Threat-Informed Defense:

Tramsformacja Cyber Zagrożeń na Przeciwdziałania

Grzegorz Molski / Wojciech Lesicki

Standard Chartered

O nas

Grzegorz Molski

Wojciech Lesicki

Pracujemy Standard Chartered Bank w zespole Threat Assessment and Countermeasures

TID – czym jest?

„Threat-Informed Defense is the systematic application of a deep understanding of adversary tradecraft and technology to improve defenses.”

źródło Measure, Maximize, and Mature Threat-Informed Defense

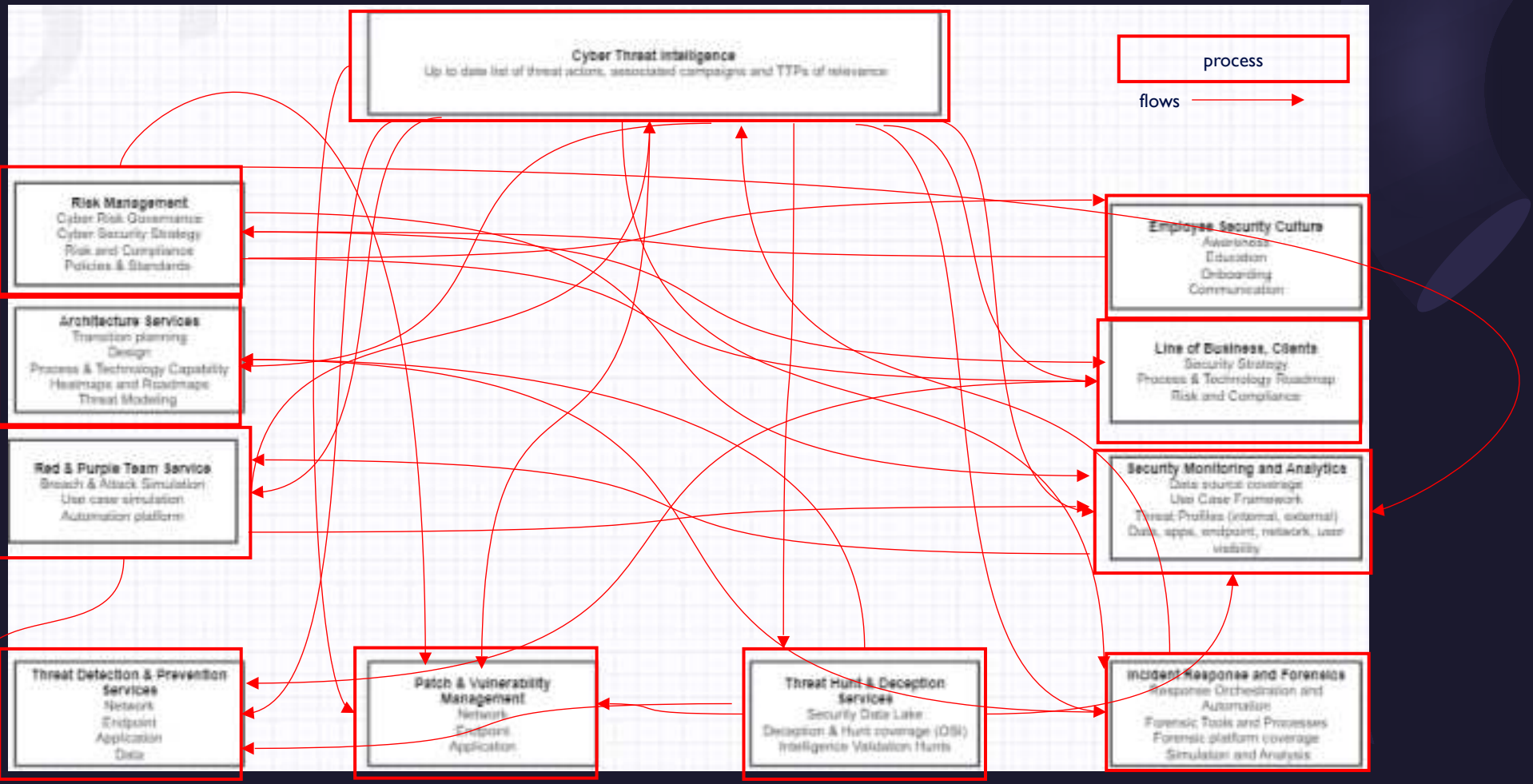
TID – po co?

