrovne domény, nie na úrovni celej URL adresy, čo nám umožňuje spojiť jeden odkaz so širšou infraštruktúrou, reputáciou a historickou aktivitou.

Hlavné nevýhody a obmedzenia obohacovania URLs sú, že obsah URL je veľmi časovo citlivý, presmerovania a payloady sa môžu rýchlo meniť, niektoré stránky slúžia rôznemu obsahu podľa geografickej lokácie návštevníka alebo podľa user-agent, a záznamy v registroch reputácie môžu zaostávať, ak je URL aktívne zneužívaná. Z tohto dôvodu by sa URL mala považovať za **časovo viazaný artefakt**, a preto by sa vyšetrovatelia mali snažiť skúmať pôvodný reťazec aj pozorované správanie čo najskôr.

4.26.2 Typické artefakty obsahujúce údaje

Keď skúmame Windows endpointy, bežne obnovujeme URL z histórie prehliadača, cache, cookies, záznamov o sťahovaní, súborov obnovenia relácie a registrových artefaktov TypedURLs. Nachádzame ich tiež v Outlook OST alebo PST súboroch, e-mailových hlavičkách, artefaktoch z chatových a kolaboračných SW, Office dokumentoch s vloženými odkazmi, PDF metadátach, Teams správach, artefaktoch clipboardu, LNK súboroch, jump listoch, histórii PowerShellu, RunMRU záznamoch, v naplánovaných úlohách a skriptoch.

URL adresy sa často objavujú v EDR telemetrii, proxy logoch, firewallových logoch, Sysmon udalostiach, Windows Event Logs, v RAM, Prefetchi a konfiguračných alebo staging súboroch malvéru. Skrátené URL adresy môžu byť zachované v e-mailoch alebo chatovacích správach aj vtedy, keď prehliadač neskôr zaznamenáva len rozšírený cieľ, preto sa snažíme zhromažďovať pôvodný zdroj, Referrer aj skutočný cieľ, kam sa obeť dostala. Vizuálne prvky ako vykreslená stránka, názov a stiahnuté súbory zvyčajne nie sú úplne zachované v natívnych artefaktoch

Windows endpointov, pokiaľ ich nepodporuje cache prehliadača, snímky obrazovky, pamäť alebo externá telemetria, preto je potrebné po zbere rekonštruovať časť kontextu okolo URL.

Najsilnejšia dôkazná hodnota pramení z korelácie URL s akciou používateľa, použitým prehliadačom, reťazcom presmerovania a akoukoľvek následnou udalosťou sťahovania alebo autentifikácie.

4.26.3 Spôsoby a nástroje na obohatenie

V navrhovanom pracovnom postupe obohacovanie URL zvyčajne začína parsovaním URL na jej komponenty a extrahovaním domény, aby bolo možné aplikovať rôzne obohatenia domény a FQDN. Potom vyhľadávame reputáciu a využívame služby ako VirusTotal, urlscan.io a Google Safe Browsing aby sme zistili, či už URL bola klasifikovaná ako škodlivá, phishingová, podozrivá alebo čistá. Aby sme pochopili správanie „naživo“, naši analytici zvyčajne kontrolujú HTTP response kód, sledujú presmerovania na konečné miesto, potvrdzujú typ hostovaného obsahu a kontrolujú názov stránky a metadáta pomocou nástrojov ako curl, webové nástroje na načítanie, wget, BeautifulSoup a urlscan.io. Kde je to potrebné, obohacovací model by mal byť schopný skúmať vložené objekty, skripty, iframy a sťahovania prostredníctvom urlscan.io, sandboxových platforiem ako Any.Run alebo iných kontrolovaných dynamických analytických prostredí. Ak je zapojený skracovač (URL shortener), rozšírime proces o služby ako CheckShortURL alebo podobné nástroje pred pokračovaním v analýze. Pre historický kontext môžeme konzultovať archívne snímky, ako je Wayback Machine, a na vizuálne potvrdenie si prezeráme renderované snímky obrazovky z urlscan.io alebo automatizačných frameworkov prehliadača, ako je Puppeteer. Najspoľahlivejším procesom by bolo zachovať pôvodnú URL, zaznamenať jej pozorované presmerovania a správanie obsahu, extrahovať a obohatiť podkladovú doménu a korelovať tento výsledok s artefaktmi koncových bodov a akýmkoľvek následným vykonávaním kódu alebo sieťovou aktivitou.

4.27 Používateľský účet

Detekcia kompromitovaných účtov, vyhodnocovanie eskalácie privilégií, audit prístupu.

4.27.1 Význam a použitie

Z pohľadu forenzného analytika nám obohacovanie používateľských účtov vo Windows pomáha prejsť od používateľského mena alebo SID k jasnejšiemu pochopeniu identity, privilégií, rizika a pravdepodobného dopadu kompromitácie účtu. Vlastnosti ako typ účtu, členstvo v skupinách, úroveň privilegovaného prístupu, stav účtu, posledné prihlásenie, posledná zmena hesla, stav MFA, počet neúspešných prihlásení, anomálie prihlásenia, pridružené zariadenia a SPN sú obzvlášť dôležité na rozlíšenie bežnej aktivity používateľa od správcu, servisného účtu alebo správania kompromitovaného účtu.

Organizačný kontext ako oddelenie, manažér, titul a pracovný status je tiež dôležitý, pretože nám pomáha posúdiť, či pozorovaná aktivita zodpovedá očakávanej úlohe používateľa a či by účet vôbec mal byť aktívny. Dôležitosť by sa mala klásť najmä na privilegované členstvá, zastarané heslá, chýbajúce MFA, podozrivé geografické polohy alebo zariadenia, nedávne zablokovanie účtu a priradenia SPN, pretože tieto môžu naznačovať zvýšené riziko kompromitácie, prebiehanie útoku Password spraying, vystavenie konta Kerberoastingu alebo zneužívanie neaktívnych účtov. Zároveň je nutné tieto údaje dôkladne zhodnotiť: atribúty konta v Active Directory nemusia odrážať aktuálnu realitu, lastLogonTimestamp nie je vždy presný, servisné účty sa môžu správať inak ako ľudskí používatelia a nezvyčajné prihlasovacie vzory (napríklad Impossible travel scenáre) nie sú nevyhnutne škodlivé, pokiaľ nie sú korelované s dôkazmi zo zariadenia, siete a autentifikácie.

