Załącznik nr 1 do Zapytania

162848

Opis Przedmiotu Zamówienia

1. Przedmiot zamówienia.

1.1. Przedmiotem zamówienia jest **Dostawa licencji do platformy Cyber Threat Intelligence** (dalej Platforma) rozumiana jako dostawa Licencji umożliwiających Zamawiającemu dostęp do Platformy wraz ze wsparciem producenta, na zasadach określonych w OPZ

1.2. Realizacja przedmiotu zamówienia polega na dostawie licencji uprawniającej do 24 miesięcznego dostępu do platformy Cyber Threat Intelligence (CTI).

1.3. W szczególności przedmiot zamówienia obejmuje:

1.3.1. dostawę niezbędnych licencji.

1.3.2. świadczenie usługi wsparcia producenta przez okres 24 miesięcy od daty dostarczenia licencji.

1.3.3. zaimportowanie reguł, filtrów oraz skonfigurowanie API.

1.4. Zamawiający wymaga przeprowadzenia testów Proof of Concept wszystkich lub wybranych funkcjonalności na etapie wyboru ofert w celu weryfikacji zgodności z OPZ.

2. Udostępnienie Platformy.

2.1. Wykonawca zapewni działanie 5 kont dostępowych do Platformy dla wskazanych przez Zamawiającego dwóch analityków.

2.2. Wykonawca zapewni działanie konta niezbędnego do pobierania informacji za pomocą dedykowanego połączenia, np. API.

2.3. Dostęp do Platformy przyznany zostanie na 24 miesiące.

3. Wymagania minimalne dla platformy CTI:

3.1. **Architektura Systemu.**

3.1.1. Platforma powinna być udostępniona jako usługa typu SaaS (Software-as-a-Service) dostępna co najmniej przez przeglądarkę internetową.

3.1.2. Usługa musi być dostępna za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w wersjach aktualnych na dzień składania oferty.

3.1.3. Wymagana jest możliwość wykorzystania mechanizmu proxy do komunikacji z Platformą.

3.1.4. Platforma musi być dostępna poprzez szyfrowany protokół TLS w wersji co najmniej 1.2.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.1.5. Platforma musi wspierać konfigurację wielośrodowiskową (multi-tenancy) dla minimum 2 niezależnych środowisk, gdzie każde sub-środowisko będzie posiadać osobną konfigurację monitorowanych zasobów, filtrów lub innych specyficznych ustawień.

3.2. **Wymagania odnośnie producenta**

3.2.1. Producent Platformy musi posiadać ważną certyfikację ISO 27701 oraz być zgodny z GDPR/RODO.

3.2.2. Producent Platformy musi posiadać ważną certyfikację SOC 2 Type II.

3.2.3. Producent Platformy musi posiadać usługę wsparcia od dedykowanego konsultanta technicznego, która uwzględnia minimum autorskie szkolenia (polsko języczny konsultant), konsultacje alarmów i wyników, wsparcie i konsultacje przy wykorzystaniu API rozwiązania, wdrożenie i rozwój PIR (Priority Intelligence Requirements), przekazywanie strategicznych informacji wywiadowczych, cykliczny przegląd architektury.

3.2.4. Producent Platformy musi zapewnić wsparcie na etapie wdrożenia rozwiązania.(j.polski) z UoP.

3.2.5. Producent Platformy musi posiadać dedykowany zespół analityków CTI, których zadaniem jest opracowywanie raportów z bieżących zagrożeń w kraju i na świecie.

3.3. **Zarządzanie dostępem do Platformy.**

3.3.1. Platforma musi umożliwiać przyznanie indywidualnych kont dla każdego z 5 analityków do wszystkich obligatoryjnych funkcjonalności w punkcie 3.4.

3.3.2. Platforma musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Platformy.

3.3.3. Platforma musi zapewnić możliwość przyznania dostępów na podstawie ról, tzw. RBAC (Role Based Access Control) lub inną metodę pozwalającą na granulację dostępów do modułów i konfiguracji.

3.3.4. Platforma musi umożliwiać logowanie wieloskładnikowe, tzw. MFA (Multifactor Authorization) np. za pomocą rozwiązania typu OTP (One-Time Password).

3.4. **Obligatoryjne wymagania funkcjonalne.**

3.4.1. Platforma musi być dostępna w trybie 24h / 7 przez cały rok z SLA na poziomie 99,5 , za wyjątkiem zgłoszonej wcześniej niedostępności.

