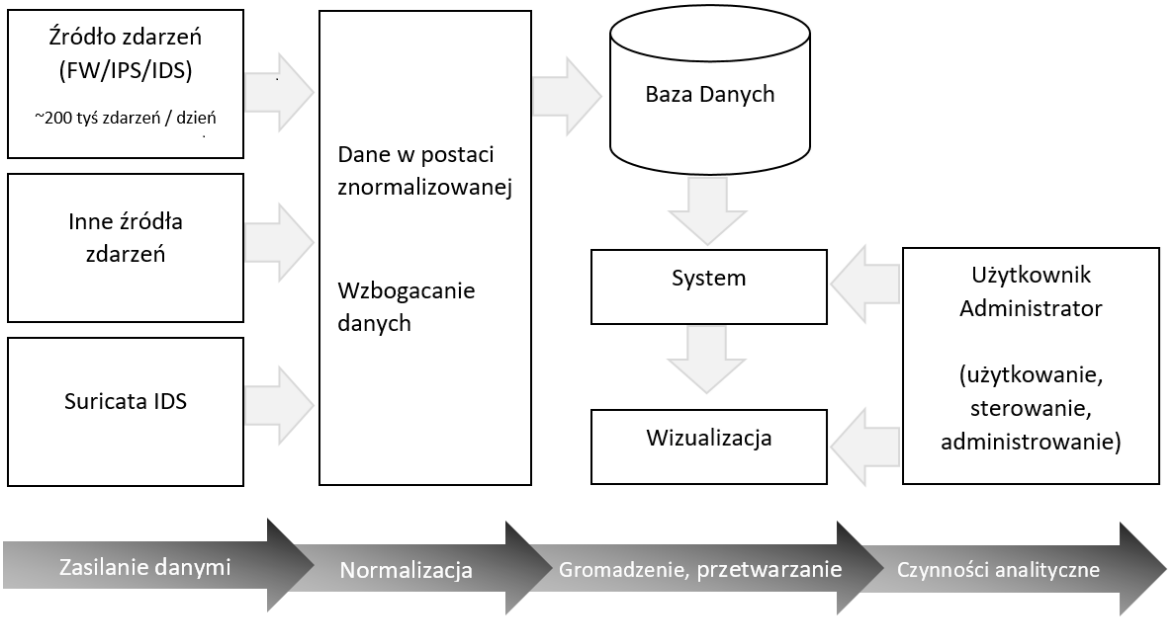
OPIS PRZEDMIOTU ZAMÓWIENIA
„CyberMapa”

Dialog techniczny, w ramach tegorocznej edycji GovTech Polska, ma na celu budowę systemu zobrazowania sytuacji w cyberprzestrzeni – „CyberMapy” - obejmującej zwizualizowanie i przetworzenie zarejestrowanych zdarzeń i incydentów bezpieczeństwa, ich charakteru (port/usługa), takich jak: skan/rekonesans, atak, normalny ruch, anomalie/ anormalny ruch, kierunków oddziaływania (geoIP) wraz z zestawem widżetów (widget – GUI) do filtrowania prezentowanej aktywności oraz wyświetlania informacji statystycznych i trendów.

I. WPROWADZENIE

CyberMapa ma stanowić wysokopoziomowe zobrazowanie sytuacyjne w monitorowanej sieci wspomagające identyfikowanie długofalowych i rozproszonych działań, trendów jak również budowanie strategii obrony przed nowo pojawiającymi się zagrożeniami. Głównymi użytkownikami CyberMapy będą osoby zarządzające ochroną Cyberprzestrzeni jak również osoby odpowiedzialne za budowanie strategii działań. Kluczowym elementem ma być zobrazowanie sytuacji w Cyberprzestrzeni obejmujące zwizualizowanie zarejestrowanych przez komórki bezpieczeństwa archiwalnych i bieżących zdarzeń i incydentów bezpieczeństwa.



Rys. Schemat architektury systemu

System CyberMapy jak przedstawiono na Rys. zasilany jest danymi ze źródeł danych, dane są normalizowane, gromadzone i przetwarzane przez system a następnie wizualizowane na potrzeby analityki i zobrazowania.

Kluczowymi funkcjami CyberMapy są:

a) Umożliwienie zobrazowania geoprzestrzennego cyberzagrożeń wraz z filtrowaniem zdarzeń na potrzeby wsparcia procesu analitycznego stanów w cyberprzestrzeni,
b) Analiza wzorców geoprzestrzennych,
c) Przedstawienie w czasie rzeczywistym zarejestrowanych aktywności w cyberprzestrzeni lub za zadane okno czasowe (zdarzenia archiwalne),
d) Generowanie tzw. heatmap wskazujących obszar geograficzny z którego prowadzono atak/aktywność sieciową,
e) Wyliczanie statystyk i istotnych metryk za zadane okno czasowe.