4.27.2 Typické artefakty obsahujúce údaje

Keď skúmame používateľské účty na systémoch Windows, často obnovujeme relevantné informácie zo Security.evtx logu, najmä zo záznamov úspešných a neúspešných prihlásení ako sú udalosti s ID 4624, 4625, 4634, 4648, 4672, 4768, 4769 a 4776, spolu s korelovanými autentifikačnými záznamami zo Sysmon, EDR telemetrie a SIEM. Názvy účtov, SID, členstvo v skupinách, typy prihlásení, zdrojové zariadenia, z ktorých k prihláseniu došlo, a časové pečiatky sa môžu tiež objaviť v registroch, profilových adresároch používateľov, naplánovaných úlohách, službách, artefaktoch RDP, jump listoch, LNK súboroch, PowerShell logoch, v logoch a artefaktoch rôznych nástrojov na vzdialený prístup, medzi nacacheovanými prihlasovacími údajmi a v RAM. Na systémoch pripojených k doméne je často možné korelovať kontext súvisiaci s AD prostredníctvom informácií o prihlasovacom serveri, Kerberos tiketoch, oprávneniach priradených v tokenoch, aktivity súvisiacej so SPN, či pomocou informácií cacheovaných lokálne alebo v bezpečnostných nástrojoch. Často tiež používame artefakty z koncových PC na prepojenie účtu s (inými) pripojenými zariadeniami, používateľskými reláciami, aktivitou prehliadača, spustenými nástrojmi a aktivitami VPN alebo vzdialeného prístupu zaznamenanými v samostatných logoch. Niektoré obohacovacie polia, ako napríklad zamestnanie, manažér, typ účtu, IAM stav, registrácia MFA a členstvo v skupine, zvyčajne neexistujú natívne na koncovom bode, ale musia byť pridané z Active Directory, IAM, HR, PAM, Intune, SCCM, EDR, VPN platforiem a centrálnych autentifikačných systémov. Najsilnejšiu dôkaznú hodnotu prináša korelácia Axtive Directory a IAM údajov s artefaktmi endpointu, ktoré ukazujú, kedy, kde a ako sa účet skutočne autentifikoval a aké aktivity vykonával potom.

4.27.3 Spôsoby a nástroje na obohatenie

V našom pracovnom postupe sa obohacovanie používateľských účtov zvyčajne začína vyhľadávaním v Active Directory a IAM, kde sa určuje typ účtu, členstvo v skupinách, úroveň oprávnení, stav účtu, čas zmeny hesiel, prítomnosť SPN a organizačné atribúty. Potom prechádzame na zdroje záznamov o autentifikácií, ako sú logy Windows Security, logy doménového radiča, SIEM, Azure AD alebo Entra logy prihlásenia, VPN telemetria, záznamy poskytovateľov MFA a analytiku z UEBA (User and Entity Behaviour Analytics), aby sme overili

nedávne záznamy, neúspešné pokusy, anomálne vzory a históriu vzdialeného prístupu. Kontext pridruženého zariadenia sa zvyčajne vytvára z EDR, SCCM, Intune, vzťahov medzi zariadeniami v AD (napríklad delegácie, členstvá v OU či skupinách a podobne) a telemetrie prihlasovania vyšetrovaného konta na koncové body, zatiaľ čo kontext pracovného zaradenia konta a prislúchajúcej manažérskej línie je potvrdený prostredníctvom HR a IAM systémov. Pre privilegované alebo servisné účty tiež preverujeme PAM dáta, priradenia administratívnych skupín, aktivitu servisných Kerberos tiketov a registrácie SPN, aby sme posúdili zneužitie alebo mieru vystavenia kerberoastingu. Na základe skúseností nášho tímu je najspoľahlivejším procesom začať s identifikátorom účtu, overiť jeho stav v Active Directory, overiť jeho autentifikačné správanie naprieč dostupnými logmi, porovnať to s artefaktmi získanými z koncových bodov a používaním zariadení (k akým zariadeniam sa konto prihlasovalo?) a až potom vyvodiť závery o kompromitácii, zneužití práv alebo anomálnom prístupe.

4.28 User-Agent reťazec

Detekcia škodlivých nástrojov, C2 frameworkov a anomálnych klientov

4.28.1 Význam a použitie

Obohacovanie hlavičky User Agent nám pomáha získať zmysluplnejší pohľad na to, čo pravdepodobne vygenerovalo webovú požiadavku a či táto aktivita zodpovedá očakávanému správaniu. Možnosť pridávať polia ako použitý webový prehliadač a jeho verzia, operačný systém, známe zhody malvéru, indikátory botov alebo webových crawlerov a detekcia anomálií či falšovania je obzvlášť užitočná, keď sa snažíme rozlíšiť bežné surfovanie používateľov od automatizovaných, skriptovaných aktivít, komoditných nástrojov, komunikácie s malvérom alebo pokusov o zamaskovanie prevádzky. Analyzovaný User-Agent nám môže pomôcť rýchlo posúdiť, či je požiadavka konzistentná s pracovnou stanicou používateľa a nainštalovaným softvérom, zatiaľ čo User-Agenti viazaní na známe nástroje alebo malware môžu poskytnúť cenné stopy pri vyšetrovaní incidentov. Používame tiež zriedkavé alebo deformované User-Agent reťazce ako indikátory pre triedenie, najmä ak sa nezhodujú so skutočnou platformou hostiteľa alebo sa v prostredí javia štatisticky nezvyčajne. Dáta User-Agent by sa však mali interpretovať opatrne: je ľahké ich sfalšovať, niektoré aplikácie používajú generické alebo zavádzajúce hodnoty, bezpečnostné nástroje môžu normalizovať hlavičky a mnohé legitímne automatizované služby sa tiež identifikujú ako boti alebo crawlery. Z tohto dôvodu vnímame údaje User-Agent ako užitočný kontextový indikátor, nie ako artefakt postačujúci na atribúciu samostatne.

