Narodowe Centrum Badań i Rozwoju

Projekt realizowany w konkursie CYBERSECIDENT

CYBERSECIDENT/487845/IV/NCBR/2021

Zaawansowane metody i techniki wykrywania i przeciwdziałania atakom na infrastrukturę dostępową i aplikacje sieci 5G

Finalna wersja raportu P6.3 - Dokumentacja techniczna systemu 5gSTAR

Wersja:	**1.0**
Autor:	**Krzysztof Kosmowski**
Data:	**12.08.2024**

REJESTR ZMIAN

Lp.	Wersja	Data	Wprowadzający	Opis zmiany
1.	1.0	12.08.2024	K. Kosmowski	Wersja inicjalna
2.				
3.				

Spis treści

Wstęp

Niniejszy raport jest elementem realizacji Projektu pt. „Zaawansowane metody i techniki wykrywania i przeciwdziałania atakom na infrastrukturę dostępową i aplikacje sieci 5G” i przedstawia część wyników prac zrealizowanych w Zadaniu 6. Jest to produkt 6.3 etapu A projektu 5gSTAR [1].

Struktura dokumentu jest następująca:

Rozdział 1 – System5gSTAR;

Rozdział 2 – Aplikacja Przeciwdziałania Atakom (WIŁ);

Rozdział 3 – Aplikacja Przeciwdziałania Atakom (GM);

Rozdział 4 – Detektory SI dla SCADA i IIoT.

1 System 5gSTAR

System 5gSTAR jest zestawem zaawansowanych metod i technik wykrywania oraz przeciwdziałania atakom na infrastrukturę dostępową i aplikacje sieci 5G zaimplementowanych w postaci modułów programowych. Został on opracowany zgodnie z założeniami zawartymi w projekcie technicznym [2].

Ogólna idea działania systemu 5gSTAR jest następująca: detektory 5gSTAR wykrywają zagrożenia w systemie, który monitorują i zgłaszają alerty o wykryciu ataku bądź jego symptomów do elementów, które składują i przetwarzają te dane. Następnie informacje o zdarzeniu są udostępniane Operatorowi systemu poprzez dedykowaną konsolę (aplikację przeglądarkową). Na bazie informacji o zagrożeniu Operator może podjąć akcje zaradcze wykorzystując do tego celu dedykowane moduły APA (Aplikacja Przeciwdziałania Atakom). Akcje zaradcze, w zależności od rodzaju zagrożenia, mogą być realizowane w sposób automatyczny – poprzez uruchomienie dedykowanego skryptu automatyzującego lub manualny – lista kroków jakie powinien wykonać Operator systemu.

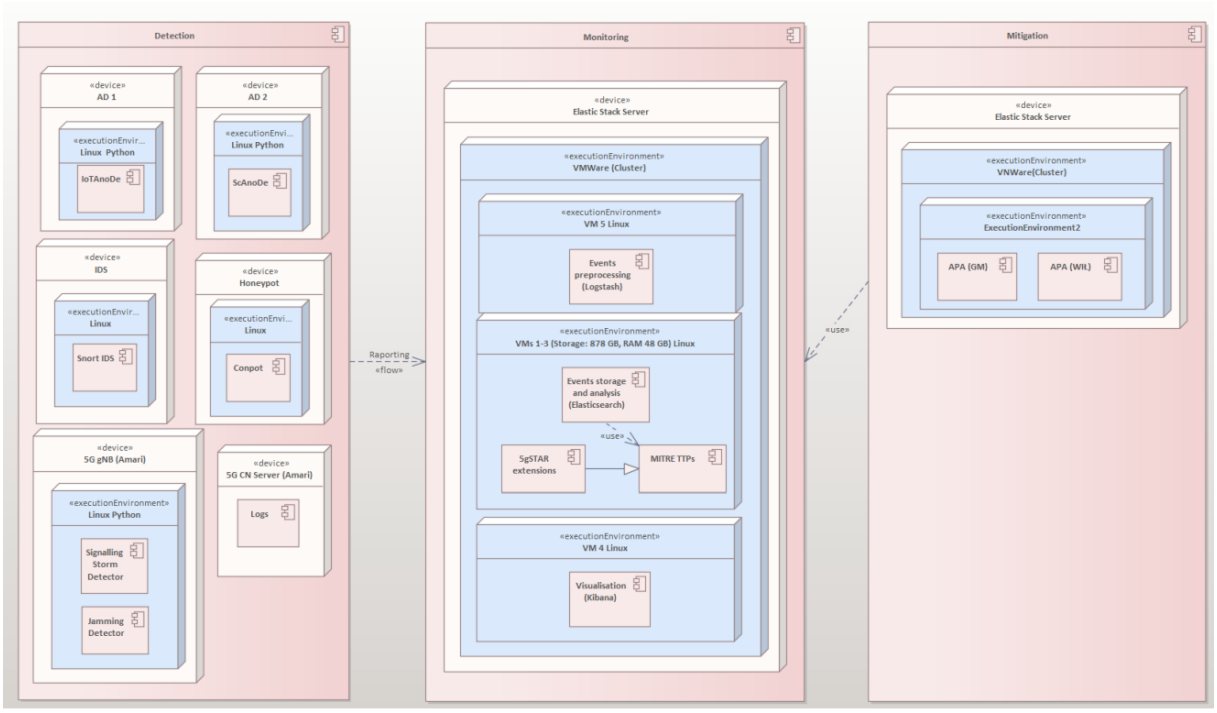
Na potrzeby walidacji System 5gSTAR został uruchomiony i przetestowany w środowisku składającym się z infrastruktury dostępowej 5G w wariancie SA (*stand alone*), modelu stacji elektroenergetycznej oraz sieci IIoT (*Industrial Internet of Things*). Szczegółowy opis układu testowego znajduje się w [3].

1.1 Ogólna architektura systemu 5GStar

Zgodnie z projektem technicznym systemu można w nim wyróżnić trzy grupy komponentów, które ze względu na swoją funkcjonalność tworzą następujące podsystemy:

- detekcji,
- monitorowania,
- mitygacji.

Architekturę systemu 5gSTAR przedstawiono na Rys. 1-1. Oprócz komponentów systemu 5gSTAR zaznaczono na nim również warstwę sprzętową oraz środowiska uruchomieniowe. Większość modułów systemu 5gSTAR działa w środowisku Linux instalowanym natywnie na sprzęcie komputerowym lub w postaci maszyn wirtualnych.



Rys. 1-1 Projekt Systemu 5gSTAR w formie diagramu UML wdrożenia

W ramach systemu 5gSTAR wyróżnić można:

- zestaw autorskich detektorów dla sieci przemysłowej SCADA (*Supervisory Control and Data Acquisition*), IIoT oraz sieci dostępowej 5G:
    - IoTAnoDe,
    - ScAnoDe,
    - Signalling Storm Detector,
    - Jamming Detector,
- uzupełniające detektory COTS (*Commercial Off the Shelf*) rozszerzone o autorskie reguły detekcji:
    - Snort IDS (Snort2 oraz Snort3),
    - system pułapkowy Conpot,
- system monitorowania uzupełniony o autorskie rozszerzenia instrukcji postępowania opracowane na bazie TTP (*Tactics, Techniques, Procedures*) modeli MITRE FiGHT i ATT&CK [4]:
    - APA (GM) – Aplikacja Przeciwdziałania Atakom opracowana przez firmę Grandmetric pełniąca funkcję centralnego systemu monitorowania;
    - APA(WIŁ) - Aplikacja Przeciwdziałania Atakom opracowana w Wojskowym Instytucie Łączności – PIB pełniąca funkcję lokalnego systemu monitorowania.

1.2 Zagrożenia identyfikowane przez system 5gSTAR

System 5gSTAR został zaprojektowany w ten sposób, aby umożliwiał wykrywanie różnorodnych symptomów ataku, które mogą być elementem wieloetapowego ataku cybernetycznego. Zastosowanie elementów COTS pozwala na monitorowanie ruchu i wykrywanie standardowych zagrożeń dla sieci teleinformatycznych, natomiast opracowane w ramach projektu detektory anomalii oraz autorskie reguły detekcji są nakierowane na zagrożenia związane z protokołami i technologiami specyficznymi dla aplikacji przemysłowych wykorzystujących infrastrukturę 5G.

W systemie 5gSTAR zaimplementowano trzy rodzaje detektorów:

- detektory wykorzystujące algorytmy SI (IoTAnoDe, ScAnoDe), które zostały wytrenowane w kierunku wykrywania anomalii w ruchu sieciowym;
- detektory wykorzystujące reguły decyzyjne (IDS Snort) ukierunkowane na specyficzne rodzaje ataków cybernetycznych;
- system pułapkowy dla SCADA (Conpot).

Dzięki takiemu podejściu system może reagować na zagrożenia cybernetyczne, które zostały zidentyfikowane w trakcie realizacji projektu jako istotne dla rozpatrywanego zastosowania, ale również powinien być w stanie zgłaszać symptomy innych ataków, np. takich których nie stosowano w odniesieniu do danej technologii lub całkowicie nowych.

Poniżej w tabeli przedstawiono zestawienie specyficznych ataków wykrywanych przez system 5gSTAR.

Tab. 1-1 Zestawienie specyficznych ataków rozpoznawanych przez system 5gSTAR

Cel ataku	**Działanie atakującego**
ATAK NA ELEMENTY SCADA Z SIECI WEWNĘTRZNEJ	• Rekonesans sieciowy • Atak MITM • Atak zalewowy typu odmowa usługi (*Denial of Service*) • Modyfikacja pakietów IEC-104 • Przerwanie komunikacji • Rozsynchronizowanie czasu

ATAKI NA KOMUNIKACJĘ SENSORA IIoT 5G	• Podsłuch ruchu MQTT • Atak słownikowy na uwierzytelnianie • Rozpoznanie możliwości i funkcjonalności brokera MQTT • Rozpoznanie subskrybowanych tematów przez rozpoznanych użytkowników • Rozpoznanie możliwości publikowania wiadomości • Atak typu DDOS na broker MQTT • Atak typu Slow DDOS na broker MQTT • Atak typu man-in-the-middle – fałszowanie zawartości wiadomości
ATAK NA SIEĆ RDZENIOWĄ 5G	• Usuwanie sesji pomiędzy 'UPF' a 'UE' • Odrzucanie żądań zestawienia sesji przez 'UPF' dla 'EU'
ATAK NA INTERFEJS RADIOWY 5G (5G NR)	• Atak typu zagłuszanie (*jamming*) • Atak typu odmowa usługi (*signalling storm*)

1.2.1 Wykrywanie symptomów ataku

Detektory wymienione w pkt. 1.1 posiadają zaimplementowane reguły decyzyjne ukierunkowane na wektory ataków związane z poszczególnymi technologiami wykorzystywanymi w układzie testowym 5GStar, czyli:

- sieć przemysłowa SCADA,
- sieci IIoT,
- sieci szkieletowa 5G,
- sieć dostępowa 5G (interfejs radiowy 5G, 5G NR).

Detektory bazujące na regułach decyzyjnych po wykryciu konkretnego ataku cybernetycznego zgłaszają ten fakt do systemu monitorowania. Detektory bazujące na algorytmach SI, jeżeli są w stanie zidentyfikować konkretny atak również zgłaszają ten fakt, w innym przypadku raportują wykrycie anomalii w ruchu sieciowym.

Reguły decyzyjne detektorów wraz z wektorem ataku oraz przyporządkowaniem do technik ataku zgodnie z taksonomia MITRE zostały zinwentaryzowane i przedstawione poniżej.

- **Id_reguły5Gstar 1** – T0842, network sniffing - SCADA, wykrywanie skanowania sieci np. za pomocą skanera nmap;
- **Id_reguły5Gstar 2** – T0830, Adversary-in-the-Middle - SCADA, Reguła ta sprawdza ilość prób zestawienia sesji ze stacji nadzorczej do koncentratora, tj. ilość połączeń z ustawioną flagą w protokole TCP typu 'SYN' w określonym przedziale czasowym - PROTOCOL-SCADA IEC 104 TCP SYN.

- **Id_reguły5Gstar 3** – T0814 Denial of Service - SCADA, wbudowana reguła dla tego typu ataku wbudowana, ‘tcp syn flood’. Reguła taka charakteryzuje się wykrywaniem dużej ilość połączeń w określonym przedziale czasowym (w przypadku poniższej reguły jest to 50 zdarzeń w czasie 2 sekund) z ustawioną flagą TCP typu ‘SYN’
- **Id_reguły5Gstar 4** – T0855 Unauthorized Command Message – protokół NTP, celem ewentualnego wykrycia ataku ‘MitM’ można wziąć pod uwagę niezbyt dokładnie przeprowadzony atak. W ataku takim niewyłączenie opcji ‘send_redirects’ w systemie atakującego (np. w systemie operacyjnym Kali Linux) powoduje wysyłanie komunikatów sieciowych ‘icmp’ typu 5 i kodzie 1 (‘Redirect for host’) odpowiednio do stacji nadzorczej ‘SCADA’ oraz do serwera NTP informacji o tym, że jest bardziej optymalna trasa, która można przesłać pakiet.
- **Id_reguły5Gstar 5** – T0855 Unauthorized Command Message - SCADA, Wykonanie ataku ‘MitM’ umożliwia wykonanie w następnym etapie dodatkowego ataku na przekazywane w protokole IEC-104 wartości dla poszczególnych adresów ‘IOA’. Celem wykrycia modyfikacji pakietu utworzono regułę weryfikującą poprawny zakres wartości dla adresu IOA 30001 w warstwie sieciowej. Reguła ma na celu odnotowanie w logach aplikacji ‘snort3’ o przekroczeniu zakresu wartości (241,000– 246,999) dla wskazanego adresu.
- **Id_reguły5Gstar 6** – T0814 Denial of Service, T0813 Denial of Control - SCADA, zrywanie sesji IEC-104. Wpierw resetowana jest sesja TCP/IP. Po resecie sesji TCP/IP następuje próba zestawienia połączenia IEC-104 w czasie, którego przesyłane są pakiety kontrolne (‘U-Frames’) protokołu IEC-104. W czasie ataku skrypt weryfikuje czy ta komunikacja wystąpiła i po jej zakończeniu, kiedy zaczyna się standardowe przesyłanie pakietów (‘I-Frames’) następuje ustawienie obu wartości ‘Tx’ oraz ‘Rx’ na zero. Tym samym powoduje to zakłócenie sesji protokołu IEC-104 co powoduje ponowne zestawienie kolejnej sesji IEC-104 – cykl ten jest powtarzany do momentu przerwania działania skryptu. Celem wykrycia tego typu ataku utworzono regułę, która weryfikuje ilość prób zestawienia sesji w jednostce czasu.
- **Id_reguły5Gstar 7** – T0842, network sniffing - IIoT, MQTT, wbudowana, ARP Spoof Inspector
- **Id_reguły5Gstar 8** – T1110.001 brute force – IIoT, atak słownikowy na broker MQTT. Polega on na wielokrotnym wysyłaniu pakietu MQTT zawierającego kolejne dane logujące. W przypadku powodzenia zostanie wysłany pakiet connect ACK z potwierdzeniem lub

flagą błędu. Pakiety te są przesyłane w datagramach TCP. Własna reguła dla protokołu MQTT wykrywająca nadmiarowy ruch pakietów connect ACK z flagą błędu.

- **Id_reguły5Gstar 9** – T1595 Active Scanning, T0846 Remote System Discovery - IoT, rozpoznania możliwości i funkcjonalności brokera MQTT np. poprzez odczyt tematów „$SYS/#".
- **Id_reguły5Gstar 10** – T1565 Data Manipulation, T0855 Unauthorized Command Message - IoT, MQTT, próby subskrypcji tematów ze znakami specjalnymi. własna reguła dla protokołu MQTT wykrywająca próby wysyłania pakietów subscribe zawierających żądanie dla tematów systemowych zawierających znaki specjalne.
- **Id_reguły5Gstar 11** – T1565 Data Manipulation, T0855 Unauthorized Command Message - IOT, MQTT, atakujący w zależności od konfiguracji serwera MQTT może zyskać możliwość publikowania wiadomości. Własna reguła dla protokołu MQTT wykrywająca próby publikowania wiadomości MQTT z nowego adresu IP.
- **Id_reguły5Gstar 12** – T0813 Denial of Control, T0814 Denial of Service - IoT, MQTT, detekcja ruchu nadmiarowego jako DDoS.
- **Id_reguły5Gstar 13** – T0813 Denial of Control, T0814 Denial of Service - IoT, MQTT, atak SlowDDoS. Wykrywanie wielokrotnych połączeń np. z jednego adresu IP z ustawionym długim czasem keep-alive.
- **Id_reguły5Gstar 14** – T0830 Adversary-in-the-Middle - IoT, MQTT, Wykrywanie przez IDS podmian adresów MAC techniką ARP Poisoning.
- **Id_reguły5Gstar 15** – SCADA, atak przy użyciu protokołu MODBUS, port 502 – zdarzenie traktowane jako atak z użyciem techniki T0836 – Modyfikacja parametrów przemysłowych systemów kontrolnych;
- **Id_reguły5Gstar 16** – SCADA, atak przy użyciu protokołu Bacnet, port 47808 – zdarzenie traktowane jako atak z użyciem techniki T0836 – Modyfikacja parametrów przemysłowych systemów kontrolnych;
- **Id_reguły5Gstar 17** – SCADA, atak przy użyciu protokołu http, port 80 – zdarzenie traktowane jako atak z użyciem techniki T0836 – Modyfikacja parametrów przemysłowych systemów kontrolnych;

- **Id_reguły5Gstar 18** – SCADA, Atak przy użyciu protokołu IEC 104, port 2404, ramka „I” – zdarzenie traktowane, jako atak przy użyciu techniki T0831 – Manipulacja parametrami kontrolnymi urządzeń przemysłowych oraz wydawanie poleceń do urządzeń wykonawczych innych niż ze stacji kontrolnej;
- **Id_reguły5Gstar 19** – SCADA, atak przy użyciu protokołu IEC 104, port 2404, ramka „U” – zdarzenie traktowane jako atak przy użyciu techniki T0827 – Utrata kontroli nad zarządzanymi urządzeniami przemysłowymi, atak na funkcje kontroli i utrzymania komunikacji pomiędzy urządzeniami;
- **Id_reguły5Gstar 20** – SCADA, atak przy użyciu protokołu IEC 104, port 2404, ramka „S” – zdarzenie traktowane jako atak przy użyciu techniki T0832 – Manipulacja informacjami raportowanymi z urządzeń wykonawczych do kontrolera, przekłamywanie raportowanych stanów urządzeń oraz procesów;
- **Id_reguły5Gstar 21** – SCADA, atak przy użyciu protokołu IEC 104 – w przypadku nie wykrycia poprawnej ramki protokołu IEC zdarzenie traktowane jest jako atak przy użyciu techniki T0846 – Rekonesans, próba rozpoznania aktywnych urządzeń kontrolnych systemów przemysłowych.
- **Id_reguły5Gstar 22** - T1464 Network Denial of Service – 5G, monitorowanie i raportowanie parametrów SNR i EPRE - ustawiono alarmy, których zadaniem jest informowanie o występowaniu wartości SNR i EPRE poniżej określonych poziomów. Alarm wyzwalany, gdy wartości parametrów wskazujące na pogorszenie się kanału utrzymują się przez określony czas (5 min).
- **Id_reguły5Gstar 23** - T0811 Data from Information Repositories, T0859 Valid Accounts – 5G, monitorowanie i raportowanie zdarzeń żądań dowiązania terminala UE i ich odrzucania – alarm wyzwalany w sytuacji, gdy ilość odrzuconych żądań w jednostce czasu (1 minuta) przekraczała określoną wartość (powyżej 2 żądania w emulowanym ataku poprzez rzeczywisty UE1). Podczas rzeczywistego ataku można spodziewać się większej ilości odrzucenia żądań. Dodatkowo ustawiono alarm, który monitoruje dwa parametry, tj. żądania i ich odrzucenia. Warunkiem uruchomienia alarmu jest wystąpienie tej samej ilości żądań i odrzuceń w jednostce czasu przekraczających określoną ilość (po dwa żądania i odrzucenia w tym samym czasie). Alarm ten wskazuje, iż występuje natłok żądań dowiązania do sieci i ich odrzucania, co może wskazywać na próbę potencjalnego ataku, np. rozpoznania identyfikatora IMSI.

