OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest udostępnienie rozwiązania informatycznego obejmującego dostęp do platformy internetowej (aplikacji webowej) oferującej funkcjonalność Systemu służącego do dostarczania informacji z zakresu Cyber Threat Intelligence (rozpoznawanie zagrożeń w cyberprzestrzeni) o poziomie operacyjnym na rzecz podmiotów KSC (Krajowego Systemu Cyberbezpieczeństwa) zapewniających bezpieczeństwo teleinformatyczne na poziomie krajowym.

W ramach Opisu Przedmiotu Zamówienia obowiązują następujące pojęcia:

1. OPZ - Opis Przedmiotu Zamówienia;
2. Podmioty KSC – 2 wskazanych przez Zamawiającego Instytucji (beneficjentów), które otrzymają dostęp do Systemu (w tym Instytucja Zamawiającego);
3. System - rozwiązanie informatyczne będące przedmiotem zamówienia obejmujące funkcjonalność chmurowej platformy służącej do dostarczania informacji z zakresu Cyber Threat Intelligence o poziomie operacyjnym, którego funkcjonalności opisuje OPZ;
4. Licencja – konta lub klucze lub inne środki pochodzące bezpośrednio od Producenta Systemu pozwalające na uzyskanie dostępu do Systemu przez użytkownika na czas określony w OPZ i wykorzystanie wszystkich funkcjonalności Systemu, które w przypadku danego konta powinny się zawierać;
5. Udostępnienie – dostarczenie Licencji na dostęp do usługi dla wskazanych użytkowników do osoby lub osób wskazanych przez Zamawiającego;

# Przedmiot zamówienia

1. Przedmiotem zamówienia jest udostępnienie przez Wykonawcę na rzecz Zamawiającego rozwiązania informatycznego obejmującego dostęp do platformy internetowej (aplikacji webowej) oferującej funkcjonalność Systemu służącego do dostarczania informacji z zakresu Cyber Threat Intelligence (rozpoznawanie zagrożeń w cyberprzestrzeni) o poziomie operacyjnym na rzecz podmiotów KSC (Krajowego Systemu Cyberbezpieczeństwa) zapewniających bezpieczeństwo teleinformatyczne na poziomie krajowym.
2. System musi zapewnić mechanizmy dodatkowego zabezpieczenia kont użytkowników takie jak:
   1. Uwierzytelnianie wieloskładnikowe;
   2. Automatyczne wylogowanie konta po określonym czasie nieaktywności użytkownika w tym przynajmniej po 30 minutach nieaktywności;
   3. Kontrolę dostępu opartą na rolach (tak zwany "Role Based Access Control").
3. Producent musi stale utrzymywać i certyfikować bezpieczeństwo swojego Systemu oraz jego bazy danych poprzez zgodność z normami z zakresu cyberbezpieczeństwa w tym przynajmniej ISO 27001 oraz jedno spośród wymienionych poniżej:
   1. NIST Cybersecurity Framework.
   2. ISO 27002.
   3. SOC2.
   4. NERC-CIP.
   5. HIPAA.
   6. GDPR.
   7. FISMA.
4. Skuteczność Systemu musi być opisana i sklasyfikowana w publicznie dostępnych raportach i analizach, przynajmniej Frost Radar: Cyber Threat Intelligence Market lub rónoważnych.
5. System musi posiadać wyłącznie scentralizowane bazy danych gwarantujące jednakowy dostęp dla wszystkich użytkowników. **Nie dopuszcza się rozwiązania kreującego indywidualną bazę dla indywidualnych klientów lub użytkowników.**
   1. Dane zawarte w Systemie muszą pochodzić z przynajmniej ostatnich 3 lat od dnia składania ofert;
   2. System nie może być ograniczony tylko do wyznaczonych regionów geograficznych;
   3. System nie może usuwać zmagazynowanych danych. Wyjątek stanowią portale

społecznościowe z własną polityką prywatności.

1. System musi być udostępniony w formie dostępu do chmurowej platformy Producenta. Dostęp do Systemu musi być zgodny z pkt. [1](#_bookmark0) Wymagań Dotyczących Oferowanego Rozwiązania.
2. Funkcjonalności Systemu muszą obejmować wszystkie zawarte w punktach od 1 do 8 Wymagań Dotyczących Oferowanego Rozwiązania.
3. System musi zapewnić dostęp za pośrednictwem API.
4. System ma umożliwić integracje z innymi systemami zgodnie z pkt. [9](#_bookmark1) Wymagań Dotyczących

Oferowanego Rozwiązania.

1. Każde konto w ramach Systemu musi posiadać wsparcie techniczne Producenta zgodnie z pkt. [10](#_bookmark2) Wymagań Dotyczących Oferowanego Rozwiązania.
2. Udostępnienie wraz z dostarczeniem dokumentacji użytkowej musi być zgodne z pkt. [11](#_bookmark3) Wymagań Dotyczących Oferowanego Rozwiązania.
3. System musi wymagać tylko jednego konta od użytkownika, niezależnie od ilości funkcjonalności,

do których użytkownik ma dostęp.

# Wymagania dotyczące oferowanego rozwiązania

1. **DOSTĘP DO SYSTEMU**
   1. Dostęp do Systemu musi odbywać się za pośrednictwem dedykowanego interfejsu www, interfejsu API oraz dedykowanych i natywnych integracji z innymi rozwiązaniami bezpieczeństwa.
   2. Dostęp do Systemu poprzez interfejs www musi być możliwy poprzez interfejs graficzny w postaci dynamicznej aplikacji internetowej (ang. dynamic website).
      1. Interfejs www Systemu musi być dostępny przez wszystkie z niżej wymienionych

przeglądarek:

* + - 1. Google Chrome;
      2. Mozilla Firefox;
      3. Opera;
      4. Microsoft Edge;
    1. Dostęp do Systemu musi być możliwy jedynie poprzez kanały szyfrowane jak HTTPS lub

równoważny zapewniający poufność przesyłanych danych.