Aby z pewnością ocenić stan bezpieczeństwa względem istonych zagrożen

Strategiczne problemy	Konsekwencje
Zdecentralizowany process zarzadzania zagrożeniami (oraz ryzk) bez centralnego widoku na stan bezpieczeństwa, podatności oraz ryzyk	Negatwyny wpływ na process podejmowania decyzji względem priorytetów**.**
Brak efektywnej koordynacji pomiedzy funkacjmi zajmujacymy sie adresowaniem zagrożen	Malo efektwyny process korelacji danych oraz idących za tym czynności rekomendowanych dla priorytetow
Brak spojnej taxonomii oraz centralnego repozytorium zagrożen kluczowych elementów do korelacji zagrożen-assetow-kontrolii, pozwalajacych na efektywny przepływ informacjii oraz możliwość podejmowania decyzji na ich podstawie.	Silosowa i manualna konsumpcja oraz korelacja danych co jest czasochłonne oraz podatne na błędy**.**
Brak jednego i spojengo widoku na stan bezpieczeństwa względem zagrożeń obecnych jak rownież przyszlych	Nie efektywna priorytezacja inwestycji cyber bezpieczeństwa względem przypuszczeń odnośnie z zagrożenia, jego siły oraz jakie wykorzystywane są podatności

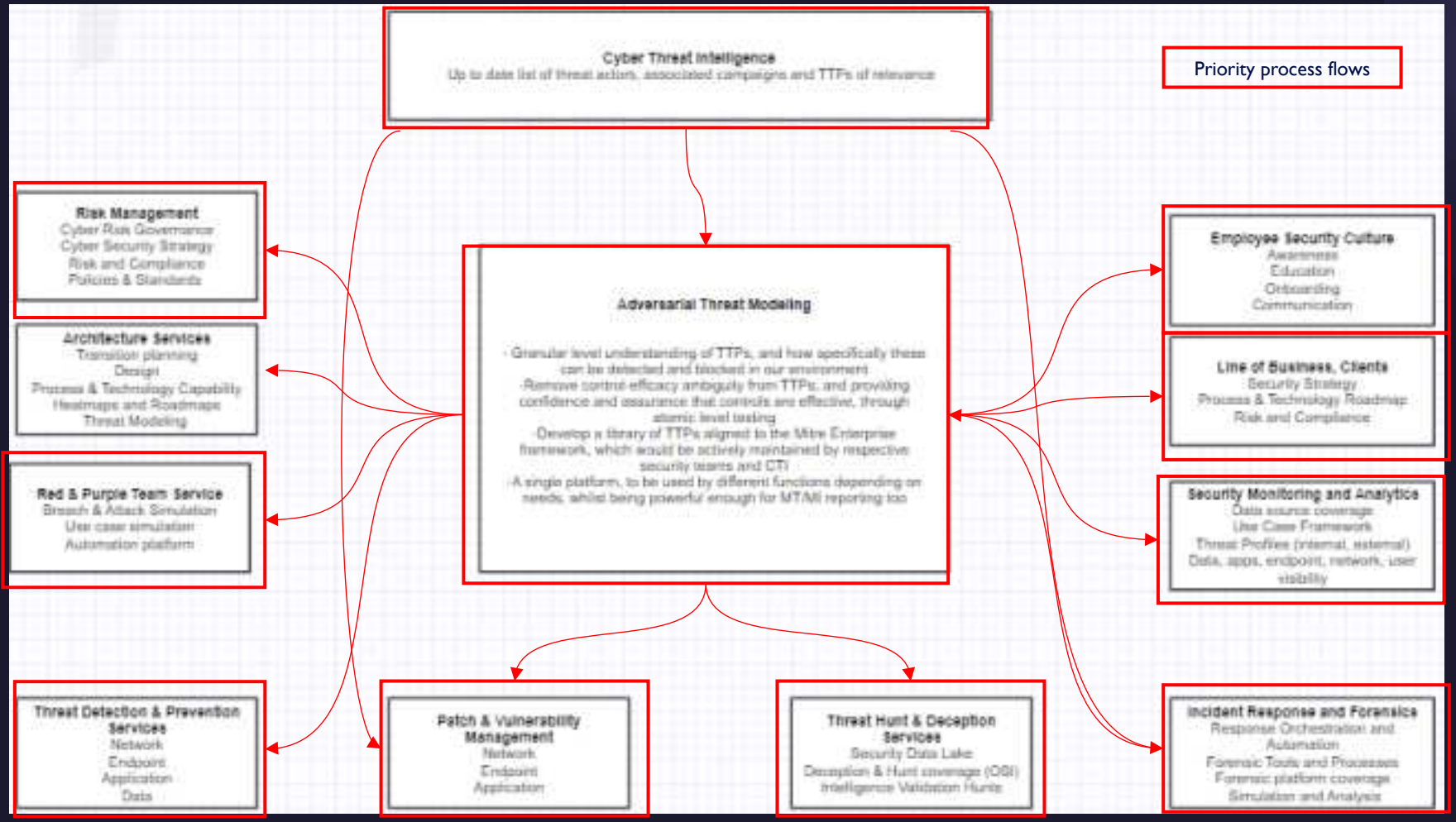
TID – czemu potrzebujemy?