II. WIZJA

We współczesnym świecie umiejętność ochrony własnych sieci i systemów teleinformatycznych jest jednym z fundamentów bezpieczeństwa, a doskonalenie technologii wykorzystywanych do prowadzenia działań w cyberprzestrzeni oraz szkolenia personelu i ekspertów w tej dziedzinie stało się nowym wyzwaniem
dla Sił Zbrojnych. Kluczowym elementem jest zobrazowanie sytuacji w cyberprzestrzeni obejmującej zwizualizowanie zarejestrowanych zdarzeń bezpieczeństwa przez komórki bezpieczeństwa. Zdolność zobrazowania cyberprzestrzeni jest jednym z podstawowych etapów budowy jednolitego połączonego stanu cyberprzestrzeni (Cyber Common Operational Picture - CyCOP) na potrzeby świadomości sytuacyjnej a także do wsparcia planowania bieżącego i oceny bieżącej sytuacji w cyberprzestrzeni.

Zamawiający zakłada możliwość wykorzystania doświadczeń i końcowego wyniku pracy systemu Cybermapy na potrzeby odrębnych postępowań i opracowania systemu CyCOP wg poniższych założeń:

Etap	Nazwa etapu	Przykładowe rozwiązania
I	System Zobrazowania Cyberprzestrzeni Cybermapa.	Przykłady rozwiązań dostępnych w Internecie https:// geekflare.com/real-time-cyber-attacks).
II	Wykorzystanie lub rozwinięcie systemu Cybermapy do opracowania systemu CyCOP	Towards a Cyber Common Operating Picture, CCDCOE, 2018 Cyber Common Operational Picture: A tool for CyHSA, NATO STO, 2016

Monitorowanie systemów przyłączonych do sieci Internet związane jest z generowaniem, przetwarzaniem i obserwowaniem znacznego wolumenu logów/zdarzeń z zarejestrowanych aktywności (zdarzenia bezpieczeństwa, net-flow, zdarzenia informacyjne, anomalie). Z uwagi na znaczną liczbę danych analityk wykorzystuje dedykowane widoki (dashboard'y), które utrudniają analizę tzw. „big picture" uniemożliwiającą analizę bieżącą (wraz z oknem archiwalnym np. 1 godziny) stanu cyberprzestrzeni będącej w zainteresowaniu operacyjnym.

III. ROZWIĄZANIE

Propozycją Resortu Obrony Narodowej jest opracowanie koncepcji systemu CyberMapa z zastosowaniem technologii wizualizacji (akceleracja sprzętowa, widok 3D) jako graficzny sposób przedstawienia dużego wolumenu zdarzeń bezpieczeństwa np. odpowiadających atakowi DDoS lub rozpoznaniu infrastruktury resortowej), itp., a ponadto koncepcji systemu wyliczania statystyk i istotnych metryk za dane okno czasowe wskazujących potencjalne stany anormalne lub potencjalne zagrożenie w cyberprzestrzeni. Opracowanie architektury systemu, technologii, relacji i interfejsów systemu CyberMapy. Opracowanie metod normalizacji danych (kategorie zdarzeń i sposobu ich odwzorowania graficznego).
System powinien zostać zbudowany w oparciu o rozwiązanie stworzone od podstaw, umożliwiające dostosowanie do potrzeb Zamawiającego w ciągu prowadzenia postępowania/odbiorów etapowych (np. przez tworzenie filtrów wyświetlanej aktywności, wyświetlanie wielu niezależnych widoków mapy, edytowanie graficznej reprezentacji oddziaływania, dodawanie elementów infrastruktury IT na mapę).

<u>Dane systemu CyberMapy:</u>

System Cybermapy pobiera dane do zwizualizowania z systemu bazodanowego, którego dane o zdarzeniach bezpieczeństwa są znormalizowane przez Zamawiającego lub poprzez API CyberMapy. Dodatkowo Zamawiający wymaga aby Wykonawca w pierwszym etapie projektu jako system źródła zdarzeń bezpieczeństwa wykorzystał rozwiązanie Suricata IDS.
Dane znormalizowane będą dostarczone przez Zamawiającego w następującej postaci:
Koncepcja kategorii zdarzeń:

- SCAN/REKONESANS– zdarzenie związane ze skanowaniem/rozpoznaniem,

- MALWAREC2– zdarzenie zawiązane z C2 malware (lub inne zdarzenie którego źródłem jest wnętrze monitorowanego systemu a które terminuje się poza monitorowanym system),
- ATTACK – zdarzenie związane z atakiem w cyberprzestrzeni,
- ANOMALY – zdarzenie związane z wykryciem anomalii, podejrzanej aktywności,
- REGULAR/NETFLOW – zdarzenie związane z normalnym ruchem.

