OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest **dostawa rozwiązania informatycznego obejmującego funkcjonalność systemu służącego do weryfikacji, zarządzania i poprawy efektywności systemów bezpieczeństwa na rzecz sądów, Ministerstwa Sprawiedliwości wraz z usługami towarzyszącymi.**

STOSOWANE DEFINICJE

1. **Dokumentacja** – Dokumentacja Projektowa oraz Dokumentacja Powykonawcza;
2. **Dokumentacja Projektowa** – Projekt Wdrożenia Systemu, w tym Dokumentacja Testów Akceptacyjnych;
3. **Dokumentacja Testów Akceptacyjnych** – opis działań, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z OPZ i Umową;
4. **Dokumentacja Powykonawcza** – dokumentacja spełniająca wymogi określone w OPZ; w tym opis działań jakie zostały wykonane, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z OPZ i Umową;
5. **Gwarancja** – gwarancja jakości obejmująca w szczególności usługi gwarancyjne, udzielona przez Wykonawcę na System;
6. **Umowa –** Umowa o udzielenie zamówienia publicznego, którego dotyczy niniejszy OPZ, zawarta między Zamawiającym, a Wykonawcą wraz ze wszystkimi Załącznikami oraz Aneksami.
7. **Jednostka** – jednostka organizacyjna sądownictwa powszechnego, w tym Zamawiający – na rzecz których zawarta została Umowa,
8. **Odbiorca** – Ministerstwo Sprawiedliwości, na rzecz którego prowadzone jest postępowanie;
9. **OPZ** – niniejszy Opis Przedmiotu Zamówienia wraz z załącznikami;
10. **Oprogramowanie** – wszystkie programy komputerowe, aplikacje, obrazy maszyn wirtualnych oraz wszelkie pozostałe oprogramowanie, w tym oprogramowanie instalowane na serwerach oraz całość usług, umożliwiające realizację funkcjonalności Systemu zgodnie z Umową oraz OPZ;
11. **System** – całość oferowanego rozwiązania, składającego się z wymaganych Modułów obejmującego funkcjonalność symulacji cyberataków w infrastrukturze Jednostek oraz Odbiorcy wraz z dostępem do usług informacji o zagrożeniach zawierająca wszystkie niezbędne elementy w tym: wszystkie licencje i Oprogramowanie, umożliwiające realizację funkcjonalności Systemu zgodnie z OPZ.
12. **Producent** – osoba fizyczna lub prawna oferująca Oprogramowanie pod własną nazwą lub znakiem towarowym.
13. **Usługa Chmurowa (Saas)** – Model świadczenia usługi zdalnego dostępu do Oprogramowania, w którym aplikacja jest przechowywana i wykonywana w środowisku Producenta usługi i jest udostępniana Zamawiającemu, Odbiorcy przez Internet przy zachowaniu wysokiego poziomu bezpieczeństwa danych (tj. poufności, integralności i dostępności danych).
14. **Dni Robocze** - dni pracy, od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
15. **Zgłoszenie Serwisowe** – zgłoszenie Awarii Systemu przekazane poprzez zapewnione przez Wykonawcę oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu zgłoszenia Awarii, przekazane przez osobę upoważnioną ze strony Odbiorcy, . Zgłoszenie Serwisowe staje się skuteczne (zostaje dokonane) z chwilą wprowadzenia Zgłoszenia Serwisowego do oprogramowania umożliwiającego zdalne zgłaszanie i monitorowanie statusu zgłoszenia Awarii.
16. **Projekt Wdrożenia Systemu** – dokumentacja opisująca sposób wykonania i wdrożenia Systemu zawierająca co najmniej: opis funkcjonalny Systemu, wykaz wymaganych elementów, sposób ich wdrożenia i konfiguracji, wykaz licencji niezbędnej dla działania Systemu jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Odbiorcy, harmonogram wdrożenia;
17. **Protokół Odbioru Projektu** – protokół odbioru stwierdzający sposób wykonania przez Wykonawcę Dokumentacji Projektowej,
18. **Protokół Odbioru Wdrożenia Systemu** – protokół stwierdzający sposób wykonania przez Wykonawcę elementów zamówienia, które nie podlegają odbiorowi na gruncie innych protokołów, w tym stwierdzający uruchomienie funkcjonalność symulacji cyberataków w infrastrukturze Jednostek oraz Odbiorcy wraz z dostępem do usług informacji o zagrożeniach.
19. **Zespół Odbiorowy** – wyznaczeni przez Zamawiającego, wskazani w Umowie przedstawiciele odpowiedzialni za dokonanie odpowiednich protokolarnych odbiorów.
20. **Czas Reakcji –** czas liczony od momentu Zgłoszenia Serwisowego do chwili poinformowania Zamawiającego o podjęciu działań zmierzających do ustalenia przyczyn i dokonania Naprawy.
21. **Czas Naprawy** – czas liczony od momentu przekazania Zgłoszenia Serwisowego przez

Zamawiającego do chwili dokonania Naprawy; do czasu Naprawy wliczany jest Czas Reakcji;

1. **Naprawa** – trwałe usunięcie awarii poprzez usunięcie przyczyny powstania awarii skutkujące przywróceniem pełnej sprawności Systemu po wystąpieniu awarii, w tym również zakończenie innych działań naprawczych.
2. **Awaria** – niesprawność Systemu uniemożliwiająca niezakłócone korzystanie ze wszystkich funkcjonalności Systemu. Za Awarię będzie uznawane również uszkodzenie/usunięcie danych, jeżeli zostało spowodowane okolicznościami, o których mowa w zdaniu pierwszym lub w związku z Naprawą Awarii. Awarie Systemu mogą mieć charakter Awarii Krytycznej albo Awarii Niekrytycznej.

**I Przedmiot zamówienia**

1. Przedmiotem zamówienia jest dostarczenie i wdrożenie przez Wykonawcę na rzecz Odbiorcy oraz Jednostek rozwiązania informatycznego obejmującego funkcjonalność systemu służącego do weryfikacji, zarządzania i poprawy efektywności systemów bezpieczeństwa, a więc systemu symulacji cyberataków w infrastrukturze Jednostek oraz Odbiorcy wraz z dostępem do usług informacji o zagrożeniach (threat intelligence). Wdrożenie obejmować będzie uruchomienie Systemu, oraz konfigurację zgodnie z wymaganiami Zamawiającego w zakresie niezbędnym do poprawnego działania tego Systemu.
2. W ramach przedmiotu zamówienia Wykonawca zobowiązuje się w szczególności:
	1. dostarczyć, wdrożyć, uruchomić i skonfigurować System;
	2. wykonać Dokumentację,
	3. wykonać transfer wiedzy dla osób wskazanych przez Odbiorcę dla max. 6 osób wskazanych przez Odbiorcę z zakresu funkcjonowania dostarczonego Systemu
	i administrowania nim w wymiarze po 8 godzin (dla każdej z osób),
	4. udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości jak i poszczególnych jego elementów dla 80 tysięcy użytkowników w rozproszonej strukturze 150 tysięcy adresów IP . Licencjobiorcą jest Odbiorca, a podmiotami uprawnionymi do korzystania z Systemu są Jednostki.
	5. przenieść na Odbiorcę autorskie prawa majątkowe do Dokumentacji opracowanej przez Wykonawcę w ramach Umowy.
	6. udzielić Odbiorcy Gwarancji na dostarczony w ramach Umowy System, w tym gwarancji na Oprogramowanie, na okres 36 miesięcy od podpisania Protokołu Odbioru Wdrożenia Systemu oraz świadczyć w tym okresie usługi gwarancyjne w zakresie wdrożonego Systemu, w ramach wynagrodzenia wynikającego z Umowy.
	7. Zapewnić przeprowadzenie szkoleń związanych z oferowanym rozwiązaniem (Systemem) w zakresie i na warunkach opisanych w Rozdziale X niniejszego dokumentu.
	8. zapewnić usługi asysty technicznej w maksymalnej ilości 200 roboczogodzin w okresie obowiązywania umowy świadczonej w języku polskim

# **II. Wymagania dotyczące oferowanego rozwiązania**

1. Oferowany System składać się musi co najmniej z:
	* + - 1. modułu symulacji cyberataków;
				2. subskrypcji usługi dostarczania informacji o zagrożeniach pochodzącej od tego samego Producenta co moduł symulacji cyberataków;
				3. dodatkowej usługi dostarczania informacji o zagrożeniach pochodzącej od innego Producenta niż moduł symulacji cyberataków.

 Wszystkie elementy Systemu muszą pochodzić tylko z oficjalnych kanałów dystrybucyjnych Producentów oferowanego rozwiązania w tym zakresie.

1. Każdy moduł/subskrypcja stanowiący element Systemu musi stanowić jednolite środowisko programowe, tj. współpracować ze sobą bez konieczności stosowania dodatkowych elementów niebędących standardową częścią oferowanego Modułu/subskrypcji np. pochodzić od innego Producenta. Warunek ten nie dotyczy dodatkowej usługi dostarczania informacji o zagrożeniach pochodzącej od innego Producenta niż moduł symulacji cyberataków.

Warunek ten nie dotyczy również elementu Systemu do rejestracji Zgłoszeń Serwisowych.