PRZECIEŻ INFORMACJA JUZ PRZEPŁYWA, PRAWDA?



TID – jak?

- KIERUNEK I KONTROLA PRZEPŁYWU



Ale...

Ale zanim tam będziemy musimy poradzić sobie z kilkoma problemami w obszarach:

- Ludzie
- Proces
- Tech

Problemy/przeszkody i nasze propozycje rozwiązań

Problem #1 – umiejętności i wiedza

- Możemy mieć najlepszych analityków CTI i nie być w stanie działać skutecznie w ramach TDI
- Musimy zrozumieć zagrożenia, ale także znać jak przed nimi można się bronić. Musimy znać różne usługi/rozwiązania dostępne na rynku (czy też w open source). Rozumieć ich limity.
- Musimy również znać swoją organizację

Rozwiązanie #1 – dedykowany zespół

- Potrzebujemy połączenie różnych doświadczeń czy związanych z IR, threat hunting, ale także z wdrażaniem różnych rozwiązań bezpieczeństwa i świadomością aktualnych zagrożeń

- Pozwól analitykom CTI skupić się na śledzeniu threat actors

- Dane CTI są nadal kluczowe, nadal ich potrzebujemy od dedykowanego zespołu albo z innych źródeł

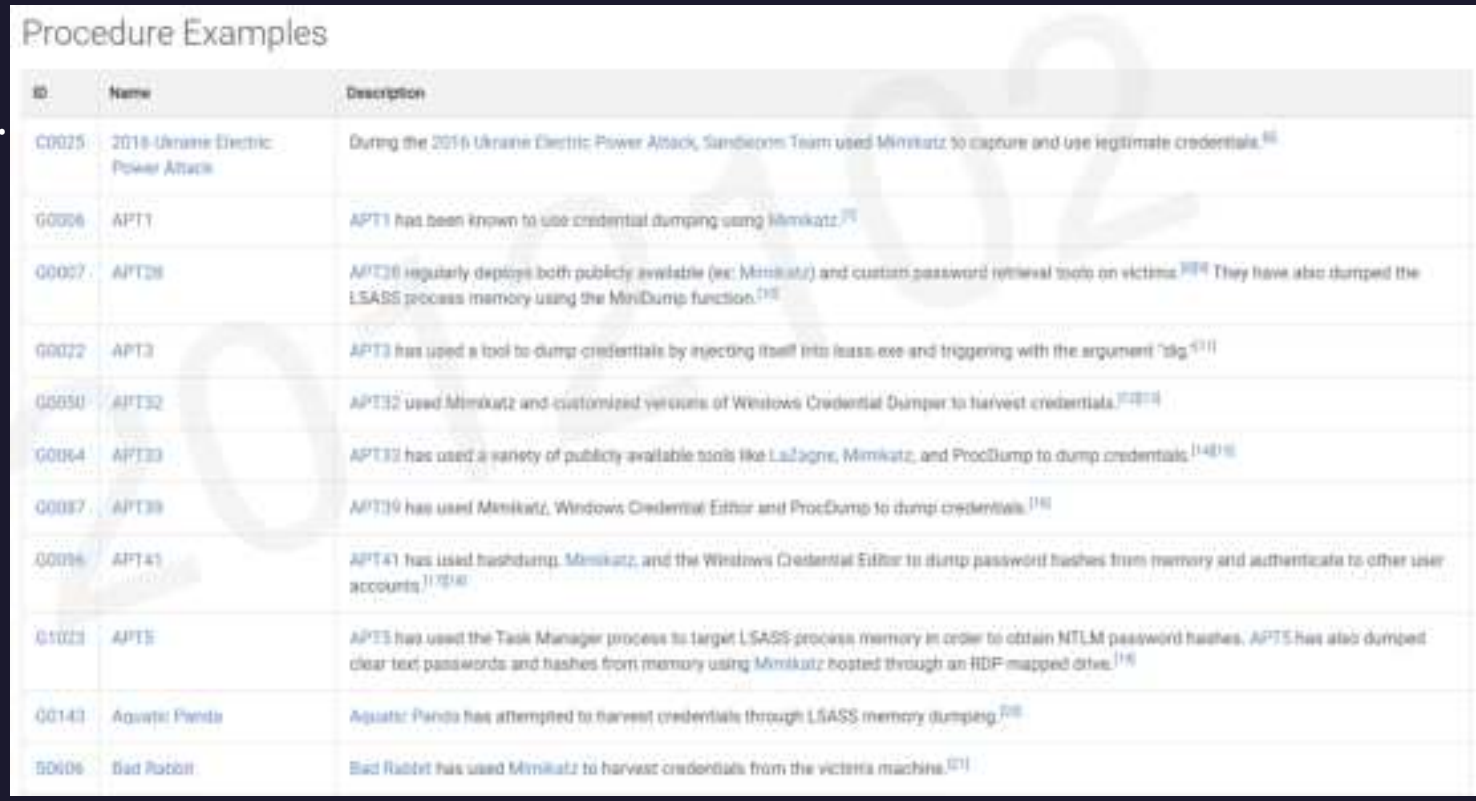
Problem #2 – problem z procedurami

- Dla skutecznego działania dla TDI, nie możemy zatrzymać się na ogólnym poziomie technik (np. „czy mamy odpowiednie mechanizmy obronne dotyczące T1003?”). Konieczne jest działanie na poziomie procedur (np. „czy możemy zapobiec użyciu <polecenie> i czy mamy odpowiednią detekcję? Czy nasze testy purple/red to potwierdziły?”).
- Raporty CTI, nawet jeśli poprawnie wymieniają procedury, nie ułatwiają tego zadania...

Problem #2 – problem z procedurami

Sam framework ATT&CK MITRE i znajdujące się tam „procedure examples” nie są wystarczające

Miks informacji o grupach, narzędzia, kampaniach...



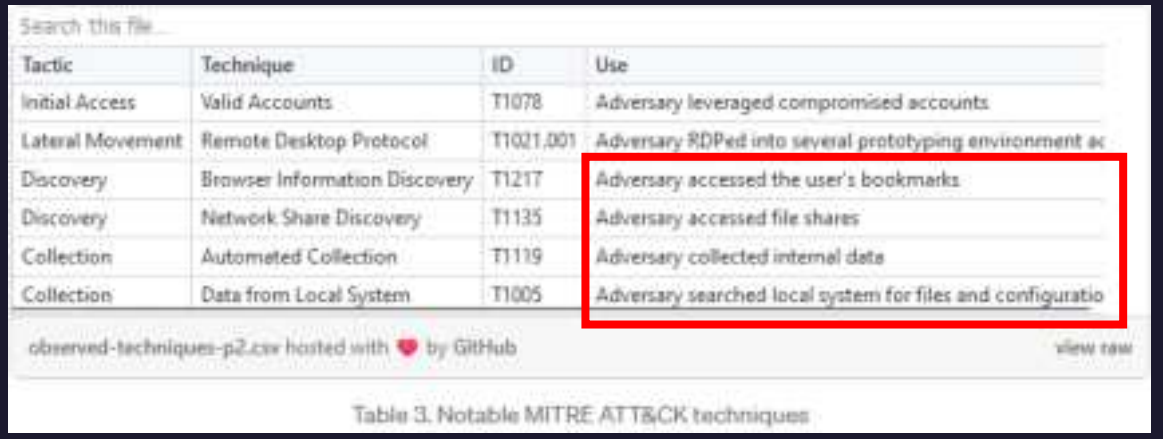
