Opis Przedmiotu Zamówienia

Dostawa i wdrożenie systemu EDR (ang. Endpoint Detection and Response) do wykrywania i analizy zaawansowanych zagrożeń

Przedmiotem zamówienia jest dostawa licencji na oprogramowanie, urządzeń typu appliance oraz wykonanie wdrożenia systemu EDR (ang. Endpoint Detection and Response) do zaawansowanej ochrony 9000 urządzeń pracujących w środowisku sieci korporacyjnej statystyki publicznej.

W szczególności przedmiot zamówienia obejmuje następujące zadania do realizacji przez Wykonawcę:

1. Dostawę licencji oprogramowania do zaawansowanej ochrony 9000 urządzeń wraz z dwuletnim wsparciem producenta, rozliczanych w okresach rocznych.
2. Wdrożenie systemu EDR w środowisku sieci korporacyjnej statystyki publicznej.
3. Realizację warsztatu szkoleniowego.

I. Opis środowiska Zamawiającego

Prace wdrożeniowe i konfiguracyjne będą realizowane w Centrum Przetwarzania Danych mieszczącym się w siedzibie Zamawiającego w GUS Warszawa. Natomiast usługi świadczone przez system muszą być dostępne we wszystkich lokalizacjach, jednostkach służb statystyki publicznej (jssp), czyli Centrum Przetwarzania Danych GUS, Zakładzie CIS w Radomiu, 16 Urzędach Statystycznych oraz 48 oddziałach terenowych. Wszystkie jednostki statystyki są połączone poprzez sieć WAN statystyki publicznej.

System ma zostać wdrożony w Głównym Urzędzie Statystycznym w Warszawie, al. Niepodległości 208 i 19 podległych i podporządkowanych Prezesowi GUS samobilansujących jednostkach służb statystyki publicznej zwanych dalej JSSP, tj.:

1. w Warszawie, al. Niepodległości 208 w siedzibie Centrum Informatyki Statystycznej,
2. w Warszawie, al. Niepodległości 208 w siedzibie Zakładu Wydawnictw Statystycznych,
3. w Warszawie, al. Niepodległości 208 w siedzibie Centralnej Biblioteki Statystycznej,
4. w Warszawie, ul. 1 Sierpnia 21 w siedzibie Urzędu Statystycznego w Warszawie,
5. w Białymstoku, ul. Krakowska 13 w siedzibie Urzędu Statystycznego w Białymstoku,
6. w Bydgoszczy, ul. Ks. Stanisława Konarskiego 1-3 w siedzibie Urzędu Statystycznego w Bydgoszczy,
7. Gdańsku, ul. Danusi 4 w siedzibie Urzędu Statystycznego w Gdańsku,
8. w Katowicach, ul. Owocowa 3 w siedzibie Urzędu Statystycznego w Katowicach,
9. w Kielcach, ul. Zygmunta Wróblewskiego 2 w siedzibie Urzędu Statystycznego w Kielcach,
10. w Krakowie, ul. Kazimierza Wyki 3 w siedzibie Urzędu Statystycznego w Krakowie,
11. w Lublinie, ul. Stanisława Leszczyńskiego 48 w siedzibie Urzędu Statystycznego w Lublinie,
12. w Łodzi, ul. Suwalska 29 w siedzibie Urzędu Statystycznego w Łodzi,
13. w Olsztynie, ul. Tadeusza Kościuszki 78/82 w siedzibie Urzędu Statystycznego w Olsztynie,
14. w Opolu, ul. Ks. Hugona Kołłątaja 5B w siedzibie Urzędu Statystycznego w Opolu,
15. w Poznaniu, ul. Wojska Polskiego 27/29 w siedzibie Urzędu Statystycznego w Poznaniu,
16. w Rzeszowie, ul. Jana III Sobieskiego 10 w siedzibie Urzędu Statystycznego w Rzeszowie,
17. w Szczecinie, ul. Jana Matejki 22 w siedzibie Urzędu Statystycznego w Szczecinie,
18. we Wrocławiu, ul. Oławska 31 w siedzibie Urzędu Statystycznego we Wrocławiu,
19. w Zielonej Górze, ul. Spokojna 1 w siedzibie Urzędu Statystycznego w Zielonej Górze.

Z uwagi na fakt, iż prace wdrożeniowe i rekonfiguracyjne będą prowadzone na działającym środowisku sprzętowo–systemowo–aplikacyjnym, wymagane jest zachowanie ciągłości działania tego środowiska, oraz szczegółowe zaplanowanie wszelkich prac.