1. Oferowane rozwiązanie ma stanowić jednolity i kompleksowy System składający się z wymaganych Modułów/subskrypcji. Skalowalny i elastyczny w kontekście potencjalnej rozbudowy tj. objęcia ochroną kolejnych użytkowników.
2. Wymaganiem Zamawiającego jest, aby każdy Moduł/subskrypcja posiadał tylko jedną konsolę zarządzającą.
3. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
4. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
5. Zamawiający wymaga, aby wszystkie elementy dostarczanego Systemu były w najnowszej i aktualnej wersji (tzn. najnowszej i aktualnej udostępnionej przez Producenta oferowanego rozwiązania w tym zakresie) na dzień wdrożenia Systemu.
6. Żaden z elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez Producenta do wycofania z produkcji lub sprzedaży.
7. Czynności związane z wdrożeniem i konfiguracją Systemu w infrastrukturze Odbiorcy Systemu muszą być przeprowadzone przez personel Wykonawcy w obecności personelu IT Odbiorcy.

# **III. Wymagania w zakresie Gwarancji Systemu**

1. W ramach udzielonej Gwarancji Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu Zgłoszenia Serwisowego Awarii, oprogramowanie to musi zapewnić Odbiorcy brak ograniczeń, co do liczby dokonywanych Zgłoszeń Serwisowych w zakresie Awarii.
2. Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do Systemu przez Odbiorcę.
3. W ramach udzielonej gwarancji Wykonawca będzie realizował Zgłoszenia Serwisowe Awarii Systemu w następujący sposób:
	1. **Awaria Krytyczna**, wada skutkująca nieprawidłowym działaniem Systemu powodująca całkowity brak możliwości korzystania z Systemu przez co najmniej jednego użytkownika końcowego albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje. Czas Naprawy do 12 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę;
	2. **Awaria Niekrytyczna** wada skutkująca nieprawidłowym działaniem Systemu powodująca ograniczenie korzystania z Systemu, nie powodując skutków opisanych dla Awarii Krytycznej: . Czas Naprawy do 72 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę.
	3. Wszelkie Awarie będą zgłaszane przez Odbiorcę za pomocą udostępnionego przez Wykonawcę oprogramowania, o którym mowa w punkcie 1 powyżej.
	4. W przypadku potrzeby wydania poprawki do Systemu przez Producenta, na wniosek Wykonawcy złożony w formie elektronicznej, Odbiorca może zawiesić czas usunięcia Awarii Niekrytycznych, maksymalnie na 40 dni kalendarzowych.
	5. Obsługa Zgłoszeń Serwisowych musi obejmować co najmniej:
4. rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą Systemu.
5. W ramach udzielonej gwarancji Odbiorcy przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji Systemu udostępnianych przez Producentów elementów wchodzących w skład Systemu bez ponoszenia dodatkowych kosztów finansowych przez Odbiorcę. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Odbiorcy.

# **IV. Wymagania w zakresie dokumentacji**

1. Wykonawca w uzgodnieniu z Zespołem Odbiorowym opracuje i przekaże Dokumentację Projektową:

1. Projekt Wdrożenia Systemu, który musi zawierać co najmniej: opis funkcjonalny Systemu, wykaz wymaganych elementów Systemu, sposób ich wdrożenia i konfiguracji, wykaz licencji niezbędnych dla działania Systemu jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Odbiorcy, harmonogram wdrożenia,
2. Dokumentację Testów Akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z opisem przedmiotu zamówienia. Testy akceptacyjne mają być realizowane w środowisku produkcyjnym, zgodnie ze scenariuszami testowymi opracowanymi przez Wykonawcę i zaakceptowanymi przez Zespół Odbiorowy na etapie odbioru Dokumentacji Projektowej.

2. Wykonawca opracuje i przekaże Dokumentację Powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu, w tym co najmniej:

1. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,
2. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
3. instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,
4. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem Zespołu Odbiorowego.

3. Dokumentacja musi być przekazana w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje Producenta mogą być przekazane w języku angielskim lub polskim.

# **V. Wymagania w zakresie transferu wiedzy**

1) W ramach wdrożenia Wykonawca umożliwi Odbiorcy w siedzibie i w środowisku Odbiorcy transfer wiedzy dla max. 6 osób wskazanych przez Odbiorcę polegający na możliwości uczestniczenia ww. osób przy wdrażaniu, konfiguracji i administracji Systemem. Transfer wiedzy polegać będzie na:

1. zapewnieniu możliwości udziału osób wskazanych przez Odbiorcę przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,
2. udzielaniu odpowiedzi na pytania zadawane przez osoby wskazane przez Odbiorcę w zakresie zagadnień związanych z czynnościami administracyjnymi, funkcjonowaniem wdrożonego

Systemu w środowisku produkcyjnym Odbiorcy, w tym omówieniu wraz z przeprowadzeniem praktycznych scenariuszy możliwości Systemu w zakresie wykrywania, przeciwdziałania i blokowania dostarczenia złośliwego oprogramowania,

1. Zapewnieniu transferu wiedzy w zakresie konfiguracji Systemu i administracji Systemem, który musi być prowadzony na bieżąco w trakcie wdrożenia, lecz przed zakończeniem wdrożenia. Transfer wiedzy przeprowadzony zostanie w języku polskim.
2. potwierdzeniem prawidłowej realizacji transferu wiedzy będzie podpisany bez zastrzeżeń przez Zespół Odbiorowy Protokół Odbioru Wdrożenia Systemu.

# **VI. Wymagania w zakresie wdrożenia**

1. Odbiorca przekaże wszystkie niezbędne zasoby informatyczne potrzebne do wdrożenia elementów Systemu. Zakres integracji wdrażanego Systemu z systemami Odbiorcy polegać będzie co najmniej na przekazaniu przez Wykonawcę wymaganych do prawidłowego działania Systemu informacji o koniecznych zmianach w konfiguracji systemów Odbiorcy w postaci instrukcji, opisu konfiguracji itp.
2. W ramach wdrożenia Systemu Wykonawca dokona dostawy, zainstaluje i skonfiguruje System, zgodnie z zaakceptowanym przez Zespół Odbiorowy Projektem Wdrożenia.
3. Miejsca realizacji przedmiotu Umowy: ul. Czerniakowska 100, 00-454 Warszawa. Na wniosek Wykonawcy Zespół Odbiorowy może wyrazić zgodę w formie elektronicznej (e-mail) lub dokumentowej na wykonanie prac zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Odbiorcę.
4. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Odbiorcy.
5. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy, w zakresie Dokumentacji Projektowej, będzie podpisany bez zastrzeżeń Protokół Odbioru Projektu (zgodnie z postanowieniami Istotnych Postanowień Umowy) zawierający co najmniej: odbiór Dokumentacji Projektowej tj. Projektu Wdrożenia Systemu, Dokumentacji Testów Akceptacyjnych.
6. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy w zakresie uruchomienia i skonfigurowania Systemu będzie podpisany bez zastrzeżeń Protokół Odbioru Wdrożenia Systemu (zgodnie z postanowieniami Istotnych Postanowień Umowy) zawierający co najmniej:
	1. odbiór Systemu w infrastrukturze Zamawiającego wraz z dostępem do subskrypcji informacji o zagrożeniach wraz z wchodzącymi w skład Systemu wszystkimi elementami , na podstawie przeprowadzonych Testów Akceptacyjnych,
	2. odbiór Dokumentacji Powykonawczej,
	3. odbiór realizacji transferu wiedzy.