Procedure Examples

ID	Name	Description
C0025	2016 Ukraine Electric Power Attack	During the 2016 Ukraine Electric Power Attack, Sandworm Team used Mimikatz to capture and use legitimate credentials.
G0006	APT1	APT1 has been known to use credential dumping using Mimikatz.
G0007	APT28	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims. They have also dumped the LSASS process memory using the MiniDump function.
G0022	APT3	APT3 has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig".
G0050	APT32	APT32 used Mimikatz and customized versions of Windows Credential Dumper to harvest credentials.
G0064	APT33	APT33 has used a variety of publicly available tools like LaZagne, Mimikatz, and ProcDump to dump credentials.
G0087	APT39	APT39 has used Mimikatz, Windows Credential Editor and ProcDump to dump credentials.
G0096	APT41	APT41 has used hashdump, Mimikatz, and the Windows Credential Editor to dump password hashes from memory and authenticate to other user accounts.
G1023	APT5	APT5 has used the Task Manager process to target LSASS process memory in order to obtain NTLM password hashes. APT5 has also dumped clear text passwords and hashes from memory using Mimikatz hosted through an RDP mapped drive.
G0143	Aquatic Panda	Aquatic Panda has attempted to harvest credentials through LSASS memory dumping.
S0606	Bad Rabbit	Bad Rabbit has used Mimikatz to harvest credentials from the victims machine.

Problem #2 – problem z procedurami

Różne raporty CTI przedstawiają procedury w różny sposób; nie mamy tutaj standardów/best practise

Dobry przykładem jak to powinno wyglądać jest raport samej organizacji MITRE odnośnie ataku na nich...ale...