3.4.2.Informacje zawarte w Platformie muszą być wzbogacone o notatki i analizy opracowane przez zespół analityczny producenta.

3.4.3. Platforma nie może być ograniczona tylko do wybranych regionów geograficznych.

3.4.4. Baza danych platformy nie może być różna dla zakupionych kont. Jedyna różnica może wynikać z zakresu licencji lub przyznanych użytkownikom ról.

3.4.5. Platforma musi umożliwiać automatyczne wzbogacanie informacji o kontekst, odniesienia oraz powiązane informacje w celu budowy kompletnej informacji.

3.4.6. Platforma musi pozwalać na tzw. Drill Down, czyli drążenie w wynikach wyszukiwania bez konieczności tworzenia za każdym razem nowych zapytań.

3.4.7. Platforma musi wspierać algorytmy Natural Language Processing co najmniej w językach:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.4.7.1. Polski
3.4.7.2. Angielski
3.4.7.3. Rosyjski
3.4.7.4. Chiński
3.4.7.5. Arabski
3.4.7.6. Perski

3.4.8. Platforma musi zbierać i udostępniać dane z raportów oraz analiz bezpieczeństwa:
3.4.8.1. Producentów oprogramowania
3.4.8.2. Dostawców rozwiązań z zakresu cyberbezpieczeństwa.
3.4.8.3. Autorów analiz malware.
3.4.8.4. Własnych

3.4.9. Platforma musi zbierać dodatkowe informacje z niżej wymienionych źródeł trzecich:
3.4.9.1. Shodan
3.4.9.2. Polyswarm
3.4.9.3. URLScan
3.4.9.4. Autoryzowane CSIRTy
3.4.9.5. Inne agencje rządowe

3.4.10. Platforma musi umożliwiać przeglądania danych co najmniej z:
3.4.10.1. Internetu
3.4.10.2. Dark web
3.4.10.3. Deep web

3.4.11. Zakres źródeł informacji otwartych to co najmniej:
3.4.11.1. Fora internetowe
3.4.11.2. Media społecznościowe
3.4.11.3. Strony typu onion w sieci Tor
3.4.11.4. Blogi
3.4.11.5. Kanały IRC
3.4.11.6. Strony typu Pastebin
3.4.11.7. Grupy na komunikatorach
3.4.11.8. Repozytoria kodu
3.4.11.9. Kanały Telegram
3.4.11.10. Strony wymuszające grup ransomware

3.4.12. Platforma musi udostępniać kolekcję danych z zamkniętych źródeł danych tj.:
3.4.12.1. Fora hakerskie.
3.4.12.2. Portale i fora w sieci Tor.
3.4.12.3. Portale i fora wymagające specjalnych dostępów.

3.4.13. Platforma musi umożliwiać monitorowanie grup przestępczych oraz APT (Advanced Persistent Threat) pod kątem:
3.4.13.1. Kraju pochodzenia
3.4.13.2. Regionu prowadzonych działań
3.4.13.3. Profilu działalności grupy
3.4.13.4. Używanej przez grupę infrastruktury

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

3.4.13.5. Stosowanych TTP (Tactics, Techniques and Procedures)
3.4.13.6. Aktywności
3.4.13.7. Celów ataku
3.4.13.8. Używanym kodzie złośliwym
3.4.13.9. Wykorzystywanych podatnościach.
3.4.13.10. Wykorzystywanych wektorach ataku
3.4.13.11. Identyfikatory Mitre Att@ck Framework
3.4.13.12. Trendów
3.4.13.13. Inne powiązane IoC (Indicator of Compromise)

3.4.14. Platforma musi udostępniać dane w czasie rzeczywistym.

3.4.15. Platforma musi udostępniać dynamiczną klasyfikację zagrożeń w czasie rzeczywistym.

3.4.16. Platforma musi dostarczać automatyczną ocenę ryzyka dla IoC typu:
3.4.16.1. Adres IP
3.4.16.2. Domena
3.4.16.3. URL
3.4.16.4. Hash
3.4.16.5. Identyfikator CVE

3.4.17. Platforma musi dostarczać informacje na temat każdego IoC w tym co najmniej:
3.4.17.1. Metadane
3.4.17.2. Ocenę ryzyka
3.4.17.3. Inne powiązane IoC
3.4.17.4. Powiązania z grupami przestępczymi

3.4.18. Platforma w ramach udostępnianego kontekstu musi dostarczać też informacje WHOIS.

3.4.19. Platforma musi oferować możliwość oceny ryzyka dla przeglądanych IoC w postaci jednej finalnej wartości w zakresie od 1 do 99.

