Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia - Przedłużenie licencji i wsparcia na system ochrony i reagowania na zaawansowane zagrożenia.

Przedmiotem zamówienia jest przedłużenie licencji systemu FortiEDR Discover, Protect & Respond w modelu On-Premise Internet Access Enabled Deployment dla 500 endpointów wraz z zachowaniem ciągłości subskrypcji i wsparcia producenta przez okres 36 miesięcy.

II. Wsparcie:

1. Wykonawca udziela Zamawiającemu wsparcia na Oprogramowanie FortiEDR przez okres 36 miesięcy, jednak nie wcześniej niż od dnia 27.12.2026 r.
2. Jakakolwiek wada Oprogramowania, która nastąpi w okresie trwania wsparcia, będzie przez Wykonawcę usunięta w ramach wynagrodzenia. Koszt wsparcia zawiera koszty związane z dojazdem serwisu i koszty robocizny.
3. Wykonawca zobowiązuje się do przyjmowania zgłoszeń w dni robocze[1] w godzinach od 8.00 – 17.00.
4. Obsługa zgłoszeń w ramach wsparcia będzie się odbywać w języku polskim.
5. Naprawy będą dokonywane przez Wykonawcę w dni robocze oraz w dni ustawowo wolne od pracy, w siedzibie Zamawiającego lub poprzez zdalny dostęp.
6. W przypadku ujawnienia wady (nieprawidłowości, awarii lub uszkodzenia) Oprogramowania, powstałej w okresie wsparcia, Wykonawca zobowiązany

[1] Przez dzień roboczy należy rozumieć każdy dzień tygodnia od poniedziałku do piątku, z wyłączeniem dni wolnych od pracy wskazanych ustawą z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz.U. z 2020 r., poz. 1920).

będzie do usunięcia wady (naprawy) lub udzielenia wsparcia, w następujących terminach, liczonych od dnia dokonania zgłoszenia:

1) 24 godziny dla wady krytycznej, tj. wady powodującej zatrzymanie pracy Oprogramowania lub objawiającej się brakiem dostępu do Oprogramowania, niedziałaniem Oprogramowania.
2) 48 godzin dla wady ważnej, tj. wady polegającej na tym, że Oprogramowanie działa, lecz przynajmniej jedna z kluczowych funkcjonalności[2] jest niedostępna,
3) 5 dni roboczych dla wady istotnej, tj. wady polegającej na tym, że Oprogramowanie działa i realizuje kluczowe funkcjonalności, jednak występują utrudnienia w pracy bądź obsłudze Oprogramowania lub niektóre funkcjonalności niekrytyczne[3] nie są dostępne.
4) 10 dni roboczych dla udzielenia wsparcia, tj. obsługa, zmiana konfiguracji lub wsparcie w innym zakresie Przedmiotu umowy nie dotyczącym usunięcia wady (naprawy) Oprogramowania.

7. Kwalifikacja ujawnionej wady do kategorii wad, o których mowa w pkt 6, należy każdorazowo do kompetencji Zamawiającego. Zamawiający dopuszcza możliwość zmiany kategorii wady na wniosek Wykonawcy, jedynie w przypadku, gdy Wykonawca zaproponuje i zastosuje jej skuteczne obejście[4]. Ocena skuteczności obejścia i jego przyjęcie należy do Zamawiającego.
8. W okresie wsparcia, Wykonawca zapewni Zamawiającemu usługę wsparcia technicznego w procesie aktualizacji i modyfikacji konfiguracji oferowanego

[2] Przez kluczową funkcjonalność należy rozumieć funkcjonalność wpływającą na niezawodność Oprogramowania lub obniżenie poziomu bezpieczeństwa.

[3] Przez funkcjonalności niekrytyczne należy rozumieć funkcjonalności nie wpływające na niezawodność Oprogramowania lub obniżenie poziomu bezpieczeństwa.