**VII. WYMAGANIA MODUŁU SYMULACJI CYBERATAKÓW**

1. **Wymagania ogólne**
2. Moduł symulacji cyberataków musi realizować funkcjonalność symulacji cyberataków w infrastrukturze Jednostek oraz Odbiorcy
3. Symulacje cyberataków muszą być przeprowadzane przy zachowaniu następujących wymagań:
	1. Nie jest dopuszczalne aktywne atakowanie realnymi narzędziami produkcyjnych serwerów czy stacji końcowych zamawiającego.
	2. Przeprowadzone ataki muszą być wykonywane z wykorzystaniem dedykowanych elementów rozwiązania dostarczonych przez Producenta, które będą włączone w strukturę sieci Jednostek oraz Odbiorcy
	3. Włączone do sieci komponenty modułu, sondy, serwery, stacje robocze, dedykowane narzędzia modułu itp. muszą być zabezpieczone i przygotowane przez dostarczone przez Producenta oprogramowanie, tak aby symulacje ataków w żaden sposób nie zagrażały środowiskom produkcyjnym.
	4. Elementy modułu weryfikujące ataki muszą odzwierciedlać konfiguracje, wersje i systemy posiadane przez Jednostki oraz Odbiorcę. Nie jest dozwolone, aby do celów weryfikacji powodzenia ataków wykorzystywać infrastrukturę informatyczną Jednostek oraz Odbiorcy.
4. Moduł symulacji cyberataków musi umożliwiać wdrożenie w produkcyjnym środowisku lokalnym (tzw. on-premise), w tym na sprzęcie fizycznym oraz środowisku maszyn wirtualnych opartych o Vmware.
5. Moduł symulacji cyberataków musi posiadać funkcjonalność zarządzania wszystkimi funkcjonalnościami tego modułu w tym konfiguracją dedykowanych sond analitycznych (czujników) zainstalowanych w wybranych miejscach infrastruktury informatycznej w celu wykonywania precyzyjnych testów ataków cybernetycznych.
6. Dostarczona licencja musi umożliwiać instalacje w środowisku przynajmniej 80000 użytkowników, dla rozproszonej struktury 150 000 adresów IP.
7. Licencjonowanie musi umożliwiać instalacje minimum 13 sond w postaci maszyny wirtualnej w odrębnych lokalizacjach.
8. Moduł symulacji cyberataków musi umożliwiać wdrożenie w środowisku chmurowym w celu symulowania ataków także w tym obszarze, przynajmniej w zakresie chmur AWS (obraz AMI) i AZURE (VHD) z oficjalnym wsparciem Producenta.
9. Moduł symulacji cyberataków musi obsługiwać komunikację z Internetem z wykorzystaniem proxy, jeżeli będzie potrzeba takiej komunikacji.
10. Moduł symulacji cyberataków musi wspierać łączność jego komponentów (sond analitycznych) z wykorzystaniem komponentu zarządzania (centralne zarządzanie), szczególnie pomiędzy wewnętrznymi strefami sieci, które w normalnych warunkach są od siebie odseparowane sieciowo (z wykorzystaniem bezpiecznego protokołu).
11. Moduł symulacji cyberataków musi obejmować obsługę i testowanie wielu stref bezpieczeństwa w sieci, przynajmniej stref użytkowników, stref datacenter i DMZ w kwestii wdrożenia sond.
12. Moduł symulacji cyberataków musi obejmować możliwość samodzielnego zarządzania czasem i synchronizowania go we wszystkich systemach wykorzystując oprogramowanie Producenta, bez udziału systemu operacyjnego, aby zapewnić odpowiednią korelację i walidację zdarzeń.
13. Moduł symulacji cyberataków musi być skalowalny i obsługiwać minimum 100 czujników/węzłów wykorzystywanych do symulacji ataków.
14. Moduł symulacji cyberataków musi być w pełni funkcjonalny bez połączenia internetowego z siecią Producenta.
15. Moduł symulacji cyberataków musi mieć swoją bazę danych i musi być ona zainstalowana na centralnej konsoli zarządzania.
16. Komunikacja czujników z konsolą zażądania musi być możliwa w obu kierunkach, niezależnie od tego, w którym kierunku zostanie zainicjowane połącznie.
17. Dla wszystkich elementów modułu musi być dostępna dokumentacja, zwłaszcza instrukcje instalacji i obsługi przynajmniej w języku polskim lub angielskim.
18. Moduł symulacji cyberataków musi być dostarczony jako pakiet oprogramowania lub jak gotowe obrazy maszyn wirtualnych.
19. Obrazy maszyn wirtualnych muszą być dostarczone przynajmniej jako OVA dla VMware, VHD i VHDx dla Microsoft Hyper-V i Azure, AWS AMI.
20. Moduł symulacji cyberataków musi wspierać proces automatycznego wdrażania, minimum posiadać wbudowany kreator dla tworzenia zadań i automatycznie weryfikować poprawność ich działania oraz poprawność prac czujników.
21. Czujniki modułu muszą być dostarczone jako pakiet oprogramowania na wymagane systemy operacyjne lub gotowe obrazy maszyn wirtualnych.
22. Czujniki modułu muszą być dostarczone przynajmniej dla systemu Microsoft Windows, w wersji Windows 10 i wyższej.
23. Czujniki modułu (sondy) muszą mieć opcję wdrożenia na systemie Linux, przynajmniej dla dystrybucji Redhat i Ubuntu.
24. Czujniki modułu muszą mieć opcję wdrożenia na systemie MacOS.
25. Czujniki modułu muszą mieć opcję zainstalowania na niestandardowych złotych obrazach, przynajmniej dla systemów Windows, Linux oraz MacOS.
26. Moduł symulacji cyberataków musi obejmować dyskretne poziomy uprawnień i konta użytkowników z określonymi uprawnieniami dla każdego z nich (np. RBAC).
27. Moduł symulacji cyberataków musi obejmować możliwość grupowania użytkowników i przypisywania określonych uprawnień według grup.
28. Moduł symulacji cyberataków musi zawierać mechanizmy kontroli dostępu do kont użytkowników modułu i zarządzania hasłami.
29. Moduł symulacji cyberataków musi generować dziennik audytu wszystkich operacji, w tym działań poszczególnych użytkowników.

**B. Wymagane integracje modułu symulacji cyberataków z rozwiązaniami bezpieczeństwa**

1. Moduł symulacji cyberataków musi być bezpośrednio zintegrowany z popularnymi komercyjnymi rozwiązaniami SIEM, wymagana jest integracja przynajmniej z:
* Splunk,
* Qradar,
* ArcSight,
* McAfee,
1. Moduł symulacji cyberataków musi pozwalać na automatyczne wykrywanie posiadanych systemów bezpieczeństwa na podstawie logów wysyłanych do SIEM.
2. Moduł symulacji cyberataków musi weryfikować skuteczność kontroli bezpieczeństwa punktów końcowych poprzez weryfikacje logów i zdarzeń z rozwiązania SIEM.
3. Moduł symulacji cyberataków musi być bezpośrednio zintegrowany (bez wykorzystywania logów z tych systemów) z powszechnie stosowanymi komercyjnymi mechanizmami kontroli bezpieczeństwa punktów końcowych. Wymagamy przynajmniej integracji z CarbonBlack, Cisco AMP, FireEye HX, McAfee EPO, Symantec EP, CrowdStrike.
4. Moduł symulacji cyberataków musi być bezpośrednio zintegrowany ze standardowymi mechanizmami kontroli bezpieczeństwa stacji roboczych typu open source, przynajmniej dla WinLogBeat.
5. Sondy analizujące skuteczność ataków muszą mieć możliwość zainstalowania i pełnej funkcjonalności pracy wymienionych systemów ochrony stacji roboczych.
6. Moduł symulacji cyberataków musi weryfikować skuteczność kontroli bezpieczeństwa sieci z wykorzystaniem logów z rozwiązania SIEM.
7. Moduł symulacji cyberataków musi być bezpośrednio zintegrowany (bez wykorzystywania logów z tych systemów) ze standardowymi mechanizmami kontroli bezpieczeństwa sieci komercyjnych. Wymagamy przynajmniej integracji z McAfee, Palo Alto FW, CheckPoint NGFW, RSA NetWitness, Cisco FirePower, FireEye NX, DarkTrace, Symantec DLP, FireEye ETP.
8. Moduł symulacji cyberataków musi być bezpośrednio zintegrowane ze standardowymi mechanizmami kontroli bezpieczeństwa sieci typu open source, przynajmniej dla Zeek.
9. Moduł symulacji cyberataków musi weryfikować skuteczność kontroli bezpieczeństwa poczty e-mail z wykorzystaniem logów z rozwiązania SIEM.
10. Moduł symulacji cyberataków musi obejmować obsługę protokołów e-mail POP3, POP3 SSL, IMAP i SMTP z SSL, TLS i STARTTLS.
11. Moduł musi obejmować obsługę wspólnych dostawców poczty e-mail, w tym usługi Office 365, Gmail i Outlook.
12. Moduł symulacji cyberataków musi bezpośrednio integrować się z rozwiązaniami Microsoft Exchange w celu odbierania i wysłania poczty.
13. Moduł symulacji cyberataków musi obejmować obsługę haseł aplikacji umożliwiających dostęp do dostawców poczty.
14. Moduł symulacji cyberataków musi być wyposażony w przynajmniej dwie instancje sond, które będą weryfikować kontrolę bezpieczeństwa poczty e-mail.
15. Moduł symulacji cyberataków musi obejmować obsługę definiowania i dodawania niestandardowych mechanizmów zabezpieczeń, które będą w przyszłości wdrażane w infrastrukturze zamawiającego.
16. Moduł symulacji cyberataków musi obejmować obsługę definiowania i dodawania niestandardowych metod automatycznego wykrywania poprzez wskazanie własnych wskaźników wykrycia incydentu bezpieczeństwa.
17. **Badanie wpływu złośliwego, destrukcyjnego oprogramowania .**
18. Moduł symulacji cyberataków musi uwzględniać platformę lub elementy Systemu, które będą pozwalały na destrukcyjne uruchomienie złośliwego oprogramowania.
19. Moduł symulacji cyberataków musi zapewniać izolację środowiska testowego przed potencjalnym rozprzestrzenianiem na produkcyjne środowisko Jednostek oraz Odbiorcy.
20. Po wykonaniu scenariusza testowego –moduł symulacji cyberataków musi umożliwiać automatyczne przywrócenie jego konfiguracji do stanu sprzed realizowanego ataku/scenariusza. Moduł symulacji cyberataków musi umożliwiać dodanie bazowego obrazu „golden image”, który będzie podlegał tym testom destruktywnym próbek złośliwego oprogramowania (np. Windows 7, Windows 10, Windows Server 2012R2, Windows Server 2016, Windows Server 2019).
21. **Biblioteka ataków:**
22. Moduł symulacji cyberataków musi zapewniać łączną liczbę minimum 2000 unikalnych ataków w bibliotece ataków. Ataki różniące się tylko wskaźnikami naruszenia bezpieczeństwa lub stosowanymi wariantami złośliwego oprogramowania różniące się tylko hash’em są liczone jako pojedynczy atak.
23. Każdy atak w bibliotece ataków musi zawierać pisemny opis ataku, czemu ma służyć, co weryfikuje, jak jest wykonywany, przedstawione krok po kroku komendy z ataku.
24. Każdy atak w bibliotece ataków musi zawierać opisane znaczniki kontrolne, po których można go zidentyfikować.
25. Każdy atak w bibliotece ataków musi wskazać użytkownikowi wszystkie operacje wiersza poleceń, których używa do przeprowadzenia ataku.
26. Ataki sieciowe w bibliotece ataków muszą zawierać komunikację sieciową skojarzoną z sygnaturami wykrywania przez mechanizmy kontroli bezpieczeństwa sieci, które zwykle alertują tego typu działania.
27. Moduł symulacji cyberataków musi obejmować łagodne ataki o niskim poziomie zagrożenia przydatne do testowania prawidłowego wykonania ataków i ich ścieżek.
28. Moduł symulacji cyberataków musi obejmować możliwość pobierania złośliwej zawartości (próbki), która jest elementem ataku na potrzeby przeprowadzenia pełnego zakresu scenariusza testów.
29. Moduł symulacji cyberataków musi zawierać zdefiniowane i wyszczególnione skróty plików dla złośliwego oprogramowania związanego z przeprowadzanymi atakami.
30. Moduł symulacji cyberataków musi zawierać predefiniowane scenariusze złożone z dwóch lub więcej pojedynczych ataków, aby reprezentować cały proces cyklu życia ataku. Wymagane jest, aby moduł zawierał minimum 100 różnych wbudowanych scenariuszy.
31. Moduł symulacji cyberataków musi pozwalać na dodawanie zdefiniowanych przerw czasowych pomiędzy poszczególnymi częściami sekwencji ataku.
32. Moduł symulacji cyberataków musi zawierać predefiniowane oceny przypadków użycia i powodzenia ataków, takie jak oceny scenariusza z serią dwóch lub więcej pojedynczych ataków.
33. Moduł symulacji cyberataków musi być dostarczany z gotową biblioteką ataków, z podziałem na poniższe taktyki/fazy ataku:

 • Initial Access – uzyskanie dostępu

• Execution – wykonanie

• Persistence – instalacja trwała

• Privilege Escalation – podniesienie uprawnień

• Defense Evasion – unikanie wykrycia

• Credential Access – dostęp do poświadczeń

• Discovery – wykrywanie środowiska

• Lateral Movement – rozprzestrzenianie ataku

• Collection – zbieranie danych

• Exfiltration - eksfiltracja

• Command and Control – uzyskanie kontroli

• Impact – działanie

1. Moduł symulacji cyberataków musi obejmować możliwość pobierania danych z komercyjnych platform Threat Intelligence (informacje na temat ataków cyberbezpieczeństwa). Wymagane wsparcie minimum dla: Anomali, CrowdStrike Intel, Threat Connect, Intel471, Mandiant Threat Intelligence.
2. Integracja z komercyjnymi źródłami Threat Intelligence musi dostarczać profile ataków Threat Actors (grup przestępczych), wraz ze scenariuszami ataków, w których wykonywane są TTPs (taktyki, narzędzia, procedury) aktorów.
3. Moduł symulacji cyberataków musi obejmować ataki oparte na złośliwym oprogramowaniu, oprogramowaniu typu ransomware, trojan oraz innych złośliwych działaniach o charakterze technicznym.
4. Moduł symulacji cyberataków musi obejmować ataki zawierające pełne taktyki, techniki i procedury cyberprzestępców (TTPs).
5. Moduł symulacji cyberataków musi obejmować ataki emulujące grupy typu Nation-State (sponsorowane przez obce Państwa) oraz Espionage (obcy wywiad).
6. Moduł symulacji cyberataków musi obejmować ataki emulujące grupy przestępcze ukierunkowane na kradzież danych i zasobów finansowych.
7. Moduł symulacji cyberataków musi obejmować ataki wykonujące rekonesans sieciowy i skanowania przygotowawcze przed docelowymi fazami.
8. Moduł symulacji cyberataków musi obejmować ataki, które wykorzystują techniki tunelowania w dobrze znanych/powszechnie używanych protokołach, przynajmniej SSH, http/https, DNS.
9. Moduł symulacji cyberataków musi obejmować ataki wykorzystujące techniki phishing, z przygotowanymi scenariuszami takich ataków.
10. Moduł symulacji cyberataków musi obejmować ataki wykorzystujące luki w zabezpieczeniach aplikacji, nie tylko systemów operacyjnych.
11. Moduł symulacji cyberataków musi zawierać rzeczywiste wskaźniki włamania (IOCs), w tym adresy URL, nazwy DNS i adresy IP i umożliwiać ich użycie, w bezpieczny sposób podczas wykonywania ataków.
12. Moduł symulacji cyberataków musi obejmować ataki z wykorzystaniem destrukcyjnego złośliwego oprogramowania (wchodzą w skład modułu i scenariuszy, które są przeprowadzane w kontrolowany sposób.
13. Moduł symulacji cyberataków musi obejmować opcję bezpiecznego wykonywania żądań internetowych do rzeczywistych złośliwych adresów URL.
14. Moduł symulacji cyberataków musi umożliwiać przeprowadzanie ataków na punkty końcowe przy jednoczesnym wykorzystaniu różnych profili użytkowników (na przykład systemu, administratorów, użytkowników, itp.).
15. Moduł symulacji cyberataków musi obejmować ataki opierające się na top 10 najistotniejszych w danym kwartale rodzinach malware, które muszą dostarczane przez Producenta podczas aktualizacji wraz z próbkami.
16. Kategoria top 10 najpopularniejszych/najistotniejszych rodzin złośliwego oprogramowania musi być wyselekcjonowana poprzez analityków Threat Intelligence dostawcy modułu rozwiązania.
17. Moduł symulacji cyberataków musi obejmować ataki oparte na prywatnych informacjach o zagrożeniach zbieranych przez Producenta, jak również na publicznie dostępnych informacjach o zagrożeniach, aby uwzględnić dane wejściowe z możliwie najszerszego spektrum.
18. Moduł symulacji cyberataków musi zawierać scenariusze ataków oparte na zachowaniu rzeczywistych grup APT, które znajdują się w bibliotece modułu.
19. Wszystkie ataki muszą być zorganizowane w oddzielnych etapach cyklu życia ataku, które są przewidziane w scenariuszach.
20. Moduł symulacji cyberataków musi obejmować co najmniej 100 ataków w każdej z wymaganych faz.
21. Moduł symulacji cyberataków musi obejmować co najmniej 500 ataków dla fazy Delivery oraz co najmniej 300 ataków dla fazy Execution.
22. Wszystkie ataki muszą być oznaczone/zmapowane do struktury MITRE v9 i NIST 800-53.
23. Moduł symulacji cyberataków musi udostępniać przejrzysty panel MITRE, prezentujący wykonane w ramach każdej z taktyk MITRE ataki, z możliwością rozwinięcia poszczególnych technik oraz subtechnik.
24. Moduł symulacji cyberataków musi obejmować co najmniej 25 ataków dla każdej taktyki MITRE.
25. Moduł symulacji cyberataków musi obejmować co najmniej 200 ataków dla każdej z taktyk Initial Access, Defense Evasion, Lateral Movement oraz C&C.
26. Biblioteka ataków musi zawierać zalecenia MITRE ATT&CK Mitigation i odpowiednie zadania kontrolne NIST 800-53 dla odpowiednich ataków.
27. Moduł symulacji cyberataków musi obejmować możliwość dostosowywania istniejących wcześniej ataków, z opcją klonowania i edycji wg własnych potrzeb.
28. Moduł symulacji cyberataków musi obejmować możliwość tworzenia zupełnie nowych niestandardowych ataków, w tym (między innymi):
	1. Malicious File Transfers – transfer niebezpiecznego wybranego pliku
	2. PCAP-based – wykorzystanie wybranej próbki ruchu
	3. Host CLI – lista komend
	4. Malicious DNS Query – zapytania DNS
	5. TCP Port Scan – skanowanie wybranych portów
	6. Web – ataki w wykorzystaniem przeglądarki
29. Moduł symulacji cyberataków musi zawierać znaczniki kontrolne dla wykonywanych procesów bezpieczeństwa we wszystkich atakach oraz możliwość dodawania niestandardowych znaczników w celu weryfikacji procesów bezpieczeństwa do każdego ataku.
30. Moduł symulacji cyberataków musi obejmować możliwość dodawania niestandardowych tagów (znaczników) do dowolnego ataku, w tym predefiniowanych sekwencji ataków.
31. Moduł symulacji cyberataków musi obejmować możliwość definiowania szablonów, które można wykorzystać do szybszego generowania niestandardowych ataków.
32. Moduł symulacji cyberataków musi obejmować możliwość wykorzystania złośliwego oprogramowania, na przykład oprogramowania ransomware, przesłanego przez użytkownika w ramach scenariusza ataku ransomware.
33. Moduł symulacji cyberataków musi obejmować możliwość wykorzystania w ramach ataków przechwyconych, przesłanych i dostosowanych pakietów danych.
34. Moduł symulacji cyberataków musi obejmować możliwość wykorzystania w ramach ataków przechwyconych pakietów, z pełnym odwzorowaniem połączeń sieciowych w nich zapisanych, tak jakby był to rzeczywisty network flow.
35. Moduł symulacji cyberataków musi obejmować anonimizację adresu IP i adresu MAC przy wykonywaniu ataków w oparciu o dostarczone pliki PCAP.
36. **Automatyzacja walidacji i wyniki**

**Wizualizacja infrastruktury:**

1. Moduł symulacji cyberataków musi zawierać funkcjonalność umożliwiającą graficzną reprezentację (mapę) topologii infrastruktury organizacyjnej.
2. Mapa graficzna musi obejmować systemy i urządzenia istotne dla procesu walidacji efektywności systemów bezpieczeństwa.
3. Mapa graficzna musi zawierać wybrane strefy bezpieczeństwa istotne dla walidacji.
4. Mapa graficzna musi uwzględniać kierunek przepływów w sieci między wszystkimi wizualnymi komponentami i musi wykluczać przepływy, które są blokowane przez systemy bezpieczeństwa i/ lub segmentację.
5. Moduł symulacji cyberataków musi monitorować pożądany, znany stan systemów kontroli bezpieczeństwa w odniesieniu do przeprowadzanych scenariuszy testowych i ataków oraz alarmować o wynikach testów, które odbiegają od oczekiwanych.
6. Moduł symulacji cyberataków musi umożliwiać zdefiniowanie oczekiwanych rezultatów każdego ataku i oczekiwanych alertów/komunikatów/zdarzeń generowanych przez SIEM i inne mechanizmy kontroli bezpieczeństwa wskazane przez operatora.
7. Moduł symulacji cyberataków musi ostrzegać w przypadku, gdy kontrola bezpieczeństwa lub stos zabezpieczeń nie reagują w sposób, w jaki została ustawiona linia bazowa, w odniesieniu do oczekiwanego alertu/zdarzenia lub zachowania blokującego/wykrywającego.