3.4.20. Platforma musi udostępniać możliwość detekcji oraz monitorowanie stron phishingowych oraz witryn dystrybuujących złośliwe oprogramowanie.

3.4.21. Platforma musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.

3.4.22. Platforma musi umożliwiać wyszukiwanie oraz alertowanie o publikacjach nowych PoC (Proof-of-Concept) exploitów.

3.4.23. Platforma musi pozwalać na skonfigurowanie dla każdej reguły, harmonogramu uwzględniającego częstotliwość oraz godzinę otrzymania powiadomień.

3.4.24. Platforma musi umożliwić wyszukiwanie i alertowanie o nowych podatnościach oraz podatnościach ze względu na monitorowanych vendorów.

3.4.25. Platforma musi udostępniać możliwość wyszukiwania i alertowania o wystąpieniu wcześniej skonfigurowanych fraz kluczowych.

3.4.26. Platforma musi umożliwiać wyszukiwanie ze względu na zdefiniowane sektory gospodarcze.

3.4.27. Platforma musi udostępniać podgląd typu top 10 ze względu na:
3.4.27.1. Najczęściej wykorzystywane podatności.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.4.27.2. Najczęściej wykorzystywane metody.
3.4.27.3. Najczęściej atakowane cele.
3.4.27.4. Najbardziej aktywne grupy przestępcze.

3.4.28. Platforma musi posiadać funkcjonalność wyszukiwania za pomocą wyrażeń regularnych, w celu wyszukania:
3.4.28.1. Adresów IP
3.4.28.2. Adresów URL
3.4.28.3. Domeny
3.4.28.4. Hashy plików
3.4.28.5. Nazw użytkowników
3.4.28.6. Adresów email
3.4.28.7. Lokalizacji
3.4.28.8. Zawartości w plikach
3.4.28.9. Tekstu pisanego w różnych językach

3.4.29. Platforma musi umożliwiać alertowanie o publikacjach sprzedaży na forach poświadczeń wykradzionych w Polsce.

3.4.30. Platforma musi umożliwiać budowanie różnych, własnych alarmów.

3.4.31. Platforma musi umożliwić ustawienie różnych interwałów alarmowania - od alarmów co kilkanaście minut do dobowych i tygodniowych.

3.4.32. Alarmy wygenerowane przez Platformę muszą być wysyłane co najmniej emailem.

3.4.33. Platforma musi umożliwiać ustawienie różnych odbiorców dla różnych reguł.

3.4.34. Platforma musi udostępniać możliwość przeglądania danych historycznych na co najmniej 5 lat wstecz.

3.4.35. Platforma musi udostępniać możliwość przeglądania informacji od ogółu do szczegółu.

3.4.36. Platforma musi udostępniać możliwość pobierania reguł detekcji w formatach co najmniej:
3.4.36.1. YARA
3.4.36.2. Snort
3.4.36.3. Sigma

3.4.37. Platforma musi udostępniać możliwość pobierania informacji o zagrożeniach (tzw. feed'ów) co najmniej w formatach:
3.4.37.1. STIX
3.4.37.2. TAXII
3.4.37.3. JSON

3.4.38. Platforma musi udostępniać możliwość eksportu danych w formatach co najmniej:
3.4.38.1. JSON
3.4.38.2. CSV
3.4.38.3. STIX
3.4.38.4. PDF
3.4.38.5. DOCX

3.4.39. Platforma musi umożliwiać prezentowanie informacji w formatach co najmniej:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.4.39.1. Widok tabelaryczny
3.4.39.2. Oś czasu
3.4.39.3. Mapa

3.4.40. Platforma musi umożliwiać zapisywanie zapytań w celu ich przyszłego ponownego uruchomienia.

3.4.41. Platforma musi udostępniać dedykowany graficzny kreator zapytań. Logika zapytań musi zawierać co najmniej:
3.4.41.1. Słowa kluczowe
3.4.41.2. Typ zdarzenia
3.4.41.3. Zakres czasowy
3.4.41.4. Źródło danych
3.4.41.5. Lokalizacje źródła
3.4.41.6. Oryginalny język
3.4.41.7. Wykluczenia

3.4.42. Platforma musi prowadzić ocenę ryzyka podatności na bazie informacji ze źródeł zewnętrznych, co najmniej:
3.4.42.1. Raporty bezpieczeństwa
3.4.42.2. NIST
3.4.42.3. NVD
3.4.42.4. Analizy i badania
3.4.42.5. Notatki i artykuły producentów oprogramowania
3.4.42.6. Fora Dark Web
3.4.42.7. Repozytoria kodu (np. GitHub).