- **Id_reguły5Gstar 24** - T0811 Data from Information Repositories, T0859 Valid Accounts – 5G, monitorowanie i raportowanie zdarzeń żądań uwierzytelniania terminala UE i ich odrzucania - alarmy ustawione w taki sposób, aby sygnalizować wystąpienie natłoku odrzuceń uwierzytelniania (powyżej 22) w jednostce czasu (jedna minuta) dla parametru liczby odrzuconych żądań uwierzytelniania (Authentication Reject) oraz jednakowa liczba wystąpień żądań i odrzuceń w danej jednostce czasu dla parametru liczby żądań uwierzytelniania (Authentication Request), co wskazywało na próby uwierzytelniania, które były odrzucane.
- **Id_reguły5Gstar 25** - T0811 Data from Information Repositories, T0859 Valid Accounts – 5G, monitorowanie i raportowanie zdarzeń żądań zestawienia sesji PDU i ich odrzucania - alarm wyzwalany, gdy przyrost liczby żądań oraz odrzuceń w jednostce czasu (1 minuta) przekroczy ustaloną liczbę.
- **Id_reguły5Gstar 26** – T0855 Unauthorized Command Message, T0830 Adversary-in-the-Middle, T0803 Block Command Message, T0831 Manipulation of Control – 5G, monitorowanie i raportowanie ataku na sesję PDU w protokole PFCP poprzez usuwanie.
- **Id_reguły5Gstar 27** – jamming – 5G NR.
- **Id_reguły5Gstar 28** – signalling storm – 5G NR.

1.2.2 Działania zaradcze

W systemie 5gSTAR przewidziano szereg działań zaradczych jakie mogą zostać podjęte po wykryciu symptomów ataku. Część z nich jest realizowana automatycznie (mitygacja ataków na interfejs radiowy 5GNR), część zaś wymaga reakcji użytkownika systemu np. poprzez uruchomienie skryptu automatyzującego kroki mitygacji lub w postaci instrukcji specyfikującej kolejne kroki, które należy wykonać.

Poszczególne działania zaradcze z przyporządkowaniem do technik mitygacji zgodnie z taksonomią MITRE zostały zinwentaryzowane i przedstawione poniżej.

- **Id_mitygacji5Gstar 1** - Szyfrowanie ruchu (M0808) - Zastosowana implementacja systemu IoT w sieci testowej umożliwia uruchomienie uwierzytelniania oraz szyfrowania danych za pomocą protokołów TLS/SSL. W tym celu operator lub skrypt musi wykonać czynności na

serwerze IoT (hoście Brokera MQTT). Skrypt ssl_mosquitto_M0808 znajdujący się na serwerze IoT w katalogu ~/mitygacja

- **Id_mitygacji5Gstar 2** - Statyczna konfiguracja sieci (M0814) – rekonfiguracja serwera IoT oraz maszyn klienckich. Skrypt realizujący odpowiednie kroki na hoście Brokera MQT static_net_M0814 w katalogu ~/mitygacja
- **Id_mitygacji5Gstar 3** - Przeciwdziałanie atakom słownikowym na uwierzytelnianie w serwerze IoT (M1027) - rekonfiguracja serwera IoT oraz jego ponowne uruchomienie z poziomu maszyny serwera. W celu automatyzacji tego procesu przygotowany został skrypt na maszynie serwera IoT o nazwie users_conf_M1027 znajdujący się w katalogu ~/mitygacja
- **Id_mitygacji5Gstar 4** - Przeciwdziałanie próbom rozpoznania możliwości i funkcjonalności serwera IoT (M1056, M0926) - rekonfiguracja serwera IoT oraz jego ponowne uruchomienie z poziomu hosta. skrypt na hoście serwera IoT o nazwie users_policies_M1056_M0926 znajdujący się w katalogu ~/mitygacja
- **Id_mitygacji5Gstar 5** - Przeciwdziałanie próbom rozpoznania subskrybowanych tematów przez rozpoznanych użytkowników (M1056, M0926) - W celu zabezpieczenia systemu IoT przed atakami rozpoznania tematów należy uruchomić skrypt na maszynie serwera IoT o nazwie users_policies_M1056_M0926 znajdujący się w katalogu ~/mitygacja
- **Id_mitygacji5Gstar 6** - dostęp do określonych zasobów serwera IoT tylko dla ściśle określonych urządzeń (M0807) - skrypt na maszynie serwera IoT o nazwie ip_filter_M0807 znajdujący się w katalogu ~/mitygacja
- **Id_mitygacji5Gstar 7** - Przeciwdziałanie atakom typu DDoS/Slow DDoS na IoT (M0815) - przeciwdziałanie z poziomu serwera, restart interfejsu oraz samej usługi. Skrypt o nazwie restart_M0815 znajdujący się w katalogu ~/mitygacja
- **Id_mitygacji5GStar 8** - Przeciwdziałanie nieautoryzowanemu dostępowi do sieci 5G (M0926) - metoda polega na blokowaniu nieznanych identyfikatorów IMEI terminali użytkowników. Operator w celu uruchomienia takiej blokady powinien dokonać konfiguracji bazy list identyfikatorów blokowanych, zaufanych oraz nieznanych. Konfigurację operator może przeprowadzić poprzez edycję pliku konfiguracyjnego lub uruchomić skrypt automatyzujący to zadanie. Skrypt o nazwie allowlist_M0926 znajdujący się w katalogu /mitygacja na maszynie Amarisoft;

- **Id_mitygacji5GStar 9** - Ochrona dostępu do maszyn z uruchomionymi modułami 5G (M0807) – w tym celu operator powinien wszelkimi sposobami zabezpieczyć fizyczny dostęp do zasobów maszyny poprzez nadanie uprawnień i ich weryfikację użytkownikom systemu operacyjnego maszyny (M0926), a także uruchomić skrypt ip_filter_5G_M0807 na maszynach z uruchomionymi modułami.
- **Id_mitygacji5GStar 10** - Ochrona komunikacji pomiędzy modułami sieci szkieletowej 5G (M0808) - realizuje się poprzez ukrycie przesyłanych danych pomiędzy współpracującymi modułami. Ukrycie polega na zaszyfrowaniu wiadomości, np. poprzez zestawienie szyfrowanego tunelu. W tym celu operator powinien uruchomić skrypt tun_5G_M0808 na maszynach współpracujących modułów
- **ID_mitygacji5GStar 11** - Ochrona poprzez statyczną konfigurację sieci (M0814) - Ochrona poprzez statyczną konfigurację ustawień sieci IP ma na celu zapobiegać próbom przekierowania ruchu sieciowego pomiędzy modułami sieci szkieletowej 5G. Ochrona polega na uruchomieniu skryptu ip_static_5G_M0814
- **ID_mitygacji5GStar 12** - M0937 Filter Network Traffic, IoT - Należy uaktualnić politykę firewall hosta, na którym został uruchomiony broker MQTT, tak aby blokował on połączenia od podejrzanego adresu IP przychodzące na TCP na port 1883. W zależności od tego, jaką informację zwrotną ma otrzymać atakujący zamiast polityki DROP może zostać zastosowana polityka REJECT.
- **ID_mitygacji5GStar 13** - M0807 Network Allowlists, IoT - Należy uaktualnić politykę firewall hosta, na którym został uruchomiony broker MQTT, tak aby blokował wszystkie połączenia za wyjątkiem listy dopuszczonych adresów IP.
- **ID_mitygacji5GStar 14** - M0810 Out-of-Band Communications Channel, IoT - należy skonfigurować broker tak, aby nasłuchiwał na dodatkowym porcie (dodatkowego listenera na nowym numerze portu na przykład 2000). W przypadku podejrzenia, że dotychczasowa komunikacja została skompromitowana i wysyłane są fałszywe dane należy uruchomić nową instancję publishera na tym samym hoście (np. raspberry pi), który będzie publikował te same informacje co skompromitowany.
- **ID_mitygacji5GStar 15** - M0811 Redundancy of Service, IoT - Uruchomienie nowej instancji brokera z nowym listenerem (na przykład na porcie 2000) a następnie przekierowanie ruchu z podejrzanego adresu IP na nowy port. W ten sposób nowy broker

będzie działał jako honeypot, natomiast subskrybenci będą mogli otrzymywać informacje bez przeszkód.

- **ID_mitygacji5GStar 16** - M0815 Watchdog Timers, IoT - Na hoście brokera uruchomiony jest publisher, który wysyła informacje „keep alive" – jeżeli nie zostaną wysłane 3 razy następuje reset portu /ponowne uruchomienie brokera.
- **ID_mitygacji5GStar 17** – M0814, SCADA, MiTM arp spoofing - celem uniemożliwienia przeprowadzenia ataku 'MiTM arp spoofing' zastosowano zabezpieczenie na przełączniku sieciowym drugiej warstwy. Mechanizm 'Arp Spoofing Prevention' wbudowany w przełącznik D-Link DGS-3100-24 umożliwia ręczne zdefiniowanie i przypisanie adresu IP oraz MAC adresu do fizycznego portu na przełączniku.
- **ID_mitygacji5GStar 18** – M0814, SCADA MiTM arp spoofing - dodatkowe zabezpieczenia na przełączniku sieciowym - testowego zastosowano dodatkowe zabezpieczenia na przełączniku sieciowym, tj.:
  - mechanizm 'port security',
  - protokół 'STP' – 'spanning tree protocol'
- **ID_mitygacji5GStar 19** - M0814, SCADA, MiTM arp spoofing, wykorzystanie listy kontroli dostępu 'ACL' na routerze. Użyta rozszerzona lista kontroli dostępu zezwala na komunikację sieciową z adresu 192.168.12.88 do adresu IP koncentratora 192.168.6.85 na porcie docelowy TCP/2404 i została zastosowana na interfejsie GigabitEthernet0/0 dla ruchu przychodzącego – w przypadku reguł 'ACL' domyślnie pozostała część ruchu jest blokowana.
- **ID_mitygacji5GStar 20** – 5GNR – działanie automatyczne.
- **ID_mitygacji5GStar 21** – 5GNR – działanie automatyczne.

1.3 System detekcji

W standardowym systemie teleinformatycznym zbudowanym zgodnie ze sztuką stosuje się szereg zabezpieczeń oraz rozwiązań sieciowych takich jak Firewalle, tzw. „strefy zdemilitaryzowane", systemy IDS/IPS (ang. *Intrusion Detection System /Intrusion Prevention System*), itp.

System detekcji 5gSTAR ma stanowić uzupełnienie tego typu rozwiązań koncentrując się na aplikacjach przemysłowych, stąd w jego skład wchodzą specjalizowane detektory działające

na kopii ruchu sieciowego (w trybie „*inline*”) do wykrywania symptomów ataku w sieciach przemysłowych SCADA i IIoT oraz sieci dostępowej 5G.

System detekcji składa się z następujących detektorów (autorskich oraz COTS):

- **Detektor anomalii w sieciach IIoT – IoTAnoDe**:
    - Środowisko uruchomieniowe Linux Ubuntu lub WSL (ang. *Windows Subsystem for Linux*);
    - Tryb pracy – kopia ruchu, wymaga podłączenia do portu przełącznika sieciowego skonfigurowanego jako *SPAN PORT*/*Port Mirroring*[1];
    - Zasada działania – algorytmy SI do wykrywania anomalii w ruchu sieciowym:
        - algorytm uczenia maszynowego OneClassSVM;
        - algorytm uczenia głębokiego Autoencoder;
    - język programowania Python 3;
- **Detektor regułowy dla sieci IIoT – IDS Snort2**:
    - Środowisko uruchomieniowe Linux Ubuntu;
    - Tryb pracy – kopia ruchu, wymaga podłączenia do portu przełącznika sieciowego skonfigurowanego jako *SPAN PORT*/*Port Mirroring;*
    - Zasada działania – analiza ruchu sieciowego dla protokołu MQTT na podstawie opracowanych reguł detekcji symptomów ataku;
- **Detektor anomalii w sieciach przemysłowych SCADA – ScAnoDe**:
    - Środowisko uruchomieniowe Linux Ubuntu lub WSL (ang. *Windows Subsystem for Linux*);
    - Tryb pracy – kopia ruchu, wymaga podłączenia do portu przełącznika sieciowego skonfigurowanego jako *SPAN PORT*/*Port Mirroring;*
    - Zasada działania – algorytmy SI do wykrywania anomalii w ruchu sieciowym:
        - algorytm uczenia maszynowego OneClassSVM;
        - algorytm uczenia głębokiego Autoencoder;
    - język programowania Python 3;
- **Detektor regułowy dla sieci przemysłowych SCADA – IDS Snort3**:
    - Środowisko uruchomieniowe Linux Ubuntu;

[1] Kopiowanie ruchu sieciowego na przełączniku z jednego lub kilku interfejsów na interfejsy przeznaczone do SPAN

- Tryb pracy – kopia ruchu, wymaga podłączenia do portu przełącznika sieciowego skonfigurowanego jako *SPAN PORT*/*Port Mirroring*
- Zasada działania – analiza ruchu sieciowego dla protokołów SCADA na podstawie opracowanych reguł detekcji symptomów ataku

- **System pułapkowy dla sieci przemysłowych SCADA – Conpot**:
  - Środowisko uruchomieniowe Linux;
  - Zasada działania – symulacja sieci IEC104;
  - Język programowania Python 3;
- **Detektor regułowy dla sieci szkieletowej 5G:**
  - Środowisko uruchomieniowe Linux Ubuntu;
  - Zasada działania – analiza logów zgłaszanych przez moduły sieci szkieletowej 5G;
- **Detektor zagłuszania dla RAN 5G - Jamming Detector**:
  - Środowisko uruchomieniowe Linuks Fedora;
  - Tryb pracy – on-line, automatyczna reakcja na wykryte zagrożenia;
  - Zasada działania – algorytm ML z wykorzystaniem metody uczenia nienadzorowanego analizujący rozkład dwuwymiarowy wartości CQI i RSVP zgłaszanych przez gNodeB;
  - język programowania Python 3;
- **Detektor ataku typu odmowa usługi poprzez przeciążenie sygnalizacji dla RAN 5G - Signalling Storm Detector**:
  - Środowisko uruchomieniowe Linuks Fedora;
  - Tryb pracy – on-line, automatyczna reakcja na wykryte zagrożenia;
  - Zasada działania - na podstawie Profilu KPI oraz aktualnie zaobserwowanej liczbie zgłoszeń do sieci 5G obliczane są dane wejściowe dla ważonej wersji algorytmu grupującego DBSCAN;
  - język programowania Python 3.

1.4 System monitorowania

System monitorowania 5gSTAR został zaprojektowany jako centralny system zbierania danych oraz system lokalny, który może być uruchamiany w różnych segmentach sieci zapewniając redundancję w przypadku utraty łączności z systemem centralnym.

1.4.1 Centralny system monitorowania

Zasadniczym elementem systemu monitorowania jest platforma Elastic Stack uruchomiona na dedykowanej platformie sprzętowej w postaci serwerów Fujitsu PRIMERGY RX2530 M5 (2 sztuki) oraz macierzy dyskowej NetApp EF300. Szczegółowy opis rozwiązania umieszczono w [2].

Stanowi ona podstawę centralnego systemu monitorowania zdarzeń natomiast interfejsem użytkownika jest Aplikacja Monitorowania, której zadaniem jest wizualizacja danych zebranych w bazie elasticsearch. Interfejs użytkownika wykorzystuje wchodzące w skład platformy Elastic Stack narzędzie Kibana.

1.4.2 Lokalny system monitorowania

W systemie 5gSTAR przewidziano również rozwiązanie redundantne w postaci lokalnego systemu monitoringu, który może być uruchomiony z wykorzystaniem znacznie mniejszych zasobów sprzętowych. Posiada on kopię danych z bazy danych elasticsearch z ostatnich 96 godzin pracy systemu.

Interfejsem użytkownika jest Aplikacja Przeciwdziałania Atakom (WIŁ) przedstawiona w pkt. 1.5.4. Interfejs aplikacji został wykonany w oparciu o framework django, bibliotekę bootstrap, chart.js oraz serwer www apache.

1.5 System mitygacji

System mitygacji podobnie jak system monitorowania został zaprojektowane jako rozwiązanie centralne oraz lokalne.

1.5.1 Centralny system mitygacji

W przypadku centralnego systemu mitygacji ze względu na ograniczenia Kibany, która z założenia jest narzędziem do wizualizacji i poza filtrowaniem danych nie umożliwia stworzenia pulpitu, w którym mogłyby być podejmowane akcje konieczne było stworzenie dodatkowego składnika, który dla danego zagrożenia wyświetli podsumowanie, rekomendowane mitygacje wskazywane przez bazę MITRE oraz umożliwi mitygację danego zagożenia w sposób predefiniowany dla konkretnego narzędzia oraz obszaru sieci w jakiej zostało ono wykryte. Jest to realizowane przez Aplikację Przeciwdziałania Atakom (GM). Z aplikacją tą połączona jest aplikacja do mitygacji zagrożeń w ten sposób, że jest on połączona ze stosem Elastic za pomocą REST API z elasticsearch w celu pobierania i zapisywania danych oraz możliwie jest swobodne przełączanie się pomiędzy widokami części wizualizacyjnej i mitygacyjnej.

Zarówno Aplikacja Monitorowania jak też APA(GM) jak też Aplikacja Przeciwdziałania Atakom (WIŁ) są aplikacjami uruchamianymi w przeglądarce. Interfejsy obu aplikacji przedstawiono odpowiednio w pkt. 2 oraz pkt. 3.

1.5.2 Lokalny system mitygacji

Filozofia działania lokalnego systemu mitygacji jest taka sama jak w przypadku centralnego systemu mitygacji, przy czym ze względu na wybór innych technologii programistycznych nie ma tutaj ograniczeń jak wprowadzane przez Kibanę. Stąd też Aplikacja Przeciwdziałania Atakom (WIŁ) integruje w sobie wszystkie działania związane z monitorowaniem i wizualizacją procesów związanych z cyberbezpieczeństwem. Głównym celem jest uproszczenie wszystkich pozyskanych informacji z poszczególnych detektorów oraz ich usystematyzowanie w taki sposób, żeby zapewnić operatorowi przejrzysty i jednoznaczny przegląd zdarzeń z jednoczesną możliwością uzyskania dodatkowych szczegółów w kwestii zastosowanej techniki ataku oraz możliwości jej mitygacji. Aplikacja Przeciwdziałania Atakom (WIŁ) została przedstawiona w pkt. 1.5.4.