II. Opis infrastruktury sprzętowo-systemowej oraz licencji oprogramowania posiadanych przez Zamawiającego

Zamawiający posiada lub wykorzystuje:

1. System usług katalogowych bazujący na MS Active Directory w wersji Windows Server 2019 o funkcjonalności lasu i domeny na poziomie wersji Windows Server 2012 R2.
2. Środowisko do wirtualizacji serwerów bazujących na oprogramowaniu VMware Cloud Foundation Advanced z funkcjami NSX i vSAN oraz vCenter Server 7.0.3.
3. Wdrożony, scentralizowany system EDR firmy Broadcom (ang. Endpoint Detection and Response), dawna nazwa ATP (ang. Advanced Threat Protection) działający z w oparciu o licencje Broadcom Endpoint Security Complete (Includes New SES/SEP Subscription), Hybrid Subscription License with Support, Per Device, 1Y, SKU SESC-SES-SUB do ochrony 9000 urządzeń.
4. Wdrożony, scentralizowany system ochrony antywirusowej oparty na oprogramowaniu Symantec Endpoint Protection.
5. Fizyczny sandbox Blue Coat Content Analysis System S500-A1.
6. Na stacjach roboczych i serwerach zainstalowane są następujące systemy operacyjne posiadane przez Zamawiającego: MS Windows 10 Pro, MS Windows Server 2019, serwerowe systemy Linux.

III. Szczegółowa specyfikacja i opisy zadań do realizacji przez Wykonawcę

Zadanie 1 - Dostawa licencji oprogramowania do zaawansowanej ochrony 9000 urządzeń wraz z rocznym wsparciem producenta.

Oferowane przez Wykonawcę oprogramowanie musi spełniać wszystkie wymagania wymienione poniżej i posiadać wbudowane cechy oraz funkcjonalności.

A. Wymagania ogólne

1. Wykaz zamawianego oprogramowania: Broadcom Endpoint Security Complete, Per Device lub równoważne- 9000 szt.
2. Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego. Za oprogramowanie równoważne do wskazanego w specyfikacji przy pomocy nazwy oraz źródła pochodzenia uznaje się oprogramowanie posiadające następujące cechy:
   a) zakres funkcjonalny oprogramowania jest w pełni zgodny z zakresem funkcjonalnym oprogramowania wskazanego;
   b) warunki licencjonowania oprogramowania nie mniej korzystne niż licencje oprogramowania wskazanego.
3. Wykazanie równoważności złożonej oferty leży po stronie Wykonawcy i w razie wątpliwości powinno zostać udokumentowane w możliwie najbardziej obiektywny sposób.
4. Dostarczone oprogramowanie **musi być aktywowane od 23 kwietnia 2024**.
5. Dostarczone oprogramowanie nie może być zabronione do stosowania przez administrację któregokolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).
6. Zamawiający wymaga, aby Wykonawca dostarczył i wdrożył kompletne środowisko sprzętowo-programowe, **w tym urządzenia typu appliance, oprogramowanie oraz inne komponenty niezbędne dla oferowanego rozwiązania.**
7. Wszystkie elementy sprzętowe i programowe muszą być dostarczone **z dwuletnim wsparciem producenta** pozwalającym na:
   a) pobieranie kontentu bezpieczeństwa używanego przez oprogramowanie ze stron producenta oprogramowania;
   b) pobieranie najnowszych wersji oprogramowania ze stron producenta;
   c) pobieranie poprawek i łat bezpieczeństwa ze stron producenta;
   d) dostęp 24/7 do technicznej pomocy producenta (konsultacje online oraz realizacja zgłoszeń).
8. System EDR wraz z konsolą zarządzającą musi pracować w środowisku **on-premise.**
9. System musi umożliwiać zaawansowaną ochronę 9000 urządzeń.
10. System musi być dostępny w formie fizycznego urządzenia bądź wirtualnego appliance.