4.28.2 Typické artefakty obsahujúce údaje

Keď vyšetrujeme incidenty v prostredí Windows, najčastejšie sa stretávame s reťazcami User-Agent v proxy logoch, logoch z webovej gateway, logoch IIS alebo aplikácií. Takisto sa nachádzajú v údajoch telemetrie siete z EDR, v zachytených paketoch, vo vývojárskych dátach prehliadača a v záznamoch pamäte RAM obsahujúcich HTTP požiadavky.

Na samotnom koncovom bode sa dôkazy z User-Agenta môžu objaviť aj v cache prehliadača, artefaktoch relácií prehliadača, histórii sťahovania, bezpečnostnej telemetrii e-mailov, v histórii webových požiadaviek iniciovaných PowerShellom (napr. Invoke-IEX), súboroch skriptov, konfiguračných súboroch malvéru a artefaktoch príkazového riadku viazaných na nástroje ako curl, PowerShell, Python knižníc určených na dopytovanie webu, alebo z iných LoLBIN nástrojov, ktoré sa dajú použiť či zneužiť na sťahovanie z webu. V niektorých prípadoch môžeme korelovať User-Agenta s konkrétnym spustiteľným súborom prehliadača, procesom alebo podozrivým reťazcom procesov rodič-dieťa pomocou EDR, Sysmon, prefetch, Amcache, Shimcache a artefaktov vykonávania príkazov.

Windows event log štandardne konzistentne neuchováva kompletné reťazce User-Agent, takže veľká časť týchto dôkazov pochádza z telemetrie orientovanej na sieť, nie z klasických lokálnych logov OS. Podľa našich skúseností je možné najhodnotnejšie forenzné využitie User-Agenta vtedy, keď ho môžeme pripojiť ku konkrétnemu procesu, používateľskej relácii, cieľovej URL a časovej pečiatky, čo nám umožňuje posúdiť, či deklarovaný prehliadač a operačný systém zodpovedajú koncovému bodu, ktorý požiadavku vykonal.

4.28.3 Spôsoby a nástroje na obohatenie

V navrhovanom modelovom workflow by obohacovanie User-Agenta mohlo začať parsovaním surového reťazca pomocou štandardných knižníc na UA parsing alebo pomocou referenčných služieb na odvodenie rodiny prehliadačov, verzie prehliadača, operačného systému a indikácií, o aké zariadenie ide. Potom porovnávame reťazec s internými detekciami, spravodajstvom o hrozbách (threat intelligence), Sigma detekciami, správami o škodlivom softvéri a dokumentáciou známych útočných frameworkov, aby sme zistili, či UA zodpovedá bežne pozorovaným škodlivým alebo skriptovacím a automatizačným nástrojom. Pre analýzu automatizácie skontrolujte databázy botov a crawlerov a hľadajte reťazce spojené s vyhľadávačmi, web scrapermi, headless prehliadačmi alebo HTTP klientmi založenými na knižniciach. Môžeme tiež vykonať analýzu anomálií špecifických pre prostredie v platforme SIEM alebo UEBA, aby sme zistili, či je User-Agent zriedkavý, predtým nevidený, nekonzistentný s aktívami, z ktorých pochádza alebo zjavne vymyslený – hľadáme napríklad nemožné kombinácie prehliadača a operačného systému.

Odporúčaným analytickým prístupom je analyzovať User-Agenta, overiť jeho legitimitu podľa známych faktov o zariadení, z ktorého pochádza, ako je nainštalovaná verzia prehliadača a operačný systém, porovnať UA so známymi neškodnými a škodlivými vzormi a potom ho interpretovať spolu s ďalšími stopami/artefaktami (proces, cieľ požiadavky, kde UA bol, a časový rámec).

4.29 WiFi SSID / BSSID

Detekcia neautorizovaných prístupových bodov a sledovanie fyzickej blízkosti.

4.29.1 Význam a použitie

Obohatenie Wi-Fi SSID a BSSID nám pomáha určiť, či je bezdrôtová sieť v danej lokalite očakávaná, podozrivá alebo slabo chránená. Podľa skúseností nášho tímu je najužitočnejšie zistiť, či SSID alebo BSSID zodpovedá autorizovanej sieti, kde sa prístupový bod nachádza a aký typ šifrovania sa používa. Hlavnou výhradou je, že SSID sa dajú ľahko kopírovať, takže BSSID a okolitý kontext zvyčajne majú väčší význam než samotný názov siete.

4.29.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa SSID a BSSID často obnovujú z WLAN profilov, artefaktov v registri (pozri artefakty obsahujúce údaje o sieťových nastaveniach), Event logov, EDR telemetrie, z obrazu pamäte RAM, údajov z bezdrôtového adaptéra a výstupov príkazov, ako sú „netsh wlan show interfaces“ alebo zoznamy profilov. Vidíme ich tiež v zálohách z mobilných zariadení, screenshotoch a v niektorých prípadoch i v používateľských dokumentoch. Geolokácia a hodnotenie škodlivého AP (rogue access point) sú zvyčajne obohacujúce prvky pridané analytikom, nie natívne údaje z koncových bodov.

4.29.3 Spôsoby a nástroje na obohatenie

Odporúčame porovnať SSID a BSSID s inventármi autorizovaných sietí alebo WIPS dátami, skontrolovať, či BSSID mapuje na pravdepodobné fyzické miesto, a skontrolovať typ šifrovania na posúdenie rizika dotyčnej bezdrôtovej siete. Tiež hľadáme známky napodobňovania (impersonation podvrhnutého AP za legitímny), ako je známy SSID s neznámym BSSID alebo slabšie bezpečnostné nastavenia. Na základe skúseností nášho tímu je obohatenie Wi-Fi najužitočnejšie, keď sa kombinuje s dôkazmi o zariadení, polohe a časovej osi.

4.30 Windows Event ID

Vytvorenie časovej osi útoku, detekcia konkrétnej techniky protivníka.