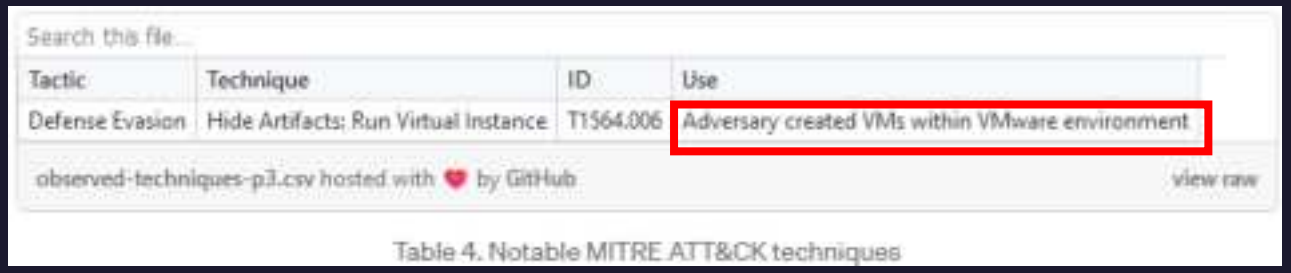


Search this file...

Tactic	Technique	ID	Use
Initial Access	Valid Accounts	T1078	Adversary leveraged compromised accounts
Lateral Movement	Remote Desktop Protocol	T1021.001	Adversary RDPed into several prototyping environment ac
Discovery	Browser Information Discovery	T1217	Adversary accessed the user's bookmarks
Discovery	Network Share Discovery	T1135	Adversary accessed file shares
Collection	Automated Collection	T1119	Adversary collected internal data
Collection	Data from Local System	T1005	Adversary searched local system for files and configuratio

observed-techniques-p2.csv hosted with ♥ by GitHub view raw

Table 3. Notable MITRE ATT&CK techniques



Search this file...

Tactic	Technique	ID	Use
Defense Evasion	Hide Artifacts: Run Virtual Instance	T1564.006	Adversary created VMs within VMware environment

observed-techniques-p3.csv hosted with ♥ by GitHub view raw

Table 4. Notable MITRE ATT&CK techniques

Problem #2 – problem z procedurami

```
C:\Windows\system32\schtasks.exe /Create /RU NT AUTHORITY\SYSTEM /tn
ayttpnzc /tr regsvr32.exe -s "c:\Users\[REDACTED]
\Desktop\7611346142\c2ba065654f13612ae63bca7f972ea91c6fe97291caeaaa3a
28a180fb1912b3a.dll" /SC ONCE /Z /ST 15:21 /ET, 15:33
```

Nie ma standardów dotyczących tego jak powinniśmy rozróżniać procedur pomiędzy sobą...

```
"C:\Windows\System32\schtasks.exe" /CREATE /SC ONCE /ST 17:21:58 /TN
9T6ukfi6 /TR "'C:\Users\pagefilerpqy.exe'" /f /RL HIGHEST
```

...czy powinniśmy dodawać im kolejnych numer/nazwę...

T1053.005.000x?

...lub śledzi prace związane z tą procedurą

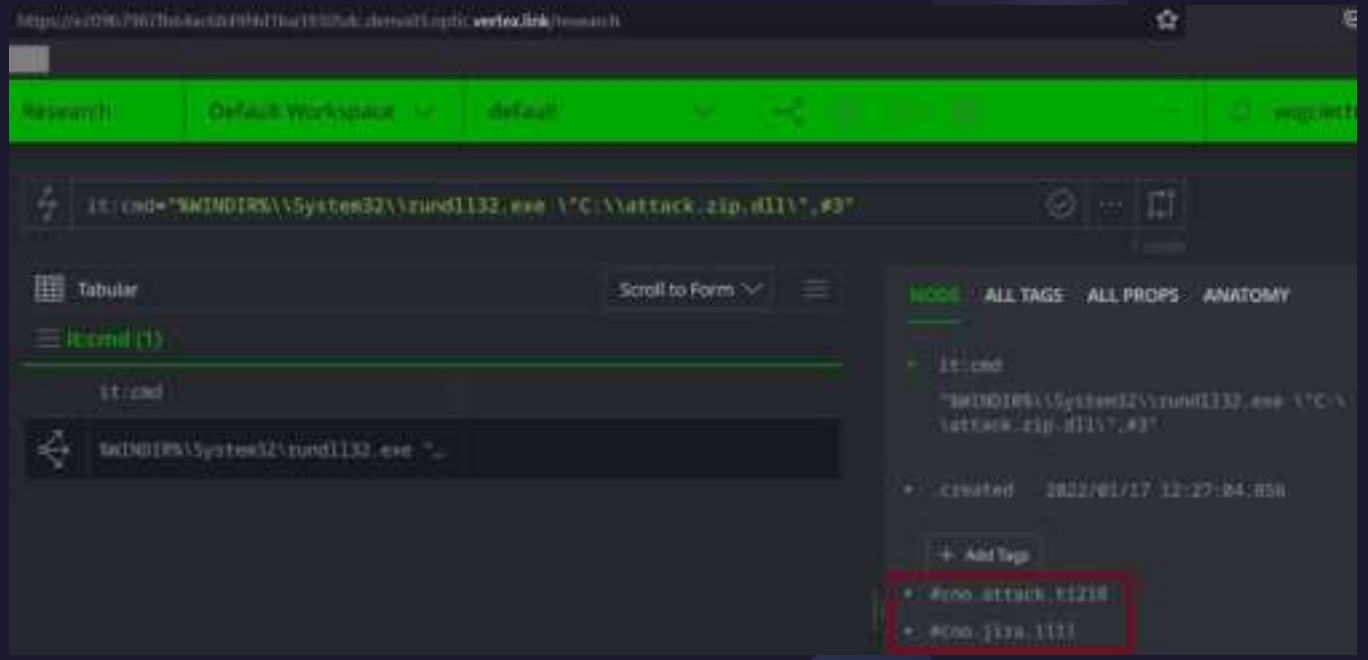
Rozwiązanie #2 – zacznijmy od mały kroków, ale pamiętajmy gdzie chemy być