1.5.3 Mapowanie metod mitygacji

W ramach projektu 5gSTAR zidentyfikowano szereg ataków cybernetycznych, których symptomy są raportowane przez system detekcji do systemu monitorowania, ten zaś poprzez

aplikacje APA pozwala na wyświetlenie odpowiednich działań zaradczych. Zarówno techniki ataków cybernetycznych jak i metody ich mitygacji odniesiono do MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*), czyli zbioru taktyk, technik i metod używanych przez atakujących w celu naruszenia bezpieczeństwa systemów informatycznych. Poniżej przedstawiono mapowanie jakie zostało zaimplementowane w aplikacjach APA.

Tab. 1-2 Zestawienie metod wykrywania symptomów ataków cybernetycznych oraz adekwatnych dla danego zagrożenia odpowiedzi opracowanych w projekcie 5GStar

Reguła 5GStar wykrywająca symptom ataku/ Kod MITRE/Cel	**Metoda mitygacji 5 GSTAR zaimplementowana w układzie testowym/ Kod MITRE**	**Uwagi**
Id_reguły5Gstar 1/ T0842/ SCADA	**Id_mitygacji5Gstar 19/** M0814 Static Network Configuration	
Id_reguły5Gstar 2/ T0830/ SCADA	**Id_mitygacji5Gstar 17/** M0814 Static Network Configuration **Id_mitygacji5Gstar 18/** M0814 Static Network Configuration	
Id_reguły5Gstar 3/ T0814/ SCADA	**Id_mitygacji5Gstar 17/** M0814 Static Network Configuration **Id_mitygacji5Gstar 18/** M0814 Static Network Configuration	
Id_reguły5Gstar 4/ T0855/ SCADA	**Id_mitygacji5Gstar 17/** M0814 Static Network Configuration **Id_mitygacji5Gstar 18/** M0814 Static Network Configuration	
Id_reguły5Gstar 5/ T0855/ SCADA	**Id_mitygacji5Gstar 17/** M0814 Static Network Configuration **Id_mitygacji5Gstar 18/** M0814 Static Network Configuration	
Id_reguły5Gstar 6/ T0813/ SCADA	**Id_mitygacji5Gstar 17/** M0814 Static Network Configuration **Id_mitygacji5Gstar 18/** M0814 Static Network Configuration	
Id_reguły5Gstar 7/ T0842/ IoT	**Id_mitygacji5Gstar 1**/M0808 Encrypt Network Traffic M0930 Network Segmentation **Id_mitygacji5Gstar 5/**M0926 Privileged Account Management **Id_mitygacji5Gstar 2/**M0814 Static Network Configuration	
Id_reguły5Gstar 8/ T1110.001/ IoT	**Id_mitygacji5Gstar 3/**M1027 Password Policies	
Id_reguły5Gstar 9/ T1595, T0846/ IoT	**Id_mitygacji5Gstar 2/**M0814 Static Network Configuration **Id_mitygacji5Gstar 4/M1056**	
Id_reguły5Gstar 10/ T1565, T0855/ IoT	**Id_mitygacji5Gstar 6/**M0807 Network Allowlist **ID_mitygacji5Gstar 13/**M0807 Network Allowlist **ID_mitygacji5Gstar 12/**M0937 Filter Network Traffic	

Id_reguły5Gstar 11/ T1565, T0855/ IoT	**Id_mitygacji5Gstar 6/** M0807 Network Allowlist **ID_mitygacji5Gstar 13/**M0807 Network Allowlist **ID_mitygacji5Gstar 12/**M0937 Filter Network Traffic	
Id_reguły5Gstar 12/ T0813, T0814/ IoT	**ID_mitygacji5Gstar 14/**M0810 Out-of-Band Communications Channel **ID_mitygacji5Gstar 15/**M0811 Redundancy of Service **Id_mitygacji5Gstar 7/** M0815 – Watchdog Timers **ID_mitygacji5Gstar 16/** M0815 – Watchdog Timers	
Id_reguły5Gstar 13/ T0813, T0814/ IoT	**ID_mitygacji5Gstar 14/**M0810 Out-of-Band Communications Channel **ID_mitygacji5Gstar 15/**M0811 Redundancy of Service **Id_mitygacji5Gstar 7/** M0815 – Watchdog Timers **ID_mitygacji5Gstar 16/** M0815 – Watchdog Timers	
Id_reguły5Gstar 14/ T0830/ IoT	**ID_mitygacji5Gstar 14/**M0810 Out-of-Band Communications Channel **Id_mitygacj5Gstar 2/**M0814 Static Network Configuration	
Id_reguły5Gstar 15/T0836/ SCADA	--	Honeypot
Id_reguły5Gstar 16/T0836/ SCADA	--	Honeypot
Id_reguły5Gstar 17/T0836/ SCADA	--	Honeypot
Id_reguły5Gstar 18/T0831/ SCADA	--	Honeypot
Id_reguły5Gstar 19/T0827/ SCADA	--	Honeypot
Id_reguły5Gstar 20/T0832/ SCADA	--	Honeypot
Id_reguły5Gstar 21/T0846/ SCADA	--	Honeypot
Id_reguły5Gstar 22/ T1464/ 5G	--	
Id_reguły5Gstar 23/ T0811, T0859/ 5G	**Id_mitygacji5GStar 8/** M0926 - Privileged Account Management,	
Id_reguły5Gstar 24/ T0811, T0859/ 5G	**Id_mitygacji5GStar 8/** M0926 - Privileged Account Management,	
Id_reguły5Gstar 25/ T0811, T0859/ 5G	**Id_mitygacji5GStar 8/** M0926 - Privileged Account Management	
Id_reguły5Gstar 26/ T0855, T0830, T0803/ 5G	**Id_mitygacji5GStar 9/** M0807 - Network Allowlists) **Id_mitygacji5GStar 10/** M0808 - Encrypt Network Traffic **Id_mitygacji5GStar 8/** M0926 - Privileged Account Management	

1.5.4 Koszty mitygacji

Kategorie w jakich można sklasyfikować koszty poszczególnych typów mitygacji są różnorakie i obejmują wiele aspektów zarówno technicznych, jak też finansowych, czy też wizerunkowych. Zagadnienie to znajduje odzwierciedlenie w literaturze przedmiotu, np. [13], czy też w dostępnych w Internecie webinariach. W ogólności koszty te mogą obejmować takie kategorie jak:

1. Personel i zasoby ludzkie: Koszty związane z zatrudnianiem, szkoleniem i utrzymaniem personelu odpowiedzialnego za reakcję na incydenty cybernetyczne, w tym specjalistów ds. bezpieczeństwa IT, analityków bezpieczeństwa, specjalistów ds. wykrywania zagrożeń itp.;
2. Narzędzia i technologie: Koszty związane z zakupem, wdrożeniem i utrzymaniem narzędzi i technologii wspierających reakcję na incydenty, takich jak systemy detekcji zagrożeń, oprogramowanie do zarządzania incydentami, narzędzia do analizy logów itp.;
3. Usługi zewnętrzne: Koszty związane z wynajmem usług zewnętrznych, takich jak usługi konsultingowe ds. bezpieczeństwa IT, zewnętrzne centra operacji bezpieczeństwa (SOC), usługi reagowania na incydenty itp.;
4. Przywracanie systemu: Koszty związane z przywracaniem funkcjonalności systemu po ataku, takie jak naprawa infrastruktury, przywracanie danych, odtwarzanie usług itp.;
5. Komunikacja i zarządzanie incydentami: Koszty związane z komunikacją wewnętrzną i zewnętrzną w związku z incydentem, zarządzaniem incydentami, koordynacją działań reakcji na incydent itp.;
6. Prawne i regulacyjne: Koszty związane z zachowaniem zgodności z przepisami prawnymi i regulacyjnymi w związku z incydentem, takimi jak kary finansowe, koszty audytów, koszty obrony prawnej itp.;
7. Wyszukiwanie przyczyn i analiza: Koszty związane z przeprowadzeniem dochodzenia w celu zidentyfikowania przyczyn incydentu, analizą ataku, identyfikacją działań naprawczych itp.
8. Reputacja i wizerunek firmy: Koszty związane z odbudowaniem zaufania klientów, partnerów biznesowych i opinii publicznej po incydencie, takie jak kampanie marketingowe, działania PR, rekompensaty dla klientów itp.;

9. Czas i produktywność: Koszty związane z utratą czasu i produktywności pracowników w wyniku przerw w działaniu systemów lub usług spowodowanych incydentem;
10. Szkody finansowe: Koszty związane z bezpośrednimi szkodami finansowymi wynikającymi z ataku, takimi jak utrata przychodów, straty z tytułu kradzieży danych, koszty rekompensat dla klientów itp.

Ponieważ w przypadku projektu 5GStar metody wykrywania symptomów ataku działają automatycznie, a więc po uruchomieniu nie generują kosztów, zatem w tym zakresie istotne są koszty działań (mitygacji) stanowiące odpowiedzi na dane zagrożenie cybernetyczne.

Zgodnie z założeniami centralny system zbierania danych oparty o stos ELK otrzymuje ostrzeżenia z poszczególnych detektorów o wykryciu symptomów ataku (metody kategorii Wykrywanie). W odpowiedzi na zidentyfikowane zagrożenia z poziomu ELK oraz APA dostępna jest lista adekwatnych metod mitygacji (kategorii Odpowiedź). Mitygacjom tym przypisano pewne koszty mogące stanowić kryteria ich wyboru.

Biorąc pod uwagę specyfikę zaproponowanych metod mitygacji ich koszty mogą być określone biorąc pod uwagę takie kategorie jak Personel i zasoby ludzkie, Narzędzia i technologie oraz Usługi zewnętrzne. Uszczegółowiając, przyjęto następujące kategorie kosztów oraz ich poziomy:

1. czas potrzebny na wdrożenie działań zabezpieczających:
    - krótki < 1h, waga 1;
    - średni 1h < 8h, waga 3;
    - długi > 8h, waga 5;

2. kompetencje techniczne personelu:
    - niskie – wystarczy uruchomić gotowy skrypt, waga 1
    - średnie – wymaga wykonania większej ilości działań/ zmian konfiguracji za pomocą komend wydawanych w terminalu danego hosta, waga 3;
    - specjalistyczne, waga 5;

3. koszt finansowy związany z zasobami ludzkimi:
    - niski – w ramach obowiązków pracownika SOC, waga 1;

- średni – konieczne powiadomienie specjalistów zatrudnionych w ramach firmy, waga 3;
- wysoki – konieczne zatrudnienie podmiotu zewnętrznego, waga 5;

4. koszt finansowy związany z infrastrukturą teleinformatyczną:
   - niski – potrzebne są jedynie działania np. konfiguracyjne w obrębie posiadanego wyposażenia, waga 1;
   - wysoki – konieczny jest zakup/wymiana urządzeń i/lub licencji, waga 5;

5. ograniczenie dostępności usługi:
- niskie – ograniczenie dostępności dla pojedynczych hostów, waga 1;
- średnie – zezwolenie na dostęp dla określonych hostów, waga 3;
- wysokie – całkowita blokada usługi, waga 5.

Poniżej, w tabeli przedstawiono szacowane koszty poszczególnych metod.

Tab. 1-3 Specyfikacja kosztów metod mitygacji opracowanych w ramach projektu 5GStar

Metoda mitygacji 5 GSTAR zaimplementowana w układzie testowym	**Specyfikacja Kosztów**				
	czas potrzebny na wdrożenie działań zabezpieczających	kompetencje techniczne personelu	koszt finansowy związany z zasobami ludzkimi	Koszt finansowy związany z infrastrukturą teleinformatyczną	ograniczenie dostępności usługi
Id_mitygacj5Gstar 1	1	2	1	1	2
Id_mitygacj5Gstar 2	1	1	1	1	2
Id_mitygacj5Gstar 3	1	1	1	1	2
Id_mitygacj5Gstar 4	1	1	1	1	2
Id_mitygacj5Gstar 5	1	1	1	1	2
Id_mitygacj5Gstar 6	1	1	1	1	2
Id_mitygacj5Gstar 7	1	1	1	1	0
Id_mitygacj5Gstar 8	1	2	1	1	2
Id_mitygacj5Gstar 9	2	2	2	1	2
Id_mitygacj5Gstar 10	1	2	2	1	0
Id_mitygacj5Gstar 11	1	2	2	1	0
Id_mitygacj5Gstar 12	1	2	2	1	1
Id_mitygacj5Gstar 13	1	2	2	1	2
Id_mitygacj5Gstar 14	1	2	2	2	2
Id_mitygacj5Gstar 15	1	2	2	2	2
Id_mitygacj5Gstar 16	1	2	2	1	0
Id_mitygacj5Gstar 17	1	2	2	1	2
Id_mitygacj5Gstar 18	1	2	2	1	2
Id_mitygacj5Gstar 19	1	2	2	1	2

2 Aplikacja Przeciwdziałania Atakom (WIŁ)

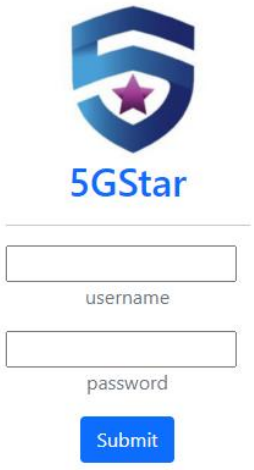
Aplikacja Przeciwdziałania Atakom (WIŁ). ma za zadanie rozpoznanie, alarmowanie i informowanie operatora aplikacji o przeprowadzonych atakach lub ich próbach na Sieć 5G jak również o proponowanych sposobach ich mitygacji. Aplikacja ta wykorzystuje lokalną kopię danych z centralnego systemu monitoringu z ostatnich 96 godzin. Poniżej przedstawiono niezbędne informacje na temat obsługi i zarządzania aplikacją APA z poziomu interfejsu www. Opisana została funkcjonalność interfejsu użytkownika oraz panelu administracyjnego.

Panel administracyjny zapewnia zarządzanie użytkownikami aplikacji oraz obiektami w bazie danych jak również możliwość tworzenia własnych technik ataku oraz powiązanych mitygacji.

Interfejs użytkownika umożliwia przegląd zdarzeń, zapoznanie się z opisem ataku oraz podjęcie odpowiednich działań w zależności od powiązanych z danym atakiem mitygacji.

2.1 Logowanie do aplikacji APA

Logowanie użytkownika do interfejsu aplikacji odbywa się za pomocą wygenerowanego wcześniej przez administratora loginu i hasła. Celem zalogowania należy wpisać w przeglądarce internetowej adres, pod którym dostępna jest aplikacja, tj. https://192.168.6.10/. Połączenie odbywa się za pomocą zabezpieczonego protokołu HTTPS (ang. *Hypertext Transfer Protocol Secure*).



Rys. 2-1 Okno logowanie APA(WIŁ)

2.2 Interfejs główny aplikacji

Interfejs aplikacji został wykonany w oparciu o framework django [6], bibliotekę bootstrap [7], chart.js [8] oraz serwer www apache [9]. Instalacja i konfiguracja aplikacji została opisana w [10]. Aplikacja nie zapewnia automatycznego odświeżania strony.

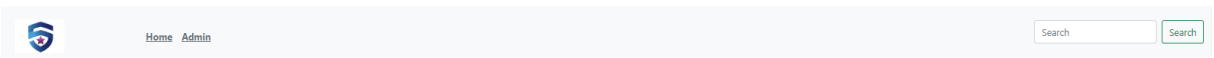
Po poprawnym zalogowaniu użytkownika do aplikacji wyświetlony zostanie w przeglądarce interfejs główny aplikacji (Rys. 2-2).

Rys. 2-2 Interfejs główny aplikacji

W interfejsie głównym aplikacji przedstawione są podstawowe informacje dotyczące wykrytych przez poszczególne detektory zagrożeń z ostatnich 4 dni (96 godzin).

2.2.1 Panel nawigacyjny

Panel nawigacyjny (Rys. 2-3) zawiera odnośniki do strony głównej aplikacji, odnośnik do strony administracyjnej aplikacji oraz pole do wyszukiwania.



Rys. 2-3 Panel nawigacyjny

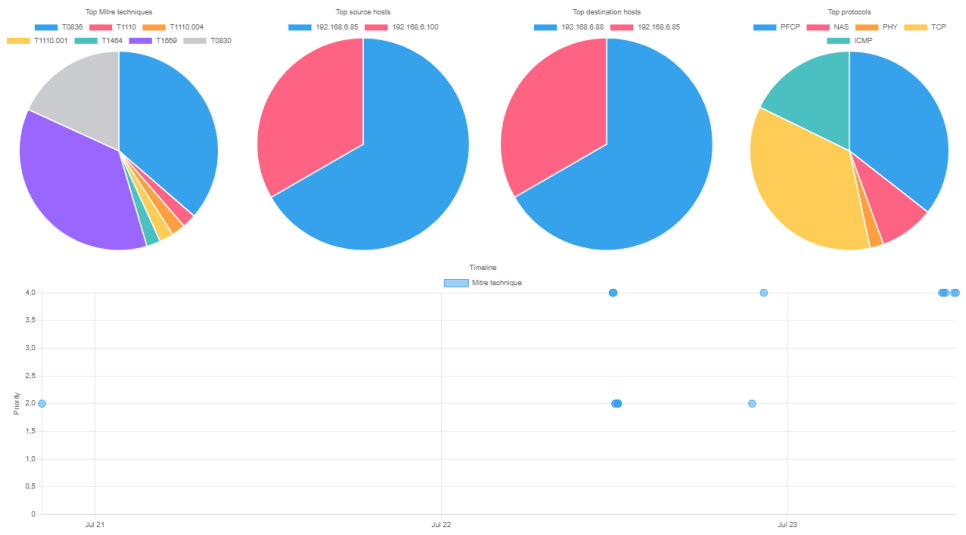
Pole wyszukiwania Search umożliwia wyszukiwanie zdarzeń według następujących wyrażeń:

- nazwa detektora raportującego zdarzenie;
- nazwa techniki ataku Mitre przypisanej dla danego zdarzenia;
- źródłowy/docelowy adres IP, dla którego zostało wykryte zagrożenie;
- protokół użyty w ataku;
- docelowy numer portu;
- priorytet zdarzenia przypisany do danego zdarzenia przez detektor.

Strony administracyjna aplikacji umożliwia zarządzanie użytkownikami, dostępem do edycji dodatkowych danych (np. dodawanie własnych technik i mitygacji itp.) oraz widoku rekordów z bazy danych.

2.2.2 Wizualizacja

Celem wizualizacji wykrytych zagrożeń w interfejsie graficznym aplikacji zastosowano cztery wykresy kołowe oraz jeden wykres bąbelkowy (Rys. 2-4).



Rys. 2-4 Wygenerowane wykresy dla poszczególnych zdarzeń

Wykresy kołowe przedstawiają odpowiednio:

- ilość wykrytych technik ataków w danej jednostce czasu;
- adresy IP, z których najczęściej przeprowadzone zostały ataki;
- adresy IP, które były najczęściej atakowane;

- najczęściej używane protokoły podczas przeprowadzonych ataków.