4.30.1 Význam a použitie

Z pohľadu forenzného analytika nám obohacovanie ID udalostí v Event logoch pomáha pochopiť, čo znamená záznam v logu a aký je dôležitý v kontexte. Podľa skúseností nášho tímu spočíva kľúčová hodnota v preklade ID udalosti na jednoduchý význam, jeho mapovaní na možné techniky ATT&CK, identifikácii súvisiacich detekcií Sigma, odhadnutí jeho forenzného významu a poznaniu, ktoré ďalšie ID udalostí by sa mali preskúmať spolu s ním. Hlavnou nevýhodou je, že Event ID zriedka samo o sebe preukazuje škodlivú aktivitu. Jeho význam závisí najmä od zdroja logu, okolitých udalostí, úlohy endpointu a načasovania.

4.30.2 Typické artefakty obsahujúce údaje

Na Windows systémoch tieto údaje pochádzajú priamo z EVTX súborov, ako sú Security, System, Application, PowerShell, Sysmon, TaskScheduler a ďalšie prevádzkové logy. Event ID je natívne pre artefakt, zatiaľ čo mapovania ATT&CK, hodnotenia významnosti, zhody so Sigma pravidlami a ďalšie korelácie sú obohatenia pridané analytikom. V praxi zvyčajne korelujeme udalosť so susednými záznamami, prihlasovacími reláciami, aktivitou procesu a telemetriou koncových bodov, aby sme pochopili, čo sa vlastne stalo.

4.30.3 Spôsoby a nástroje na obohatenie

Referencie na Microsoft a SANS môžu byť použité na potvrdenie významu udalosti, potom ju namapovať na ATT&CK maticu a skontrolovať relevantné Sigma pravidlá. Tiež kontrolujeme bežné sprievodné Event ID, aby sme vytvorili úplnejšiu časovú os a priradili hrubý forenzný význam na základe typu vyšetrovania. Obohatenie ID udalostí môže byť najužitočnejšie, keď podporuje širšiu koreláciu udalostí.

4.31 Windows služba

Detekcia perzistencie na základe služieb a eskalácie privilégií.

4.31.1 Význam a použitie

Obohacovanie Windows servisov nám pomáha rozhodnúť, či je prítomnosť služby normálnym správaním systému alebo pravdepodobným mechanizmom perzistencie či zneužívania oprávnení. Najužitočnejšie doplnkové parametre servisu sú jeho meno (display name), cesta k binárnemu súboru (ImagePath), typ spustenia (StartupType), účet, pod ktorým služba beží, známy legitímny stav a digitálny podpis podkladového binárneho súboru. Hlavnou nevýhodou je, že známy názov služby môže byť zavádzajúci, takže je nutné kontrolovať konfigurovanú cesta (k spustiteľnému súboru) a kontext, v akom služba beží.

4.31.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sa tieto detaily bežne obnovujú z hivov SYSTEM a SOFTWARE - konfigurácie služieb v registri (kľúč Services), výstupu príkazu „sc qc“, údajov Autoruns, telemetrie EDR a binárneho súboru tej-ktorej služby na disku. Často korelujeme službu s Prefetchom, Amcache, logmi tvorby procesov (Security.evtx, event ID 4688) a metadátami súboru, aby sme potvrdili, čo na zariadení bežalo a pod ktorým účtom. V praxi vyplýva najsilnejšia hodnota z prepojenia definície služby s dôkazmi vykonávania programov/procesov a skutočným binárnym súborom.

4.31.3 Spôsoby a nástroje na obohatenie

V našom pracovnom postupe zvyčajne kontrolujeme konfiguráciu služby, aby sme identifikovali ImagePath, režim spustenia (Startup type), účet pod akým servis beží a popisné metadáta, a potom porovnávame službu so známymi Windows servismi a schválenými službami tretích strán (ak je takýto zoznam k dispozícií). Odporúča sa tiež porovnávať reťazce vykonávania procesov so známymi stromami procesov, ako sú prezentované napríklad na plagáte SANS „Hunt evil“. Tiež overujeme, či je podkladový spustiteľný súbor servisu (ImagePath) podpísaný a či sa nachádza v očakávanej trase. Obohatenie služby musí byť kombinované s artefaktami perzistencie, vykonávania a overenia dôvery v súbory.

4.32 YARA a Sigma pravidlá

Rozsah infekcie malvérom a overenie pokrytia detekcie pravidlami.

4.32.1 Význam a použitie

Obohacovanie pravidiel YARA a Sigma nám pomáha pochopiť, čo má detekcia nájsť, aká je špecifická a akú váhu prikladať zhode. Najdôležitejšie parametre sú názov a účel pravidla, cieľová rodina malvéru alebo TTP, počet zhôd v prostredí, požadované zdroje logov, mapovanie na ATT&CK a známe falošné pozitíva (false positives, nepravdivé detekcie). Hlavnou výhradou je, že zhoda s detekčným pravidlom je analytický lead, nie dôkaz sám o sebe. Preto ho vždy posudzujeme v kontexte súboru, ktorého sa detekcia týka, udalosti z logu, z informácií o zariadení a časovej osi. Je nevyhnutné zhody pravidiel overovať.

4.32.2 Typické artefakty obsahujúce údaje

Na systémoch Windows sú zhody s YARA pravidlami zvyčajne viazané na súbory, regióny v pamäti RAM, výpisy procesov, vzorky malvéru, na dáta zbierané EDR riešeniami alebo na smätný threat hunting. Oproti tomu sú Sigma zásahy viazané na logy ako Security, Sysmon, PowerShell, TaskScheduler, firewall a ďalšie zdroje importované do SIEM. **Samotné metadáta pravidla nie sú natívnym forenzným artefaktom**; Zvyčajne obnovíme zodpovedajúci súbor, proces, pamäťový objekt alebo záznam udalosti a následne pridáme kontext pravidla. V praxi najsilnejšia hodnota prichádza z prepojenia zhody pravidla s presným artefaktom, ktorý ju spustil, a z kontroly, či sa podobné zhody neobjavujú aj inde v prostredí.