**Wykonywanie ataków:**

1. Moduł symulacji cyberataków musi umożliwiać bezpieczne emulowanie ataków na systemy i sieci produkcyjne.
2. Moduł symulacji cyberataków musi obsługiwać ataki w ramach zarówno sieci wewnętrznych jak i zewnętrznych organizacji, wraz z obrazowaniem wyników.
3. Moduł symulacji cyberataków musi umożliwiać użytkownikom zdefiniowanie dokładnej ścieżki ataku.
4. Moduł symulacji cyberataków musi umożliwiać testowanie prawdziwych zapytań do złośliwych adresów URL i złośliwych nazw DNS bez docierania tych zapytań do serwerów C&C.
5. Moduł symulacji cyberataków musi umożliwiać bezpieczne przeprowadzenie ataków w taki sposób, aby nie wpływać na inne wykluczone z testowania systemy i sieci produkcyjne Jednostek oraz Odbiorcy
6. Moduł symulacji cyberataków musi obejmować filtry wyszukiwania biblioteki ataków według wektora ataku, typu zachowania, systemu operacyjnego lub określonego systemu kontroli bezpieczeństwa.
7. Moduł symulacji cyberataków musi umożliwiać wykonywanie testów na żądanie bądź w określonych interwałach czasowych, cyklicznie i automatycznie.

**Wyniki testów:**

1. Moduł symulacji cyberataków musi zawierać wyniki dla każdego ataku, zawierające dokładny czas wykonania, użytkownika, który zainicjował test, fazę ataku oraz elementy systemów bezpieczeństwa biorące udział w wykryciu/prewencji ataku.
2. Wyniki każdego ataku muszą być automatycznie skorelowane z logami w rozwiązaniach SIEM i/lub systemami zbierania logów.
3. Wyniki każdego ataku muszą obejmować systemy bezpieczeństwa, które zignorowały, zaalarmowały i zapobiegły atakowi.
4. Moduł symulacji cyberataków musi zawierać możliwość eksportu wyników każdego ataku w formacie CSV.
5. Wyniki każdego ataku, który wygenerował alert lub blokadę, muszą zawierać powiązane nieprzetworzone dzienniki zdarzeń z systemów kontroli bezpieczeństwa (tzw. raw events) zbierane przez moduł.
6. Moduł symulacji cyberataków musi zawierać szczegółowe wyniki każdego zdarzenia wygenerowanego na podstawie alertu lub zablokowania, powiązanego z danym atakiem.
7. Moduł symulacji cyberataków musi obejmować możliwość wysyłania powiadomień do systemów zewnętrznych poprzez HTTP POST lub Syslog o zakończeniu ataku.

**Pulpity nawigacyjne i raportowanie:**

1. Moduł symulacji cyberataków musi zawierać graficzne dashboardy wyników walidacji skuteczności bezpieczeństwa.
2. Moduł symulacji cyberataków musi zawierać co najmniej jeden graficzny pulpit nawigacyjny, który przedstawia ilościowe wyniki według liczby ataków i procentu ataków według etapu.
3. Moduł symulacji cyberataków musi obejmować możliwość tworzenia i eksportowania raportów niestandardowych (za pomocą wbudowanego narzędzia do tworzenia raportów), które zapewniają wgląd w działanie narzędzi bezpieczeństwa.
4. Raporty niestandardowe muszą wykorzystywać informacje o atakach, które zostały wykonane i można je skonfigurować tak, aby wyświetlały dane w formie graficznej lub tabelarycznej.
5. Moduł symulacji cyberataków musi obejmować możliwość eksportowania wszystkich obrazów graficznych w pulpitach nawigacyjnych, raportach i mapach ataków.
6. Moduł symulacji cyberataków musi obejmować możliwość eksportowania głównych pulpitów nawigacyjnych, raportów i map ataków w formacie PDF.
7. Moduł symulacji cyberataków musi umożliwiać dynamiczną zmianę zakresu czasu w dashboardach.

**Obsługiwane przypadki użycia:**

1. Moduł symulacji cyberataków musi obejmować obsługę ciągłej oceny środków kontroli bezpieczeństwa, w wybranych przez operatora cyklach i zakresie.
2. Moduł symulacji cyberataków musi obejmować obsługę sprawdzania poprawności DLP.
3. Moduł symulacji cyberataków musi obejmować obsługę sprawdzania poprawności zapobiegania ransomware.
4. Moduł symulacji cyberataków musi obejmować wsparcie dla testów środowisk produkcyjnych na żywo, jeżeli takie będą wymagane przez operatora modułu.
5. Moduł symulacji cyberataków musi obejmować obsługę walidacji nowych, nieznanych segmentów sieci dołączanych do aktualnego środowiska
6. Moduł symulacji cyberataków musi obejmować wsparcie dla emulacji testów z wykorzystaniem profili grup APT/FIN.
7. Moduł symulacji cyberataków musi obejmować wsparcie dla red team-u.
8. Moduł symulacji cyberataków musi obejmować obsługę zespołu purple team.

**Rozszerzalność i automatyzacja:**

1. Moduł symulacji cyberataków musi zawierać dwukierunkowe REST API z opublikowaną dokumentacją.
2. Interfejs API modułu symulacji cyberataków musi obsługiwać zarówno formaty JSON, jak i XML.
3. Interfejs API modułu symulacji cyberataków musi obejmować możliwość listowania i manipulowania topologią infrastruktury, w tym komponentami walidacji, a także konfiguracją infrastruktury, taką jak ustalone strefy bezpieczeństwa.
4. Interfejs API modułu symulacji cyberataków musi obejmować możliwość listowania i manipulowania integracjami rozwiązań zabezpieczających.
5. Interfejs API modułu symulacji cyberataków musi obejmować możliwość tworzenia, aktualizowania i wykonywania ataków i sekwencji ataków oraz pobierania ich wyników.
6. Interfejs API modułu symulacji cyberataków musi obejmować możliwość listowania kont i ustawień użytkowników oraz manipulowania nimi.
7. Interfejs API modułu symulacji cyberataków musi obejmować możliwość eksportu danych wykorzystywanych we wszelkich graficznych panelach kontrolnych i raportach.