* 1. Wykonawca musi zapewnić nielimitowaną liczbę kont użytkowników dla wszystkich wskazanych w OPZ funkcjonalności dla wskazanych użytkowników z podmiotów KSC
  2. W przypadku wskazania przez Zamawiającego zamiaru przydzielenia Licencji dla kolejnego użytkownika z danego podmiotu lub zmiany zakresu funkcjonalności, do których użytkownik posiada dostęp, Wykonawca musi wykonać wszelkie niezbędne czynności, by zrealizować zamiar Zamawiającego w tym również przydzielić kolejne Licencje.
  3. Dostęp do Systemu musi być zapewniony przez (12/24/36) miesięcy od momentu Udostępnienia.
     1. W przypadku uzyskania Licencji dla nowego użytkownika po momencie początkowego Udostępnienia jej ważność trwa krócej - do momentu upłynięcia 12/24/36 miesięcy od początkowego Udostępnienia.
  4. Dostępność Systemu poprzez dedykowany interfejs WWW i API musi wynosić co najmniej 99,9% czasu ważności licencji. Przykładowo:

„W przypadku licencji na czas 365 dni dostępność musi wynosić 365 x 0,999 = 364,635 co przekłada się na 364 dni 12 godzin 42 minuty.”

## Moduł-1 Funkcjonalność rozpoznawania zagrożeń w cyberprzestrzeni

* 1. System musi zapewnić funkcjonalność automatycznego zbierania danych z cyberprzestrzeni z zakresu Cyber Threat Intelligence.
  2. System musi w sposób stały (w czasie rzeczywistym) zbierać (kolekcjonować) dane z:
     1. Open, deep oraz dark web, w tym:
        1. Media społecznościowe;
        2. Portale informacyjne;
        3. Fora;
        4. Blogi;
        5. Grupy na komunikatorach.
        6. Fora hakerskie (w tym fora wymagające dodatkowej weryfikacji);
        7. Portale i fora dostępne przez sieć tor;
        8. Portale i fora w dark web;
     2. Kanałów IRC;
     3. Stron typu pastebin;
     4. Stron typu onion dostępnych przez sieć tor;
     5. Repozytoriów kodu.
  3. System musi kolekcjonować dane:
     1. Z minimum 1500 portali dark web i forów hakerskich;
     2. Dane na temat loC (Indicator of Compromise) typu:
        1. Adresy IP;
        2. Domeny;
        3. Adresy URL;
        4. Hash'e plików, ze źródeł pochodzących od firm trzecich, nie mniej niż 50 różnych

"Threat Feeds".

* + 1. Dane z opracowań technicznych z zakresu cyberbezpieczeństwa, przynajmniej:
       1. Raporty i analizy bezpieczeństwa producentów oprogramowania;
       2. Raporty i analizy bezpieczeństwa dostawców rozwiązań cybersecurity;
       3. Analizy malware.
    2. Dane z:
       1. Źródeł trzecich, takich jak: Shodan, Polyswarm, URLscan, itp.;
       2. Zaufanych dostawców: CSIRT'ów, ISAC, agencji rządowych, VISA, itp.;
    3. Dane pochodzące z bezpośredniej interakcji z cyberprzestępcami oraz użytkownikami w dark web;
    4. Aktywności sieci typu botnet.
  1. Funkcjonalność wywiadu w cyberprzestrzeni dostępna w Systemie musi zawierać:
     1. Analizę zagrożeń w czasie rzeczywistym, dynamiczną klasyfikację oraz dane wywiadowcze na temat grup cyberprzestępczych, operacji, podatności, złośliwego oprogramowania, TTP oraz innych loC wraz z pełnym kontekstem;
     2. Wizualizację zagrożeń, indeksowanie danych opublikowanych w sieci Internet z uwzględnieniem źródeł typu open, deep, oraz dark web odnoszących się do cyberzagrożeń, terroryzmu, geopolitycznych, przestępczych - stałe indeksowanie i analiza z wykorzystaniem NLP (Natural Language Processing);
     3. Historyczne dane o zagrożeniach oraz ich archiwum (baza danych z minimum 10 lat), z minimalną ilością miliarda obiektów - skorelowanych i dostarczonych w formie danych wywiadowczych;
     4. Szybkie przejścia w formie "od ogółu do szczegółu” do realizacji szczegółowej analizy referencji oraz obiektów;
     5. Artykuły i notatki opracowane przez dział analityczny Producenta.
  2. System musi w sposób automatyczny budować ontologie wewnątrz swojej bazy pomiędzy obiektami skutkujące dostarczeniem kompletnej informacji typu intelligence. Przykładowo: „Conti Gang (grupa cyberprzestępcza) wykorzystuje Conti Ransomware (złośliwe oprogramowanie), które exploituje CVE-2021-1675 (podatność) i wykorzystuje 1.2.3.4 (adres IP) do komunikacji C2 z ofiarą ACME (firma/organizacji) zlokalizowaną w Polsce (kraj)”.
  3. System musi wykorzystywać algorytmy uczenia maszynowego, Natural Language Processing, wykrywanie wzorców dla celów kolekcji, indeksowania i analizy danych.
  4. System musi walidować dane ze źródeł przed oficjalnym dodaniem źródła do Systemu.
  5. System musi wspierać algorytmy Natural Language Processing oraz deep data analysis dostępne

minimum dla:

* + 1. Angielski;
    2. Rosyjski;
    3. Arabski;
    4. Niemiecki;
    5. Chiński;
    6. Japoński;
    7. Francuski;
    8. Polski;
    9. Hiszpański.
  1. System musi wykorzystywać wzorce i wyrażenia regularne celem detekcji:
     1. Adresów IP;
     2. Adresów URL;
     3. Domen;
     4. Hash'y plików;
     5. Nazw użytkowników;
     6. Adresów E-mail;
     7. Miast;
     8. Lokalizacji;
     9. Firm.

Wewnątrz:

* + 1. Tekstu pisanego w różnych językach;
    2. Kodu źródłowego w różnych językach programowania;
    3. Plikach z logami;
    4. Obrazów (OCR).
  1. System musi posiadać licencjonowany interfejs API umożliwiający pobranie listy feed'ów w formatach JSON, TAXII oraz CVS-STIX.
     1. Interfejs API, nie może posiadać ograniczeń na liczbę oraz na rozmiar zapytań.
  2. System musi udostępniać graficzny kreator typu API Swagger automatycznie generujący kod zapytania dla: cURL, Python, JavaScript.
  3. System musi umożliwiać eksport danych z platformy w różnych formatach, minimum:
     1. JSON;
     2. CSV;
     3. STIX;
     4. PPT;
     5. PNG;
     6. PDF;
     7. DOC.
  4. System musi posiadać integracje z innymi systemami z dziedziny cyberbezpieczeństwa,

przynajmniej z:

* + 1. Splunk;
    2. Palo Alto Networks;
    3. Microsoft;
    4. Rapid7
    5. Trend Micro
    6. Oraz udostępniać dostęp API RESTowe

## Moduł-2 Funkcjonalność Priorytetyzacji Podatności

* 1. System musi zapewnić funkcjonalność służącą do wsparcia procesu priorytetyzacji podatności pod

kątem kolejności działań remediacyjnych.