4.32.3 Spôsoby a nástroje na obohatenie

Odporúčame začať preštudovaním metadát YARA alebo Sigma pravidiel, aby ste potvrdili, čo má pravidlo detegovať, na ktorú rodinu malvéru alebo správanie cieli, na aké techniky ATT&CK sa mapuje a aké falošné poplachy (false positives) sa očakávajú. Pre YARA potom meriame počet zhôd naprieč súbormi alebo pamäťou; pre Sigma overujeme, či existujú požadované zdroje a polia logov a prezeráme udalosti identifikované pravidlom v kontexte. Obohatenie pravidiel je najužitočnejšie, keď podporuje vyšetrovanie založené na artefaktoch.

5 Schematický návrh modelu na obohacovanie digitálnych stôp

5.1 Vyťažovanie dát na obohatenie zo sparsovaných dát

V prvom rade je potrebné definovať, ktoré IOCs bude náš model obohacovať, a akým spôsobom ich dokážeme zo sparsovaných stôp extrahovať. Ako sme spomínali v kapitole *0*

Zložitosť obohacovania digitálneho artefaktu – predspracovanie, nie všetky údaje, ktoré je možné obohatiť, sa nachádzajú priamo medzi sparsovanými artefaktami. Takže ešte pred samotným procesom obohatenia sa potrebujeme uistiť, že:

1. Vieme, kde (v akom artefakte) údaje hľadať.
2. Je definovaný spôsob, ktorým sa k informácií dostaneme (či už priamo parsovaním, alebo dodatočným spracovaním sparsovaných dát).

V praxi to znamená, že už automatizovaná extrakcia a parsovanie relevantných artefaktov je pripravené na postprocessing. Obohacované údaje môžu byť počas parsovania alebo po ňom napríklad označené príslušným **tagom** – napríklad IP_PUBLIC, IP_PRIVATE, HOSTNAME, PROCESS_NAME a podobne (zameriame sa najprv na atomické údaje, ktoré je možné kategorizovať takto jednoducho). Model na obohatenie tieto dáta vyžaduje na vstupe, a na základe nich spustí nad všetkými údajmi, ktoré určitým tagom disponujú, nadizajnovaný proces obohatenia.

Tagovanie by bolo možné implementovať i vo forme registra všetkých možných obohatení, ktoré by boli modelu dostupné (ako separátne obohacovacie funkcie).

V prípade, že údaj na obohacovanie je potrebné vypočítať, procedúra by mala byť zahrnutá vo fáze parsovania digitálnej stopy. Napríklad tak, že sa z každého súboru, ktorý je identifikovaný prostredníctvom záznamu v MFT, alebo je obnovený pomocou carvingu, vypočíta jeho hash (MD5 kvôli rýchlosti, SHA1 a SHA256 kvôli väčšej flexibilite a bezpečnosti).

Vyššie popísané idey sú iba **príkladom**, ako by mohli byť pre model dáta predspracované. V rámci projektu to však hlbšie nebudeme rozvíjať, keďže to závisí od konkrétnych dát, ktoré je potrebné obohacovať. Model sa snažíme definovať čo možno najvšeobecnejšie a uviesť prerekvizity – nie konrétny spôsob, ako prerekvizity detailne naplniť.

Jednotlivé údaje na obohatenie - entity, ktoré budú vstupovať do modelu na obohacovanie - by mali spĺňať určité základné parametre:

Vhodne navrhnutá entita, vytvorená zo sparsovaných forenzných artefaktov, by mala mať polia na jej identifikáciu, obohatenie, dohľadanie pôvodu (v pôvodnej digitálnej stope) a korelácie (s inými artefaktami a/alebo entitami).

Identifikácia identity

`id` - stabilný unikátny identifikátor, napríklad ip:8.8.8.8 alebo hash:<sha256>
`type` - entity type - ako `ip, domain, url, file_hash, user_account, process, registry_key`
`value` – raw hodnota, to jest IP adresa, doména, hash, username a pod., viď predošlá kapitola
`normalized_value` – normalizovaná forma použiteľná na strojové spracovanie - spárovanie a deduplikácia

Kontext zo sparsovaniho artefaktu

`source_artifact` – odkiaľ daná informácia pochádza, Security.evtx, Amcache.hve, NTUSER.DAT, browser history, ...
`source_record_id` – na zváženie, malo by ísť o číslo záznamu, event record ID, číslo stĺpca v tabuľke či iný referenciu, špecifickú pre artefakt
`host` - hostname alebo zariadenie, kde bol artefakt nájdený
`user` - asociovaný používateľ, ak je známy
`timestamp` – časová pečiatka, asociovaná s dobou pozorovania artefaktu
`artifact_field` - špecifické pole, z ktorého entita pochádza, napr. SourceWorkstationName, DestinationIp, URL, ImagePath, ...

Metadáta o prípade a korelácií
`case_id` – ID prípadu
`parent_entities` - ktoré predchádzajúce entity viedli k tejto
`related_entities` - už známe súvisiace entity
`relationship_type` – ako sú entity asociované, napríklad `resolved_to, downloaded_from, executed_by, queried_by`

Stav obohatenia
`attributes` – akumulované výstupy obohatenia
`enrichment_status` - napríklad not_started, partial, complete, failed
`applied_enrichments` - zoznam obohacovacích modulov, ktoré už boli spustené
`pending_enrichments` – moduly, ktoré ešte len budú bežať