[4] Przywrócenie w czasie naprawy funkcjonowania Oprogramowania poprzez zminimalizowanie uciążliwości wady i doprowadzenie Oprogramowania do działania zgodnego z wymaganiami, bez trwałego i całkowitego usuwania wady.

Oprogramowania.

9. W okresie wsparcia, Wykonawca zapewni Zamawiającemu prawo do subskrypcji świadczonej przez producenta Systemu.
10. Prawo do subskrypcji obejmuje:
    1) prawo do otrzymywania aktualnych wersji oprogramowania oraz publikowanych poprawek,
    2) internetowy dostęp do dokumentacji i bazy wiedzy.

III. Główne funkcjonalności systemu ochrony i reagowania na zaawansowane zagrożenia (EDR) w przypadku zaoferowania rozwiązania równoważnego:

1. System ochrony i reagowania na zaawansowane zagrożenia dla urządzeń końcowych musi zapewniać kompleksową ochronę przed malware, zaawansowanymi atakami wykorzystującymi techniki opisane w modelu MITRE™ ATT&CK, ataki typu „fileless" - bez użycia plików, ataki z wykorzystaniem oprogramowania dostępnego w ramach systemu operacyjnego lub w znanych aplikacjach tzw. „LOLBAS". System musi zarówno wykrywać zagrożenia na poszczególnych etapach infekcji jak i mieć możliwość granularnego reagowania na wykryte incydenty zależnie od poziomu klasyfikacji danego zagrożenia.
2. System musi wspierać ochronę dla minimum następujących systemów operacyjnych (agentów działających na poniższych systemach operacyjnych):
    a) Windows 11
    b) Windows Server 2016/Server 2019/Serwer 2022
    c) Linux - Ubuntu 22.04.x, Debian 11
3. Możliwość instalacji agenta poprzez SCCM.
4. Możliwość aktualizacji/zmiany wersji agenta z poziomu konsoli zarządzania bez udziału użytkownika hosta końcowego.

5. System musi dostarczać możliwość kreowania instalatorów zawierających parametry umożliwiające podłączenie się danego agenta do określonej grupy hostów oraz danej instancji systemu zarządzającego.
6. Podłączanie się do systemu zarządzającego musi wymagać podania hasła w postaci parametru – bez podania poprawnego hasła nie może być możliwości podłączenia się do systemu zarządzania.
7. Poziom zużycia pamięci RAM dla procesów agenta musi wynosić średnio 200MB.
8. Średni poziom zużycia procesora (CPU) dla procesów agenta musi wynosić średnio do 2% (na stacji PC).
9. Instalator oprogramowania nie może zajmować więcej niż 100MB.
10. System musi umożliwiać agentowi wykrywanie i reagowanie na zagrożenia w przypadku odłączenia od sieci (offline).
11. System musi umożliwiać wykrywanie podejrzanych aktywności dla działających, uruchamianych i zatrzymywanych procesów oraz w ramach interakcji pomiędzy procesami.
12. System musi umożliwiać analizę i odzwierciedlanie informacji o parametrach z jakimi został wykonany dany proces (np. parametry z linii poleceń).
13. System musi umożliwiać wykrywanie złośliwych zmian w rejestrach co najmniej w kontekście śledzonego wykonania danego procesu.
14. System musi umożliwiać wykrywanie żądań DNS wysyłanych z chronionej stacji.
15. System musi umożliwiać wykrywanie podejrzanej aktywności związanej z używaniem dynamicznie ładowanych bibliotek DLL.
16. System musi identyfikować podejrzane zachowanie użytkownika jak i samej stacji końcowej.
17. System musi posiadać zintegrowane informacje na temat zagrożeń bezpieczeństwa (tzw. Threat Intelligence) pozwalające na dokładniejszą

analizę zagrożenia.