* + 1. System musi umożliwiać transparentną priorytetyzację podatności bazując na posiadanych w bazie danych Systemu zasobach oraz danych zewnętrznych.
    2. System musi wspierać automatyczną ocenę ryzyka podatności określonych jako identyfikatory CVE.
  1. Mechanizm oceny ryzyka w Systemie musi bazować na dedykowanych regułach wyzwalanych automatycznie przez System, których włączenie skutkuje konkretną oceną ryzyka wyrażoną liczbowo.
  2. System musi prowadzić ocenę ryzyka podatności na bazie informacji ze źródeł zewnętrznych,

przynajmniej:

* + 1. Raporty bezpieczeństwa;
    2. NIST;
    3. NVD;
    4. Analizy i badania;
    5. Notatki i artykuły producentów oprogramowania;
    6. Fora Dark Web;
    7. Repozytoria kodu (np. GitHub).
  1. System musi prowadzić ocenę ryzyka podatności będących w tak zwanej fazie "PreNVD" - zarezerwowane identyfikatory CVE bez oceny ryzyka CVSS.
     1. System musi generować alarm w sytuacji pojawienia się krytycznej podatności w fazie "PreNVD" dotykającej skonfigurowany stos technologiczny.
  2. Ocena ryzyka w Systemie musi bazować minimum na:
     1. Faktach o wykorzystaniu podatności przez aktywnie działające i infekujące złośliwe

oprogramowanie;

* + 1. Wskaźnik CVSS;
    2. Poziom krytyczności według producenta podatnego oprogramowania;
    3. Publicznie dostępny i zweryfikowany kod Proof-of-Concept umożliwiający exploitację podatności;
    4. Faktach o zaangażowaniu w bieżącą kampanię cyberprzestępczą.
  1. System musi umożliwiać przeszukiwanie i wizualizację danych dla dowolnego identyfikatora CVE. Jakiekolwiek limity na zakres, częstotliwość oraz liczbę zapytań są niedopuszczalne.
  2. System musi dodawać dane i kontekst z NVD w sytuacjach, gdzie takowe dane zostały

opublikowane.

* 1. System musi generować alarm w sytuacji pojawienia się nowej krytycznej podatności na skonfigurowany stos technologiczny.
  2. System musi definiować nową krytyczną podatność nie tylko na podstawie jej wieku, ale również na bazie zmieniającej się w czasie oceny ryzyka. Przykładowo: „CVE z 2021 roku jest uznane za nową krytyczną podatność jeżeli jego ocena ryzyka gwałtownie wzrosła do poziomu krytycznego z powodu exploitacji w bieżących atakach”.
  3. System musi generować alarm w sytuacji wykrycia rozmów (na minimum: forach hakerskich, grupach Telegram) na temat exploit'a lub exploit-kit'a na podatność obecną na skonfigurowanym stosie technologicznym.
  4. System musi generować alarm w sytuacji pojawienia się nowego kodu typu Proof-of-Concept

umożliwiającego wykorzystanie podatności obecnej na skonfigurowanym stosie technologicznym.

* 1. System musi generować alarm w sytuacji wykrycia CVE będącego obecnie wykorzystywanym przez aktywny malware. W ramach alarmu System musi dostarczać informacje na temat: informacji ogólnych o podatności, powodów i dowodów podniesienia alarmu (kontekst) oraz listy podatnych produktów wraz z ich wersjami.
  2. System musi dostarczać informacji na temat trendów w zakresie podatności oprogramowania.
  3. System musi dostarczać widok obrazujący obecne trendy dla podatności.
  4. System musi dostarczać widok prezentujący aktualne trendy w świecie podatności wyfiltrowane

wyłącznie dla CVE obecnych wyłącznie na wskazanym stosie technologicznym.

* 1. System musi dostarczać dedykowany widok prezentujący minimum: listę wygenerowanych alarmów dotyczących podatności, listę podatności koniecznych do obsługi z podziałem na kategorie związane z cyklem życia podatności.

## Moduł-3 Funkcjonalność Wyszukiwania Zagrożeń

* 1. System musi zapewnić funkcjonalność wyszukiwania zagrożeń w zakresie cyberbezpieczeństwa

(ang. threat hunting).

* 1. System musi dostarczać automatycznej oceny ryzyka dla loC typu:
     1. Adres IP;
     2. Domena;
     3. URL;
     4. Hash;
     5. Identyfikator CVE;
     6. Ocena ryzyka subskrypcji.
  2. System musi bazować na transparentnych regułach ryzyka produkujących finalną wartość liczbową

ryzyka.

* 1. Reguły muszą stanowić zestaw opisujący poziom niebezpieczeństwa i ryzyka dedykowany dla

każdego z typów loC.

* 1. System musi dostarczać informacji na temat każdego loC za pośrednictwem centralnej wizualizacji

zawierającej:

* + 1. Metadane dla loC;
    2. Ocenę ryzyka (wyrażoną liczbowo);
    3. Uruchomione reguły;
    4. Inne skorelowane loC;
    5. Ontologie do grup hakerskich, typów ataków, kodów MITRE oraz złośliwego

oprogramowania.

* 1. System musi dostarczać kontekst dla loC typu:
     1. Adres lP;
     2. Domena;
     3. URL;
     4. Hash;
     5. CVE.
  2. System musi posiadać informacje WHOIS.
  3. System musi dostarczać wizualizacje opisujące konkretne grupy cyberprzestępcze w sposób scentralizowany i zawierające komplet najważniejszych informacji o grupie lub osobie, minimum:
     1. Wykorzystywane wektory ataku;
     2. Identyfikatory z MITRE ATT&CK Framework;
     3. Wykorzystywany malware;
     4. Używane loCs;
     5. Używane technologie;
     6. Kategoria i profil działalności grupy;
     7. Referencje do grupy;
     8. Nazwy użytkowników na forach lub adresy e-mail;
     9. Kraje pochodzenia i kraje działania;
     10. Cele grupy;
     11. Artykuły opracowane przez zespół badawczy dostawcy.
  4. System musi monitorować minimum:
     1. 100 różnych grup APT;
     2. 150 różnych grup haktywistycznych.
  5. System musi umożliwiać określenie i monitorowanie grup cyberprzestępczych atakujących

organizacje i firmy ze zdefiniowanych sektorów działalności.