11. System musi opierać się na agentowej ochronie stacji.
12. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi i serwerami (np. w przypadku wymiany sprzętu) oraz zapewniać możliwość sublicencjonowania dla jednostek służb statystyki publicznej.
13. Oprogramowanie musi być dostarczone w najwyższej (najnowszej) wersji, na moment złożenia oferty przez Wykonawcę.
14. Rozwiązanie ma chronić stacje i serwery z systemem MS Windows 10 Pro (32-bit i 64-bit), MS Windows Server 2012R2-2019, serwerowe systemy Linux.
15. Musi posiadać mechanizmy wykrywania zaawansowanych zagrożeń na urządzeniu końcowym.
16. Rozwiązanie musi tworzyć incydenty z wykrytych zdarzeń.
17. Rozwiązanie musi posiadać możliwość korelowania zdarzeń z różnych elementów detekcji w celu ustalenia wagi incydentu.
18. W przypadku wykrycia złośliwego oprogramowania w dowolnym kanale system musi automatycznie sprawdzić, czy oprogramowanie antywirusowe zablokowało uruchomienie próbki.
19. Rozwiązanie musi być zintegrowane z platformą wymiany informacji producenta i dawać możliwość skorzystania z wiedzy o wykrytych zagrożeniach przez innych użytkowników systemu.
20. Musi istnieć automatyczna korelacja obserwowanych zdarzeń z IoC znanych kampanii APT.
21. Rozwiązanie musi zachowywać pełną funkcjonalność w przypadku, gdy zostanie wyłączona opcja dzielenia się informacjami z innymi klientami poprzez usługę producenta.
22. System musi umożliwiać dokładną analizę graficzną wektorów ataku dla danego zagrożenia, za pomocą jednej konsoli zarządzającej.
23. Rozwiązanie musi posiadać mechanizmy RBAC i integrować się z MS Active Directory.
24. System musi posiadać możliwość integracji z rozwiązaniami SIEM innych producentów poprzez syslog. Rozwiązanie musi logować dane w formacie CEF.
25. Rozwiązanie musi pozwalać na import pliku STIX w celu wykonania przeszukania bazy danych w poszukiwaniu IoC.
26. System musi umożliwiać generowanie raportów z własnego działania zarówno w formie na żądanie jak i zaplanowanych z możliwością wysyłania wygenerowanego raportu na określony adres email.
27. System musi umożliwiać logowanie w dziennikach zdarzeń (logach systemowych) działania użytkowników w roli administratora.
28. System musi zapewnić szyfrowanie logowania operatorów do konsoli zarządzania oraz szyfrowanie transmisji danych.

B. Metody detekcji

1. System musi posiadać wiele mechanizmów detekcji w celu zapewnienia najwyższego poziomu bezpieczeństwa.
2. Rozwiązanie musi wykorzystywać mechanizmy globalnej i lokalnej reputacji.
3. System musi posiadać mechanizm statycznej i dynamicznej analizy kodu.
4. System musi posiadać mechanizm tradycyjnego skanowania sygnaturowego.
5. System musi posiadać mechanizmy detekcji oparte na uczeniu maszynowym.
6. System musi umożliwiać sprawdzenie sumy kontrolnej danego pliku w portalu Virustotal lub równoważnym.
7. W przypadku wykrycia zagrożenia, którego nie daje się jednoznacznie zidentyfikować system musi umożliwiać wysłanie próbki tego zagrożenia w celu dokładnej analizy jego działania w oparciu o technologię sandboxingu.
8. System musi umożliwiać podłączenie do fizycznego sandboxa w celu wykonania analizy próbki.
9. System musi być kompatybilny z otwartym standardem REST API posiadanego przez Zamawiającego sandboxa w celu analizy próbki.

C. Metody analizy

1. System musi analizować wszystkie etapy wielostopniowego ataku - od momentu uzyskania uprawnień do próby eksfiltracji danych.

2. System musi umożliwiać przeprowadzenie analizy behawioralnej monitorowanych urządzeń w celu znalezienia i zaraportowania podejrzanych zachowań na podstawie korelacji, analizy i interpretacji zdarzeń odnotowanych na urządzeniu.
3. System musi wizualizować wszystkie zarejestrowane czynności wykonane przez analizowaną próbkę w formie raportu.
4. Raport dla próbki musi zawierać informację o komunikacji sieciowej, zmianach w systemie plików i rejestrze.
5. Jeżeli analizowana próbka wykonywała próbę połączenia z Internetem system musi automatycznie zestawiać tę informację z informacjami z globalnej bazy reputacji w celu celniejszego wykrywania zagrożeń.
6. Rozwiązanie musi raportować źródłowe IP, docelowe IP, C&C, URL, klasę złośliwego oprogramowania, użyte protokoły i wagę ataku (*severity).*
7. Administrator musi posiadać opcję ręcznego zlecenia przeanalizowania próbki zarówno dla pliku jak i URL.
8. System musi zastosować właściwe czynności do wywołania aktywności złośliwego oprogramowania. Jako wymaganie minimalne system musi uruchamiać próbkę wykrywającą wirtualne środowisko w środowisku fizycznym oraz oszukiwać próbki, które czekają przez długi czas zanim uruchomią szkodliwe działanie.