**VIII. Subskrypcja Threat Intelligence zasilająca moduł symulacji cyberataków**

1. Rozwiązanie musi być dostarczone wraz z subskrypcją Threat Intelligence (dostęp do usługi informacji o zagrożeniach) i pochodzić od tego samego Producenta co moduł symulacji cyberataków.
2. Subskrypcja Threat Intelligence musi być dostępny w formie usługi SaaS (oprogramowanie jako serwis) dostępnej dla co najmniej 20 administratorów.
3. Skuteczność dostarczonej subskrypcji Threat Intelligence, musi być potwierdzona w dostępnych publicznie raportach, przynajmniej dla „The Forrester WaveTM: External Threat Intelligence Services” lub innych równoważnych raportach.
4. Dostępność portalu (SLA), jak i API musi wynosić co najmniej 99,9%.
5. Limit zapytań API musi wynosić minimum 1 milion zapytań miesięcznie.
6. Limit API musi być rozliczany w cyklach miesięcznych, bez limitów dobowych i tygodniowych.
7. Obsługa subskrypcji Threat Intelligence musi odbywać się przez przeglądarkę internetową (Chrome lub Firefox) oraz API.
8. Dostawca subskrypcji Threat Intelligence musi zapewnić co najmniej 50 000 nowych IoC miesięcznie.
9. Subskrypcja Threat Intelligence musi zbierać zagrożenia związane z Intelligence nie tylko ze źródeł open source (OSINT) i danych typu machine learning, ale także dane zbierane o grupach APT/FIN/TEMP przez wyspecjalizowany zespół i narzędzia.
10. Subskrypcja Threat Intelligence musi posiadać niepubliczne źródła danych o zagrożeniach, w tym darknet.
11. Subskrypcja Threat Intelligence musi posiadać możliwość pobrania IoC dla zagrożeń w formatach co najmniej XML, STIX, CSV.
12. Subskrypcja Threat Intelligence musi udostępniać informacje o zagrożeniach i jego kontekście w zakresie: celu i motywacji aktora, grupy, rodzaju stosowanego malware, metod mitygacji zagrożeń, ocen wiarygodności źródła.
13. Informacje o zagrożeniach muszą posiadać wskazówki jak chronić się przed atakami.
14. Subskrypcja Threat Intelligence musi udostępniać dane o zagrożeniach z informacjami co najmniej o: adresach IP, adresach URL, adresach e-mail, domenach, hash/skrótach plików lub ich nazwach.
15. Subskrypcja Threat Intelligence musi posiadać w swojej bazie co najmniej 50 000 dedykowanych raportów bezpieczeństwa.
16. Subskrypcja Threat Intelligence musi udostępniać graf połączeń pomiędzy Threat Actor (adwersarz zagrożenia, grupa przestępcza) a technikami, jakie wykorzystuje, rodzinami malware powiązanymi z danym Threat Actor, oraz IoCs skojarzonymi z daną grupą.
17. Subskrypcja Threat Intelligence musi udostępniać narzędzie do filtrowania technik/taktyk MITRE, które są wykorzystywane przez wskazanych Threat Actors.
18. Subskrypcja Threat Intelligence udostępniająca dane o zagrożeniach musi posiadać możliwość wyszukiwania po parametrach dostępnych w zagrożeniach, a także danych lokalnych specyficznych dla danego kraju czy sektora (gałęzi) gospodarki celem lepszej klasyfikacji danych.
19. Subskrypcja Threat Intelligence musi udostępniać dane Intel (TTP) dedykowane dla szpiegostwa gospodarczego.
20. Subskrypcja Threat Intelligence musi udostępniać dane Intel (TTP) dedykowane dla wyłudzeń danych.
21. Subskrypcja Threat Intelligence musi udostępniać dane Intel (TTP) dedykowane dla sektora rządowego.
22. Subskrypcja Threat Intelligence musi posiadać TTP (taktyki, narzędzia, procedury) oraz IoC zebrane podczas procesów Incident Response wykonywanych dla innych klientów, którzy zlecili takie zadania.
23. Subskrypcja Threat Intelligence musi dostarczać informacje o aktualnych trendach w cyberbezpieczeństwie na podstawie doniesień medialnych (światowych).
24. Subskrypcja Threat Intelligence musi posiadać informacje o grupach malware lub pojedynczych rodzinach malware sklasyfikowanych i łatwych w nawigacji w portalu www.
25. Subskrypcja Threat Intelligence poza informacjami technicznymi musi dostarczać kontekst zagrożeń w tym kontekst działalności grup APT/FIN.
26. Subskrypcja Threat Intelligence musi posiadać informacje o zagrożeniach związanych z RANSOMWARE.
27. Subskrypcja Threat Intelligence musi posiadać dedykowane informacje dla ukierunkowanych zagrożeń dla Polski i możliwość ich filtracji na portalu www.
28. Subskrypcja Threat Intelligence musi posiadać możliwość analizy próbek (pliki, adresy URL, skróty plików, adresy IP) w celu potwierdzenia zagrożenia i musi udostępniać pełną informacje na temat wyszukanych domen czy próbek malware dostępną w źródłach producenta.
29. Subskrypcja Threat Intelligence musi posiadać bazę o zagrożeniach malware co najmniej dla: backdoor, botnet, webshell, crypto-miner, credential-harvester, driver, exploit, installer, keylogger, lateral movement, macro, proxy, rootlet, screen-capture, shell-code, sniffer, spambot, tunneler, uploader, utility.
30. Subskrypcja Threat Intelligence musi posiadać bazę zagrożeń dla Systemu Android, Linux, Mac OSX, Windows.
31. Subskrypcja Threat Intelligence musi posiadać informacje kontekstową dla co najmniej 80 grup APT/FIN/TEMP, w tym szczególnie aktywnych w Polsce: APT32, APT37, APT41, Turla Team, FIN1, FIN7, Temp. Armageddon, ZeroWing Team.
32. Subskrypcja Threat Intelligence musi posiadać API w celu integracji z innymi Systemami z opisaną dokumentacją i przykładami wykorzystania w różnych językach skryptowych.
33. Subskrypcja Threat Intelligence musi posiadać profile Threat Actor i skorelowane z nimi TTPs, które mogą być w sposób automatyczny zaimportowane do systemu klasy Breach and Attack Simulation, w wyniku czego system BAS będzie zawierał scenariusze ataków, które będą możliwe do przetestowania we własnym środowisku. W ramach integracji muszą być przekazywane realne próbki malware oraz narzędzia, wykorzystywane przez grupy APT/FIN.
34. Subskrypcja Threat Intelligence musi posiadać dodatkowe mechanizmy ułatwiające wyszukiwanie IoC na przeglądanych stronach www – dedykowana wtyczka do przeglądarki.
35. Subskrypcja Threat Intelligence musi umożliwiać dostęp na żądanie do analityków bezpieczeństwa Producenta modułu.
36. Subskrypcja Threat Intelligence musi posiadać tagi kategoryzujące informacje w celu lepszego wyszukiwania.

**IX.** **Dodatkowa Subskrypcja Threat Intelligence zasilająca moduł symulacji cyberataków**

1. W ramach dostawy platformy symulacji cyberataków wymagane jest dostarczenie uzupełniającej subskrypcji Threat Intelligence, od innego Producenta niż moduł symulacji cyberataków.
2. Skuteczność dostarczonej dodatkowej subskrypcji Threat Intelligence, musi być sklasyfikowana w dostępnych publicznie raportach, przynajmniej dla Frost Radar: Global Cyber Threat Intelligence Market. lub innych równoważnych raportach.
3. Dodatkowa Subskrypcja Threat Intelligenece musi zawierać dane z publicznych/otwartych źródeł danych np. strony internetowe, repozytoria kodu itp.
4. Dodatkowa Subskrypcja Threat Intelligenece musi zawierać dane z niepublicznych/zamkniętych źródeł danych np. portale i fora dostępne za pośrednictwem sieci TOR, portale i fora dostępne z sieci darknet, portale i fora wymagające weryfikacji użytkownika przed nadaniem dostępu. Nie mniej niż 1500 Forum Hakerskich i Dark Netowych.
5. Dodatkowa Subskrypcja Threat Intelligenece musi być zasilany wskaźnikami zagrożeń takim jak np. IP, Domeny, URLe, skróty plików. Nie mniej niż 55 źródeł “Threat Feeds”.
6. Dodatkowa Subskrypcja Threat Intelligenece musi zawierać dane z źródeł o charakterze technicznym np. witryny służące do analizy złośliwego oprogramowania.
7. Dodatkowa Subskrypcja Threat Intelligenece musi zawierać uzupełniające informacje:
	1. dostarczane przez firmy trzecie, w tym co najmniej: Shodan, Avast, URLscan, itp.
	2. dostarczane z zaufanych źródeł np. organizacji zajmujących się bezpieczeństwem takie jak ISAC, organy rządowe, VISA itp
8. Dodatkowa Subskrypcja Threat Intelligenece musi poddawać weryfikacji dane dostarczane przez firmy trzecie.
9. Dodatkowa Subskrypcja Threat Intelligenece musi zawierać dane z otwartych źródeł darknetu.
10. Dodatkowa Subskrypcja Threat Intelligenece musi zawierać dane z chronionych źródeł darknetu wymagających weryfikacji użytkownika.
11. Dodatkowa Subskrypcja Threat Intelligenece musi zawierać dane pozyskane w wyniku bezpośredniej interakcji z użytkownikami darknetu, np. zamknięte fora, sklepy itp.
12. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość śledzenia sieci botnetów.
13. Dodatkowa Subskrypcja Threat Intelligenece musi wykorzystywać przetwarzanie języka naturalnego (NLP) do głębokiej analizy danych dostępnych w minimalnie 10 językach, w tym:
* arabski
* chiński (zarówno pismo uproszczone, jak i tradycyjne)
* angielski
* perski
* japoński
* rosyjski
1. Dodatkowa Subskrypcja Threat Intelligenece musi wykorzystywać wzorce tekstowe do wykrywania:
* adresów URL
* adresów IP
* adresów Email
* skrótów plików (hash)
* nazwy użytkowników treści publikowanych na Twitterze

dla:

* Treści w dowolnym języku
* Kod źródłowy w różnych językach programowania
* Tekstu oraz plików logów
1. Dodatkowa Subskrypcja Threat Intelligenece musi udostępniać dostęp do danych o zagrożeniach za pośrednictwem interfejsu API wykorzystującego JSON, TAXII oraz CVS-STIX.
2. Licencja dodatkowej Subskrypcja Threat Intelligenece nie może w żadnym elemencie i zakresie limitować ilości zapytań API.
3. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać graficzny kreator zapytań API, automatycznie generujący kod zapytania przynajmniej dla:
* cURL
* Python
* JavaScript
1. Dodatkowa Subskrypcja Threat Intelligenece musi umożliwiać eksport danych do formatów:
* JSON
* CSV
* STIX
* PPT
* PNG
* PDF
* Dokumenty MS Word
1. Dodatkowa Subskrypcja Threat Intelligenece musi umożliwiać kontrolę dostępu opartą na rolach użytkowników.
2. Dodatkowa Subskrypcja Threat Intelligenece musi dbać o bezpieczeństwo zbioru danych o klientach wykorzystując co najmniej:
* Szyfrowanie i haszowanie haseł
* Wykorzystanie aktywnego system anty DDoS
* Automatycznego blokowania konta przy braku aktywności
* Rozbudowana kontrola dostępu do obiektów
* Uwierzytelnienie wieloskładnikowe
* Kompleksowy program analizy zagrożeń
* Automatyczne skany podatności systemów
* Bieżące testy penetracyjne
* Rozbudowany system budowania świadomości i szkolenia personelu
* Posiadanie dedykowanego zespołu do analizy podatności w rozwiązaniu
* Prowadzenie analizy danych z darknetu, otwartych i technicznych źródeł informacji w celu pojawiających się zagrożeń, które mogą mieć wpływ na organizację
1. Dodatkowa Subskrypcja Threat Intelligenece musi wykorzystywać mechanizmy uczenia maszynowego, przetwarzanie języka naturalnego oraz technologii rozpoznawania wzorców do gromadzenia, indeksowania i analizowania danych o zagrożeniach w celu aktualizacji informacji w czasie rzeczywistym.
2. Dodatkowa Subskrypcja Threat Intelligenece musi umożliwiać integrację z systemami firm trzecich w celu wzbogacenia informacji w tych systemach. Integracje muszą obejmować między innymi:
* Palo Alto Networks,
* Splunk,
* ArcSight,
* QRadar
* RSA Security Analytics
* Maltego
1. Dodatkowa Subskrypcja Threat Intelligenece nie może być ograniczona do konkretnych regionów geograficznych.
2. Dodatkowa Subskrypcja Threat Intelligenece musi zapewniać kontekst do:
* Adresów IP
* Domen
* Skrótów plików (hash)
* Złośliwego oprogramowania
1. Dodatkowa Subskrypcja Threat Intelligenece musi zapewnić informacje dotyczące organizacji w celu ochrony jej marki.
2. Dodatkowa Subskrypcja Threat Intelligenece musi generować alerty dotyczące informacji o organizacji na podstawie agregacji danych, przynajmniej z wskazanych źródeł:
* Rejestracji domen
* Wpisów w mediach społecznościowych
* Stron zawierających podejrzane treści
1. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość wyszukiwania i usuwania danych organizacji przynajmniej w zakresie:
* Typosquattingu domen (technika oszukiwania użytkowników Internetu wykorzystująca typowe błędy literowe popełniane w trakcie wpisywania adresów internetowych)
* Wycieków danych logowania
* Identyfikatorów bankowych
* Fałszywych kont w mediach społecznościowych
* Wycieków kodu źródłowego
* Rozmów o organizacji w ramach darknetu
1. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość analizy stanu bezpieczeństwa firm trzecich.
2. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość korelacji incydentów cyberbezpieczeństwa organizacji z zewnętrznymi wskaźnikami zagrożeń, w celu ułatwienia identyfikacji istotnych zagrożeń przez analityków bezpieczeństwa w organizacji.
3. Dodatkowa Subskrypcja Threat Intelligenece musi łączyć zebrane informacje i analizować zagrożenia w sposób umożliwiający ich wykorzystanie jako element proaktywnej strategii analizy bezpieczeństwa.
4. Dodatkowa Subskrypcja Threat Intelligenece musi wykorzystywać uczenie maszynowe i automatyzację do agregacji danych w celu zapewnienia kontekstu dotyczącego jaki aktor atakuje organizację, jaką ma motywację, możliwości oraz jakich wskaźników powinniśmy szukać w systemach bezpieczeństwa w celu jego wykrycia.
5. Dodatkowa Subskrypcja Threat Intelligenece musi pomagać w ustalaniu priorytetów usuwania podatności na podstawie aktualnych trendów exploitacji.

**Wymagania ochrony marki**

1. Dodatkowa Subskrypcja Threat Intelligenece musi przeszukiwać informacje w sieci darknet, zarówno automatycznie jak i ręcznie.
2. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje z portali w mediach społecznościowych w tym przynajmniej Twitter.
3. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i wykrywać potencjalne podszywanie się pod kierownictwo organizacji na portalu Linkedin.
4. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje dostępne na publicznych kanałach YouTube.
5. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i Analizować informacje dostępne na Xing.
6. Dodatkowa Subskrypcja Threat Intelligenece musi generować alerty na podstawie zagregowanych danych z profili w mediach społecznościowych, w tym VK.com
7. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować Google PlayStore w celu wykrywania fałszywych/niebezpiecznych aplikacji.
8. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować Apple App Store w celu wykrywania fałszywych/niebezpiecznych aplikacji.
9. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje z publicznych jak i prywatnych kanałów na Telegram i Discord.
10. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje z serwisów aukcyjnych w tym przynajmniej eBay.
11. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje z portali dostępnych w darknecie oferujących sprzedaż nielegalnych towarów, usług oraz skradzionych danych.
12. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje z portali do udostępniania/przesłania tekstu takich jak Pastebin. Nie miej niż 50 portali.
13. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje z portali do przechowywania repozytoriów kodu w tym przynajmniej GitHub.
14. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje z portali rejestrujących domeny.
15. Dodatkowa Subskrypcja Threat Intelligenece musi monitorować i analizować informacje z kanałów rejestracji certyfikatów SSL. Subskrypcja powinna koncentrować się na domenach, które są widziane po raz pierwszy w CTL. Takie działanie musi pozwalać na rozszerzenie wiedzy na temat subdomen, FQDN jak i TLD których rejestratorzy domen mają na celu zapewnienie dużej prywatności i utajnienie danych.
16. Dodatkowa Subskrypcja Threat Intelligenece musi obsługiwać wykrywanie podszywania się pod kierownictwo firmy, strony internetowe, domeny i logo.
17. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość wykrywania przejętych kont na portalach społecznościowych, w tym przynajmniej Linkedin i Twitter.
18. Dodatkowa Subskrypcja Threat Intelligenece musi wykrywać wycieki danych PII (Personally Identifiable Information) w tym adresy email, hasła i dane osobowe kadry kierowniczej.
19. Dodatkowa Subskrypcja Threat Intelligenece musi wykrywać naruszenia związane z znakiem towarowym.
20. Dodatkowa Subskrypcja Threat Intelligenece musi wykrywać techniki Typosquattingu domen na podstawie danych od rejestratorów domen.
21. Dodatkowa Subskrypcja Threat Intelligenece musi analizować informacje w celu zidentyfikowania danych uwierzytelniających, które mogą być nazwami użytkowników, loginami oraz hasłami. Źródłem danych do analizy musi być Internet jak i Darknet. Źródła w szczególności powinny obejmować:
* Portale typu Pastebin
* Blogi
* Fora dyskusyjne
* Kanały IRC
* Media społecznościowe
* Niszowe strony
* Raporty techniczne złośliwego oprogramowania/luk w zabezpieczeniach
* Wiadomości mainstreamowe
* Giełdy finansowe
* Oficjalne komunikaty rządowe
* Wiadomości inwestycyjne
* Oficjalne listy firmowe
* Organizacje pozarządowe
* Czasopisma branżowe
* Podcasty
* Komunikaty prasowe
* Czasopisma naukowe
1. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać komponent umożliwiający zgłoszenie co najmniej w zakresie:
* Globalnego zablokowania nazwy domenowej
* Globalnego zablokowania wskazanych adresów URL
* Usunięcia wpisów w mediach społecznościowych (np. fałszywy profil na Twitter, fałszywe ogłoszenia o pracę na Linkedin)
* Usunięcia fałszywych aplikacji mobilnych z oficjalnych sklepów z aplikacjami (np. AppStore, GooglePlay))
* Wyłączenia serwerów złośliwego oprogramowania (C&C, repozytoria złośliwego oprogramowania)
1. Dodatkowa Subskrypcja Threat Intelligenece musi umożliwiać śledzenie zgłoszonego żądania usunięcia danych przy pomocy dostarczonego interfejsu użytkownika.
2. Dodatkowa Subskrypcja Threat Intelligenece musi umożliwiać śledzenie danych, których usunięcie nie powiodło się.

**Wymagania do zakresu gromadzenia, przetwarzania i analizy danych o zagrożeniach**

1. Dodatkowa Subskrypcja Threat Intelligenece musi udostępniać platformę typu sandbox do analizy złośliwego oprogramowania z możliwością wygenerowania raportu z analizy w formacie JSON. Analizowane próbki złośliwego oprogramowania musza być automatycznie mapowane na techniki MITRE ATT&CK. Każdy raport z analizy próbek złośliwego oprogramowania musi zawierać wyodrębnione:
* Domeny
* Adresy URL
* Adresy IP
* Skróty plików

które są korelowane w oferowanym rozwiązaniu w celu uzyskania dodatkowych informacji.

1. Dodatkowa Subskrypcja Threat Intelligenece musi zapewniać informacje na temat aktywności zagrożeń takich jak informacje dotyczące IoC.
2. Dodatkowa Subskrypcja Threat Intelligenece musi zapewniać kontekst związany z IoC taki jak metody ataków i informacje o aktorach.
3. Dodatkowa Subskrypcja Threat Intelligenece musi prezentować ocenę ryzyka dla obiektów w tym minimum dla:
* adresy IP
* domeny
* URL
* Hashe (skróty plików)
* CVE
* firmy/organizacje

Ocena ryzyka musi być określana na bazie predefiniowanych reguł ryzyka dedykowanych i specyficznych dla każdej kategorii obiektu.

1. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać API STIX oraz TAXII zgodne ze standardami TAXII HTTPS 1.0 i TAXII XML.
2. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać interfejsy RESTful API do integracji z systemami zewnętrznymi.