18. System musi wykrywać zagrożenia korzystając z silnika NGAV (Next-Generation Antivirus).
19. System musi umożliwiać dodawanie wykluczeń ze skanowania przez silnik NGAV (Next-Generation Antivirus).
20. System musi umożliwiać wykrywać i kategoryzować urządzenia IoT w bezpośrednim sąsiedztwie sieciowym danego agenta.
21. System musi umożliwiać blokowanie wykonania się złośliwych plików wykonywalnych i bibliotek DLL.
22. System musi umożliwiać zablokowanie połączeń sieciowych zewnętrznych jak i wewnętrznych wykonywanych przez złośliwe oprogramowanie.
23. System musi umożliwiać blokowanie manipulacji plikami przez złośliwe oprogramowanie: tworzenie, edycję, usuwanie.
24. System musi umożliwiać zastosowywanie list blokujących jak i zezwalających dla danych:
    a) Hash (funkcji skrótu) plików w formatach MD5, SHA1, SHA2
    b) Nazw plików
    c) Ścieżek plików - z możliwością używania * (wildcard) na początku, w środku oraz na końcu nazwy folderu
    d) Dla konkretnego certyfikatu, którym podpisane są pliki.
25. System musi umożliwiać blokowanie połączeń do znanych złośliwych stron internetowych, domen lub adresów IP. Lista ta musi być automatycznie akutalizowana przez producenta rozwiązania.
26. Dane historyczne metadanych zebranych z urządzeń muszą być dostępne do analizy z okresu minimum 2 lat.
27. System musi umożliwiać wyszukiwanie oznak ataków w zebranych informacjach. Wyszukiwanie musi być możliwe w oparciu o wszystkie zebrane informacje ze stacji końcowej oraz zidentyfikowane taktyki i techniki

MITRE.

28. Wyszukiwanie musi umożliwiać budowanie zaawansowanych zapytań z wykorzystaniem logicznych operatorów typu AND, OR, NOT, EXISTS, znaków wildcard, zakresów liczb (np. adresów od 10.0.0.100 do 10.0.0.200).
29. Dane do analizy muszą pochodzić bezpośrednio z urządzeń końcowych.
30. System musi w oparciu o zebrane dane samodzielnie (wykorzystując AI lub równoważne rozwiązanie) identyfikować zachowania wg nomenklatury MITRE. Zachowanie musi być również elementem w oparciu o który można wykonywać zapytania do zebranych informacji.
31. Musi istnieć możliwość zapisania utworzonych zapytań wraz z możliwością ich automatycznego uruchamiania wg określonego harmonogramu z częstotliwością minimalną 15 minut.
32. System musi umożliwiać tworzenie profili, które opisują jakie informacje z urządzenia końcowego będą zbierane.
33. Musi istnieć możliwość tworzenia różnych profili i przypisywać je do różnych grup komputerów.
34. Zbierane informacje muszą zawierać minimalnie informacje o inwentaryzacji plików, szczegółowe operacje na plikach (utworzenie, zapis, odczyt, zmiana nazwy, skasowanie, ustawienie czasu, o połączeniach sieciowych (zapytania http, zapytań DNS, zaakceptowania połączenia, nasłuchiwania na połączenie, zamknięcia połączenia), zdarzeń systemowych, szczegółowe operacje na rejestrze systemu (utworzenie, skasowanie, zmiany nazwy klucza rejestru; wpisanie, odczytanie, skasowanie wartości rejestru).
35. Z poziomu znalezionych informacji musi istnieć możliwość wykonywania akcji, np. dla znalezionego pliku, możliwość jego ściągnięcia przez operatora, usunięcia, dodania do czarnej listy.
36. System musi umożliwiać ręczne zarządzanie fałszywymi alarmami poprzez możliwość oznaczania źle sklasyfikowanej aktywności, celem poprawnego

wykrywania w przyszłości.