* 1. System musi dostarczać dedykowany widok prezentujący grupy cyberprzestępcze o najwyższym

priorytecie (stanowiące największe zagrożenie) z perspektywy chronionej organizacji.

* 1. System musi zapewniać dostęp do materiałów opracowywanych przez zespół analityczny producenta w formie artykułów typu:
     1. Krótki raport;
     2. Profil i opis złośliwego oprogramowania;
     3. Profil i opis narzędzia;
     4. Profil i opis grupy cyberprzestępczej;
     5. Planowane ataki i zagrożenia;
     6. Instancje TTP;
     7. Analiza zagrożenia;
     8. Instrukcje do threat hunting'u.
  2. System musi zapewniać dostęp i alarmowanie o specyficznych wskazówkach o zagrożeniach, np. notyfikacja o cyberprzestępcy, który opublikował wykradzioną bazę danych z konkretnej firmy lub prób sprzedaży dostępu zdalnego (np. VPN lub RDP) do konkretnej firmy lub organizacji w określonym kraju.
  3. System musi zapewniać dostęp i alarmowanie o nowych instancjach TTP (Technik, Taktyk i Procedur), np. nowej technice ataku umożliwiającej wykorzystanie podatności konkretnego oprogramowania.
  4. System musi zapewniać dostęp i alarmować o nowych instrukcjach dla śledztwa (tzw. hunting'u) dla

zagrożeń, np. instruktaż jak zidentyfikować ślady ataku lub zagrożenia w swojej infrastrukturze.

* 1. System musi pozwalać na pobranie reguł detekcyjnych bezpośrednio w platformie. Reguły detekcyjne muszą mieć odniesienie do korespondującego z nimi malware'u lub typu ataku bezpośrednio z widoku centralnego.
  2. System musi posiadać dedykowane, dodatkowo licencjonowane API, umożliwiające automatyczne pobranie reguł detekcyjnych.
  3. System musi pozwalać na korelację wewnętrznych incydentów bezpieczeństwa z zewnętrznymi danymi wywiadowczymi celem przyspieszenia identyfikacji incydentów krytycznych z perspektywy organizacji.
  4. System musi umożliwiać detekcję, monitorowanie i alarmowanie o stronach typu phishing oraz repozytoriach malware.
  5. System musi posiadać graficzny interfejs do budowania zapytań do bazy danych Systemu:
     1. Graficzny interfejs musi wspierać wykorzystywanie operatorów logicznych typu AND i OR;
     2. Graficzny interfejs musi wspierać prezentację kilku osobnych zapytań w ramach jednego zestawu danych;
     3. Graficzny interfejs musi wspierać wyszukiwanie i alarmowanie o nowym, zweryfikowanym kodzie typu proof-of-concept, umożliwiającym wykorzystanie podatności konkretnego oprogramowania;
     4. Graficzny interfejs musi wspierać wyszukiwanie i alarmowanie na temat dowolnego słowa

kluczowego w dowolnym zasobie w dowolnym czasie.

* 1. System musi prezentować wyniki zapytania w kilku różnych formatach, w tym:
     1. Widok tabelaryczny;
     2. Oś czasu;
     3. Mapa;
     4. Mapa źródeł.
  2. System musi umożliwiać eksport danych z platformy minimum w formatach CSV, JSON, DOCX, PNG lub PDF.
  3. System musi umożliwiać zapisanie opracowanych zapytań, celem ich przyszłego ponownego uruchomienia w platformie.
  4. System musi zezwalać na współdzielenie zapytań z innymi użytkownikami platformy z nadaniem

uprawnień, minimum: tylko do odczytu oraz do odczytu i edycji.

* 1. System musi wspierać budowanie autorskich alarmów bazujących na nowych zdarzeniach lub nowych referencjach pasujących do opracowanego wcześniej zapytania, celem implementacji niestandardowego/własnego scenariusza detekcji.
  2. Mechanizm alarmowania w Systemie musi umożliwiać generowanie alarmów w zadanych

interwałach np. 15 minut, 1 godzina, 8 godzin, dobowo, tygodniowo.

* 1. Mechanizm alarmowania w Systemie w trybie dobowym musi umożliwiać konfigurację dokładnego

czasu wygenerowania i otrzymania skumulowanego alarmu.

* 1. Alarmy wygenerowane przez System muszą być dostarczone m.in. w formie notyfikacji e-mail.
  2. System musi wspierać konfigurowanie listy odbiorców alarmu per reguła alarmująca.
  3. System musi zapewniać alarmowanie o trendach cyberprzestępczych oraz malware'owych na sektor finansowy i płatności.
  4. System musi zapewniać alarmowanie na temat cyberszpiegostwa w kontekście:
     1. Grup APT;
     2. Malware'u typu Remote Access Trojans;
     3. Znanych ofiar ataków.
  5. System musi zapewniać alarmowanie i monitorowanie o modyfikacjach realizowanych przez

cyberprzestępców w exploit kit'ach.

* 1. System musi zapewniać monitorowanie i alarmowanie na temat globalnych trendów

cyberbezpieczeństwa, w kontekście:

* + 1. Najczęstszych i trendujących ofiar;
    2. Najnowszych i trendujących metodach ataku;
    3. Najnowszych i trendujących operacji.
  1. System musi generować alarm o trendach w cyberzagrożeniach dla konkretnych sektorów, np.:

rządowy, transportowy, energetyczny, bankowość, ICS/SCADA.