D. Ochrona urządzenia końcowego

1. System musi umożliwiać użycie blacklisty i whitelisty dla plików definiowanych poprzez wprowadzanie MD5, SHA256.
2. W przypadku wykrycia zagrożenia na jednym urządzeniu końcowym pozostałe urządzenia muszą automatycznie współdzielić taką wiedzę w celu natychmiastowej ochrony.
3. System musi umożliwiać izolację zaatakowanej stacji roboczej od sieci produkcyjnej i podjęcie próby usunięcia zagrożenia, a po pomyślnym rozwiązaniu problemu przywrócenie stacji do normalnego działania.
4. System musi umożliwiać przeskanowanie istniejącej infrastruktury firmy pod kątem wykrycia śladów działania zaawansowanych zagrożeń w zakresie sumy kontrolnej pliku, klucza rejestru, adresu IP, adresu URL witryny.
5. System musi pozwalać na zlokalizowanie i pobranie próbki bezpośrednio z urządzenia końcowego poprzez panel administracyjny.
6. System musi umożliwiać rejestrowanie wszystkich czynności wykonywanych na urządzeniu końcowym przez wszystkie procesy.
7. Monitorowane czynności muszą odnosić się co najmniej do startu i zatrzymania procesów, otwierania, zamykania i usuwania plików, modyfikacji rejestru, otwierania połączeń.
8. System musi umożliwiać gromadzenie informacji o aktywności bezpośrednio na urządzeniu końcowym w formie bufora. Administrator musi mieć możliwość zmiany i ograniczenia wielkości tego bufora.
9. System musi oferować zbieranie danych o procesie wykonującym czynność, obiekcie, którego czynność dotyczy (np. modyfikowany plik, klucz rejestru, wartość, uruchamiany proces).
10. Administrator musi mieć możliwość filtracji, które czynności powinny zostać natychmiast przesłane do konsoli zarządzania, a które powinny zostać przechowane w buforze urządzenia końcowego.
11. System musi umożliwiać pobranie na życzenie wszystkich czynności zarejestrowanych w buforze urządzenia końcowego do konsoli zarządzania w celu analizy.
12. Musi istnieć możliwość wyboru procesu, dla którego czynności mają zostać pobrane z bufora do konsoli.
13. System musi umożliwiać stworzenie wykluczeń z monitoringu czynności dla wybranych procesów poprzez podanie nazwy procesu.
14. System musi umożliwiać przeszukiwanie zarejestrowanych czynności wprost z konsoli zarządzającej.
15. System musi umożliwiać wybór reguł, które zostaną zastosowane do wykrywania incydentów.

16. System musi wykorzystywać moduł AV i umożliwiać poddanie urządzenia końcowego kwarantannie, pobranie logów, pobieranie plików z lokalnej kwarantanny i poszukiwanie wskaźników włamania (IoC).
17. Moduł ochrony antywirusowej musi pracować w oparciu o następujące komponenty funkcjonalne:
    a) centralny system instalacji i zarządzania wszystkimi modułami wchodzącymi w skład systemu antywirusowego z wykorzystaniem konsoli zarządzającej, która odpowiada także za centralne gromadzenie zdarzeń (logów) z poszczególnych modułów i przetwarzanie ich do postaci raportów oraz konfigurowanie polityk umożliwiających przydzielenie różnych polityk do poszczególnych komputerów, grup maszyn oraz na podstawie filtrów bazujących na parametrach sprzętowych, systemowych oraz przynależności do różnych kontenerów MS Active Directory;
    b) moduł analizy w czasie rzeczywistym chroniący przed oprogramowaniem typu: wirusy, trojany, robaki, dialery, adware, spyware i innym potencjalnie złośliwym kodem dla stacji roboczych, laptopów i serwerów; moduł ochrony ma mieć możliwość definiowania wykluczeń skanowania określonych zasobów a skanowanie antywirusowe ma się odbywać w chwili dostępu, na żądanie i według harmonogramu;
    c) moduł kontroli wykorzystania portów i urządzeń podłączanych do fizycznych stacji roboczych (porty USB, szeregowe, adaptery Bluetooth) umożliwiający blokowanie portów i nieautoryzowanych urządzeń; rozwiązanie to musi przechowywać informacje o nazwie urządzenia, kodzie producenta i urządzenia oraz numerze seryjnym a konfiguracja polityki działania modułu musi umożliwiać zdefiniowanie dopuszczonych do użytkowania nośników danych USB oraz USB Attached SCSI na podstawie ich numeru seryjnego, ID producenta i produktu;
    d) moduł kontroli oprogramowania umożliwiający uruchamianie i blokowanie wskazanych aplikacji oraz blokowanie uruchamiania konkretnych procesów przez wskazane aplikacje rozróżniane po nazwie i sumie kontrolnej;
    e) moduł zapory ogniowej zabezpieczającej urządzenia przed atakami oraz nieautoryzowanym dostępem;
    f) moduł automatycznego wykrywania w sieci nowych, pozbawionych ochrony antywirusowej komputerów i urządzeń sieciowych wysyłający raporty do centralnej konsoli zarządzania.
    g) moduł IPS wykrywania i zapobiegania włamaniom wykorzystujący bazę sygnatur;
    h) moduł umożliwiający wykonywanie testów integralności pod kątem zgodności z zaimplementowanymi politykami bezpieczeństwa stacji roboczych i serwerów;
    i) moduł automatycznej aktualizacji z możliwością automatycznego instalowania na komputerach nowych silników antywirusowych, poprawek do produktów oraz hotfixów z centralnego serwera zarządzającego lub lokalnych repozytoriów.