37. System musi umożliwiać integrację z rozwiązaniami typu Network Access Control (NAC), umożliwiając izolację podejrzanego komputera do osobnego VLAN.
38. System musi posiadać mechanizm automatycznej reklasyfikacji fałszywych alarmów (False Positives) i przeciwdziałać błędnemu ich wykrywaniu w przyszłości.
39. System musi umożliwiać pobieranie fragmentów zrzutów pamięci z urządzeń końcowych.
40. System musi posiadać interfejs API pozwalający na śledzenie wykrytych incydentów oraz prowadzonych analiz zagrożeń z uwzględnieniem takich parametrów jak:
    a) Adres IP
    b) Nazwa hosta
    c) Użytkownik
    d) Data
    e) Ilość wystąpień danego zdarzenia
    f) Klasyfikacja aktywności
41. Incydenty bezpieczeństwa muszą być klasyfikowane w min. następujące grupy:
    a) Złośliwe
    b) Podejrzane
    c) Niestandardowe - wymagające głębszej analizy
    d) Niechciane tzw. PUP - Potential Unwanted Programs
    e) Prawdopodobnie bezpieczne.
42. W ramach każdej klasy zagrożeń musi istnieć możliwość zastosowania lub niezastosowania poniższej reakcji lub działania ograniczającego wpływ incydentu na bezpieczeństwo:

a) Możliwość zabicia/zatrzymania procesu
b) Możliwość usunięcia pliku
c) Możliwość przywrócenia stanu rejestru systemu do stanu sprzed wykonania się danego zagrożenia
d) Automatyczne wprowadzenie hosta w stan izolacji sieciowej - zgodnie z konfigurowalną polityką dostępu do sieci.

43. W przypadku klasyfikacji zagrożenia jako niejednoznaczne, system musi umożliwiać automatyczną detonację pliku w chmurze producenta - działanie tej funkcji może zostać wyłączona przez Zamawiającego.
44. Możliwość dynamicznej zmiany grupy agenta na inną, gdzie zostały przypisane polityki bezpieczeństwa o większych obostrzeniach.
45. Możliwość zbudowania (zaprogramowania) własnych akcji reagujących na daną klasyfikację zagrożenia.
46. Automatyczne blokowanie adresu IP z którym łączy się podejrzany proces na zewnętrznym urządzeniu firewall.
47. W ramach reakcji na incydenty musi istnieć możliwość powiadamiania innych systemów za pomocą:
    a) Wysłania wiadomości pocztowej e-mail ze szczegółami zdarzenia
    b) Wysłania informacji za pomocą protokołu SYSLOG
    c) Możliwości wysłania informacji do zewnętrznego systemu zawierającego w załączeniu dane w postaci XML lub JSON umożliwiające automatyczne założenie zgłoszenia.
48. Wszystkie powyższe akcje muszą być konfigurowalne per każda klasa zagrożenia.
49. Musi być możliwość zastosowania wszystkich akcji jednocześnie w ramach danej klasy zagrożenia (np. izolacja, wysłanie powiadomienia SYSLOG, usunięcie plików i zablokowanie niebezpiecznego adresu IP na urządzeniu Firewall).

50. Polityka reagowania na zagrożenia i incydenty bezpieczeństwa musi umożliwiać jej rozróżnienie dla poszczególnych grup agentów.
51. System musi posiadać funkcjonalność zdalnego dostępu do chronionego urządzenia końcowego (remote shell), z poziomu konsoli administratora system.
52. W ramach dostępu zdalnego (remote shell access) będą możliwe co najmniej następujące akcje:
    a) Listowanie plików w katalogach
    b) Listowanie konfiguracji adresacji IP na interfejsach
    c) Pobieranie pliku z urządzenia końcowego
    d) Wgranie pliku na urządzenie końcowe
    e) Usunięcie pliku na urządzeniu końcowym
    f) Informacja o zalogowanych użytkownikach
    g) Zwracanie sumy kontrolnej (SHA1 oraz MD5) pliku na urządzeniu
    h) Lista zadań systemu operacyjnego (tasklist)
    i) Zrzucenie pamięci danego procesu
    j) Uruchomienie powłoki systemowej
    k) Pobranie wartości rejestru
    l) Listowanie i usuwanie aplikacji w systemie, które są uruchamiane przy starcie z klucza rejestru RUN.
53. Wykrywanie i katalogowanie w czasie rzeczywistym wersji aplikacji komunikujących się za pomocą sieci.
54. Wykrywanie urządzeń IoT w sieci gdzie znajdują się chronione hosty.
55. Wykrywanie innych hostów w sieci, gdzie nie ma zainstalowanego agenta EDR.
56. System musi umożliwiać wykrywanie podatności w aplikacjach, które komunikują się za pomocą sieci z urządzeniami zewnętrznymi.
57. Musi istnieć możliwość ograniczenia ryzyka dla konkretnej podatnej wersji