* 1. System musi generować alarm o trendach w cyberzagrożeniach dla sektora działania chronionej organizacji.
  2. System musi umożliwiać alarmowanie o kampaniach typu phishing lub spam.
  3. System musi zapewnić dostęp do własnego systemu klasy Sandbox umożliwiającego analizę plików celem detekcji malware.
     1. System Sandbox musi umożliwiać transfer próbek do analizy przez minimum:

1. Transfer pliku;
2. Przekazanie URL z plikiem;
3. Interfejs API.
   * 1. System Sandbox musi umożliwiać transfer i analizę plików w formie archiwum chronionego hasłem;
     2. System Sandbox musi umożliwiać transfer i analizę plików o rozmiarze minimum 3GB;
     3. System Sandbox nie może redystrybuować zawartości analizowanego pliku;
   1. System musi udostępniać dedykowane widoki prezentujące:
      1. Globalne trendy zagrożeń;
      2. Szczegółowe trendy zagrożeń dla sektora bankowego;
      3. Szczegółowe trendy zagrożeń dla sektora ICS/SCADA;
      4. Szczegółowe trendy zagrożeń dla sektora rządowego;
      5. Szczegółowe trendy zagrożeń dla sektora energetycznego;
      6. Szczegółowe trendy zagrożeń dla sektora transportowego.

## Moduł-4 Funkcjonalność Analizy Ryzyka w Łańcuchu Dostaw

* 1. System musi zapewnić funkcjonalność obejmującą automatyczną ocenę ryzyka dla każdej firmy i organizacji z perspektywy cyberbezpieczeństwa.
  2. System musi przeprowadzać ocenę ryzyka dla firm i organizacji w skali globalnej. Ocena ryzyka musi być transparentna dzięki prezentacji czytelnych argumentów i dowodów, na bazie których ocena liczbowa została określona.
  3. System musi kalkulować ryzyko na bazie minimum:
     1. incydentów bezpieczeństwa związanych z analizowaną instytucją;
     2. złośliwej komunikacji sieciowej wychodzącej z analizowanej instytucji;
     3. skali zainteresowania instytucją na Dark Web oraz forach cyberprzestępczych;
     4. wolumenu wyciekniętych poświadczeń;
     5. podatności publicznych zasobów cyfrowych;
     6. bezpieczeństwa witryn internetowych należących do analizowanej instytucji.

Naruszenia w każdej z powyższych kategorii muszą być zdefiniowane i widoczne w platformie oferowanej przez subskrypcję.

* 1. System musi posiadać dedykowany widok typu dashboard, gdzie zaprezentowane są trendy i aktualny status bezpieczeństwa monitorowanych organizacji i firm.
  2. System musi zapewniać monitorowanie wybranego łańcucha dostaw, przynajmniej dla:
     1. Firm partnerskich;
     2. Organizacji podległych;
     3. Organizacji zależnych;
     4. Dostawców;
     5. Producentów;
     6. Organizacji stowarzyszonych.
  3. System musi zapewniać alarmowanie i notyfikację o podniesieniu się poziomu ryzyka dla dowolnej z monitorowanych firm i organizacji.
  4. System musi umożliwiać przeprowadzenie analizy ryzyka dla dowolnej firmy lub organizacji, nie zdefiniowanej na liście monitorowania, w trybie na żądanie. Celem jest możliwość wdrożenia procesu weryfikacji dostawcy lub szybkiej walidacji poziomu bezpieczeństwa organizacji zewnętrznej.
  5. System musi generować alarm w sytuacji identyfikacji krytycznej podatności obecnej na zasobach cyfrowych monitorowanej firmy lub organizacji oraz w sytuacji podniesienia się oceny ryzyka.

## Moduł-5 Funkcjonalność Ochrony przed przejęciem konta użytkownika

* 1. System musi zapewnić funkcjonalność ochrony przed przejęciem konta w formie dostępu do informacji o zidentyfikowanych wyciekach poświadczeń.
     1. System musi umożliwiać wykrycie wycieku poświadczeń pochodzących ze wskazanej domeny poczty elektronicznej.
     2. System musi mieć możliwość wykrycia wycieków poświadczeń osób trzecich ze wskazanej domeny autoryzacyjnej.
     3. System musi umożliwiać budowanie zapytań odnośnie obu typów wycieków wraz z podaniem domen zainteresowania.
  2. Dane o wyciekach muszą pochodzić przynajmniej z:
     1. Dark Web;
     2. zamkniętych forów hakerskich;
     3. zrzutów baz Dark Web;
     4. logów ze złośliwego oprogramowania typu infostealer.
  3. System musi zbierać dane o wyciekach poświadczeń zarówno w formie kolekcji maszynowej (automatycznej), jak i manualnej.
  4. Dla zapytań w platformie System musi umożliwiać filtrowanie wyników na podstawie daty pojawienia się wycieku.
  5. System musi umożliwiać filtrowanie wyników na podstawie atrybutów hasła, celem eliminacji wycieków, w których został użyty korporacyjny adres e-mail do rejestracji działań prywatnych.
  6. System musi udostępniać szczegóły dla wykrytego wycieku poświadczeń, przynajmniej:
     1. Źródła wycieku;
     2. Daty eksfiltracji danych przez malware;
     3. Informacji, czy hasło dostępne jest czystym tekstem;
     4. Popularnych skrótów hasła (MD5, NTLM, SHA), adresu usługi autoryzacyjnej, do której

hasło wyciekło;

* + 1. Skradzionych plików cookie;
    2. Typu infostealer'a;
    3. Precyzyjnej ścieżki pliku infostealera;
    4. Nazwy komputera ofiary;
    5. Nazwy użytkownika ofiary;
    6. Nazwy systemu operacyjnego ofiary.
  1. Dla wycieków pochodzących z baz Dark Web i zamkniętych forów hakerskich, skradzione poświadczenia muszą być prezentowane w identycznym formacie, bez obfuskacji, tak jak dostępne są w oryginalnym źródle.
     1. Dla haseł przedstawionych czystym tekstem w Dark Web, System również musi

prezentować je czystym tekstem.

* 1. System musi umożliwiać również dostęp do danych o wyciekach poprzez interfejs API.
  2. Komunikacja z interfejsem API musi być zabezpieczona kryptograficznie celem zapewnienia

poufności i integralności przekazywanych wrażliwych treści.