3.4.43. Platforma musi wspierać automatyczną ocenę ryzyka podatności określonych jako identyfikatory CVE.

3.4.44. Platforma musi umożliwiać przeszukiwanie i wizualizację informacji dla dowolnego identyfikatora CVE w sposób nie limitujący zakresu, częstotliwości czy też liczby zapytań.

3.4.45. Platforma musi umożliwiać konfigurację oraz generowanie alarmów w przypadku pojawienia się nowej podatności w ramach określonych, monitorowanych technologii.

3.4.46. Platforma musi alarmować także o podatnościach w fazie „PreNVD" w ramach określonych, monitorowanych technologii. Oznaczenie Pre-NVD dotyczy podatności, które otrzymały już kod CVE jednak nie otrzymały jeszcze wyniku oceny ryzyka zgodnego z metryką CVSS.

3.4.47. Platforma musi alarmować w przypadku wykrycia CVE będącego obecnie wykorzystywanym w trakcie trwających złośliwych kampanii.

3.4.48. Platforma musi dostarczać informacji na temat globalnego krajobrazu podatności.

3.4.49. Platforma musi dostarczać informacji na temat trendów w zakresie podatności oprogramowania.

3.4.50. Platforma musi dostarczać widok obrazujący obecne trendy dla podatności.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.4.51. Platforma musi dostarczać widok prezentujący aktualne trendy w świecie podatności wyfiltrowane wyłącznie dla CVE obecnych wyłącznie w ramach określonych, monitorowanych technologii.
3.4.52. Platforma musi dostarczać informacji na temat globalnego krajobrazu zagrożeń związanych z oprogramowaniem typu ransomware.
3.4.53. Platforma musi musi dostarczać widok obrazujący obecne trendy związane z oprogramowaniem typu ransomware.
3.4.54. Udzielona licencja musi umożliwiać udostępnianie w formie nieodpłatnej przetworzonych przez Zamawiającego informacji do innych podmiotów.
3.4.55. Udzielona licencja nie może ograniczać liczby odbiorców, w tym innych podmiotów, którzy będą mogli otrzymywać przetworzone przez Zamawiającego informacje.
3.4.56. Możliwość wykrywania i alterowania o próbach podszywania się pod monitorowane domeny – wykrywanie ataków typosquatting.
3.4.57. Możliwość wykrywania i alertowania o rejestracji domen lub nowych certyfikatów cyfrowych co pozwoli na detekcję prób powołania podobnych, potencjalnie podszywających się adresów lub certyfikatów.
3.4.58. Możliwość wykrywania i alertowania o wzmiankach w mediach o monitorowanych podmiotach. Także w social mediach.
3.4.59. Możliwość wykrywania i alertowania nadużyć loga monitorowanych podmiotów.
3.4.60. Dostępność dedykowanego silnika OCR (Optical Content/Character Recognition), który pozwoli na analizę obrazów pod kątem wystąpienia fraz kluczowych.
3.4.61. Możliwość alertowania o wykrytych nadużyciach na podstawie wyników analiz silnikiem OCR.
3.4.62. Możliwość wykrywania i alertowania o atakach phishingowych wykorzystujących wizerunek monitorowych podmiotów.
3.4.63. Możliwość konfiguracji dla każdej z reguł częstotliwości dostarczania alarmów. Co najmniej co 15 minut, co 1 godzinę, co 4 godziny, co 8 godzin, co 24 godziny.
3.4.64. Możliwość konfiguracji dla każdej z reguł listy odbiorców spośród założonych kont analityków.
3.4.65. Możliwość monitorowania portali branżowych pod kątem prób podszywania się pod kadrę kierowniczą Zamawiającego. Na podstawie wykrytych naruszeń musi zostać wygenerowany alert.
3.4.66. Możliwość wykrywania publikacji aplikacji mobilnych podszywających się pod aplikacje Zamawiającego. Na podstawie wykrytych naruszeń musi zostać wygenerowany alert.