- Wymagajmy szczegółowych informacji o procedurach od zespołów CTI lub vendorów
- Skupmy się na najważniejszych technikach dla swojej organizacji, np. tych związanych z threat actors, którzy stanowią dla nas największe zagrożenie. Jeśli mamy z tym problem - zacznijmy od publicznych raportów (np. z Red Canary Threat Detection Report, M-trends od Mandiant) lub od samych operatorów ransomware.
- Najpierw potwierdźmy prostsze procedury (np. uruchamianie „zwykłego” mimikatz), zanim przejdziemy do bardziej zaawansowanych.
- Zachowajmy umiar jak wiele procedur per technika chcemy (możemy) analizować

Rozwiązanie #2 – zacznijmy od mały kroków, ale pamiętajmy gdzie chcemy być

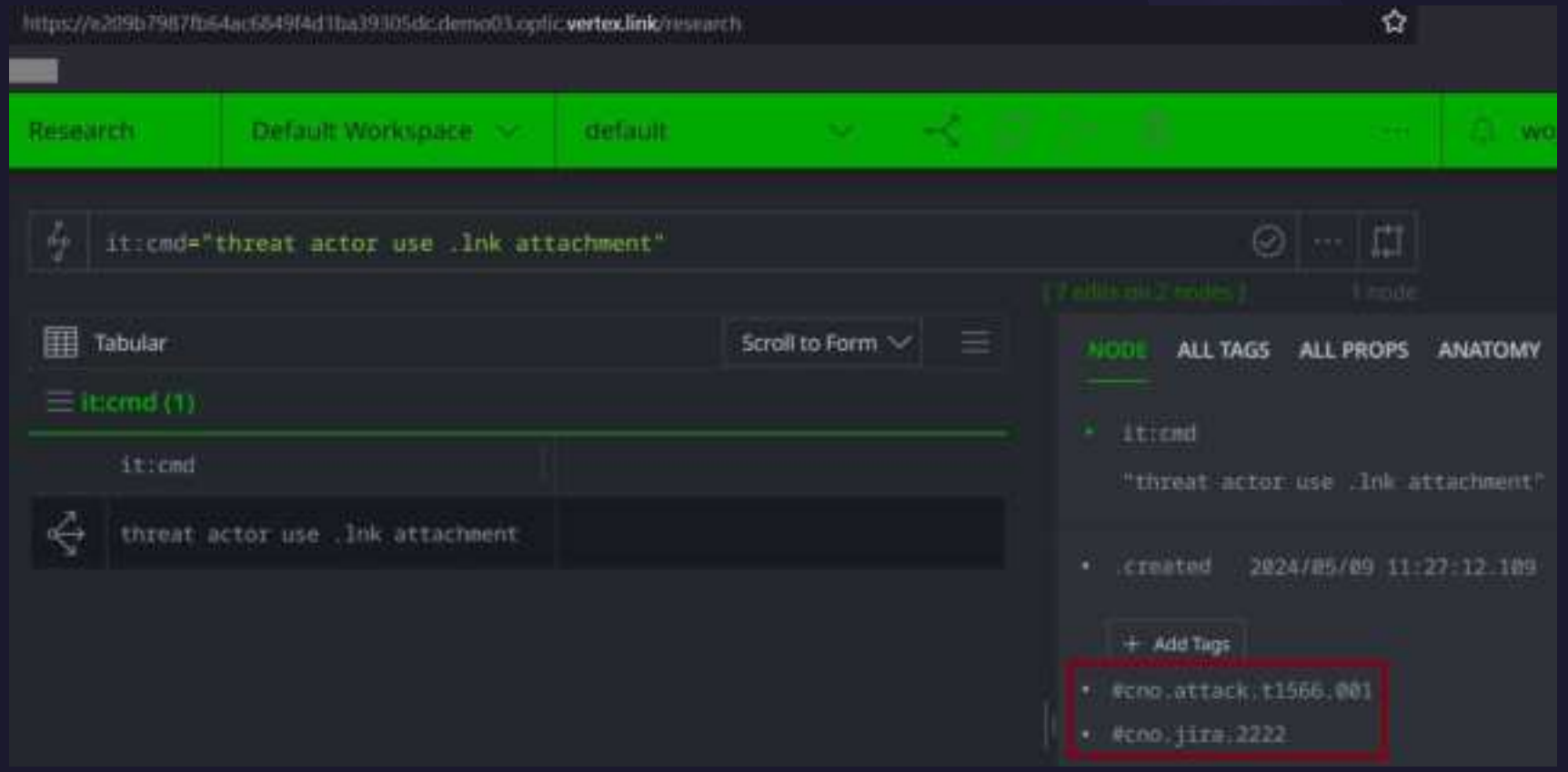
- By lepiej śledzić postępy prac dla danej procedury możemy użyć systemu ticketowego, którego używamy (np. Jira)