* 1. Komunikacja z interfejsem API musi być możliwa jedynie poprzez odpowiednie uwierzytelnianie, minimum przez dedykowany klucz API.
  2. Zapytania i odpowiedzi wykonane przez API muszą być realizowane w standardowych dla tej technologii formatach, minimum:
     1. JSON.
  3. System musi zapewniać wykrycie wycieku poświadczeń pochodzących ze wskazanej domeny poczty elektronicznej poprzez API.
  4. System musi zapewniać wykrycie wycieków poświadczeń osób trzecich ze wskazanej domeny autoryzacyjnej poprzez API.
  5. System musi posiadać tożsame metody filtracji wyników dla zapytań zrealizowanych przez API, co forma zapytania w platformie.
  6. System w ramach API musi umożliwiać zbudowanie zapytania weryfikującego, czy podane jako argument hasło lub jego skrót, historycznie wyciekło lub nie.
  7. System dzięki opcji dostępu do danych przez API, musi umożliwiać integrację funkcjonalności z panelami autoryzacyjnymi dla aplikacji bezpośrednio w kodzie aplikacji.
  8. System nie może w żadnym momencie limitować liczby zapytań wykonanych zarówno w platformie, jak i przez API.

## Moduł-6 Ochrona kont oraz treści powiązanych z organizacją

* 1. System musi zapewnić funkcjonalność dotyczącą ochrony organizacji, jej pracowników i jej własności intelektualnych poprzez monitorowanie określonych źródeł na podstawie predefiniowanych reguł alarmowania, których zadaniem jest podniesienie poziomu ochrony organizacji.
  2. System musi umożliwić konfigurację funkcjonalności poprzez zdefiniowanie chronionych przez

organizację elementów w tym:

* + 1. Nazw własnych chronionych organizacji;
    2. Nazw skrótowych chronionych organizacji (tzw. aliasy);
    3. Nazw produktów opracowanych przez chronione organizacje;
    4. Nazw domen chronionych organizacji;
    5. Oficjalnych log i infografik cyfrowych chronionych organizacji;
    6. Sektora działalności chronionych organizacji;
    7. Organizacji o podobnym profilu działalności;
    8. Zestawów publicznych adresów IP chronionych organizacji;
    9. Zestawów identyfikatorów AS chronionych organizacji;
    10. Imion i nazwisk kadry zarządzającej w chronionych organizacjach.
  1. System nie może limitować ilości i zakresu ochrony organizacji poprzez konfigurację wskazaną w pkt. 1.
  2. System musi posiadać zestaw predefiniowanych reguł alarmujących, których celem jest notyfikacja w sytuacji wykrycia potencjalnego zagrożenia. System musi zawierać przynajmniej następujące rodzaje reguł:
     1. Potencjalne podszycie;
     2. Wzmianki o marce;
     3. Wycieki poświadczeń;
     4. Zdarzenia bieżące (np. COVID-19, konflikt na Ukrainie);
     5. Raporty;
     6. Trendy zagrożeń dla sektora;
     7. Ryzyka związane z infrastrukturą;
     8. Monitoring mediów społecznościowych;
     9. Detekcja typosquatting’u.
  3. System musi umożliwić indywidualną konfigurację dotyczącą częstotliwości alarmów w związku z wykryciem potencjalnego zagrożenia na podstawie zdefiniowanych reguł przynajmniej w zakresie: czas rzeczywisty (do 5 minut), co godzinę, co 8 godzin, raz dziennie, raz w tygodniu.
  4. System musi być wyposażony w mechanizm OCR (Optical Content/Character Recognition), który musi umożliwić analizę obrazów pod kątem wystąpienia na nich słów kluczowych dotyczących chronionych marek.
  5. System musi monitorować informacje dotyczące chronionych organizacji lub posiadanych przez nią

zasobów cyfrowych (w tym domen) w źródłach typu:

* + 1. Platformy komunikacyjne (np. Telegram, Discord);
    2. Platformy komunikacyjne zorientowane na tematy cyfrowe;
    3. Sklepy z aplikacjami mobilnymi;
    4. Repozytoria kodu;
    5. Platformy typu Pastebin;
    6. Dark Web i zamknięte źródła (np. fora wymagające specjalnego dostępu lub uprawnień).
  1. System dla każdej z reguł musi umożliwić wprowadzenie indywidualnej konfiguracji dotyczącej odbiorców alarmu, przynajmniej poprzez wskazanie konkretnych użytkowników (kont) lub grupy użytkowników. Ponadto każdy z użytkowników zasubskrybowanych do otrzymywania danego alarmu musi:
     1. Mieć możliwość indywidualnej konfiguracji formy doręczenia alarmu przynajmniej poprzez notyfikację e-mail (e-mail podany przy tworzeniu konta).
     2. Mieć możliwość otrzymania powiadomienia o powstaniu alarmu za pomocą interfejsu API.
  2. System musi posiadać dedykowany dashboard prezentujący dane dla przynajmniej ostatnich 7 dni wstecz wraz z możliwością zmiany zakresu na przynajmniej 30 dni. Dashboard musi prezentować przynajmniej:
     1. Listę najnowszych alarmów;
     2. Najczęstsze typy alarmów;
     3. Najczęstsze źródła występowania wzmianek o chronionej marce;
     4. Najnowsze notatki analityków.

1. **Moduł-7** **Analiza Zagrożeń i kontekstu Geopolitycznego**
   1. System musi zapewnić funkcjonalność służącą do dostarczenia danych i narzędzi do analizy zagrożeń geopolitycznych i kinetycznych na podstawie pełnej bazy wywiadowczej dostępnej w Systemie, w tym: Open, Deep i Dark Web.
   2. System musi obliczać ocenę ryzyka dla lokalizacji poprzez identyfikację ryzyka w kategorii:
      1. Ataków terrorystycznych z podziałem na:
         1. Obecne ataki terrorystyczne;
         2. Niedawne ataki terrorystyczne;
         3. Historyczne ataki terrorystyczne;
      2. Ataków zbrojnych z podziałem na:
         1. Obecne ataki zbrojne;
         2. Niedawne ataki zbrojne;
         3. Historyczne ataki zbrojne;
      3. Występowania protestów, w tym protestów z aktami przemocy;
      4. Ostrzeżeń bezpieczeństwa dotyczących monitorowanej lokalizacji;
      5. Problemów komunikacyjnych wynikających z działań kinetycznych;
      6. Klęsk żywiołowych;
      7. Zjawisk pandemicznych i epidemicznych.
   3. System musi prowadzić ocenę ryzyka dla państw podzieloną na kategorie:
      1. Rządową – ryzyko związane z obecnym w danym kraju rządem;
      2. Bezpieczeństwo fizyczne – ryzyko związane z bezpieczeństwem kraju rozumianym w

kontekście zagrożeń od sąsiadów kraju;