Wykres bąbelkowy przedstawia przebieg danych technik ataku na linii czasu. Ten typ wykresu umożliwia zaobserwowanie przebiegu poszczególnych ataków w funkcji czasu umożliwiając tym samym określenie ich ważności (priorytetów nadanych poszczególnym atakom przez dany detektor) oraz przebiegu.

2.2.3 Przegląd zdarzeń

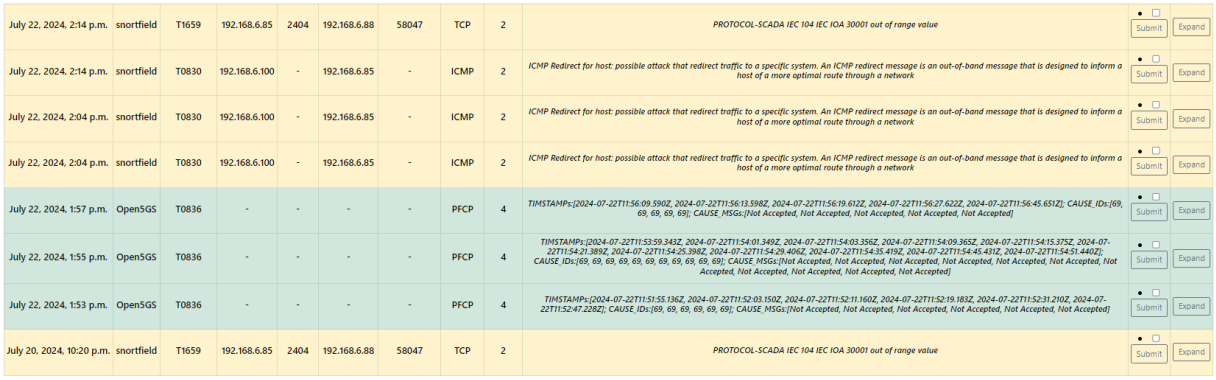
Ostatnim elementem głównego interfejsu aplikacji jest zestawienie poszczególnych zdarzeń zebranych w formie tabelarycznej. Poszczególne rzędy w tabeli są wykonane są w formie rozwijalnych pól dodatkowych. Pola te zawierają szczegółowe informacje na temat wykrytej techniki ataku jak również sposoby ich mitygacji wraz z opisem. Zależnie od priorytetu danej techniki zastosowano w wierszach tabeli odmienne kolory celem wyróżnienia ataków o większym poziomie zagrożenia.

W podstawowym widoku (Rys. 2-5) przedstawione są najważniejsze cechy danej techniki ataku:

- data i godzina zdarzenia;
- nazwa detektora generującego zdarzenie;
- wykryta technika ataku;
- adres IP i port źródłowy skąd wykonany został atak;
- adres IP o port docelowy atakowanej stacji;
- zastosowany w ataku protokół;
- priorytet danego ataku określony przez detektor;
- opis danego ataku określony przez detektor.

Na rysunku widoczne są również przyciski Submit oraz Expand. Ich rola jest następująca:

- Submit umożliwia oznaczenie danej techniki jako incydent rozwiązany/zweryfikowany;
- Expand umożliwia rozwinięcie dodatkowych szczegółów ataku oraz mitygacji.



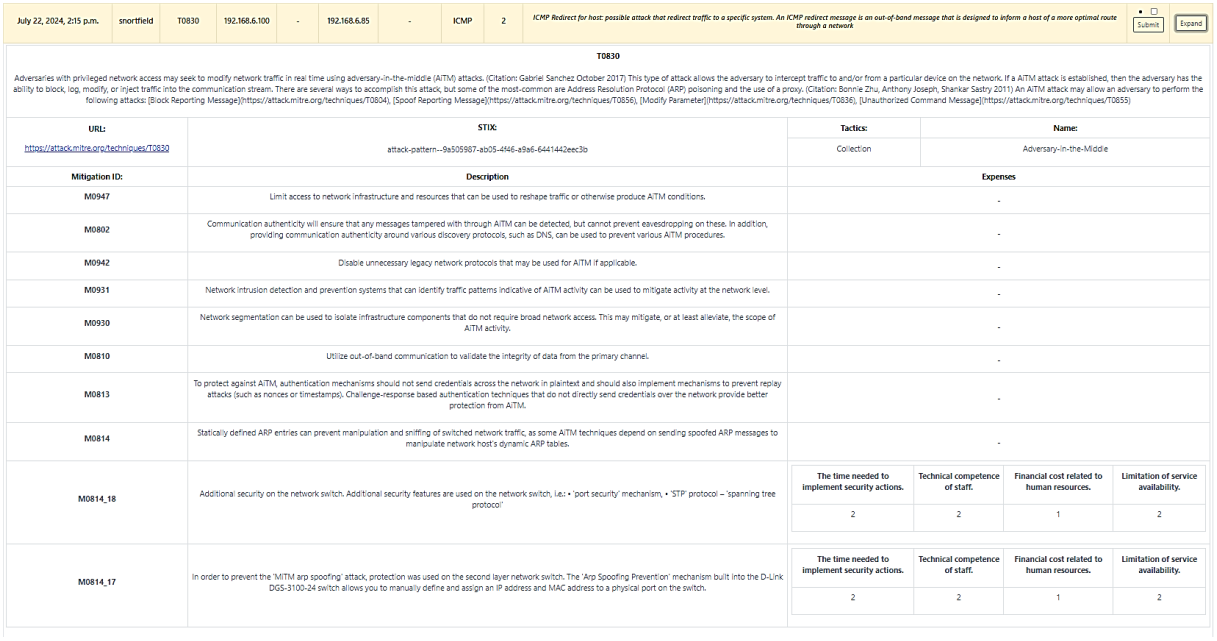
July 22, 2024, 2:14 p.m.	snortfield	T1659	192.168.6.85	2404	192.168.6.88	58047	TCP	2	PROTOCOL-SCADA IEC 104 IEC IOA 30001 out of range value	Submit Expand
July 22, 2024, 2:14 p.m.	snortfield	T0830	192.168.6.100	-	192.168.6.85	-	ICMP	2	ICMP Redirect for host: possible attack that redirect traffic to a specific system. An ICMP redirect message is an out-of-band message that is designed to inform a host of a more optimal route through a network	Submit Expand
July 22, 2024, 2:04 p.m.	snortfield	T0830	192.168.6.100	-	192.168.6.85	-	ICMP	2	ICMP Redirect for host: possible attack that redirect traffic to a specific system. An ICMP redirect message is an out-of-band message that is designed to inform a host of a more optimal route through a network	Submit Expand
July 22, 2024, 2:04 p.m.	snortfield	T0830	192.168.6.100	-	192.168.6.85	-	ICMP	2	ICMP Redirect for host: possible attack that redirect traffic to a specific system. An ICMP redirect message is an out-of-band message that is designed to inform a host of a more optimal route through a network	Submit Expand
July 22, 2024, 1:57 p.m.	Open5GS	T0836	-	-	-	-	PFCP	4	TIMSTAMPs:[2024-07-22T11:56:09.590Z, 2024-07-22T11:56:13.598Z, 2024-07-22T11:56:19.612Z, 2024-07-22T11:56:27.622Z, 2024-07-22T11:56:45.651Z]; CAUSE_IDs:[69, 69, 69, 69, 69]; CAUSE_MSGs:[Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted]	Submit Expand
July 22, 2024, 1:55 p.m.	Open5GS	T0836	-	-	-	-	PFCP	4	TIMSTAMPs:[2024-07-22T11:53:59.343Z, 2024-07-22T11:54:01.349Z, 2024-07-22T11:54:03.356Z, 2024-07-22T11:54:09.365Z, 2024-07-22T11:54:15.375Z, 2024-07-22T11:54:21.389Z, 2024-07-22T11:54:25.398Z, 2024-07-22T11:54:29.406Z, 2024-07-22T11:54:35.419Z, 2024-07-22T11:54:45.431Z, 2024-07-22T11:54:51.440Z]; CAUSE_IDs:[69, 69, 69, 69, 69, 69, 69, 69, 69, 69]; CAUSE_MSGs:[Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted]	Submit Expand
July 22, 2024, 1:53 p.m.	Open5GS	T0836	-	-	-	-	PFCP	4	TIMSTAMPs:[2024-07-22T11:51:55.136Z, 2024-07-22T11:52:03.150Z, 2024-07-22T11:52:11.160Z, 2024-07-22T11:52:19.183Z, 2024-07-22T11:52:31.210Z, 2024-07-22T11:52:47.228Z]; CAUSE_IDs:[69, 69, 69, 69, 69, 69]; CAUSE_MSGs:[Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted, Not Accepted]	Submit Expand
July 20, 2024, 10:20 p.m.	snortfield	T1659	192.168.6.85	2404	192.168.6.88	58047	TCP	2	PROTOCOL-SCADA IEC 104 IEC IOA 30001 out of range value	Submit Expand

Rys. 2-5 Podstawowy widok zebranych zdarzeń z detektorów

Rozszerzony widok (Rys. 2-6) aktywowany przyciskiem Expand dla danego zdarzenia zawiera dodatkowe informacje na temat wybranego zdarzenia oraz sposobu jego mitygacji. W przypadku, gdy dla danej techniki ataku oprócz standardowych opcji mitygacji Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) [11] przypisane zostały dedykowane mitygacje 5gSTAR powiązane z atakami przeprowadzonymi w środowisku testowym wyświetlone zostaną dodatkowe koszty (patrz pkt. 1.5.4).

W rozszerzonym widoku przedstawione są następujące informacje dla danego ataku:

- dokładny opis techniki ataku zgodnie ze zbiorem wiedzy Mitre;
- odnośnik url do strony www Mitre opisującej wskazaną technikę ataku;
- reprezentacja techniki ataku w postaci strukturalnej STIX (ang. *Structured Threat Information eXpression*) [12];
- zastosowaną nazwę ataku oraz taktykę ataku;
- lista możliwych mitygacji wraz z ich opisem.



July 22, 2024, 2:15 p.m.	snortfield	T0830	192.168.6.100	-	192.168.6.85	-	ICMP	2	*ICMP Redirect for host: possible attack that redirect traffic to a specific system. An ICMP redirect message is an out-of-band message that is designed to inform a host of a more optimal route through a network*	Submit	Expand

T0830

Adversaries with privileged network access may seek to modify network traffic in real time using adversary-in-the-middle (AITM) attacks. (Citation: Gabriel Sanchez October 2017) This type of attack allows the adversary to intercept traffic to and/or from a particular device on the network. If a AITM attack is established, then the adversary has the ability to block, log, modify, or inject traffic into the communication stream. There are several ways to accomplish this attack, but some of the most-common are Address Resolution Protocol (ARP) poisoning and the use of a proxy. (Citation: Bonnie Zhu, Anthony Joseph, Shankar Sastry 2011) An AITM attack may allow an adversary to perform the following attacks: [Block Reporting Message](https://attack.mitre.org/techniques/T0804), [Spoof Reporting Message](https://attack.mitre.org/techniques/T0856), [Modify Parameter](https://attack.mitre.org/techniques/T0836), [Unauthorized Command Message](https://attack.mitre.org/techniques/T0855)

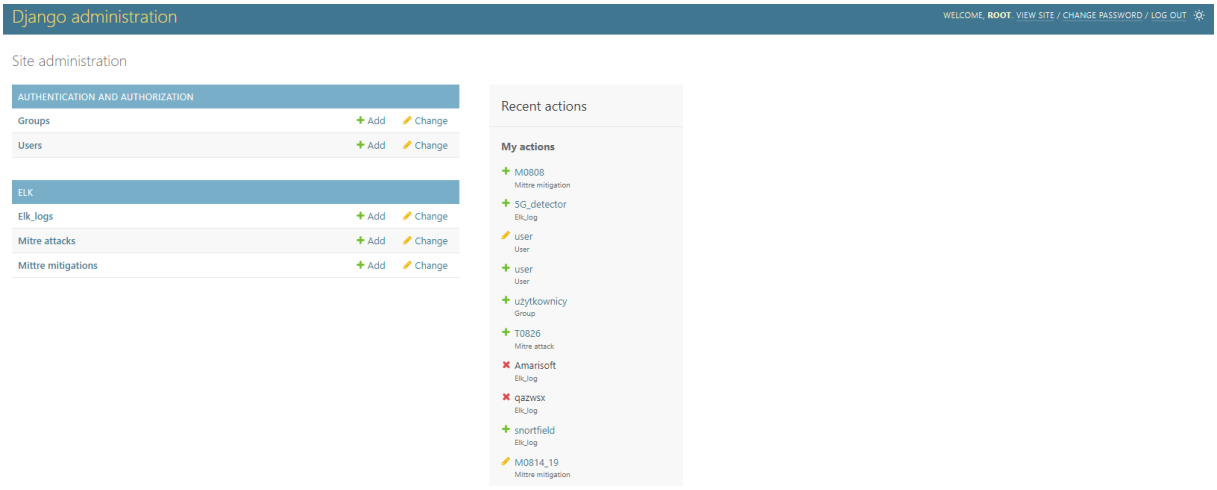
URL:	STIX:	Tactics:	Name:
https://attack.mitre.org/techniques/T0830	attack-pattern--9a505987-ab05-4f46-a9a6-6441442eec3b	Collection	Adversary-in-the-Middle

Mitigation ID:	Description	Expenses
M0947	Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AITM conditions.	-
M0802	Communication authenticity will ensure that any messages tampered with through AITM can be detected, but cannot prevent eavesdropping on these. In addition, providing communication authenticity around various discovery protocols, such as DNS, can be used to prevent various AITM procedures.	-
M0942	Disable unnecessary legacy network protocols that may be used for AITM if applicable.	-
M0931	Network intrusion detection and prevention systems that can identify traffic patterns indicative of AITM activity can be used to mitigate activity at the network level.	-
M0930	Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AITM activity.	-
M0810	Utilize out-of-band communication to validate the integrity of data from the primary channel.	-
M0813	To protect against AITM, authentication mechanisms should not send credentials across the network in plaintext and should also implement mechanisms to prevent replay attacks (such as nonces or timestamps). Challenge-response based authentication techniques that do not directly send credentials over the network provide better protection from AITM.	-
M0814	Statically defined ARP entries can prevent manipulation and sniffing of switched network traffic, as some AITM techniques depend on sending spoofed ARP messages to manipulate network host's dynamic ARP tables.	-
M0814_18	Additional security on the network switch. Additional security features are used on the network switch, i.e.: • 'port security' mechanism, • 'STP' protocol – 'spanning tree protocol'	The time needed to implement security actions.: 2 / Technical competence of staff.: 2 / Financial cost related to human resources.: 1 / Limitation of service availability.: 2
M0814_17	In order to prevent the 'MITM arp spoofing' attack, protection was used on the second layer network switch. The 'Arp Spoofing Prevention' mechanism built into the D-Link DGS-3100-24 switch allows you to manually define and assign an IP address and MAC address to a physical port on the switch.	The time needed to implement security actions.: 2 / Technical competence of staff.: 2 / Financial cost related to human resources.: 1 / Limitation of service availability.: 2

Rys. 2-6 Rozszerzony widok dla danego zdarzenia

2.3 Strona administracyjna

Po poprawnym zalogowaniu się do panelu administracyjnego aplikacji (w układzie testowym znajduje się on pod adresem *url* https://192.168.6.10/admin/) otwiera się w przeglądarce interfejs graficzny panelu (Rys. 2-7). Panel administracyjny jest w pełni konfigurowalny z poziomu pliku konfiguracyjnego admin.py znajdującego się w folderze /var/www/fivegui/elk.



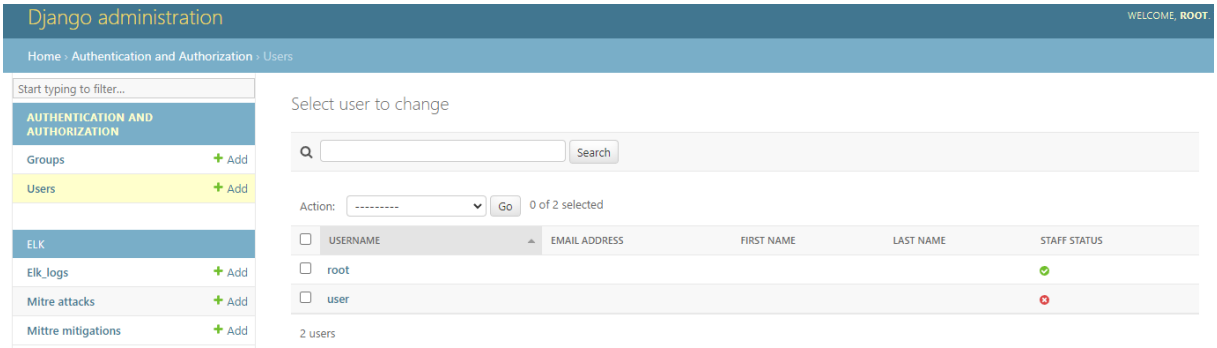
Rys. 2-7 Panel administracyjny aplikacji

Interfejs administracyjny został podzielony na dwie grupy edytowalnych elementów:

- uwierzytelnianie i autoryzacja –w tej grupie zawarte są ustawienia grup i kont użytkowników;
- dane związane z zastosowanymi w aplikacji modelami ORM aplikacji Elk – w tej grupie znajdują się rekordy pobrane z interfejsu API systemu Elk oraz zaimportowane do lokalnej bazy danych informacje dla technik i mitygacji systemu Mitre.

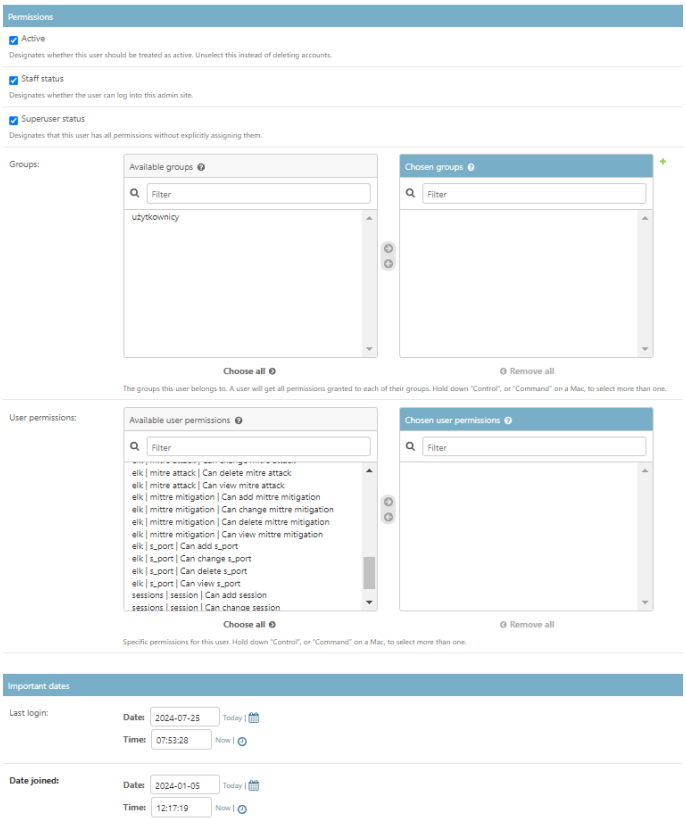
2.3.1 Konta i grupy użytkowników aplikacji APA

W aplikacji jest skonfigurowano jedno konto aktywne typu o rozszerzonych uprawnieniach (root*).* Konto to umożliwia zalogowanie zarówno to panelu głównego aplikacji oraz do panelu administracyjnego. W przypadku panelu administracyjnego konto te umożliwia edycję, dodawanie i usuwanie danych.