3.4.67. Monitorowanie i alertowanie o wykrytych publikacjach kodów źródłowych Zamawiającego w publicznych repozytoriach. Monitorowanie to musi pozwolić także na przeglądanie publikacji w Dark Web oraz na zamkniętych forach.
3.4.68. Każdy z alertów możliwy jest do podjęcia przez analityka poprzez chmurowy interfejs graficzny.
3.4.69. Niedopuszczalne jest rozdzielenie obsługi na więcej niż jeden portal.
3.4.70. Możliwość pobierania każdego z alertów za pomocą API.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.4.71. Dostępność predefiniowanych reguł alertujących.
3.4.72. Możliwość samodzielnego tworzenia dowolnej ilości własnych reguł oraz alertów.
3.4.73. Funkcjonalność zapewniającą ochronę przed przejęciem kont w formie dostępu do informacji o zidentyfikowanych wyciekach poświadczeń.
3.4.73.1. Platforma musi umożliwić wykrycie wycieku poświadczeń ze wskazanych wcześniej i monitorowanych domen będących w obszarze odpowiedzialności Zamawiającego.
3.4.73.2. Platforma musi umożliwiać wykonywanie zapytań w trybie na żądanie, odnośnie wycieków wraz z możliwością podania domen innych niż wcześniej skonfigurowane.
3.4.73.3. Platforma musi udostępniać kolekcję danych co najmniej ze źródeł danych:
3.4.73.3.1. Fora hakerskie.
3.4.73.3.2. Portale i fora w sieci Dark Web.
3.4.73.3.3. Bazy dostępne w Dark Web.
3.4.73.3.4. Logów z oprogramowania typu Infostealer.
3.4.73.4. Logi ze złośliwego oprogramowania typu Infostealer muszą obejmować co najmniej:
3.4.73.4.1. Vidar
3.4.73.4.2. Redline Stealer
3.4.73.4.3. Racoon Stealer
3.4.73.4.4. Meta Stealer
3.4.73.5. Platforma musi udostępniać szczegóły dla wykrytego wycieku poświadczeń:
3.4.73.5.1. Źródło wycieku
3.4.73.5.2. Data eksfiltracji danych
3.4.73.5.3. Informacji czy hasło dostępne jest jako czysty tekst
3.4.73.5.4. Hash hasła
3.4.73.5.5. Adres usługi lub aplikacji do której wyciekło hasło
3.4.73.5.6. Skradzione pliki cookie
3.4.73.5.7. Typ infostealera
3.4.73.5.8. Nazwa użytkownika
3.4.74. Funkcjonalność monitorowania zewnętrznych zasobów dostępnych z Internetu.
3.4.74.1. Platforma musi umożliwiać konfigurację zakresu domen i subdomen.
3.4.74.2. Platforma musi umożliwiać skonfigurowanie cyklicznych skanów wykrywających nowe zasoby, subdomeny i usługi w skonfigurowanym zakresie.
3.4.74.3. Platforma musi umożliwiać skonfigurowanie cyklicznych skanów wykrywających podatności.
3.4.74.4. Platforma musi prezentować wyniki skanów uwzględniając co najmniej:
3.4.74.4.1. Odkryte nowe zasoby
3.4.74.4.2. Ryzyka z podziałem na krytyczność
3.4.74.4.3. Najczęściej otwarte porty sieciowe
3.4.74.5. Platforma musi pozwalać na filtrowanie wyników skanów.
3.4.74.6. Platforma musi pozwalać na eksportowanie wyników skanów do pliku.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.4.74.7. Platforma musi prezentować trendy w skanowanych zasobach opierając się na wynikach wcześniej wykonywanych skanów.

3.4.75. Niedopuszczalne jest rozdzielenie obsługi na więcej niż jeden portal.

3.4.76. Platforma musi udostępniać funkcjonalność typu sandbox pozwalającą na umieszczanie plików do analizy.

3.4.77. Sandbox musi pozwalać na analizę zarówno plików jak i linków do stron nieznanego pochodzenia

3.4.78. Podczas analizy w sandboksie musi być zapewniona możliwość bezpośredniej interakcji z testowaną próbką.

3.5. **Integracje oraz API**

3.5.1. Możliwość pobierania danych, w tym różnych IoC (Indicators of Compromise), bezpośrednio do systemów bezpieczeństwa klasy SIEM za pomocą API.