Koncepcja atrybutów zdarzeń: SRC_IP, DST_IP, SRC_PORT, DST_PORT, DOMENA, PROTOKÓŁ (UDP,TCP, FTP, HTTP), SEVERITY (HIGH, MEDIUM, LOW), COUNT (liczba wystąpień, domyślnie 1), RAW_MSG (informacja o zdarzeniu z systemu bezpieczeństwa), BLOCKED (1 lub 0, jeżeli zdarzenie zostało zablokowane przez system bezpieczeństwa).

Zamawiający oczekuje, że CyberMapa umożliwi wizualizację zdarzeń znormalizowanych, których koncepcję normalizacji przedstawiono powyżej oraz zdarzeń platformy Suricata IDS (normalizacja i sposób przedstawienia wyników do opracowania przez Wykonawcę).

Systemy teleinformatyczne do zobrazowania:

CyberMapa przyjmuje informacje ze źródeł danych do wizualizacji. Zakłada się wizualizowanie następujących systemów:

- System teleinformatyczny połączony do sieci Internet (źródłem danych mogą być urządzenia brzegowe w systemie, urządzenia wewnętrze lub urządzenia umiejscowione w dowolnym miejscu w cyberprzestrzeni np. do monitorowania ruchu transgranicznego),
- System teleinformatyczny autonomiczny odłączony od sieci Internet (źródłem danych mogą być urządzenia monitorujące stan wewnątrz systemu).

Wizualizowane zdarzenia opisane są za pomocą adresów IP (SRC, DST). Obiekty CyberMapy powinny posiadać przypisane adresy IP lub grupę adresów IP (podsieć) np. Monitorowany system np. 91.231.xx.0/24, monitorowany obiekt 91.231.xx.xx. Wizualizowane zdarzenia przedstawiane są pomiędzy obiektami które posiadają adresację. W przypadku obiektów którym nie przypisano adresacji należy wykorzystać wzbogacanie danych (data enrichment) o dane geolokalizacji.

Niezbędne funkcje systemu:

- Wizualizacja na mapie zarejestrowanych incydentów. Informacja o lokalizacji incydentu będzie powiązana z lokalizacją urządzenia, z którym związany będzie zgłoszony alarm.
- CyberMapa ma umożliwiać integrację z innymi systemami poprzez API CyberMapy np. systemami SecOps Zamawiającego.
- Możliwość wizualizacji wybranego zdarzenia i incydentu w czasie zbliżonym do rzeczywistego (ze stałym opóźnieniem). Zamawiający przewiduje występowanie stałego opóźnienia na potrzeby grupowania wielu identycznych zdarzeń i przedstawienia zgrupowanych zdarzeń z dodatkowym efektem graficznym.
- Prezentowanie map wskazujących ilość zdarzeń, incydentów w danej lokalizacji. Wzrost zarejestrowanych zdarzeń w jednostce czasu (np. na sekundę, na minutę) będzie skutkował powiększaniem się punktu (heatmapay) wskazującego lokalizację.
- Prezentację regionów na których występują zdarzenia lub incydenty w różnych kolorach w zależności od nasilenia wystąpień np. w kolorze szarym dla regionów gdzie ilość wystąpień jest bliska zeru a w kolorze czerwonym dla regionu gdzie ilość wystąpień jest bardzo wysoka. W takim przypadku widok będzie posiadał legendę odzwierciedlającą kolor na ilość wystąpień.
- Odświeżanie (z określonym interwałem czasowym) punktów lokalizacji wraz ze zmianami rejestrowanych alarmów, zdarzeń i incydentów.
- Wizualizację elementów infrastruktury teleinformatycznej na mapie Polski z możliwością rozszerzenia na tereny poza krajem. Poszczególne elementy będą wizualizowane w postaci odpowiednich ikon. W przypadku dostępności informacji o połączeniach pomiędzy poszczególnymi elementami, będą one prezentowane na mapie.
- Nanoszenie lokalizacji urządzeń na mapę może odbywać się na podstawie informacji o miejscowości zawartej np. w informacji przekazanej protokołem SNMP (na terenie objętym granicami Polski).
- Możliwość odwzorowania obiektów na CyberMapie wprowadzonych przez użytkownika np. systemu teleinformatycznego lub infrastruktury teleinformatycznej własnej/przeciwnika, obiektu (serwer, komputer, router, urządzenie), relacji pomiędzy obiektami np. połączenie liniami. W przypadku określenia relacji między obiektami zdarzenia bezpieczeństwa przebiegają po określonych liniach łączących obiekty, grubość linii łączącej obiekty wzrasta wraz z natężeniem ruchu i ilością zdarzeń.