- Przechowujmy informacje o procedurach w swoich TIP...najlepiej wraz z numer zadania (wymienionym powyżej), aby analitycy CTI mieli również tą informacje



Rozwiązanie #2 – zacznijmy od mały kroków, ale pamiętajmy gdzie chcemy być

- Procedury mogą czasami być konkretnym poleceniem (cmd, powershell), ale mogą być też bardziej opisowe/wysoko poziomowe – to zależy w dużej mierze od techniki



Problem #3 – brak informacji o prewencji

- Skuteczne zatrzymywanie threat actors nie może opierać się wyłącznie na detekcji
- Od wersji ATT&CK v10 (2021) wprowadzono dwie nowe mitigation dla Enterprise, dla kilkunastu wprowadzono zmiany
- Jednocześnie widzimy w ATT&CK nowe elementy związane z detekcją...

Rozwiązanie #3 – inne źródła

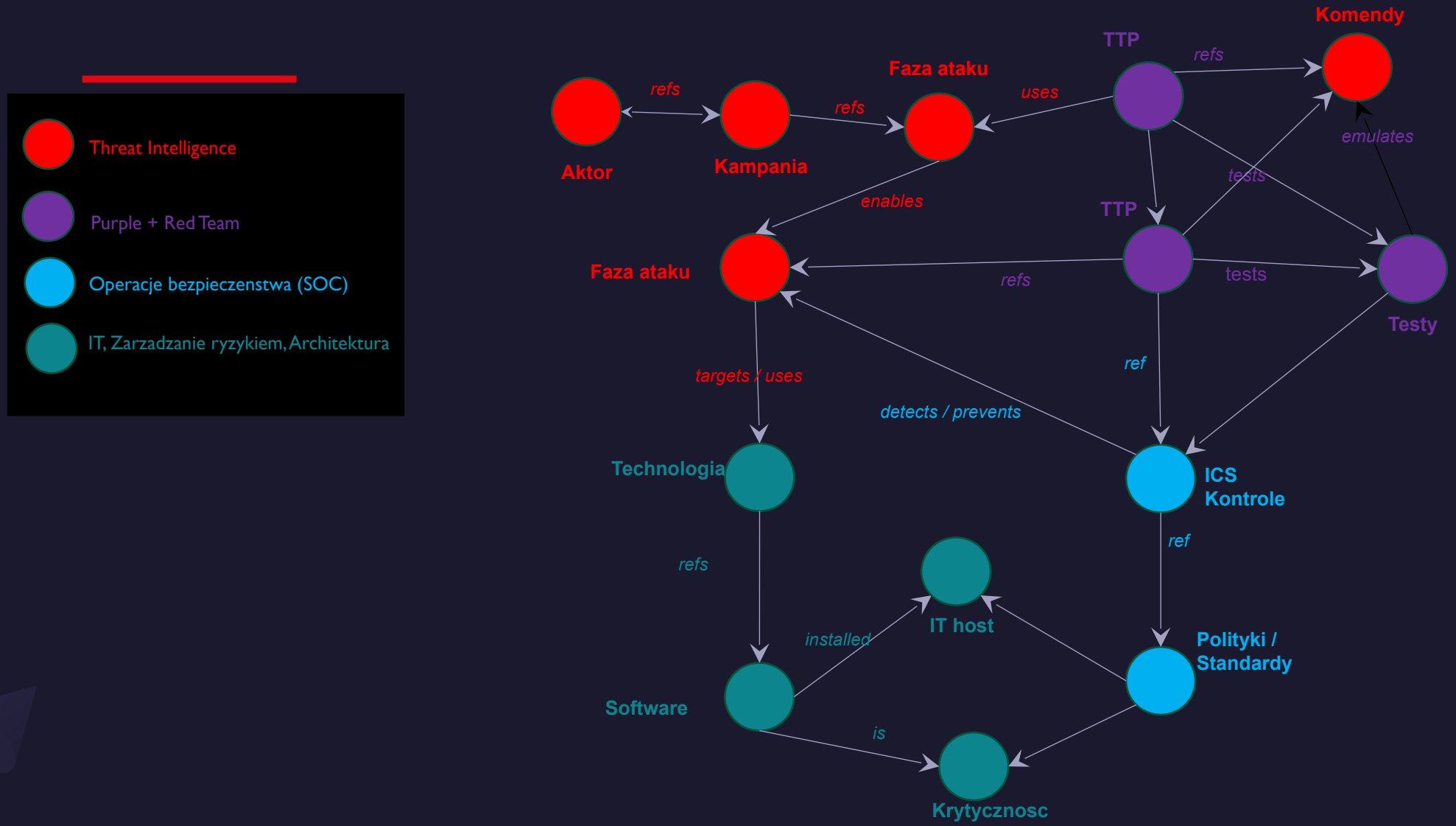
- Możemy użyć frameworku D3FEND (nawet gdy jest on w wersji beta)
- Nieliczne publikacje jak np. „Ransomware Protection and Containment Strategies” from Mandiant/Google Cloud
- Pytajmy MITRE i inne orgranizacje o więcej