Kvalita a pôvod entity
`confidence` – dôveryhodnosť extrakcie a normalizácie entity (napríklad ak je IP adresa priamo z Event logu, je dôveryhodnejšia, ako keby bola nájdená v inom type zdrojových dát napríklad pomocou regulárnych výrazov)
`provenance` - zdroj entity a zdroj každého obohatenia
`validation_status` - či už bola hodnota potvrdená, odvodená alebo neoverená
`tags` – voliteľné príznaky, napríklad `high_priority, external, ioc, rare, requires_review`

```
base_entity = {
    "id": None,                     # stable unique ID, e.g. "ip:8.8.8.8"
    "type": None,                   # ip, domain, url, file_hash,
user_account, process
    "value": None,                  # raw observed value
    "normalized_value": None,       # normalized/canonical representation

    "source_artifact": None,        # e.g. Security.evtx, Amcache.hve,
Chrome History
    "source_record_id": None,       # row/event/record identifier
    "artifact_field": None,         # parsed field name, e.g. DestinationIp,
URL, UserName
    "host": None,                   # endpoint/server where observed
    "user": None,                   # associated user if known
    "timestamp": None,              # observation time from artifact
```

```
    "case_id": None,
    "parent_entities": [],          # entities that led to this one
    "related_entities": [],         # linked entities
    "relationship_type": None,      # optional if created from a pivot

    "attributes": {},               # type-specific enrichment results
    "applied_enrichments": [],
    "enrichment_status": "not_started",

    "confidence": None,             # extraction confidence
    "validation_status": "observed",   # observed / inferred / validated /
unverified
    "provenance": [],               # extraction and enrichment provenance
    "tags": [],
    "priority": 0
}
```

5.1.1 IP address entity schema

Použiteľné pre verejné i súkomné IP adresy, odlíšiť ich možno atribútom `ip_scope`.

```
ip_entity = {
    "id": "ip:192.168.1.10",
    "type": "ip",
    "value": "192.168.1.10",
    "normalized_value": "192.168.1.10",

    "ip_version": 4,
    "ip_scope": "private",          # private / public
    "is_internal": True,
    "port": None,                   # optional if observed in connection
context
    "protocol": None,               # tcp / udp / icmp if known
    "direction": None,              # source / destination / both

    "attributes": {
        "hostname": None,
        "reverse_dns": [],
        "fqdn_candidates": [],
        "mac_address": None,
        "dhcp_lease_history": [],
        "subnet": None,
        "gateway": None,
        "vlan": None,

        "asn": None,
        "asn_org": None,
        "whois_org": None,
        "whois_country": None,
        "cidr": None,
        "geolocation": {},
        "hosting_type": None,
        "reputation": None,
        "blocklist_status": [],
        "tor_flag": None,
```

```
        "vpn_proxy_flag": None
    }
}
```

5.1.2 Domain / FQDN entity schema

```
domain_entity = {
    "id": "domain:example.com",
    "type": "domain",
    "value": "example.com",
    "normalized_value": "example.com",

    "is_fqdn": True,
    "registered_domain": "example.com",
    "subdomain": None,             # e.g. login if value is
login.example.com
    "tld": "com",

    "attributes": {
        "whois_registrant": {},
        "registrar": None,
        "registration_date": None,
        "expiration_date": None,
        "domain_age_days": None,
        "whois_privacy": None,

        "name_servers": [],
        "a_records": [],
        "aaaa_records": [],
        "mx_records": [],
        "txt_records": [],
        "cname_chain": [],
        "passive_dns_history": [],
        "subdomains": [],

        "ssl_certificates": [],
        "ct_log_entries": [],
        "web_stack": [],
        "category": None,
        "reputation": None,
        "phishing_association": None,
        "malware_association": [],
        "dga_score": None,
        "typosquat_similarity": {},
        "parking_status": None
    }
}
```

5.1.3 URL entity schema

```
url_entity = {
    "id": "url:https://example.com/login?user=test",
    "type": "url",
```

```
    "value": "https://example.com/login?user=test",
    "normalized_value": "https://example.com/login?user=test",

    "scheme": "https",
    "domain": "example.com",
    "port": 443,
    "path": "/login",
    "query": "user=test",
    "fragment": None,

    "attributes": {
        "domain_entity_id": "domain:example.com",
        "reputation": None,
        "scan_results": [],
        "http_status": None,
        "redirect_chain": [],
        "final_url": None,
        "content_type": None,
        "page_title": None,
        "page_metadata": {},
        "embedded_objects": [],
        "downloaded_files": [],
        "shortener_expanded_url": None,
        "archive_snapshots": [],
        "screenshot_refs": []
    }
}
```

5.1.4 File hash entity schema

```
hash_entity = {
    "id": "file_hash:sha256:abcd1234...",
    "type": "file_hash",
    "value": "abcd1234...",
    "normalized_value": "abcd1234...",

    "hash_algorithm": "sha256",
    "file_name": None,             # if known at time of extraction
    "file_path": None,             # if known
    "host_observed": None,

    "attributes": {
        "file_names_observed": [],
        "file_type": None,
        "magic_type": None,
        "file_size": None,
        "compile_timestamp": None,
        "packer": None,
        "digital_signature": {},
        "av_detections": [],
        "detection_ratio": None,
        "malware_family": None,
        "yara_matches": [],
        "embedded_strings": [],
```

```
        "imports": [],
        "sandbox_summary": {},
        "network_iocs": [],
        "attack_mapping": [],
        "threat_actor_association": [],
        "first_seen": None,
        "last_seen": None,
        "prevalence": None,
        "ssdeep": None,
        "tlsh": None,
        "parent_hashes": [],
        "child_hashes": []
    }
}
```

5.1.5 User account entity schema

Podobne ako pri IP adresách, pomocou atribútu “scope” odlíšime lokálne a doménové účty.

```
user_account_entity = {
    "id": "user_account:CORP\\jsmith",
    "type": "user_account",
    "value": "CORP\\jsmith",
    "normalized_value": "corp\\jsmith",

    "account_name": "jsmith",
    "domain": "CORP",
    "sid": None,
    "account_scope": "domain",     # domain / local / cloud / unknown

    "attributes": {
        "display_name": None,
        "account_type": None,      # user / admin / service / shared
        "group_memberships": [],
        "privilege_level": None,
        "account_status": None,    # enabled / disabled / locked
        "last_logon": None,
        "last_password_change": None,
        "password_policy_compliance": None,
        "mfa_status": {},
        "failed_login_count": None,
        "login_anomalies": [],
        "associated_devices": [],
        "department": None,
        "manager": None,
        "title": None,
        "employment_status": None,
        "vpn_history": [],
        "spns": []
    }
}
```