Integracja musi być zapewniona dla:

* SIEM
* SOAR
* EDR
* Systemów „tiketowych”
* Systemów skanowania/zarządzania podatnościami
1. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać przygotowaną możliwość integracji ze Splunk poprzez oficjalną aplikację znajdującą się na splunkbase.splunk.com
2. API dodatkowej Subskrypcji Threat Intelligenece musi umożliwić filtrowanie i dostosowywanie wyników zapytań.
3. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość wzbogacania informacji zawartych bezpośrednio w systemach klasy SIEM w tym:
* Splunk
* QRadar
* Exabeam
* ArcSight
* Sentinel
1. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać integrację z systemami klasy SOAR w tym:
* Siemplify
* Phantom
* XSOAR

Pozwalającą na obsługę poniższych przypadków użycia:

* Wzbogacanie
* Korelacja
* Monitoring
* Threat Hunting
1. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość wykrywania i monitorowania stron phishingowych oraz repozytoriów złośliwego oprogramowania.
2. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość generowania dla konkretnych zagrożeń lub aktorów np. QakBot, FickerStealer, kolektyw haktywistów Bax 026.
3. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość zamówienia raportów tworzonych na podstawie specjalnych wymagań klienta.
4. Dodatkowa Subskrypcja Threat Intelligenece musi tworzyć profile dla grup przestępczych zawierające poniższe dane:
* Atakowane przedsiębiorstwa i organizacje
* notatki i artykuły opracowane przez analityków producenta
* kategoria grupy (np. sponsorowana przez państwo)
* Skróty plików
* Adresy e-mail
* Domeny
* Technologie
* Adresy IP
* Kraje
* Złośliwe oprogramowanie i kategorie złośliwego oprogramowania
* Wykorzystywane luki w zabezpieczeniach
* Nazwy użytkowników
* Wektory ataku
* Referencje
1. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać profile dla grup przestępczych, minimum:
* 180 grup APT
* 200 grup o profilu haktywistycznym
1. Dodatkowa Subskrypcja Threat Intelligenece musi udostępniać i aktualizować relacje pomiędzy grupami przestępczymi.
2. Dodatkowa Subskrypcja Threat Intelligenece musi umożliwić użytkownikom wyszukiwanie informacji dotyczących cyberprzestępców, którzy atakują określone branże, w tym:
* Handel detaliczny
* Państwa
* Finanse
* Telekomunikacja
1. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać możliwość analizy zdarzeń geopolitycznych w tym:
* Geolokalizacja
* Zamachy terrorystyczne
* Wojna
* Ćwiczenia wojskowe
1. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać możliwość wyszukiwania danych przez konstruowanie bardzo szczegółowych zapytań.
2. Dodatkowa Subskrypcja Threat Intelligenece musi zapewnić bezpośredni dostęp do analityka, aby w razie potrzeby mógł udzielić wyjaśnień i pomocy dla specyficznych analiz klienta.
3. Dodatkowa Subskrypcja Threat Intelligenece musi przechowywać wszystkie zebrane dane historyczne. Na moment wdrożenia modułu dane historyczne muszą sięgać minimum 10 lat wstecz.
4. Dodatkowa Subskrypcja Threat Intelligenece musi zawierać dane typu WHOIS.
5. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać wbudowaną bazę zapytań.
6. Dodatkowa Subskrypcja Threat Intelligenece musi posiadać możliwość wyszukiwania przy użyciu operatorów logicznych, w tym minimalnie AND i OR.
7. Dodatkowa Subskrypcja Threat Intelligenece musi mieć możliwość zapisywania zapytań wyszukiwania w celu szybkiego ich wykorzystania ich w późniejszym czasie.
8. Dodatkowa Subskrypcja Threat Intelligenece musi umożliwiać zapisywania zapytań wyszukiwania jako prywatne lub współdzielone oraz minimum jako do odczytu i do edycji.
9. Dodatkowa Subskrypcja Threat Intelligenece musi generować alerty do bieżąco monitorowanych informacji i danych. Alerty muszą mieć możliwość ustawiania częstotliwości uruchamiania:
* Co 5 min
* Co 15 min
* Co godzinę
* Co 4 godziny
* Co 8 godzin
* Raz dziennie
* Raz w tygodniu
1. Dodatkowa Subskrypcja Threat Intelligenece musi umożliwiać budowę nie mniej niż 3000 warunków do generowania alertów.
2. Dodatkowa Subskrypcja Threat Intelligenece musi mapować zaobserwowane techniki, taktyki oraz schematy zagrożeń na Mitre ATT&CK framework
3. Dodatkowa Subskrypcja Threat Intelligenece musi zapewniać interaktywne widoki analityczne w tym:
* Oś czasu
* Tabela
* Mapa
* Mapa źródeł
* Feedy

**X. Szkolenia**

1. Wymagane jest przeprowadzenie dwóch szkoleń po 5-ciu uczestników, każde w terminie uzgodnionym z Zamawiającym w okresie obowiązywania umowy lecz nie później niż 6 miesiecy od daty podpisania umowy.
2. Czas trwania Szkolenia powinien wynosić minimum cztery dni robocze.
3. Wszystkie koszty z wiązane z organizacją, przeprowadzeniem, zapewnieniem ewentualnego transportu uczestnikom, materiałów szkoleniowych itp. pokrywa Wykonawca.
4. Szkolenie musi zostać przeprowadzone z wykorzystaniem dedykowanego laboratorium treningowego przygotowanego przez Producenta oprogramowania modułu symulacji cyberataków umożliwiającego przeprowadzenie co najmniej scenariuszy ćwiczeń typu „Capture the Flag”.
5. Szkolenie musi obejmować swoim zakresem specjalistyczną wiedzę z dostarczanego modułu symulacji cyberataków i obejmować przygotowanie uczestników w zakresie administrowania systemem, rozwiązywania problemów i utrzymania Systemu.
6. Szkolenie w swoim zakresie musi uwzględniać przynajmniej tematykę opisaną poniżej:
	1. wykonywanie zautomatyzowanych testów penetracyjnych, wraz z opisem procesów i typów
	2. zarządzanie i wykorzystywanie podatności
	3. opis umiejętności zakresie przeprowadzania testów automatycznych
	4. metodologia testów penetracyjnych
	5. narzędzia testów, automatyczne i manualne
	6. testy i symulacje ataków wewnętrznych i zewnętrznych.
	7. omijanie zabezpieczeń Firewall
	8. testy penetracyjne dla Windows oraz ich symulacja
	9. testy penetracyjne dla Linux oraz ich symulacja
	10. wykonywanie ataków na aplikacje web
	11. wykonywanie ataków na bazy danych
	12. ataki i symulacje dla segmentów centrów danych
	13. symulacje ataków dla środowisk chmurowych
	14. raportowanie wyników analiz
	15. przeprowadzenie minimum 5 scenariuszy ćwiczeń „Capture the Flag

## Wymagania w zakresie asysty technicznej eksperta

1. Zapewnienie usługi asysty technicznej w maksymalnej ilości 200 roboczogodzin, w okresie obowiązywania umowy, świadczonej w języku polskim.
2. Świadczenie usługi asysty technicznej jest uprawnieniem Odbiorcy. Niewykorzystanie w całości lub w jakiejkolwiek części przewidzianych w umowie roboczogodzin, nie rodzi po stronie Wykonawcy żadnych roszczeń z tego tytułu w stosunku do Zamawiającego lub Odbiorcy.
3. W roboczogodzinę asysty technicznej eksperta nie wlicza się czasu dojazdu oraz ilości osób zapewniających wsparcie tzn. nie ma znaczenia ile osób będzie świadczyło asystę techniczną eksperta w danej roboczogodzinie/roboczogodzinach u Odbiorcy. Rozliczenie roboczogodzin asysty technicznej eksperta odbywać się będzie za faktycznie wykorzystane roboczogodziny na podstawie Protokołów odbioru asysty technicznej eksperta. Do godzin asysty technicznej eksperta nie wlicza się roboczogodzin usług wykonywanych w ramach realizacji zgłoszeń awarii Systemu.
4. Asysta techniczna eksperta będzie dotyczyła oferowanego przez Wykonawcę Systemu i będzie polegała w szczególności na:
	1. bieżącym utrzymaniu i zarządzeniu Systemem,
	2. konsultacji w zakresie szczegółowej analizy zdarzeń generowanych przez System
	z wyłączeniem awarii,
5. Osoby uprawnione w umowie przez Odbiorcę będą przekazywać Wykonawcy zlecenia asysty technicznej, w których każdorazowo określony zostanie przedmiot zlecenia, oczekiwany termin realizacji zlecenia oraz miejsce realizacji zlecenia.
6. Wykonawca w terminie wyznaczonym przez Odbiorcę, od otrzymania zlecenia, przekaże Odbiorcy propozycję sposobu wykonania zlecenia zawierającą w szczególności wycenę prac zawartych w zleceniu, tj. proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
7. Odbiorca może zaakceptować propozycję sposobu wykonania zlecenia albo odrzucić ją, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, dodatkowych wyjaśnień, informacji do przedstawionej propozycji sposobu wykonania zlecenia.
8. Odbiorca zastrzega sobie prawo do zakwestionowania zaproponowanego przez Wykonawcę terminu realizacji oraz wyceny zleconych prac. W takiej sytuacji, Strony w drodze uzgodnień doprowadzą do akceptowalnej wyceny zleconych prac oraz terminu ich realizacji, co zostanie potwierdzone pisemnie, poprzez aktualizację zlecenia asysty technicznej.
9. Odbiorca zastrzega sobie prawo do ostatecznego odrzucenia propozycji Wykonawcy i rezygnacji z realizacji zleconych prac, bez ponoszenia kosztów opisu sposobu wykonania zlecenia i przygotowania wyceny przez Wykonawcę.
10. W przypadku akceptacji propozycji sposobu wykonania zlecenia, Odbiorca przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, kwotę wynagrodzenia należnego za zrealizowanie zlecenia, termin wykonania prac.
11. Rozliczenie asysty technicznej odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Odbiorcę, Protokołów odbioru asysty technicznej eksperta.
12. Odbiorca może wyrazić zgodę na wykonanie zlecenia zdalnie, w takim przypadku Wykonawca zobowiązany jest do przestrzegania wszystkich wymagań Odbiorcy. Odbiorca zastrzega sobie prawo do odmowy, przerwania świadczenia usługi zdalnego dostępu w dowolnym momencie bez wcześniejszego informowania Wykonawcy.