Problem #4 – narzędzia

Brak pojedynczej platformy do korelacji zagrożeń, aktualnego stanu mechanizmów bezpieczeństwa (czy też zagrożenie, zasoby, detekcja, zapobieganie, reagowanie) z danymi z wielu źródeł w scentralizowany sposób.

Wyizolowana korelacja danych, wykonywama manualnie = duży koszt czasowy i ryzyko błędów

Rozwiązanie #4 – relacje w jednym miejscu



Rozwiązanie #4 – jedna grafowa baza danych

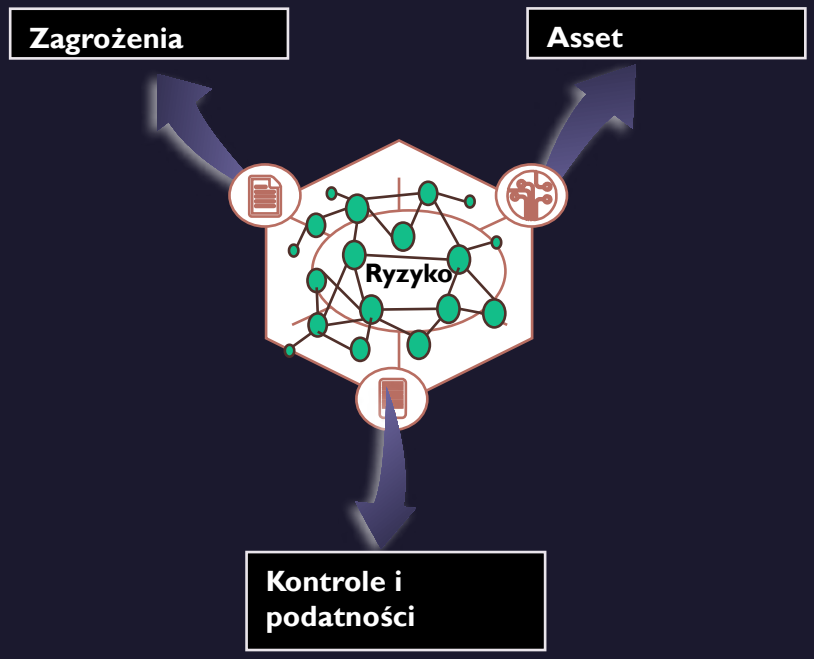
Rozwiazania umożliwiające modelowanie (grafowa baza danych) danych pochodzących z różnych repozytoriow, zarówno ustrukturyzowanych jak i nie. Jednocześnie pozwalająca na korelacje danych pod wzdględem ich wlaściwości oraz raportowanie na wielu poziomach.
Kluczowe elementy dla stworzenia modelu relacij:

- Asety
- Zagrożenia
- Kontrole
- Podatności (wszystkie)

Przykladowe raporty

Identyfikacji asetów podatnych na zagrożenia	Determinacja techniki, która przerwie łancuch ataku dla danego scenariusza	Identifikacja asetów, ktęre sa celem (zainteresowaniem) dla aktpra w danej fazie ataku

Jedno źródło dla Threat Informed Defense



Grzegorz Molski
LinkedIN:
gregmolski

Wojciech Lesicki
LinkedIN:
wojciechlesicki
Twitter/X:
@WLesicki