5.1.6 Process name entity

```
process_name_entity = {
    "id": "process_name:powershell.exe",
    "type": "process_name",
    "value": "powershell.exe",
    "normalized_value": "powershell.exe",

    "attributes": {
        "known_legitimate_application": True,
        "expected_paths": [
            r"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
        ],
        "expected_parents": [
            "explorer.exe",
            "cmd.exe",
            "services.exe"
        ],
        "lolbin_classification": True,
        "common_benign_usage": [],
        "common_malicious_usage": [],
        "prevalence_in_environment": None
    }
}
```

5.1.7 Process execution entity

```
process_execution_entity = {
    "id": "process_exec:HOST1:1234:2025-04-23T10:15:11Z",
    "type": "process_execution",
    "value": "powershell.exe -enc ...",
    "normalized_value": "powershell.exe -enc ...",

    "process_name": "powershell.exe",
    "pid": 1234,
    "ppid": 456,
    "command_line": "powershell.exe -enc ...",
    "image_path":
r"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe",
# using Python literal strings not to treat "\" as an escape character
    "attributes": {
        "parent_process_name": "cmd.exe",
        "expected_path_match": True,
        "expected_parent_match": False,
        "lolbin_classification": True,
        "digital_signature": {},
        "binary_hash": None,
        "network_connections": [],
        "user_context": None,
        "integrity_level": None,
        "session_id": None,
        "prevalence_in_environment": None
    }
}
```

5.2 1. úroveň obohatenia

Prvou úrovňou obohatenia je aplikácia postupov na primárne dátové entity. Môže ísť o dopytovanie sa cloudovej/webovej služby, internej databázy, či krížové vyhľadávanie v ostatných sparsovaných artefaktoch.

Typickým príkladom by bolo vyhľadanie verejnej IP adresy, získanej zo sparsovaného logu Security.evtx, v službe AbuseIPDB, alebo vyhľadanie doménového mena a dohľadanie informácií o SSL/TLS certifikáte prostredníctvom Censys.io.

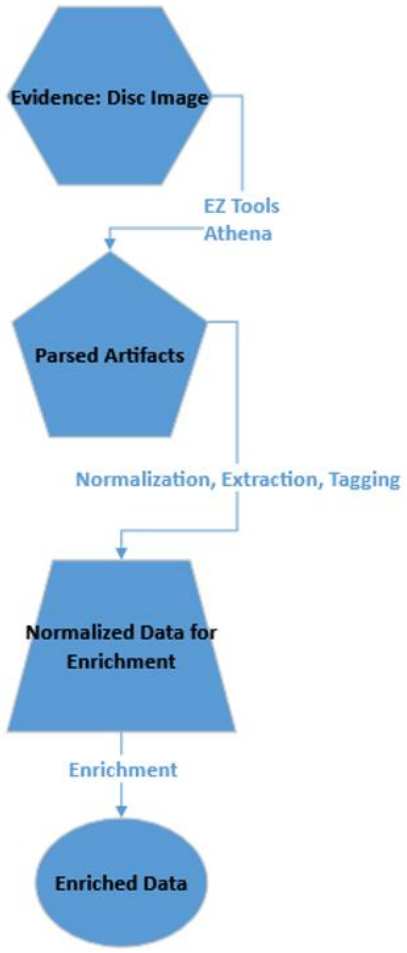
5.3 2. až N-tá úroveň obohatenia

Druhú až N-tú úroveň obohatenia predstavuje iterácia enrichment procesu na údaje získané prvotným obohatením. Ak napríklad obohacujeme meno procesu, ktorý bol identifikovaný v obraze pamäte RAM, môžeme korelovať jeho názov s hashom spustiteľného súboru, získaného z image disku. Hash sme predtým museli vypočítať a pravdepodobne sme ho už obohacovali. Meno procesu môžeme identifikovať i v review sieťových spojení, ako komunikujúci so vzdialenou privátnou IP adresou. Ak obohacujeme túto IP adresu, obohacujeme zároveň aj proces, ktorý spojenie vyvolal.

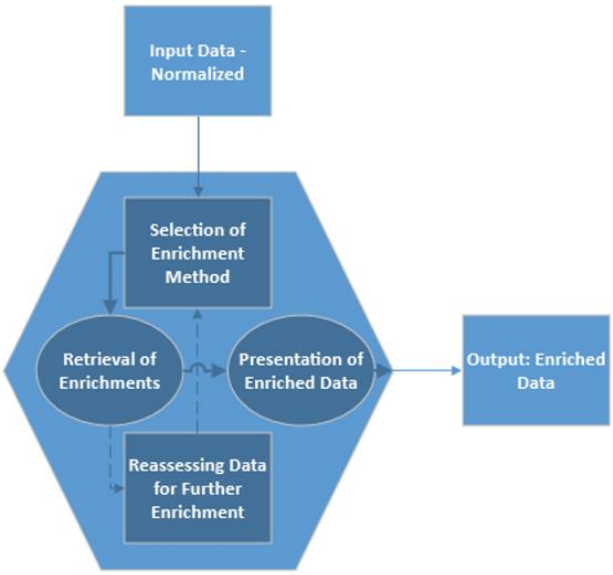
N ako počet iterácií by malo byť zhora ohraničené, aby sme predišli nekonečnému behu modelu. Zároveň je potrebné, aby každá novo identifikovaná informácia (entita) získaná procesom obohacovania bola overená na duplicitu. Je totiž možné, že na vstupe identifikujeme DNS záznam a IP adresu, ktoré by sa v procese obohacovania odkazovali samé na seba.

5.4 Schéma procesu spracovania a obohacovania stôp

Obrázok 1 podrobne popisuje úvodné fázy spracovania dôkazov až po extrakciu dát, zatiaľ čo Obrázok 2 znázorňuje následný proces ich obohacovania.