Rys. 2-8 Konta aktywnych użytkowników aplikacji

Edycja konta użytkownika umożliwia zmianę hasła, przypisanie danych personalnych oraz nadanie szczegółowych uprawnień do poszczególnych modeli w bazie danych. Dodatkowo można zweryfikować datę utworzenia danego konta oraz ostatnie logowanie.



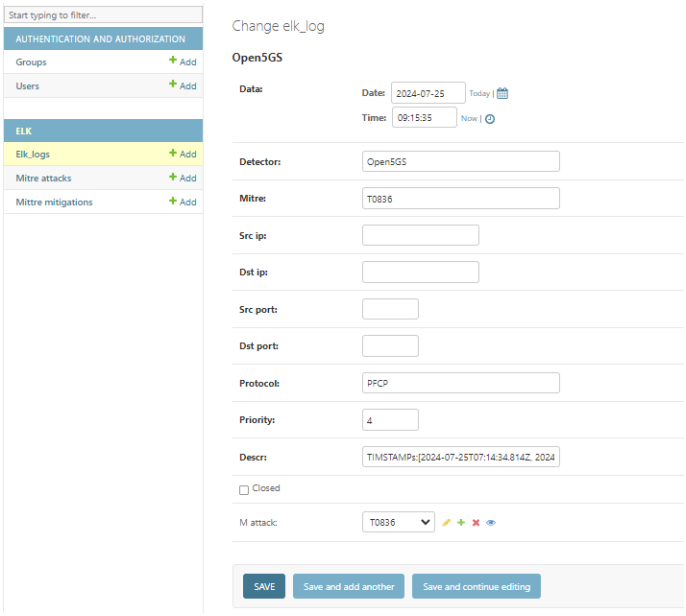
Rys. 2-9 Opcje konta użytkownika

2.3.2 Modele aplikacji

Interfejs grupy aplikacji zawiera modele związane z funkcjonalnością i przeznaczeniem aplikacji. Zalogowanie do interfejsu administracyjnego za pomocą konta typu root umożliwia pełną edycją i modyfikację, tj. tworzenie własnych rekordów dla poszczególnych modeli w tym także tworzenie własnych technik ataku oraz mitygacji specyficznych dla testowego środowiska 5G.

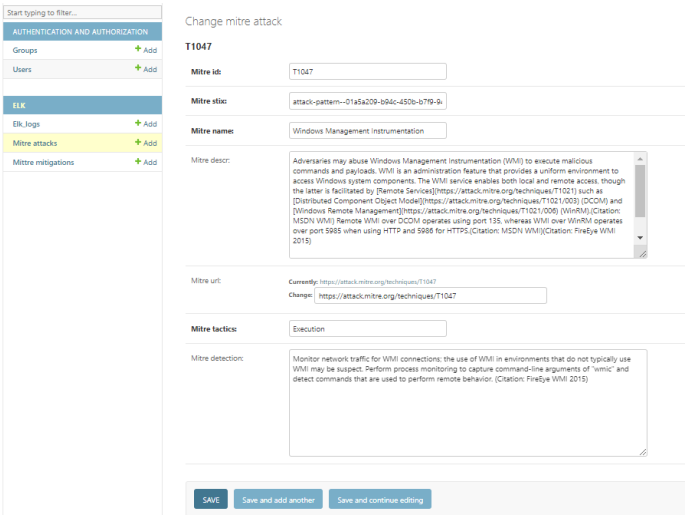
W grupie tej znajdują się następujące utworzone modele ORM:

- Elk_logs – model, w którym przechowywane są w bazie danych poszczególne zdarzenia przesłane z detektorów do systemu Elk (Rys. 2-10);



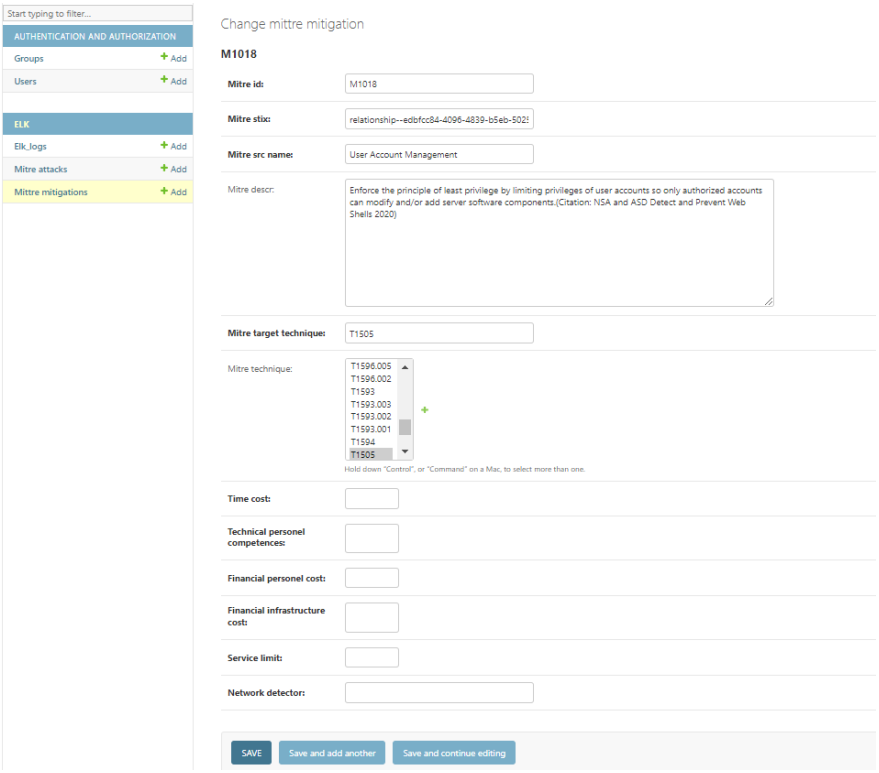
Rys. 2-10 Przykładowy rekord tylko elk_log

- Mitre attacks – **model, który zawiera zaimportowane wcześniej techniki ataku Mitre (Rys. 2-11);**



Rys. 2-11 Przykładowy rekordu tylko mitre attack

- Mittre mitigations – **model zawierający mitygacje dla poszczególnych technik ataków Mitre (Rys. 2-12).**



Rys. 2-12 Przykładowy rekord tylko mitre mitigation

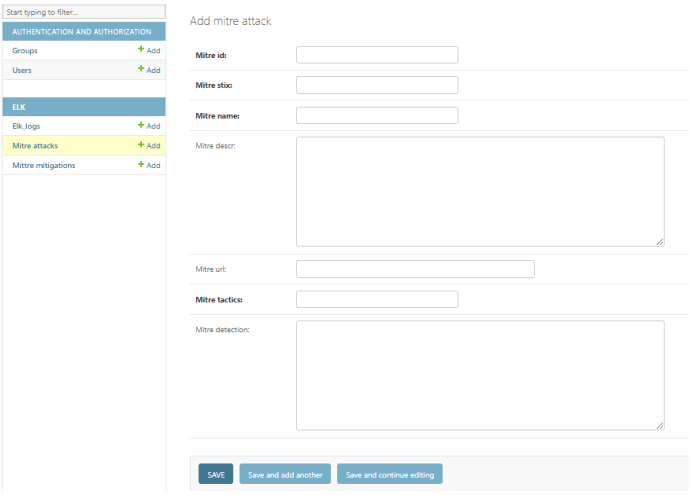
2.3.3 Dodawanie własnych technik i mitygacji

Z poziomu interfejsu panelu administracyjnego istnieje możliwość tworzenia własnych dedykowanych opisów technik ataków jak również powiązanych z nimi działań zaradczych.

Celem dodania nowej techniki należy użyć przycisku ADD MITRE ATTACK znajdującego się po prawej stronnie widoku dla modelu Mitre attacks (Rys. 2-13).

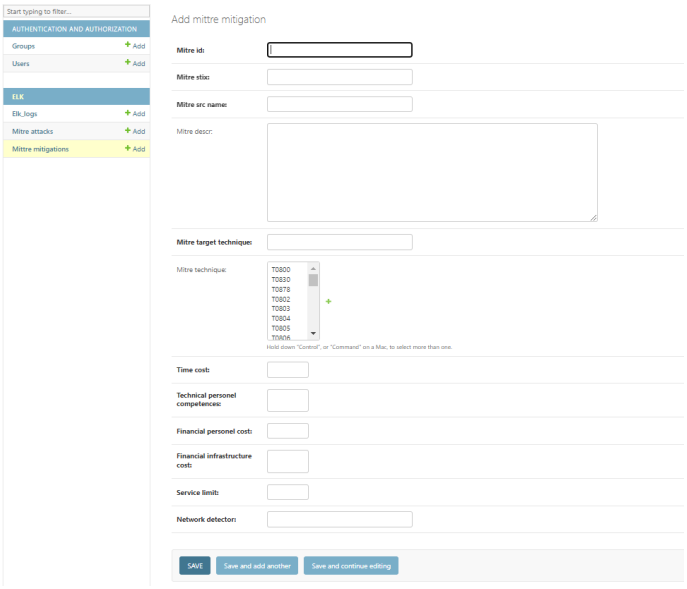
Rys. 2-13 Dodawanie własnej techniki ataku

Po kliknięciu przycisku pojawi się nowe okno umożliwiające wprowadzenie określonych danych we wprowadzanej technice (Rys. 2-14).



Rys. 2-14 Wprowadzanie nowej techniki ataku

Po zapisaniu wprowadzonej techniki ataku należy w analogiczny sposób przejść do widoku modelu Mitre mitigations i kliknąć w przycisk ADD MITRE MITIGATION a następnie uzupełnić wskazane pola i przypisać odpowiednią technikę ataku (Rys. 2-15).



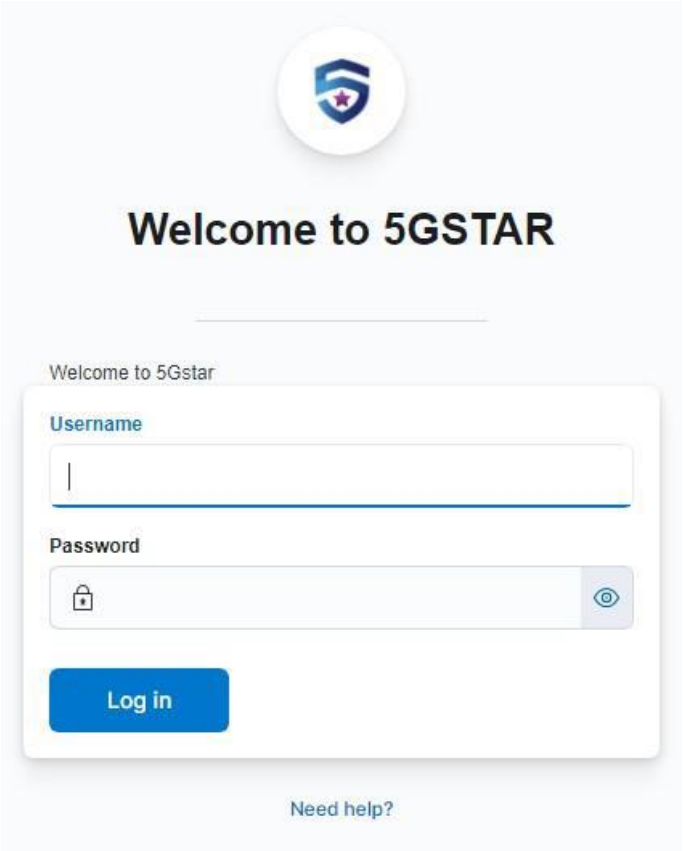
Rys. 2-15 Wprowadzanie nowej mitygacji i przypisywanie jej do odpowiedniej techniki

W obu przypadkach po zapisaniu zarówno nowej techniki ataku jak i mitygacji wszystkie zmiany będą widoczne od razu po odświeżeniu interfejsu aplikacji.

3 Aplikacja Przeciwdziałania Atakom (GM)

3.1 Logowanie do aplikacji

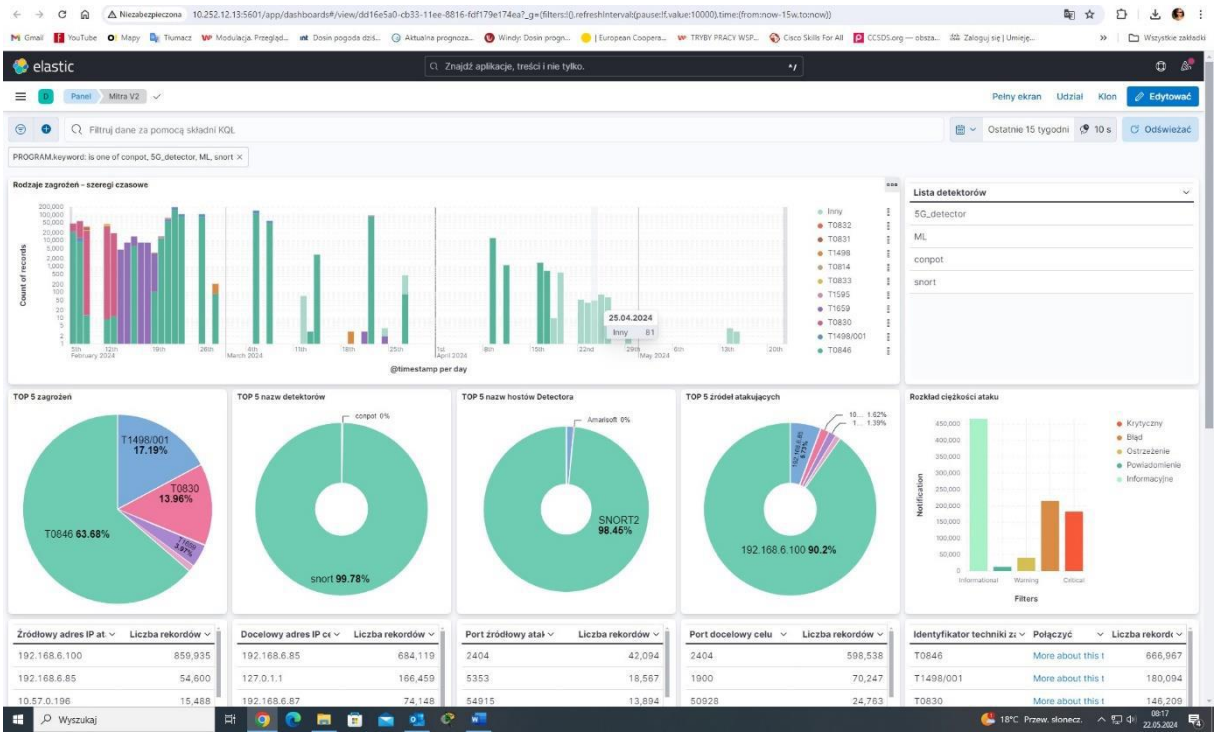
Logowanie użytkownika odbywa się standardowo za pomocą ustalonego loginu i hasła, które przy pierwszym logowaniu użytkownik otrzymuje od administratora systemu. Połączenie odbywa się za pomocą zabezpieczonego protokołu HTTPS. Ponieważ podobnie jak APA(WIŁ) jest to aplikacja przeglądarkowa przejście do okna logowania można przeprowadzić wpisując adres w dowolną przeglądarkę np. Chrome, Firefox, Edge.



Rys. 3-1 Okno logowanie do APA (GM)

3.2 Interfejs główny

Pulpit nawigacyjny (Rys. 3-1) stworzono na bazie ogólnych, gotowych schematów rozwiązań dostępnych w Elastic Stack.



Rys. 3-2 Ogólny obraz pulpitu nawigacyjnego

Na pulpicie wyświetlane są podstawowe informacje związane z zarejestrowanymi zagrożeniami (Rys. 3-3) wg następujących kategorii:

- Threat types timeseries – **rodzaje zagrożeń – szeregi czasowe z naniesionymi technikami ataków Mitre;**
- Detectors listing – **lista detektorów;**
- TOP 5 Threats – **TOP 5 zagrożeń;**
- TOP 5 Detector's names – **TOP 5 nazw detektorów;**
- TOP 5 Detector's hostnames – **TOP 5 nazw hostów detektorów;**
- TOP 5 Attacker's sources – **TOP 5 źródeł atakujących;**
- Attack's severities distribution – **Rozkład ciężkości ataku.**

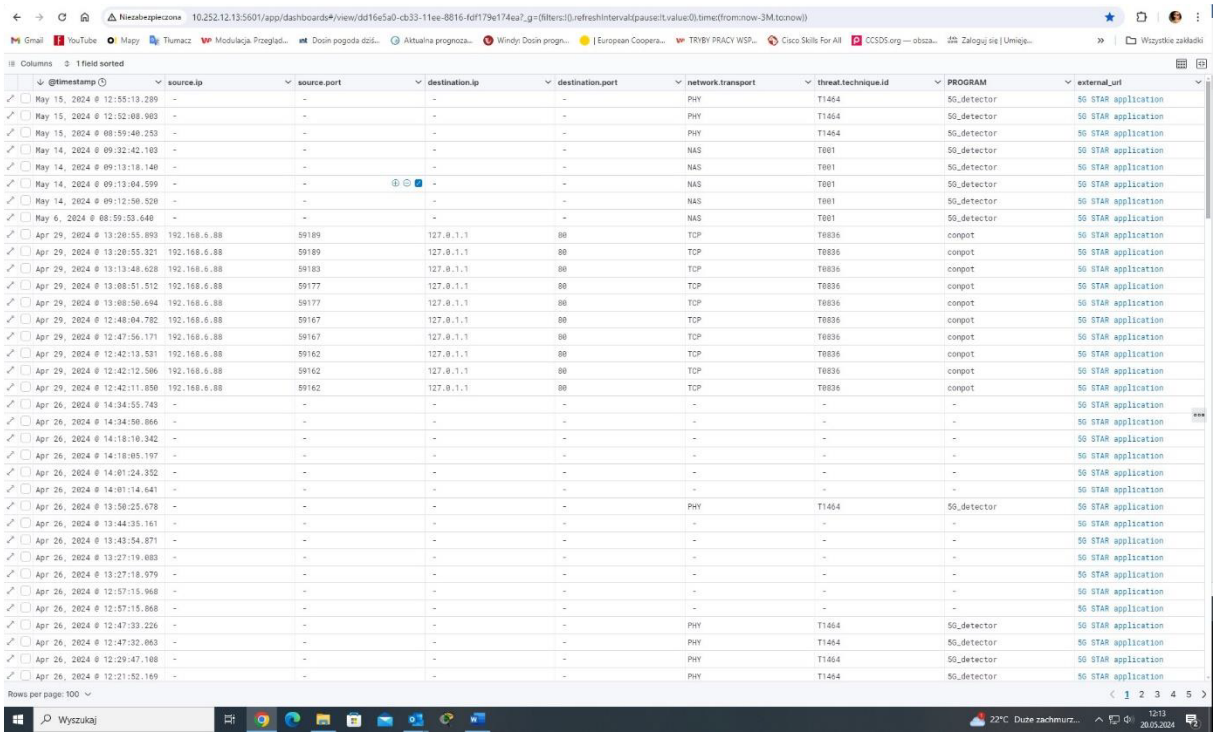
Rys. 3-3 Pulpit nawigacyjny – rodzaje zagrożeń

Dodatkowo, znajdują się tam tabele zawierające informacje o liczbie zgłoszonych do systemu zagrożeń (Rys. 3-4) w następujących kategoriach:

Rys. 3-4 Pulpit nawigacyjny – Rodzaje adresów i portów z podsumowaniem liczby rekordów

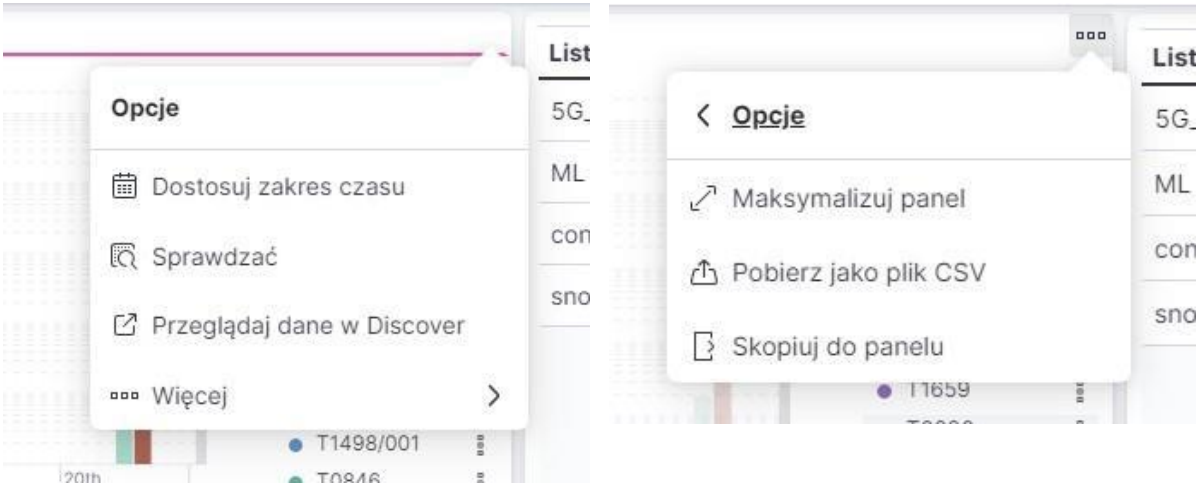
- Attacker's source IP – źródłowy adres IP atakującego;
- Target's destination IP – docelowy adres IP celu;
- Attacker's source port – port źródłowy atakującego;
- Target attack port – Docelowy port ataku i Liczba rekordów;
- Threat technique ID – Identyfikator techniki zagrożenia zgodnie z taksonomią MITRE.