aplikacji poprzez automatyczne ograniczenie możliwości komunikacji, na podstawie reguł bazujących na aktualizowanych informacjach CVE.

58. System musi działać w oparciu o mechanizmy analizy zachowań procesów i wywołań funkcji systemowych, wsparte sztuczną inteligencją, w szczególności działającymi mechanizmami opartymi o modele matematyczne algorytmów uczenia maszynowego (Machine Learning).
59. Uczenie maszynowe musi być wykorzystywane zarówno w analizie zachowań procesów jak i w analizie samych plików.
60. System musi wykrywać i umożliwiać reakcję w czasie rzeczywistym na znane zagrożenia bazując na ich zachowaniu oraz reputacji, w szczególności:
    a) Możliwość blokowania i reagowania w ramach sekwencji wykonania danego zagrożenia bazując na heurystyce zachowań (np. podczas próby szyfrowania plików przez zagrożenie typu ransomware)
    b) Możliwość korzystania z komercyjnych baz reputacji plików (np. Virus Total lub równoważna dostarczana producenta)
    c) Możliwość wykrywania zagrożeń typu RAT (Remote Acces Trojan) na podstawie zachowań
    d) Wykrywanie zagrożeń musi umożliwiać konfiguracyjnie zarówno blokowanie uruchomienia danego pliku, jak i możliwość blokowania złośliwych akcji po uruchomieniu się danego zagrożenia
    e) System musi umożliwiać blokowanie złośliwych urządzeń USB należących do innych niż dozwolone przez politykę klas
    f) System musi umożliwiać logowanie dostępu urządzeń USB mających interakcję z systemem operacyjnym
    g) System musi umożliwiać wykrywanie i blokowanie podejrzanej aktywności w interpreterach języków skryptowych min. takich jak:
        - Powershell
        - CScript

- Python
- Makra pakietu Microsoft Office.

61. Centralne zarządzanie za pomocą przeglądarki internetowej poprzez WebUI.
62. System zarządzania musi umożliwiać integrację z usługą katalogową Active Directory oraz rozwiązaniami Two Factor Authentication i rozwiązaniami typu SSO (Single Sign On).
63. System zarządzania musi umożliwiać granularną kontrolę opartą o predefiniowane role oraz wparcie dla modelu RBAC.
64. Agent systemu musi być zabezpieczony przed próbami deinstalacji z poziomu użytkownika oraz innych złośliwych procesów.
65. Skalowanie rozwiązania musi pozwalać na:
    a) Centralne zarządzanie
    b) Przechowywanie zdarzeń, incydentów, zebranych historycznych danych w centralnym systemie
    c) Funkcjonowanie oprogramowania w modelu on-prem.
66. Dostarczony system musi posiadać zgodność z RODO w zakresie możliwości usunięcia zapisanych informacji. Wyszukiwanie rekordów musi być możliwe poprzez nazwę użytkownika, nazwę urządzenia, adres IP, adres MAC.
67. System musi udostępniać API, za pomocą którego można wykonywać operacje zarządzania, konfiguracji polityki oraz wprowadzania końcówek w stan izolacji.
68. Wymagane jest przekazanie podczas dostawy dokumentacji do API.
69. System musi umożliwiać interakcję z urządzeniami typu Firewall (co najmniej Fortinet), co najmniej umożliwiając blokowanie adresów IP, z którymi komunikuje się złośliwe oprogramowanie.
70. System musi umożliwiać integrację z rozwiązaniem typu sandbox działającym lokalnie (on prem) - system sandbox nie jest przedmiotem zapytania.
71. System musi umożliwiać budowanie dopasowanej pod rozwiązanie integracji

z zewnętrznymi systemami/urządzeniami bezpieczeństwa poprzez wywoływanie własnych/zmodyfikowanych samodzielnie skryptów.