Obrázok 1: Schéma spracovania stopy až po obohatenie extrahovaných dát



Obrázok 2: Schéma procesu obohacovania dát

5.5 Pseudokód

Algoritmus spracováva normalizované forenzné záznamy ako iteratívny „pracovný zoznam“. Počíta s extrakciou obohacovateľných entít, čo však v rámci modelu bližšie neriešime. Algoritmus aplikuje pre entitu špecifické moduly obohacovania, ukladá vrátený kontext aj s referenciou na jeho pôvod a znovu zaradí novo objavené entity do zoznamu pre ďalšie kolá obohacovania, kým nezostanú žiadne nové entity alebo nie je dosiahnutý preddefinovaný limit iterácií.

```
def enrich_dataset(records, registry, max_rounds=10):
        """
        Iteratively enrich normalized forensic records.

        Parameters
        ----------
        records : list
        Pre-processed and normalized forensic records obtained from parsed
        artifacts.
        These records may come from tools that parse EVTX, Registry, Prefetch,
        browser history, Amcache, LNK files, etc.

        registry : dict
        Mapping of entity type -> list of enrichment functions.
        Example:
        {
        "ip": [enrich_ip_whois, enrich_ip_reputation],
        "domain": [enrich_domain_dns, enrich_domain_whois],
```

```
"hash": [enrich_hash_vt, enrich_hash_signature]
}

Each enrichment function is expected to accept one entity and return a
result object such as:
{
"success": True,
"data": {...},
"source": "VirusTotal",
"confidence": 0.95
}

max_rounds : int
Safety limit to prevent infinite enrichment loops. This matters because
one enrichment can reveal new entities, which can trigger more enrichment
in later rounds.

Returns
-------
output : dict
Dictionary keyed by entity ID, containing:
- the original entity
- accumulated enriched attributes
- provenance for each enrichment step
- child entities discovered from enrichment
"""

# Initial worklist of entities extracted from the normalized records.
# This function is not described in depth.
# Enrichment model assumes that input is already in necessary format.
# Examples:
# - IP addresses from firewall logs
# - domains from browser history
# - hashes from Amcache, EDR, or calculated
# - usernames from event logs and ProfileList
worklist = extract_entities(records)

# Tracks which entity IDs have already gone through enrichment.
# This prevents processing the same entity repeatedly.
processed = set()

# Final enriched output.
# One entry per entity, keyed by a stable identifier such as:
# "ip:8.8.8.8"
# "domain:example.com"
# "hash:<sha256>"
output = {}

# Run enrichment in rounds.
# Each round processes the current worklist and may discover new entities
# that will be handled in the next round.
for _ in range(max_rounds):
# Stop early if there is nothing left to enrich.
if not worklist:
break
```

```
# Collect entities discovered during this round.
# These become the next round's worklist.
new_worklist = []

# Process each entity currently waiting for enrichment.
for entity in worklist:
# Build or retrieve a stable unique ID for the entity.
# This ID is used for deduplication and for storing results.
key = get_entity_id(entity)

# Skip entities that have already been fully processed.
# This avoids loops such as:
# domain -> IP -> domain -> IP
if key in processed:
continue

# Mark this entity as processed before running enrichments.
processed.add(key)

# Ensure an output record exists for this entity.
# "attributes" will accumulate enrichment data across modules.
# "provenance" records where each enrichment came from.
# "children" tracks newly discovered related entities.
output.setdefault(key, {
"entity": entity,
"attributes": {},
"provenance": [],
"children": []
})

# Select enrichment functions based on entity type.
# Example:
# entity["type"] == "domain"
# -> run DNS, WHOIS, reputation, passive DNS enrichments etc.
for enrich in registry.get(entity["type"], []):
# Run the enrichment function for this entity.
result = enrich(entity)

# Ignore unsuccessful enrichments.
# We suggest that in PoC model, failures are logged separately.
if not result["success"]:
continue

# Merge newly returned attributes into the entity's attribute set.
# Example:
# domain enrichment may add:
# {"registrar": "...", "age_days": 3, "mx_records": [...]}
#
# Note:
# Later enrichments may add more keys or overwrite earlier values,
# depending on how update() is handled in the final implementation.
output[key]["attributes"].update(result["data"])

# Record provenance for auditability and forensic defensibility.
```

```
# This is important because enriched findings should be traceable
# back to the source and method used.
output[key]["provenance"].append({
"enrichment": enrich.__name__,
"source": result.get("source"),
"confidence": result.get("confidence")
})

# Some enrichment results reveal new entities that can themselves
# be enriched in a later round.
#
# Examples:
# - domain enrichment reveals resolved IPs
# - hash enrichment reveals contacted URLs
# - email enrichment reveals sender IP or related domain
# - sandbox analysis reveals dropped file hashes
for child in extract_new_entities(result["data"]):
child_key = get_entity_id(child)

# Preserve the fact that this parent entity led to discovery
# of another potentially relevant entity – which should be enriched separately.
output[key]["children"].append(child_key)

# Queue the new entity for later enrichment, but only if it
# has not already been processed.
if child_key not in processed:
new_worklist.append(child)

# Prepare the next round.
# This step should remove duplicates and may also prioritize entities.
# For example, public IPs, domains, hashes, or rare indicators could be
# processed before lower-value entities.
worklist = deduplicate_and_prioritize(new_worklist)

# Return the accumulated enriched dataset.
return output
```

6 Záver

Model digitálneho obohacovania dôkazov predstavený v tomto dokumente ukazuje, že systematické dopĺňanie kontextu k digitálnym stopám výrazne zvyšuje ich hodnotu pre forenznú analýzu. Cieľom bolo vytvoriť ucelený rámec, ktorý umožní efektívne prepájať artefakty s externými zdrojmi, indikátormi kompromitácie (IoC) a spravodajskými informáciami (Threat Intelligence).

Výsledkom je flexibilný a škálovateľný model, ktorý podporuje rôzne úrovne obohacovania – od jednoduchých atribútov až po komplexné zložené informácie. Tento prístup umožňuje presnejšie vyhodnocovanie a riešenie incidentov, rýchlejšiu atribúciu a lepšiu prioritizáciu činností počas IR i forenznej analýzy. Model predstavuje krok k dátovo orientovanej digitálnej forenznej analýze a tvorí pevný základ pre ďalší výskum aj praktické nasadenie.