W dolnej części okna prezentowana jest lista wszystkich zdarzeń zgłoszonych do systemu monitorowania w zadanym przedziale czasu (Rys. 3-5).



Rys. 3-5 Szczegółowe informacja o zdarzeniach

Dodatkową opcją przeglądu treści zawartych w oknach składowych są znajdujące się w prawym górnym rogu okna zakładki z rozszerzeniami - szczegóły i opcje. Standardowe informacje zawarte w tych zakładkach prezentuje Rys. 3-6.



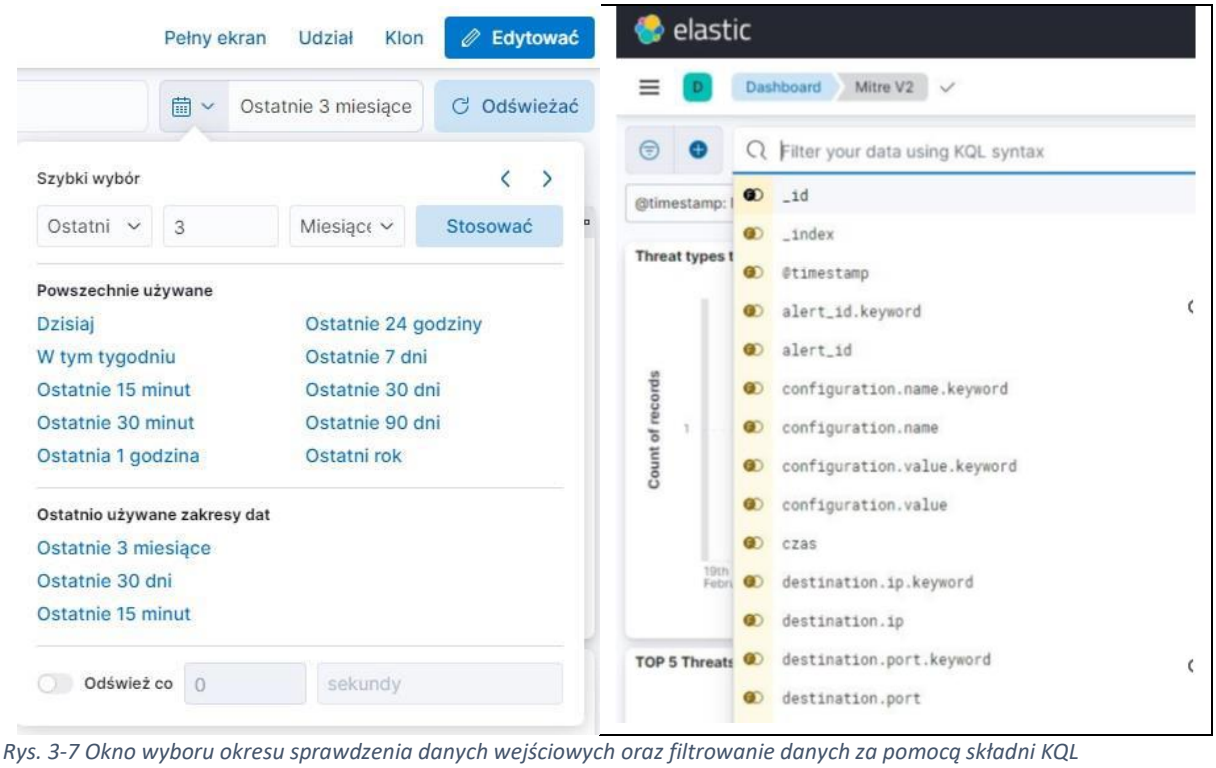
Rys. 3-6 Zakładki rozszerzeń okna Pulpitu 5gSTAR

3.3 Elementy składowe pulpitu

Pulpit aplikacji umożliwia filtracje danych w czasie, np. ostatnia określona ilość dni, przedział czasowy określony konkretnymi datami. Klikając na poszczególne wykresy można na zasadzie wyboru include/exclude wybrać dany typ zagrożenia, źródło, poziom zagrożenia, czy też docelowy adres IP ataku.

3.3.1 Wyszukiwanie, filtrowanie

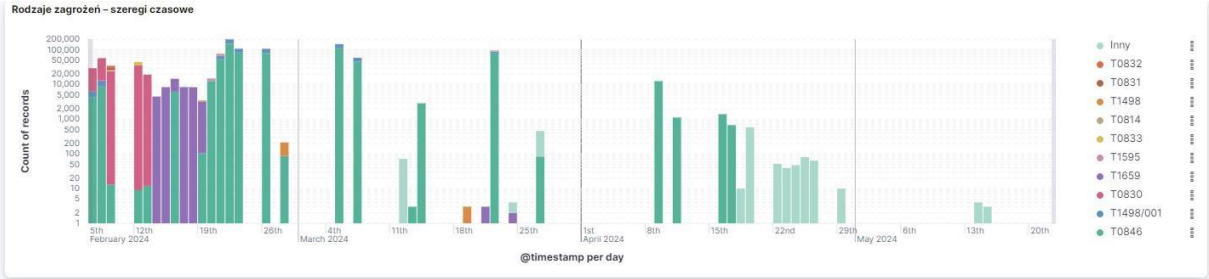
Pulpit aplikacji zbudowany jest z okien informacyjnych, które są aktualizowane na bieżąco (najkrótszy czas odświeżania danych wynosi co 1s). Każde z okien można „rozwijać" i przechodzić do treści szczegółowych w nim zawartych. Oprócz okna filtra wyszukiwarki i odświeżania, dostępne są ustawienia czasokresu wizualizacji występowania anomalii w przedziale: 15 minut – 1 rok (Rys. 3-7).



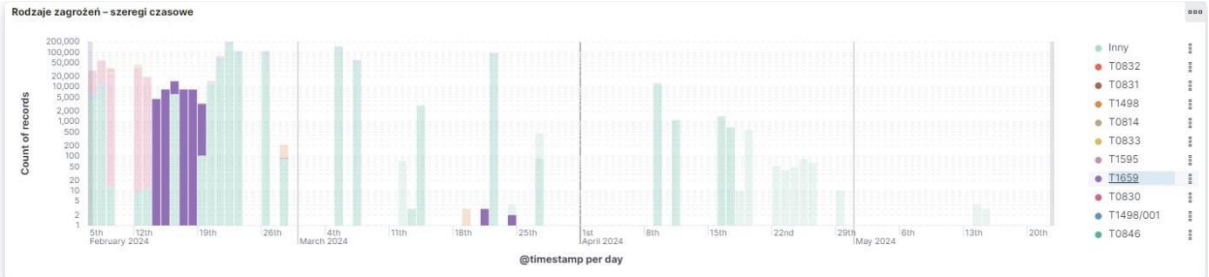
Rys. 3-7 Okno wyboru okresu sprawdzenia danych wejściowych oraz filtrowanie danych za pomocą składni KQL

3.3.2 Rodzaje zagrożeń – szeregi czasowe

Okno informuje użytkownika o liczbie zgłoszonych zagrożeń z podziałem na ich rodzaje. Są to wykresy w postaci histogramu – liczby zarejestrowanych zagrożeń w jednostce czasu (Rys. 3-8). Istnieje możliwość odfiltrowania i podglądu konkretnego zdarzenia.



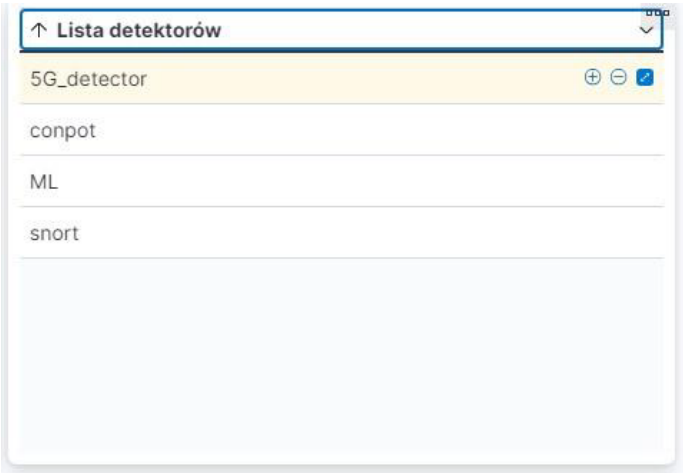
Rys. 3-8 Okno wizualizacji rodzajów zagrożeń



Rys. 3-9 Czas występowania wybranego zagrożenia - T1659

3.3.3 Lista detektorów

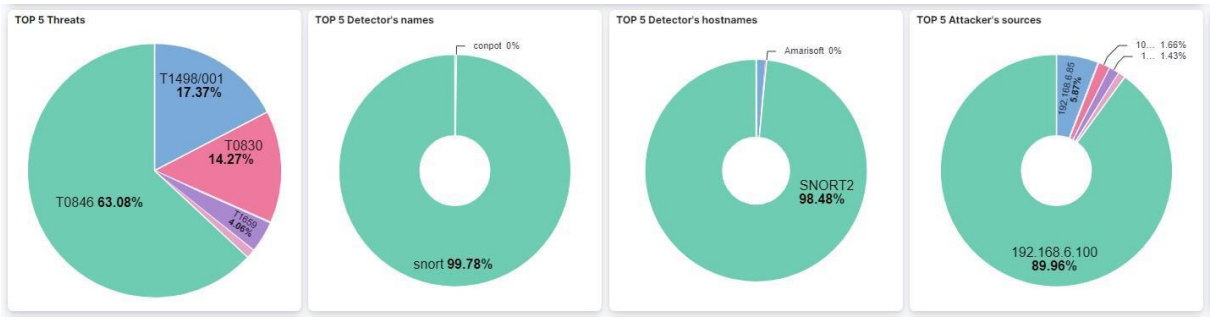
Lista zawiera wszystkie zadeklarowane detektory zdarzeń. W ramach ustawień istnieje możliwość selektywnego przeglądu każdego z wybranych detektorów, dostosowanie zakresu czasu, sprawdzenia, przeglądania danych w Discover, a także pobranie jako plik CSV lub kopiowanie do panelu.



Rys. 3-10 Lista detektorów

3.3.4 TOP 5 – zagrożenia, detektory, hosta, źródła

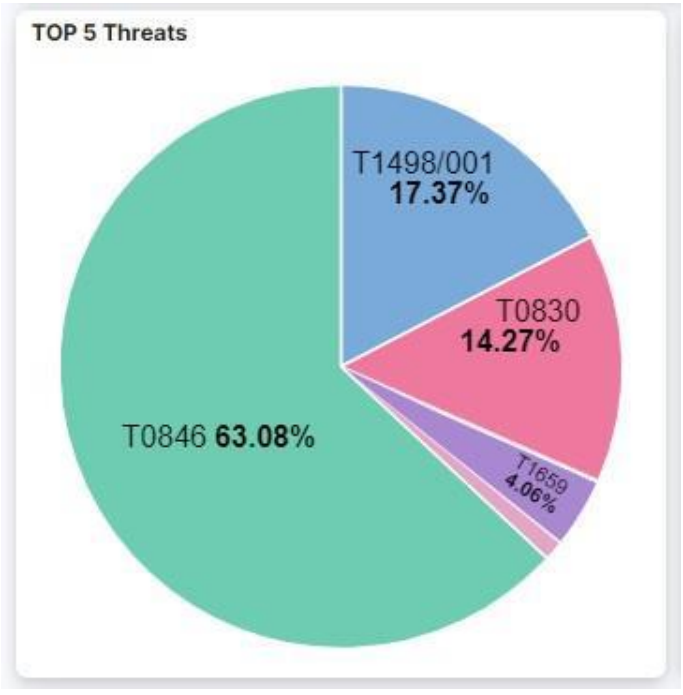
Kolejne okno Pulpitu 5gSTAR (Rys. 3-11) zostało podzielone na cztery części w formie okręgów przedstawiających zgłoszone zagrożenia w rozkładzie procentowym. TOP 5 oznacza najwyższych 5 wartości.



Rys. 3-11 Procentowy obraz zagrożeń w 5gSTAR

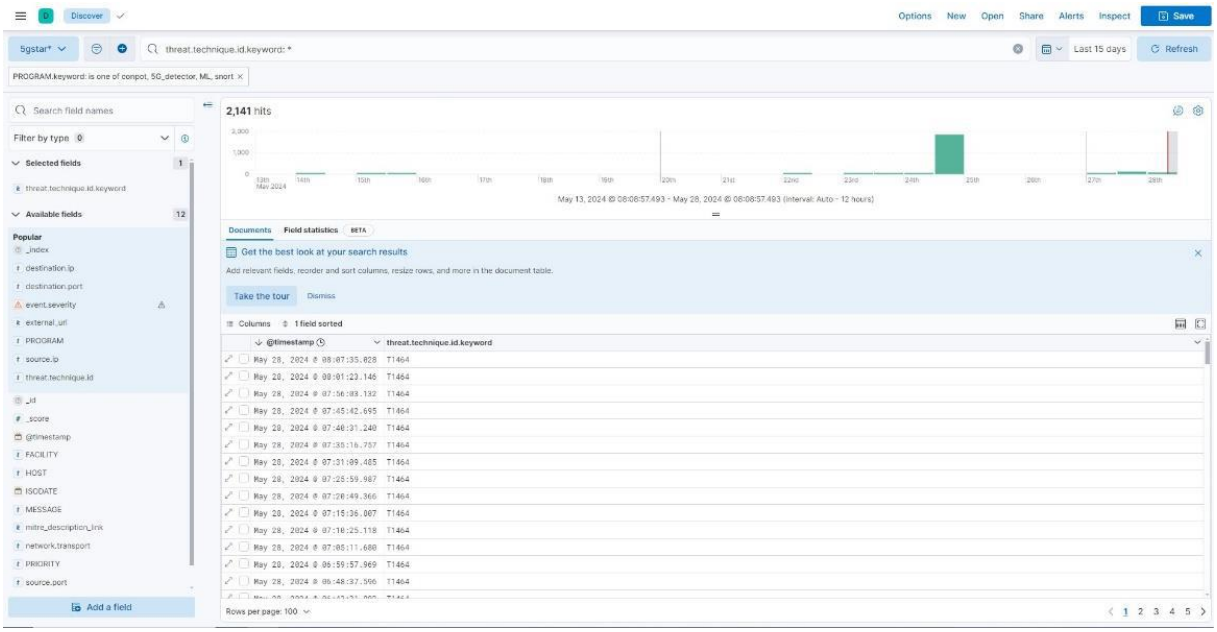
Zestawienie TOP 5 dotyczy następujących parametrów: nazwa detektora, nazwa hostów detektora oraz źródła ataku. Możliwość zobrazowania zagrożeń TOP 5 w kolejnych oknach jest podobna.

Poniżej (Rys. 3-12), okno TOP 5 Threats pokazuje procentowo udziały 5 najistotniejszych zagrożeń w okresie objętym sprawozdaniem. W prezentowanym przypadku ostatnie 15 tygodni.



Rys. 3-12 Procentowy rozkład zagrożeń TOP 5

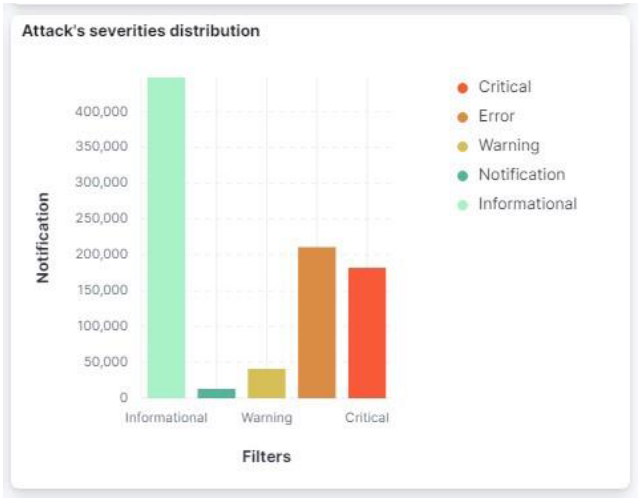
Po zainicjowaniu rozszerzenia - w prawym górnym rogu Przeglądaj dane w Discover – uzyskuje się dostęp do szczegółowych informacji na temat zagrożeń. W tym przypadku o identyfikatorach technik zagrożenia nr T0846, T1498/001, T0830, T1659 (Rys. 3-13).