72. W ramach zamówienia zostaną dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujące co najmniej następujące funkcjonalności:
    a) Całość infrastruktury zarządzającej (serwer zarządzający, jego komponenty, baza wykorzystywana do analizy historycznych zagrożeń) zainstalowana musi być w środowisku wirtualnym VM-Ware Zamawiającego (on-prem)
    b) Dostęp do baz zagrożeń bezpieczeństwa - Threat Intelligence
    c) Aktualizacje baz zagrożeń CVSS.
73. Rozwiązanie musi być dostarczone w postaci licencji/subskrypcji pozwalającej na ochronę minimum 500 urządzeń końcowych (bez względu na to, czy oprogramowanie zostanie zainstalowane na systemach typu PC, czy systemach serwerowych) na okres 36 miesięcy.
74. Wraz z licencją/subskrypcją musi zostać dostarczona usługa wsparcia technicznego, dostarczana przez producenta rozwiązania, wspomagająca proces implementacji oprogramowania w oparciu o najlepsze praktyki na okres 36 miesięcy.
75. Wykonawca zapewni na czas wdrożenia przynajmniej jedną osobę posiadającą aktualny certyfikat ze znajomości oferowanego systemu/produktu wydany przez producenta zaoferowanego oprogramowania.

IV. W przypadku zaoferowania licencji równoważnych, Wykonawca jest zobowiązany do:

1. W przypadku zaoferowania produktów lub usług z nimi związanych równoważnych względem wyspecyfikowanych przez Zamawiającego

w Opisie Przedmiotu Zamówienia, Wykonawca będzie zobowiązany na swoją odpowiedzialność i swój koszt dostarczyć wszystkie niezbędne licencje konieczne do spełnienia warunków równoważności przez oferowane oprogramowanie. Ze względu na różne modele licencjonowania produktów równoważnych, Zamawiający nie określa typów ani liczby licencji produktów równoważnych.

2. Wdrożenia w środowisku informatycznym (w ilości określonej licencją) zaoferowanego rozwiązania (instalacja na serwerach oraz stacjach roboczych, konfiguracja) w sposób zapewniający ciągłość ochrony środowiska informatycznego Zamawiającego bez przerw w dostępie do funkcji bezpieczeństwa oraz usług aktualizacyjnych producenta.
3. Przygotowanie dokumentacji przedwdrożeniowej i powdrożeniowej: Wykonawca zapewni i dostarczy w formacie DOC/DOCX dokumentację, która będzie:
    1) sporządzona w języku polskim;
    2) zawierać nazwę dokumentu;
    3) zawierać metrykę dokumentu (data, numer wersji, historia zmian, autor);
    4) zawierać spis treści;
    5) zawierać słownik pojęć;
    6) zawartość merytoryczną;
    7) opis architektury i plan wdrożenia systemu klasy EDR;
    8) opis architektury wdrożonego systemu EDR;
    9) opis konfiguracji, polityk bezpieczeństwa, reguł detekcji oraz mechanizmów ochrony i reagowania na incydenty;
    10) opis procesu wdrożenia rozwiązania równoważnego wraz z zapewnieniem ciągłości ochrony środowiska;
    11) procedury reagowania na incydenty bezpieczeństwa, obsługi alertów

oraz postępowania w przypadku awarii systemu.