* + 1. Łańcuch dostaw - kwestie bezpieczeństwa łańcucha dostaw dla kraju;
    2. Cyberbezpieczeństwo – ryzyko związane z atakami w cyberprzestrzeni wymierzonymi w

infrastrukturę danego państwa;

* + 1. Prywatność – ryzyko związane z prawem dotyczącym prywatności w danym kraju.
  1. System podczas obliczania oceny ryzyka dla państw musi uwzględniać przynajmniej:
     1. Jakość instytucji - na podstawie danych z banku światowego i World Justice Project;
     2. Poziom korupcji - na podstawie danych z banku światowego i World Justice Project;
     3. “Pranie pieniędzy” - na podstawie danych z źródeł takich jak np. OECD i FATF;
     4. Sankcje;
     5. Poziom edukacji - na podstawie danych z Banku Światowego;
     6. Służbę zdrowia i poziom majętności - na podstawie danych z Banku Światowego;
     7. Przestępczość - na podstawie danych z np. Organized Crime Index;
     8. Środowisko - na podstawie poziomów zanieczyszczenia i poziomów wód;
     9. Dostępność podstawowych usług;
     10. Jakość infrastruktury;
     11. Poziom cyberbezpieczeństwa - na podstawie danych z np. eGA i ITU;
     12. Dostępność usług VPN;
     13. Prywatność danych - na podstawie wskaźników GDPR.
  2. System musi umożliwić określenie reguł generowania alarmów w związku z zaistnieniem wydarzenia podwyższającym ryzyko lub stwarzającym zagrożenie w kategoriach:
     1. Monitorowanie kryzysowe;
     2. Bieżące wydarzenia;
     3. Aktywność geopolityczna;
     4. Ryzyko w danej lokalizacji;
     5. Wydarzenie w strefach konfliktów;
     6. Aktywności militarnej związanej z lokalizacją lub obiektem;
     7. Protestów związanych z daną lokalizacją lub obiektem;
     8. Ataków terrorystycznych w danej lokalizacji;
     9. Nowych stanowisk światowych przywódców w kontekście wojny w Ukrainie;
     10. Nowych wektorów ataków związanych z wojną w Ukrainie;
     11. Nowych zdjęć satelitarnych związanych z wojną w Ukrainie;
     12. Potencjalnych oszustw związanych z COVID-19.
  3. System musi posiadać graficzny kreator zapytań umożliwiający przeszukiwanie pełnej bazy wywiadowczej Producenta pod kątem konkretnych danych lub zdarzeń. Struktura zapytania musi składać się przynajmniej z:
     1. Słów kluczowych;
     2. Typu zdarzenia;
     3. Zakresu czasu;
     4. Źródła informacji;
     5. Lokalizacji źródła;
     6. Języka oryginalnego;
     7. Wykluczeń.
  4. Graficzny kreator zapytań musi pozwalać na:
     1. Wykorzystanie operatorów logiczny AND i OR;
     2. Prezentowanie wyników kilku niezależnych zapytań w jednym zestawie danych

wyjściowych.

* 1. Graficzny kreator zapytań musi umożliwić poszukiwanie zdarzeń typu:
     1. Protest;
     2. Konflikt zbrojny;
     3. Manewry wojskowe;
     4. Atak terrorystyczny;
     5. Wybory;
     6. Wyniki głosowania;
     7. Legislacja;
     8. Relacje dyplomatyczne;
     9. Klęska żywiołowa;
     10. Wybuch epidemii;
     11. Przemowa;
     12. Aresztowanie;
     13. Proces sądowy;
     14. Bankructwo;
     15. Zwolnienia;
     16. Reorganizacja;
     17. Inwestycja;
     18. Sojusz;
     19. Przejęcie firmy;
     20. Ogłoszenie prasowe.
  2. Graficzny kreator zapytań musi umożliwić poszukiwanie informacji z uwzględnieniem wyłącznie:
     1. Danych pisanych w konkretnym języku;
     2. Danych ze źródeł z konkretnej lokalizacji;
     3. Danych z artykułów (publikacji) konkretnego autora;
     4. Zdarzeń dotyczących wybranej geolokalizacji.
  3. System musi prezentować wyniki zapytania w kilku różnych formatach, przynajmniej w formie:
     1. Widoku tabelarycznego;
     2. Osi czasu;
     3. Mapy – poprzez pokazanie wyników spozycjonowanych na mapie świata.

1. **DOSTĘP DO INTERFEJSU API SYSTEMU**
   1. System musi oferować dedykowany dostęp do programowalnego interfejsu API, celem opracowania autorskich integracji lub skryptów/konektorów, dzięki którym interakcja z danymi zawartymi w bazie danych Systemu może być zautomatyzowana.
   2. Dostęp API do Systemu musi być zabezpieczony kryptograficznie przynajmniej protokołem

SSL/TLS.

* 1. Dostęp API do Systemu musi być wystawiony na stałym publicznie dostępnym FQDN za pomocą

standardowej komunikacji protokołem HTTPS.

* 1. Dostęp API do Systemu musi by zapewniony na zasadzie architektury RESTful API lub innej architektury bezstanowej.
  2. Dostęp API do Systemu musi wymagać uwierzytelniania przynajmniej poprzez dedykowany indywidualny token przesyłany wraz z zapytaniem.
  3. Dostęp API do Systemu musi umożliwiać wykonanie zapytania o werdykt dla IoC typu:
     1. Adres IP;
     2. Domena;
     3. URL;
     4. Hash;
     5. Identyfikator CVE.
  4. Dostęp API do Systemu musi wspierać opcje selektywnego zwracania przez System żądanych treści

- poprzez wybór kategorii informacji, które mają być zwracane per zapytanie.