Rys. 3-13 Dane szczegółowe procentowego rozkładu zagrożeń TOP 5

3.3.5 Rozkład ciężkości ataku

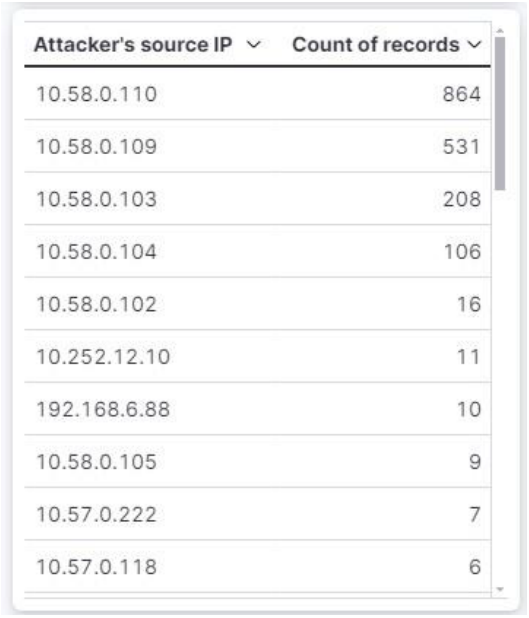
Okno przedstawia graficzną zależność ilości powiadomień o zaistniałych atakach w określonym przedziale czasowym od kategorii i priorytetu zaistniałego zdarzenia: Informacyjne, Powiadomienie, Ostrzeżenie, Błąd, Krytyczny (Rys. 3-14). Dodatkowo w opcjach istnieje możliwość dostosowania zakresu czasu, sprawdzenie, maksymalizacja panelu, pobieranie jako plik CSV oraz skopiowanie do panelu.



Rys. 3-14 Diagram ilości odnotowanych zdarzeń wg. kategorii

3.3.6 Źródłowy adres IP atakującego

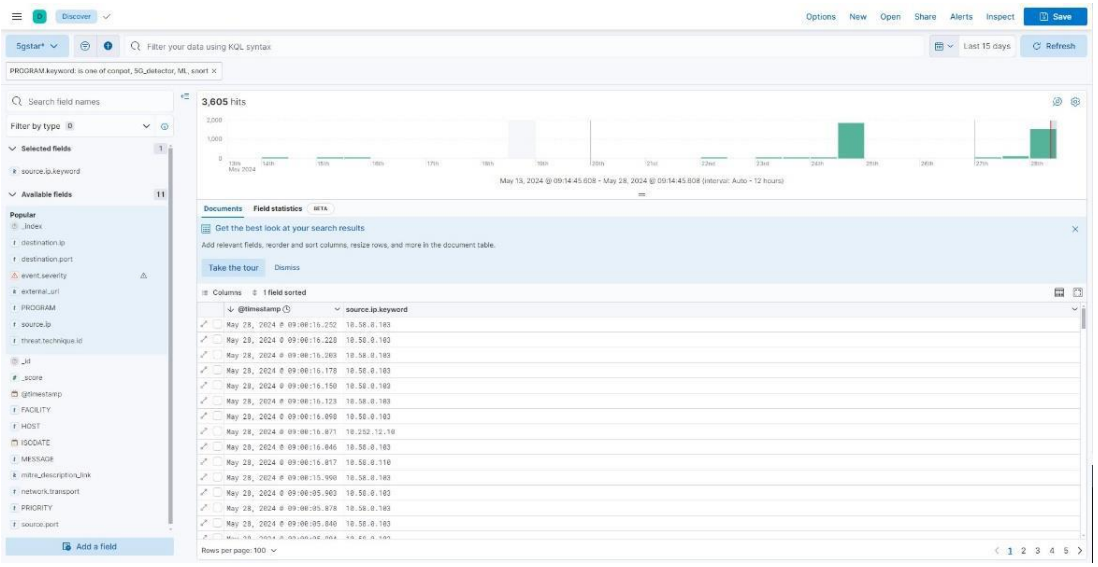
Okno przedstawia źródłowy adres IP z którego wykryto atak Rys. 3-15. Liczba rekordów (zdarzeń) mówi nam o ilości odnotowanych zdarzeń z danego adresu IP. Sortowanie wyświetlania standardowo ustawiono na „malejaco”.



Attacker's source IP	Count of records
10.58.0.110	864
10.58.0.109	531
10.58.0.103	208
10.58.0.104	106
10.58.0.102	16
10.252.12.10	11
192.168.6.88	10
10.58.0.105	9
10.57.0.222	7
10.57.0.118	6

Rys. 3-15 Okno adresu IP atakującego z liczbą przeprowadzonych ataków

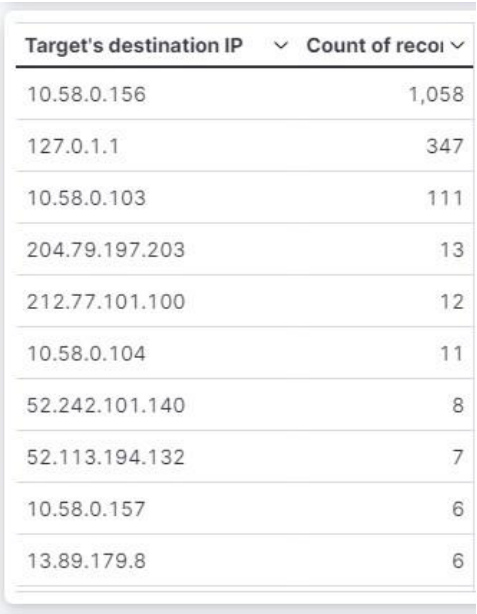
W rozszerzeniu powyższego okna można sprawdzić datę i dokładny czas każdego zdarzenia, wykonać sortowanie informacji zawartych w oknie oraz zidentyfikować źródło zagrożenia w kolumnie źródło.ip.słowo_kluczowe (Rys. 3-16).



Rys. 3-16 Szczegółowe informacje dotyczące źródeł zagrożeń

3.3.7 Docelowy adres IP celu

Okno zawiera informację o adresach IP, które są najczęściej atakowane oraz o liczbie przyporządkowanych zdarzeń dla danego adresu IP (Rys. 3-17). Sortowanie wyświetlania standardowo ustawiono na „malejąco”. Szczegóły analityczne dostępne są w formie wykresów i tabeli po rozwinięciu okna.



Target's destination IP	Count of recor
10.58.0.156	1,058
127.0.1.1	347
10.58.0.103	111
204.79.197.203	13
212.77.101.100	12
10.58.0.104	11
52.242.101.140	8
52.113.194.132	7
10.58.0.157	6
13.89.179.8	6

Rys. 3-17 Okno adresu IP celu ataku z liczbą przeprowadzonych ataków

3.3.8 Port źródłowy atakującego

W kolejnym oknie przedstawione zostały numery portów, z których zostały zainicjowane konkretne ataki do ilości zdarzeń powiązanych z konkretnym portem. Sortowanie wyświetlania ustawiono standardowo na „malejaco”. Szczegóły analityczne dostępne są w formie wykresów i tabeli po rozwinięciu okna.

Attacker's source port	Count of records
1883	51
443	25
14195	14
17	14
19164	14
19714	14
2084	14
23045	14
2586	14
27099	14

Rys. 3-18 Okno portu źródłowego atakującego z jego aktywnością

3.3.9 Docelowy port ataku

Docelowe porty na które przeprowadzane są ataki przedstawione w kolejnym oknie (Rys. 3-19), określane są numerem docelowym portu odbiorcy (usługi) na który kierowany jest atak do ilości zdarzeń zaistniałych na danym porcie.

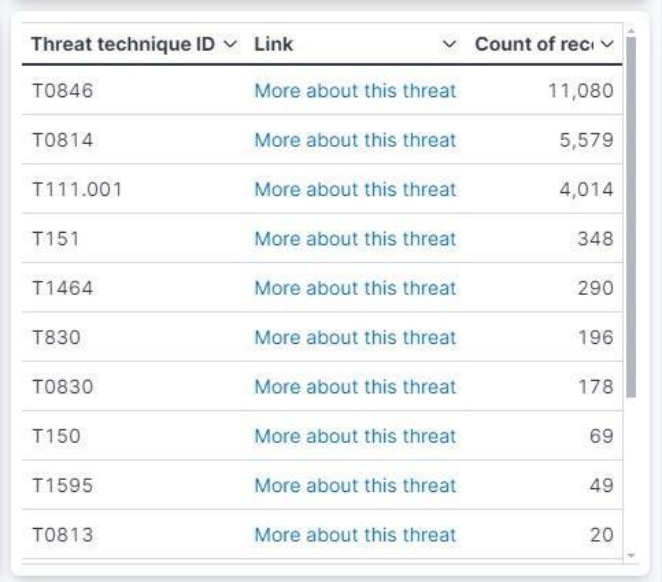
Target's attact port	Count of records
2404	68,771
102	12,524
443	3,147
1883	2,698
80	647
81	503
59611	415
7680	328
9200	299
21	233

Rys. 3-19 Okno z ilością ataków i numerami portów na które przeprowadzane są ataki

3.3.10 Identyfikator techniki zagrożenia

Okno przedstawia rodzaje identyfikatorów oznaczonych literą „T” i numerem (zgodnie z taksonomią MITRE), link z rozszerzeniem dotyczącym danego wątku oraz liczbę zdarzeń

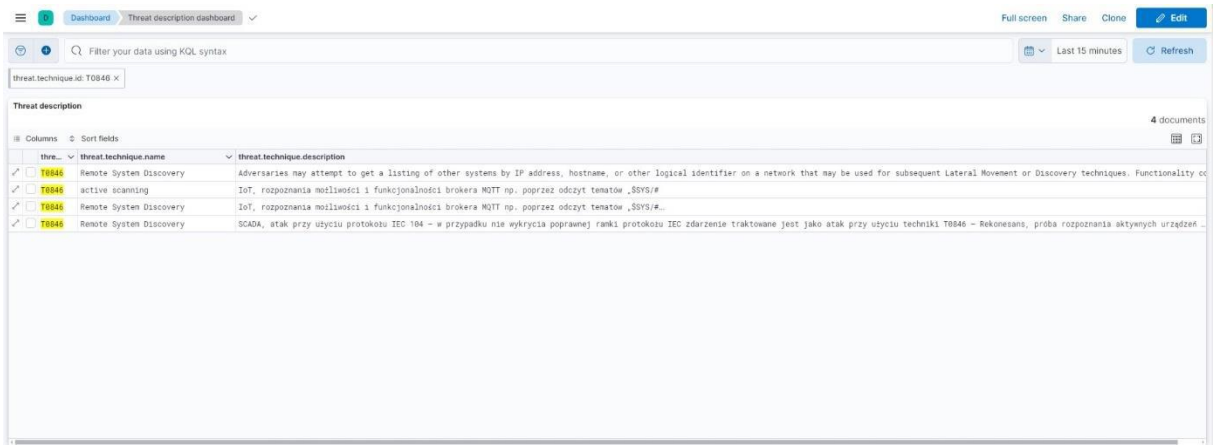
zarejestrowanych dla danego identyfikatora „T”. źródłowy adres, który jest użyty do wykonania ataku. Liczba rekordów mówi nam o ilości odnotowanych zdarzeń dla danej techniki ataku.



Threat technique ID	Link	Count of rec
T0846	More about this threat	11,080
T0814	More about this threat	5,579
T111.001	More about this threat	4,014
T151	More about this threat	348
T1464	More about this threat	290
T830	More about this threat	196
T0830	More about this threat	178
T150	More about this threat	69
T1595	More about this threat	49
T0813	More about this threat	20

Rys. 3-20 Widok ogólnego okna

W rozszerzeniu okna „więcej o tym zagrożeniu” zawarte są informacje związane z opisem zagrożenia. Tabela zawiera informacje nt.: zagrożenie.technika.ID – w prezentowanym przypadku T0846, nazwa.techniki.zagrożenia – np. aktywne skanowanie oraz opis.techniki.zagrożenia np. IoT, rozpoznanie możliwości i zastosowanie brokera MQTT np. poprzez odczyt „$SYS/# (Rys. 3-21)

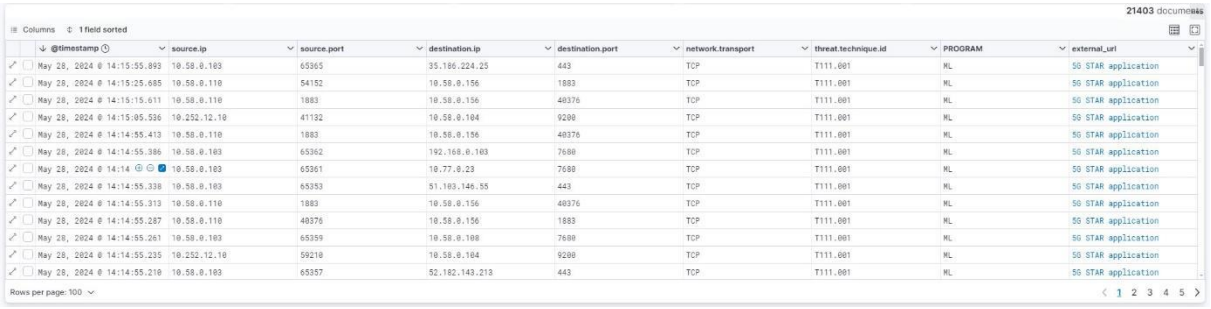


Rys. 3-21 Opis przykładowego zagrożenia dla techniki ataku o numerze T0846

3.3.11 Szczegółowa lista zdarzeń

Jest to okno w formie tabeli, które zawiera szczegółową listę wszystkich zdarzeń z danego okresu wysłanych przez detektory i link (external_url) do aplikacji umożliwiającej mitygację ataków.

Szczegółowa lista zdarzeń zawiera zestawienie informacji o danym zagrożeniu, mitygacje sugerowane przez MITRE i stworzone w ramach projektu 5gSTAR (Rys. 3-22).



Rys. 3-22 Tabelaryczna szczegółowa lista zdarzeń

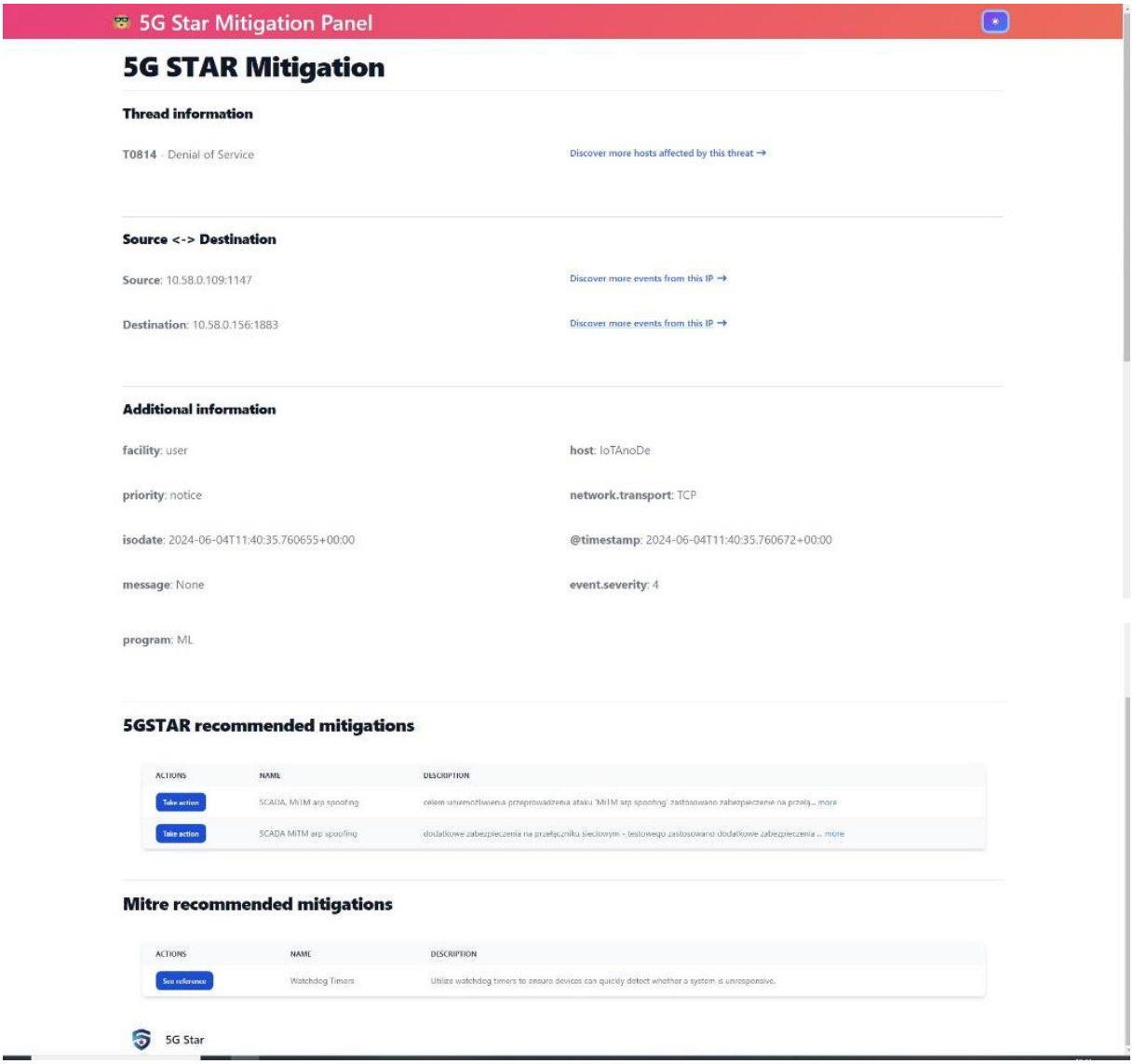
W kolejnych kolumnach zawarte są informacje na temat szczegółów z listy zdarzeń:

- @znak czasu – data i czas zdarzenia np. 31 maja 2024 o 15:40;
- źródło.IP – adres, z którego odbywa się atak np. 10.57.0.204;
- port źródłowy – numer portu, z którego następuje atak np. 57845;
- docelowy adres IP – adres, na który wymierzony jest atak np. 146.112.41.2;
- port docelowy - numer portu, na który skierowany jest atak np. 443;
- sieć.transport – rodzaj sieci, protokołu zarządzającego przepływem danych np. TCP;
- zagrożenie.technika.id – rodzaj zagrożenia np. T1464 – charakterystyka zagrożenia dostępna w Panelu Opisu Zagrożeń;
- program – detektor wykrywający ataki np. snort;
- zewnętrzny_url - 5G STAR application – przekierowanie do panelu mitygacji 5gSTAR.

3.4 Panel mitygacji 5gSTAR

Na podstawie wybranej techniki ataku istnieje możliwość wyświetlenia informacji o zdarzeniu. Oprócz informacji o wybranej technice ataku, aplikacja umożliwia wyszukanie

dodatkowych ataków dla tej techniki. W panelu otrzymujemy informacje o zagrożeniu z rozszerzeniem pozostałych hostów dotkniętych tym samym atakiem np.: T0814 – Odmowa usługi. W kategorii źródło / miejsce docelowe, określony jest adres, z którego realizowany jest atak oraz adres docelowy ataku. Istnieje możliwość podglądu pozostałych zdarzeń realizowanych z i na dany adres IP (Rys. 3-23).