3.5.2. Możliwość integracji z systemami klasy SIEM m.in.:

3.5.2.1. RSA

3.5.2.2. Microsoft

3.5.2.3. MISP

3.5.2.4. Carbon Black

3.5.2.5. IBM

3.5.2.6. Splunk

3.5.3. Połączenie za pomocą API musi się odbywać kanałem szyfrowanym z pomocą protokołu TLS co najmniej w wersji 1.2.

3.5.4. Integracja za pomocą API nie może wymagać żadnych dodatkowych urządzeń, licencji czy też skryptów.

3.5.5. Połączenie za pomocą API nie może być w żaden sposób limitowane ze względu na rozmiar danych lub rodzaj zapytań.

3.5.6. Pobieranie danych z pomocą API musi odbywać się automatycznie bez konieczności angażowania operatora systemu SIEM.

3.5.7. Integracja z systemem klasy SIEM musi pozwalać na generowanie alertów w tym systemie na podstawie otrzymywanych IoC.

3.5.8. Integracja z systemem klasy SIEM musi umożliwiać pobranie reguł detekcji.

3.6. **Wsparcie techniczne**

3.6.1. Platforma musi być dostarczona wraz z usługą wsparcia technicznego producenta rozwiązania.

3.6.2. Możliwość udziału w bezpłatnych warsztatach i szkoleniach z obsługi Platformy organizowanych przez producenta oprogramowania.

3.6.3. Usługa wsparcia musi być dostępna w trybie 24 / 7 z możliwością zgłaszania problemów za pomocą telefonu, wiadomości e-mail lub dedykowanego portalu www.

3.6.4. Możliwość skorzystania bezpłatnie z konsultacji z producentem oprogramowania.

3.6.5. Dostępność analityka na żądanie w celu dogłębnej analizy przypadku.

3.6.6. Dostępność bazy wiedzy, opisującej szczegóły konfiguracji Platformy oraz dobrych praktyk w zakresie CTI.

3.6.7. Wsparcie musi zapewniać dostęp do materiałów szkoleniowych producenta.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

3.6.8. W ramach usługi wsparcia wymaga się od konsultanta wsparcia w zakresie definicji i wdrożenia przypadków użycia oraz architektury rozwiązania.

3.7. **Instruktaż stanowiskowy**

Przeprowadzenie instruktażu dla nie więcej niż 10 wskazanych przez Zamawiającego pracowników w języku polskim.

Instruktaż przygotuje wskazanych pracowników do samodzielnego wykorzystania Platformy. Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy.

3.7.1. Instruktaż zostanie zorganizowany w czasie ustalonym z Zamawiającym po podpisaniu umowy.

3.7.2. Instruktaż będzie realizowany w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego, zdalnie lub w ustalonej sali szkoleniowej za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu.

3.7.3. Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:

3.7.3.1. Architektura produktu
3.7.3.2. Poruszanie się po interfejsie użytkownika
3.7.3.3. Planowanie wdrożenia systemu wraz z architekturą systemu
3.7.3.4. Instalacja konsoli zarządzania i agentów na stacjach końcowych
3.7.3.5. Konfiguracja reguł filtrujących/analizujących dla dedykowanego systemu końcowego.
3.7.3.6. Wykonanie przykładowych scenariuszy:
3.7.3.6.1. Zdefiniowanie list monitorowania ze względu na:
3.7.3.6.1.1. Monitorowane FQDN.
3.7.3.6.1.2. Monitorowane IP.
3.7.3.6.1.3. Monitorowany stos technologiczny.
3.7.3.6.1.4. Monitorowane kanały grup tzw. threat actors.
3.7.3.7. Zdefiniowanie alertowania wykryć:
3.7.3.7.1. Podatności.
3.7.3.7.2. Wycieków.
3.7.3.7.3. Aktywności tzw. threat actors.
3.7.3.8. Wyszukiwanie zaawansowane.
3.7.3.9. Tworzenie nowych scenariuszy monitorowania.
3.7.3.10. Konfiguracja dashboardów.
3.7.3.11. Wykorzystanie dostarczonego przez Producenta funkcjonalności klasy sandbox.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706