* 1. Selektywny wybór zwracanego pakietu treści musi być określony w samym zapytaniu poprzez ustawienie ich w finalnym URL zapytania.
  2. Dostęp API do Systemu musi wspierać otrzymywanie listy IoC:
     1. Adres IP;
     2. Domena;
     3. URL;
     4. Hash;
     5. Identyfikator CVE;
     6. Spełniających określony zestaw parametrów.
  3. Zestaw parametrów możliwych do określania musi zawierać minimum:
     1. Wskaźnik ryzyka dla IoC lub jego zakres;
     2. Znaczniki czasowe dla obserwacji;
     3. Typ związanego z IoC z ryzyka.
  4. Dostęp API do Systemu dla wyszukiwania adresów IP spełniających zestaw kryteriów musi dodatkowo wspierać filtrowanie wyników na bazie kraju zarejestrowania lub geolokalizacji adresu IP.
  5. Dostęp API do Systemu dla wyszukiwania podatności (identyfikatorów CVE) spełniających zestaw kryteriów musi dodatkowo wspierać filtrowanie na bazie:
     1. Oceny ryzyka CVSS;
     2. Produktu (oprogramowania);
     3. Kodu CPE.
  6. Dostęp API do Systemu musi wspierać otrzymywanie danych wywiadowczych na temat wskazanego

złośliwego oprogramowania (malware).

* 1. Dostęp API do Systemu dla zapytań o dane wywiadowcze dla malware musi wspierać selektywną konfigurację zwracanego zestawu treści, minimum:
     1. Notatki analityków;
     2. Kategorię;
     3. Powiązanych IoC, grup cyberprzestępczych.
  2. Dostęp API do Systemu musi umożliwiać automatyczne pobieranie predefiniowanych przez producenta list feed’ów dla:
     1. Adresów IP;
     2. Domen;
     3. URL;
     4. Hash’y;
     5. Identyfikatorów CVE.
  3. Dostęp API do Systemu musi wspierać automatyczne pobieranie alarmów wygenerowanych przez

funkcjonalność wywiadu cybernetycznego wraz z ich szczegółami.

* 1. Dostęp API do Systemu musi być oparty o format przynajmniej JSON.
  2. Dostęp API do Systemu musi umożliwiać opracowanie autorskich integracji lub własnych skryptów.
  3. Producent musi zapewnić dedykowaną specyfikację typu OpenAPI do swojego API, która zawiera graficzny kreator zapytań.
     1. Graficzny kreator zapytań musi automatycznie generować kod dla wymaganego zapytania minimum za pomocą cURL i Python (v2 i v3).

1. **WSPARCIE PRODUCENTA (W TYM WSPARCIE TECHNICZNE)**
   1. System musi być udostępniony wraz z usługą wsparcia technicznego zapewnioną przez Producenta

rozwiązania na cały okres obowiązywania umowy tj. 12/24/36 miesięcy licząc od dnia jej zawarcia.

* + 1. Wsparcie serwisowe musi uwzględniać rozwiązanie problemów z dostępem do platformy, korekcji i poprawy danych oraz konsultacji projektowych;
    2. Usługa wsparcia musi umożliwiać zakładanie spraw serwisowych w reżimie 24/7/365;
    3. Usługa wsparcia musi umożliwiać zgłaszanie problemów za pośrednictwem telefonu,

wiadomości e-mail oraz dedykowanego portalu [www.](http://www/)

* 1. Podczas inicjalnego Udostępnienia, usługa wsparcia musi zawierać współpracę z dedykowanym

zespołem Producenta odpowiedzialnym za nadzór nad całym procesem.

* 1. Usługa wsparcia musi zawierać dostęp do dedykowanego konsultanta technicznego po stronie Producenta, który stanowić ma centralny punkt kontaktowy.
     1. W ramach usługi wymaga się od konsultanta wsparcia w zakresie definicji i wdrożenia

przypadków użycia oraz architektury rozwiązania.

* 1. Poziom wsparcia musi zawierać dedykowane warsztaty techniczne dla nowych i obecnych użytkowników - szkolenia przeprowadzone przez zespół techniczny producenta, które mają na celu zaznajomienie użytkowników z funkcjonalnościami udostępnionego przez Wykonawcę Systemu i sposobami korzystania z niego.
     1. Szkolenia muszą być prowadzone przez specjalistów posiadających wiedzę techniczną niezbędną do ich przeprowadzania;
     2. Szkolenia muszą być zapewnione wraz z udzieleniem dostępu do Systemu;
     3. Szkolenia muszą być przeprowadzone dla wszystkich użytkowników Systemu po początkowym Udostępnieniu Systemu (utworzeniu kont użytkowników) i w dalszym okresie być realizowane „na żądanie” zależnie od potrzeb obecnego lub nowo dodanego użytkownika (utworzenia nowego konta w ramach posiadanej Licencji).

1. **UDOSTĘPNIENIE ORAZ DOKUMENTACJA UŻYTKOWA**
   1. Udostępnienie będzie obejmowało przekazanie Licencji przez Wykonawcę dla Zamawiającego dla wszystkich wskazanych przez Zamawiającego użytkowników. Licencje mogą zostać przekazane na co najmniej jeden z poniższych sposobów:
      1. W postaci kluczy licencyjnych, które pozwalają na samodzielne utworzenie konta w Systemie. W przypadku, gdy jeden użytkownik ma dostęp do kilku funkcjonalności to w tym przypadku musi założyć tylko jedno konto.
      2. W postaci kont, do których przypisane są odpowiednie funkcjonalności.
   2. Dane dostępowe do kont muszą zostać przekazane do wybranej przez Zamawiającego osoby. Dane kontaktowe do tej osoby w zakresie wymaganym do zrealizowania przedmiotu Umowy zostaną udostępnione Wykonawcy po podpisaniu Umowy.
   3. Dokumentacja użytkowa musi być napisana w taki sposób, by osoba posiadająca do niej dostęp była w stanie korzystać ze wszystkich dostępnych w Systemie funkcjonalności w przypadku, gdyby nie posiadała wiedzy co do określonych funkcjonalności.
      1. Dokumentacja użytkowa musi obejmować dokładny opis wszystkich funkcjonalności

Systemu.

* + 1. Każda z opisywanych w dokumentacji czynności musi być opisana co najmniej w języku

polskim lub angielskim.

* + 1. Opisy zawarte w dokumentacji powinny być wzbogacone o grafiki ułatwiające zrozumienie opisywanych czynności.
    2. Dokumentacja musi zawierać przykładowe wykorzystanie każdej z opisanych

funkcjonalności w formie pisemnej i graficznej.

* + 1. Dokumentacja musi zawierać opis metody zgłaszania problemów technicznych w formie pisemnej i graficznej.
  1. Dokumentacja użytkowa nie musi być dostarczana, jeżeli w Systemie znajduje się dokumentacja

spełniająca wszystkie wymagania w pkt. 11 ppkt. 3.