- Skalowania widoku mapy wraz z opcją klastrowania prezentowanych informacji. Zmniejszanie widoku będzie powodowało odświeżenie widoku prezentowanych informacji i dostosowanie ich poprzez agregację do skali widoku (np. połączenie alarmów z dwóch lokalizacji w Warszawie w jeden punkt).
- Dostosowanie widoku mapy przez użytkownika poprzez jej przesuwanie, skalowanie.
- W przypadku dużej ilości np. zdarzeń zarejestrowanych w krótkim czasie system ma agregować dane w celu lepszego, czytelniejszego zobrazowania.
- Wyświetlenie szczegółów dla danej lokalizacji. W przypadku kliknięcia na ikonę reprezentującą urządzenie/oprogramowanie będzie możliwe wyświetlenie jego podstawowych właściwości. W przypadku kliknięcia na ikonę reprezentującą lokalizację wystąpienia zdarzeń i incydentów będzie możliwe wyświetlenie informacji statystycznych dla tej lokalizacji, w tym: listy zdarzeń, listy incydentów, listy urządzeń występujących w lokalizacji.
- Filtrowanie wizualizowanych informacji np. tylko alarmy SIEM, zarejestrowane incydenty, zdarzenia określonego typu, itd.
- Wizualizacje danych historycznych, za zadany okres.
- Wizualizację gromadzonych danych w postaci trendów, statystyk
- Filtrowanie danych przy wizualizacji trendów np. w okres czasu, lokalizacja, typ zdarzenia, alarmu.
- Wizualizację na mapie ataków (mapa ataków) pochodzących z sieci zewnętrznej. Wizualizacja może być realizowana w oparciu o animację pomiędzy geolokalizacją nadawcy i geolokalizacją odbiorcy.
- Wyświetlanie ataków na mapie całego świata z możliwością przybliżania miast, ulic.
- Możliwość wyłączenia włączenia różnych styli prezentacji cybermapy np. z ulicami, miastami lub bez, wyłączenie heatmap itd.
- Wizualizację na mapie nasilenia ataków z danej lokalizacji na odbiorcę np. poprzez wyróżnienie punktu na mapie wskazującego lokalizację odbiorcy.
- Filtrowanie danych przy wizualizacji ataku, np. poprzez wskazanie lokalizacji docelowej ataków.
- CyberMapa powinna działać bez konieczności połączenia do Internetu.
- Dostępność interfejsu wizualizacji dla użytkowników poprzez przeglądarkę WWW.
- Dostarczenie użytkownikowi kilku widoków jednocześnie, np. w celu wyświetlenia na kilku monitorach osobnych widoków.

- Dostęp wyłącznie dla zalogowanych użytkowników o przypisanych niezbędnych uprawnieniach. Jeden użytkownik będzie miał możliwość otworzenia kilku osobnych okien przeglądarki z różnymi widokami zobrazowania.
- Gromadzenie wszystkich zdarzeń, alarmów i incydentów z minimum ostatnich 30 dni. Dane te powinny być wykorzystane do wizualizacji.
- Możliwość tagowania poszczególnych zdarzeń oraz wyszukiwanie i wyświetlanie na podstawie tagów.

Zamówienie obejmuje:

- Wykonanie i budowę systemu.
- Wykonanie projektu wdrożenia.
- Dostarczenie niezbędnego sprzętu i oprogramowania umożliwiającego prawidłowe działanie CyberMapy.
- Wstępną konfigurację parametrów działania komponentów systemu.
- Wykonawca musi przeprowadzić scenariusze testowe - eksperymenty potwierdzające przydatność rozwiązania.
- Warsztaty lub szkolenie przedstawiające szczegóły implementacji, realizowane w miejscu wdrożenia lub we wskazanym przez zamawiającego miejscu wraz z opracowaniem materiału instruktażowo-szkoleniowego.
- Dokumentację powykonawczą systemu.
- Minimum roczną gwarancję na naprawę błędów oprogramowania.
- Minimum roczne wsparcie producenta rozwiązania obejmujące wdrażanie dodatkowych funkcjonalności na potrzeby Zamawiającego, obejmujące 250 godzin wsparcia inżynierskiego.

Wymagania technologiczne:

- Przedstawione rozwiązanie nie powinno wykorzystywać rozwiązań dedykowanych do problemów BigData. Przeprowadzona analiza przez Zamawiającego wykazała, że problem BigData w systemie CyberMapa nie występuje.
- Wydajne do zobrazowania wielu elementów, przedstawienia efektów graficznych i zobrazowania środowisko wizualizacji wykorzystujące sprzętową akceleracje.

IV. **Wstępne mierniki skuteczności wdrożenia**

V. **Wstępne kryteria I Etapu**

VI. Wstępne kryteria II Etapu

VII. Podsumowanie:

Nagrody I etap:
Zwrot kosztów II etap:

Oczekiwany budżet przeznaczony na cały konkurs:
Oczekiwany czas wdrożenia: 12 miesięcy