Rys. 3-23 Podstawowe informacje zawarte w Panelu mitygacji 5gSTAR

W informacjach dodatkowych otrzymujemy uszczegółowione dane, dla przykładu:

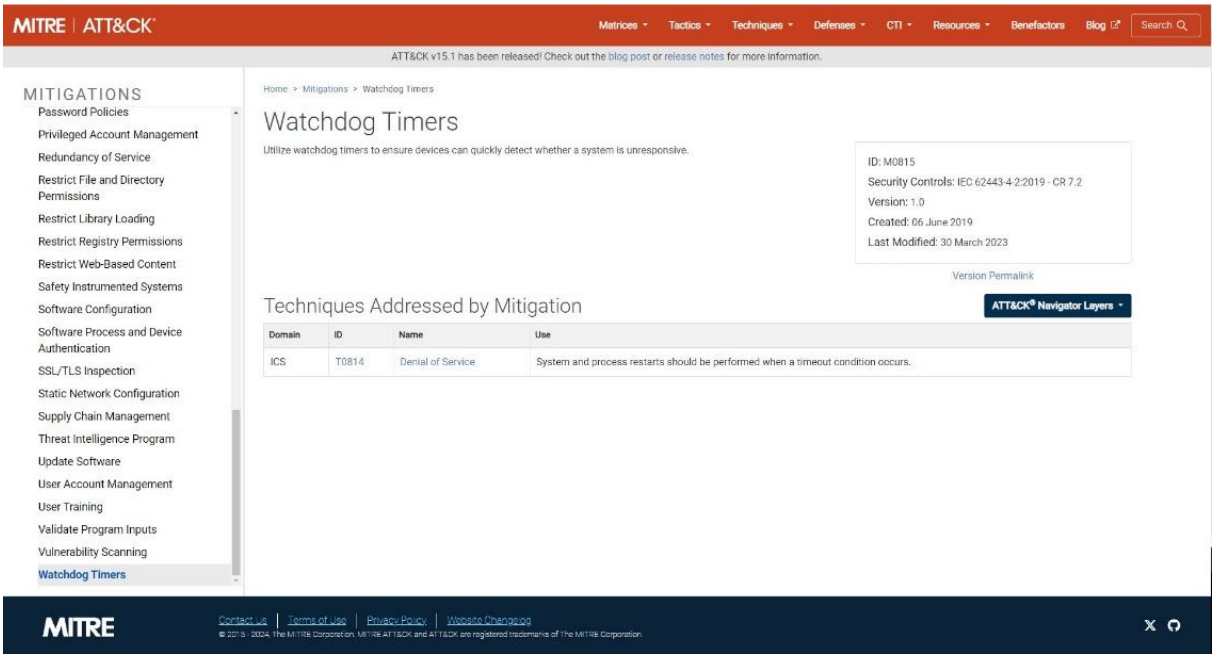
- obiekt: użytkownik;
- gospodarz: IoTAnoDe;

- priorytet: uwaga;
- transport sieciowy: TCP;
- isodata: 2024-06-04T11:40:35.760655+00:00;
- @znacznik czasu: 2024-06-04T11:40:35.760672+00:00;
- wiadomość: Brak;
- wydarzenie.ważność: 4;
- program: M.L. (Machine Learning).

Poniżej (Rys. 3-24) pokazane są środki mitygacji zalecane przez 5gSTAR. Wskazówki dotyczą nazwy zagrożenia oraz opis zaproponowanego działania.

Na dole okna zawarta jest informacja jakie środki mitygacji zalecane są przez bazę Mitre:

- zobacz odniesienie, nazwa i opis z możliwością rozszerzenia za pośrednictwem MITRE | ATT&CK



Rys. 3-24 Przykładowa, zalecana propozycja mitygacji ataku dla zdarzenia ID T0814

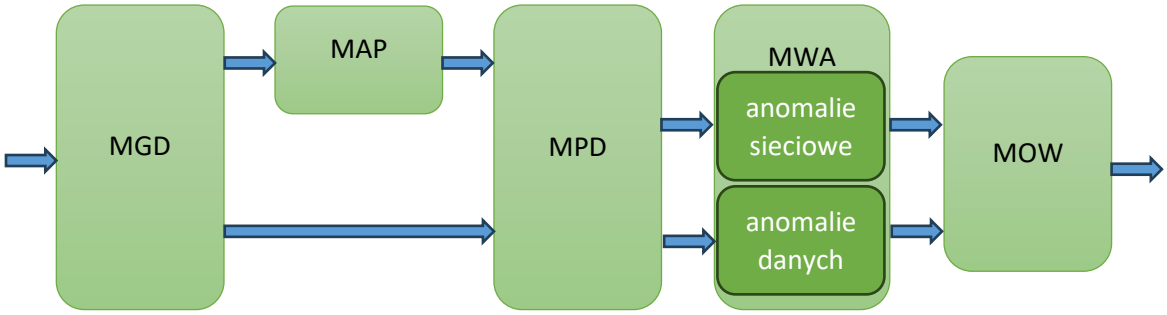
4 Detektory SI dla SCADA i IIoT

Tradycyjne uczenie maszynowe, w tym klasyfikacja, opiera się na danych treningowych, na których model jest uczony, aby rozpoznawał określone wzorce i klasyfikował dane na podstawie istniejących kategorii. Głównym wyzwaniem w wykrywaniu nowych ataków jest to, że te ataki zazwyczaj różnią się od znanych wzorców, na których model został przeszkolony. W rezultacie modele te nie są w stanie zidentyfikować nieznanych wcześniej technik i zachowań – co prowadzi do ich nieefektywności w detekcji nowych ataków.

W systemie 5gSTAR zastosowano algorytmy pozwalające wykrywać anomalie, zatem potencjalnie umożliwiające wykrywanie nieznanych dotąd ataków. W tym celu wybrano algorytm OCSVM należący do klasy algorytmów uczenia maszynowego (ML, *machine learning*) oraz algorytm Autoencoder należący do klasy algorytmów uczenia głębokiego (DL, *deep learning*). Zostały one wytrenowane do rozpoznawania anomalii w ruchu sieciowym pochodzącym od sterowników PLC (model stacji elektroenergetycznej) wykorzystujących w procesie komunikacji protokoły SCADA (IEC 104) oraz czujników IoT wykorzystujących protokół MQTT. Pierwszy z ww. algorytmów zastosowano w celu wykrywania anomalii w ruchu sieciowym, podczas gdy drugi z nich do wykrywania anomalii odczytanych danych.

4.1 Architektura detektorów SI

Proces trenowania algorytmów SI przeprowadzono osobno dla SCADA oraz dla MQTT budując w ten sposób dwa specjalizowane detektory (ukierunkowane na specyficzną technologię) o ogólnej strukturze jak na Rys. 4-1.

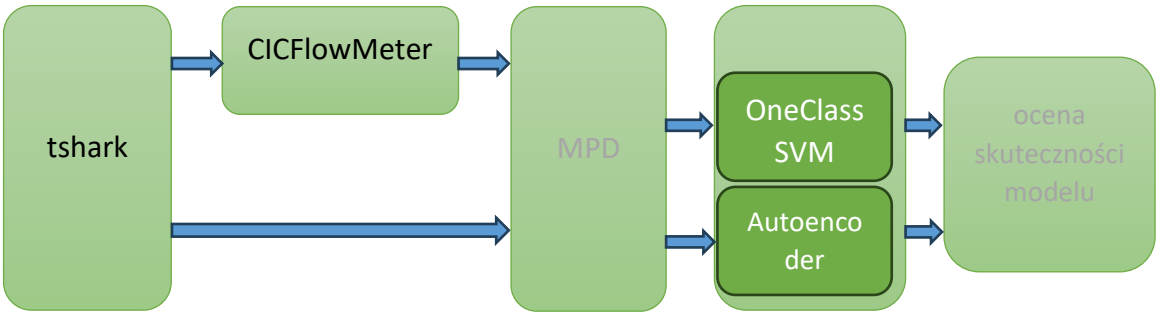


Rys. 4-1 Struktura detektorów SI

Pokazane na Rys. 4-1 detektory zbudowane są z następujących bloków:

- **MGD** (Moduł Gromadzenia Danych) - zbiera dane z ruchu sieciowego w czasie rzeczywistym, umożliwiając dalszą analizę. Wykorzystuje narzędzie tshark do przechwytywania pakietów w sieci;
- **MAP** (Moduł Analizy Przepływów) - analizuje zgromadzone dane pakietów i generuje przepływy, czyli logiczne grupy pakietów opisujące interakcje między różnymi źródłami i docelowymi adresami. Wykorzystuje narzędzie CICFlowMeter;
- **MPD** (Moduł Przetwarzania Danych) - ekstrakcja cech i standaryzacja;
- **MWA** (Moduł Wykrywania Anomalii), który wykorzystuje:
    - zaawansowany algorytm uczenia maszynowego, tj. OneClassSVM do analizy znormalizowanych cech przepływów i identyfikacji potencjalnych anomalii w ruchu sieciowym. Model OCSVM uczy się reprezentatywnych wzorców ruchu sieciowego, co pozwala na efektywne wykrywanie zachowań odstających od normy (IDS DETEKTUJĄCY ANOMALIE SIECIOWE)
    - algorytm Autoencodera, który jest modelem opartym na uczeniu głębokim do analizowania danych przenoszonych w pakietach. Algorytm Autoencodera pozwala na reprezentację danych wejściowych w niższej wymiarowości, dzięki czemu anomalie mogą być bardziej wyraźne. (IDS WYKRYWAJĄCY ANOMALIE ODCZYTANYCH DANYCH)
- **MOW** (Moduł Oceny Wyników) - ocenia wydajność modelu za pomocą różnych metryk oceny, takich jak dokładność, precyzja, czułość itp.

Algorytmy sztucznej inteligencji dla prawidłowego działania wymagają odpowiedniego przygotowania danych, które zostaną podane na ich wejście. Dlatego detektory oprócz algorytmów SI wykorzystują w tym celu tym specjalizowane narzędzia przedstawione na Rys. 4-2.



Rys. 4-2 Narzędzia i algorytmy wykorzystane w detektorach SI

Wszystkie moduły współpracują ze sobą, przetwarzając dane w sposób sekwencyjny i iteracyjny, aby umożliwić skuteczne wykrywanie anomalii w ruchu sieciowym. Architektura systemu została zaprojektowana tak, aby zautomatyzować proces analizy ruchu sieciowego i zapewnić efektywny monitoring i wykrywanie nieprawidłowości w sieci.

4.2 Skuteczność detektorów SI

Aby ocenić skuteczność danego modelu uczenia SI wykorzystuje się standardowe wskaźniki, które pozwalają porównać uzyskane w badaniach rezultaty. Detektory zaimplementowane w systemie 5gSTAR charakteryzują się skutecznością jak w Tab. 4-1.

Tab. 4-1 Wskaźniki skuteczności dla detektorów SI systemu 5gSTAR

L.P.	Nazwa wskaźnika	Wartość
1.	Accuracy	> 0.8
2.	Precision (Precyzja)	> 0.5
3.	Recall (Czułość)	> 0.7
4.	F1-Score (Średnia harmoniczna)	> 0.6
5.	AUC (Obszar pod krzywą ROC)	0.75

4.3 Kryteria skuteczności

Aby ocenić skuteczność uczenia danego algorytmu SI wykorzystuje się wskaźniki, które pozwalają porównać uzyskane w badaniach rezultaty. Opierają się one na standardowym podejściu do weryfikacji hipotez matematycznych. W tym przypadku sprowadza się to do weryfikacji hipotezy o obecności anomalii w ruchu sieciowym oraz hipotezy przeciwnej:

- H_0: ruch sieciowy nie zawiera anomalii;

- H_1: w ruchu sieciowym występują anomalie świadczące o potencjalnym ataku cybernetycznym.

Z weryfikacją ww. hipotez wiążą się dwa rodzaje błędów jakie można popełnić algorytm:

- wykrycie anomalii w ruchu sieciowym, podczas gdy w rzeczywistości one nie występują – jest to tzw. fałszywy alarm (ang. *false alarm, false positive*);
- anomalie w ruchu sieciowym nie zostaną wykryte, gdy w rzeczywistości następuje atak cybernetyczny – jest to tzw. brak alarmu (ang. *miss alarm, false negative*)

Biorąc pod uwagę, że każda z badanych hipotez matematycznych może zostać uznana za prawdziwą lub fałszywą oraz możliwe do popełnienia błędy oceny sytuacji uzyskuje się cztery współczynniki[2] służące następnie do wyznaczenia wskaźników skuteczności detektorów:

- **TN** – *True Negative* – stan sieci normalny, **detektor nie zgłasza alarmu** - wskazanie prawidłowe;
- **TP** – *True Positive* – atak cybernetyczny, **detektor zgłasza alarm** - wskazanie prawidłowe;
- **FP** – *False Positive* – stan sieci normalny, **detektor zgłasza alarm** - wskazanie nieprawidłowe;
- **FN** – *False Negative* – atak cybernetyczny, **detektor nie zgłasza alarmu** - wskazanie nieprawidłowe.

4.3.1 Precyzja detektora

Wskaźnik określany mianem **precyzji detektora** (ang. *precision*) określa odsetek poprawnie wykrytych zagrożeń (TP) w stosunku do sumy wszystkich zgłoszonych zagrożeń, zarówno tych prawdziwych jak i błędnych (TP+FP).

$$P = \frac{TP}{TP + FP}$$

Duża precyzja oznacza dużo poprawnie wykrytych anomalii.

[2] Wskaźniki te należy traktować w kategorii prawdopodobieństwa

Precision: 75% oznacza, że 75% przewidywań anomalii modelu to rzeczywiście anomalie, 25% źle wykryte anomalie.

4.3.2 Czułość detektora

Wskaźnik określany mianem **czułości detektora** (ang. *recall*) również jako TPR (ang. *True Positive Rate*) określa odsetek poprawnie wykrytych zagrożeń w stosunku do sumy poprawnie sklasyfikowanych zagrożeń oraz zagrożeń, na które detektor nie zareagował (TP+FN).

$$R = \frac{TP}{TP + FN}$$

Wysoka wartość czułości oznacza, że model jest w stanie wykryć większość rzeczywistych anomalii.

4.3.3 Średnia harmoniczna F-1

Średnia harmoniczna jest to tzw. miara położenia wyznaczana na podstawie wartości precyzji i czułości detektora.

$$F = \frac{2 * P * R}{P + R}$$

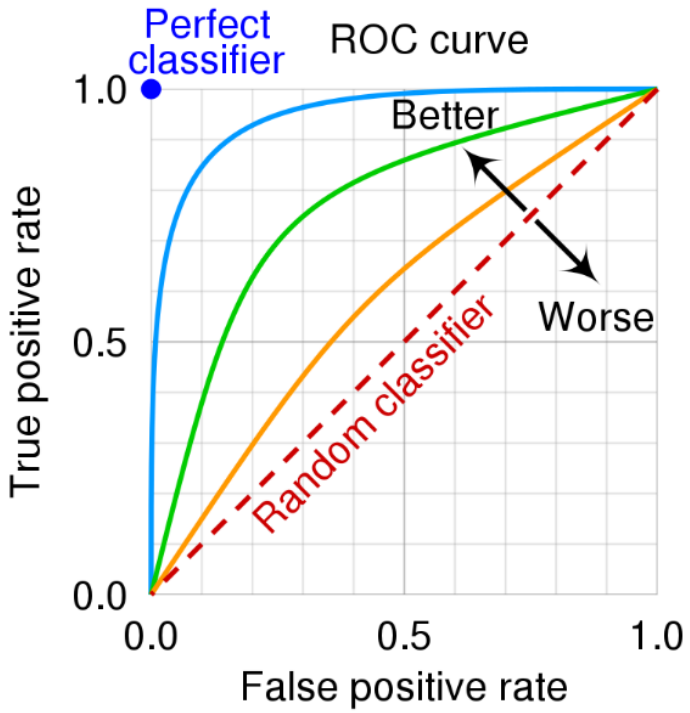
4.3.4 Obszar pod krzywą ROC

Obszar pod krzywą ROC, AUC (ang. *Area Under the ROC Curve*) jest miarą jakości, która mówi o stopniu, w jakim model jest w stanie odróżnić pozytywne przypadki od negatywnych. AUC jest wartością liczbową, która zawiera się w przedziale od 0 do 1, z wartością 1 oznaczającą, że model jest idealnie zdolny do odróżnienia pozytywnych od negatywnych przypadków.

Krzywa ROC (ang. *Receiver Operating Characteristic*) jest powszechnie używana do oceny jakości klasyfikatorów. Generalnie krzywa ROC może przedstawiać zależności pomiędzy różnymi wskaźnikami. W tym przypadku jest to zależność między współczynnikiem czułości detektora (*recall, TPR)* a wskaźnikiem określanym jako FPR (ang. *False Positive Rate*, czyli stosunkiem liczby fałszywie pozytywnych przypadków do liczby rzeczywiście negatywnych.

$$FPR = \frac{FP}{FP + TN}$$

Przykładowy przebieg krzywej ROC przedstawiono na Rys. 4-3.



Rys. 4-3 Przykład wykorzystania krzywych ROC do porównania jakości detektorów [Wikipedia]

Im wyższa wartość TPR i niższa FPR, tym lepszy jest model. Model, który ma krzywą ROC blisko lewego górnego rogu jest najlepszy, ponieważ oznacza to, że ma wysoki TPR i niski FPR. Natomiast, kiedy krzywa ROC przebiega przez linię prostą y=x, oznacza to, że jego TPR jest równy FPR, co oznacza, że model nie ma zdolności do rozróżnienia pozytywnych i negatywnych przypadków. AUC-ROC jest również powszechnie stosowana miarą oceny jakości modelu, Im większa jest AUC-ROC, tym lepszy jest model.

Wartości AUC-ROC mieszczą się w zakresie od 0 do 1. AUC-ROC równe 1 oznacza, że model jest idealny, a AUC-ROC równe 0.5 oznacza, że model jest taki sam jak losowy.

Dokumenty Związane

[1] Wniosek o projekt Zaawansowane metody i techniki wykrywania i przeciwdziałania atakom na infrastrukturę dostępową i aplikacje sieci 5G - 5gSTAR, 2021

[2] P6.1 Projekt techniczny systemu 5gSTAR

[3] P7.1 Środowisko testowe do badania systemu 5gSTAR

[4] Zespół WIŁ-PIB I PP, P4.1. Projekt mechanizmów identyfikacji ataków na aplikacje sieci 5G, 5gSTAR, 2023

[5] P6.2 Implementacja komponentów programowych

[6] https://www.djangoproject.com/ - Django framework.

[7] https://pypi.org/project/django-bootstrap-v5/ - Biblioteka django-bootstrap.

[8] https://www.chartjs.org/ - Chart.js

[9] https://httpd.apache.org/ - Apache, http server project.

[10] Wdrożenie bezpiecznej komunikacji dla systemu zbierania zdarzeń. Wykonanie dokumentacji programowej Aplikacji Przeciwdziałania Atakom (APA).

[11] https://attack.mitre.org/ - Mitre ATT&CK.

[12] https://stixproject.github.io/ - Structured Threat Information eXpression

[13] System bezpieczeństwa cyberprzestrzeni RP. Ekspertyza dotycząca rekomendowanego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, wykonana na zlecenie Ministerstwa Administracji i Cyfryzacji. NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA (NASK / CERT POLSKA) Warszawa, wrzesień 2015

Spis Rysunków

Spis Tabel

Opracował:

……..

mjr dr inż. Krzysztof Kosmowski