4. Przeprowadzenie 24 godzin instruktażu dla 8 osób w formie online w zakresie:
   1) Obsługi wdrożonego rozwiązania, w tym:
      a) architekturę i komponenty systemu,
      b) logowanie i poruszanie się po konsoli administracyjnej,
      c) monitorowanie stanu systemu,
      d) analizę zdarzeń bezpieczeństwa,
      e) generowanie raportów oraz wykorzystanie dostępnych dashboardów.
   2) Zarządzanie systemem równoważnym w zakresie oferowanych funkcjonalności, w szczególności:
      a) konfigurację polityk bezpieczeństwa,
      b) zarządzanie agentami zainstalowanymi na stacjach roboczych i serwerach,
      c) wykrywanie, analizę oraz obsługę incydentów bezpieczeństwa,
      d) konfigurację mechanizmów automatycznej reakcji na zagrożenia,
      e) zarządzanie wyjątkami, regułami i alertami,
      f) integrację z innymi systemami bezpieczeństwa funkcjonującymi u Zamawiającego,
      g) aktualizację i utrzymanie systemu.
   3) Procedury odtwarzania danych i konfiguracji, obejmujące:
      a) wykonywanie oraz weryfikację kopii zapasowych konfiguracji systemu,
      b) odtwarzanie konfiguracji po awarii,
      c) przywracanie ustawień polityk bezpieczeństwa,
      d) procedury zapewnienia ciągłości działania systemu.
   4) Omówienie różnic funkcjonalnych pomiędzy dotychczas

wykorzystywanym przez Zamawiającego rozwiązaniem FortiEDR a oferowanym rozwiązaniem równoważnym, obejmujące co najmniej:

a) mapowanie funkcjonalności obu rozwiązań,
b) wskazanie sposobu realizacji funkcji dostępnych w FortiEDR,
c) identyfikację różnic w sposobie konfiguracji, zarządzania i raportowania,
d) omówienie funkcjonalności dodatkowych oferowanego rozwiązania,
e) przedstawienie rekomendowanych procedur administracyjnych wynikających ze zmiany rozwiązania.

5) Instruktaż powinien zostać zakończony przekazaniem materiałów instruktażowych w języku polskim lub angielskim w formie elektronicznej, obejmujących zagadnienia omawiane podczas instruktażu.

5. Ponadto Wykonawca zobowiązany jest do pokrycia wszelkich kosztów związanych z wdrożeniem rozwiązania równoważnego włącznie z dostawą licencji.

V. Wymagania w zakresie ustawy o krajowym systemie Cyberbezpieczeństwa:

1. Zamawiający wymaga, aby oferowane świadczenie, w tym wszystkie produkty ICT, usługi ICT oraz procesy ICT wykorzystywane do realizacji zamówienia, zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi lub rozwiązania towarzyszące, nie obejmowało:

1) produktów ICT, usług ICT lub procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich

negatywny wpływ na podstawowy interes bezpieczeństwa państwa;

2) produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ani usług ICT lub procesów ICT określonych w tej decyzji.

2. Zamawiający informuje, że zgodnie z art. 33 ust. 4c ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa rekomendacje dotyczące produktów ICT, usług ICT lub procesów ICT publikowane są w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.
3. Wykonawca zobowiązany jest do bieżącego monitorowania publikowanych rekomendacji przez cały okres realizacji zamówienia oraz do niezwłocznego poinformowania Zamawiającego o objęciu rekomendacją produktów ICT, usług ICT lub procesów ICT wykorzystywanych przy realizacji zamówienia, zarówno jako elementów głównych, komponentów, elementów środowiska świadczenia usług, jak i rozwiązań towarzyszących.
4. W przypadku publikacji rekomendacji obejmującej rozwiązania wykorzystywane do realizacji zamówienia, Wykonawca zobowiązany będzie do przedstawienia, bez dodatkowego wynagrodzenia, propozycji rozwiązań równoważnych nieobjętych rekomendacją, w terminie określonym przez Zamawiającego lub wynikającym z postanowień Umowy.