Odbiór zadania 1

Potwierdzeniem odbioru dostawy będą podpisane z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego protokół dostawy licencji wraz ze wsparciem producenta na pierwszy rok.

Zadanie 2 - Wdrożenie systemu EDR w środowisku sieci korporacyjnej statystyki publicznej

Przedmiotem zadania 2 jest wdrożenie systemu EDR w oparciu o dostarczone oprogramowanie w środowisku sieci korporacyjnej statystyki publicznej.

Na potrzeby realizacji przedmiotu zamówienia, Zamawiający udostępni maszyny wirtualne w środowisku VMware wraz z niezbędną liczbą licencji MS Windows Server 2019 i licencji dostępowych oraz systemem backupu Veeam Backup & Replication i/lub zasoby do zaimplementowania wirtualnego urządzenia typu appliance.

W przypadku zaoferowania systemu, który nie będzie wykorzystywał udostępnionych przez Zamawiającego zasobów i posiadanych licencji, **Wykonawca dostarczy wszystkie niezbędne elementy sprzętowe, systemowe i aplikacyjne.**

Wymagania projektowe

1. W trakcie trwania wdrożenia system ochrony antywirusowej musi działać nieprzerwanie w środowisku Zamawiającego.
2. Usługi systemu EDR muszą być dostępne we wszystkich lokalizacjach włączonych do sieci korporacyjnej statystyki.
3. Wdrażany system EDR musi być zintegrowany z posiadanymi przez Zamawiającego usługami katalogowymi MS Active Directory.
4. Administratorzy systemu muszą mieć możliwość nadzorowania i zarządzania całym systemem.

Szczegółowa specyfikacja prac

W ramach przedmiotu umowy Wykonawca wykona następujące prace:

1. Przygotuje **Projekt techniczny** realizacji uzgodnionej koncepcji uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta oprogramowania zawierający:
    a) projekt architektury systemu;
    b) usługi realizowane przez system;
    c) konfigurację komponentów;
    d) nazewnictwo komponentów;
    e) model administrowania;
    f) konfigurację ustawień bezpieczeństwa;
    g) wykonywanie kopii zapasowych i odtwarzanie środowiska;
    h) monitorowanie systemu;
    i) listę procedur administracyjnych;
    j) koncepcję wdrożenia.
2. Opracuje i uzgodni szczegółowy harmonogram realizacji prac.
3. Dokona montażu urządzeń, podłączenia okablowania, instalacji oprogramowania oraz innych czynności koniecznych do uruchomienia systemu.
4. Wdroży i skonfiguruje niezbędną infrastrukturę serwerową systemu w tym urządzenia typu appliance.
5. Dokona migracji posiadanego przez Zamawiającego systemu EDR.
6. Skonfiguruje i zaimplementuje polityki ochrony urządzeń końcowych.
7. Dokona migracji lub rekonfiguracji wszystkich wskazanych przez Zamawiającego polityk antywirusowych i modułów.
8. Zapewni integrację z MS Active Directory.
9. Dokona instalacji oprogramowania na stacjach roboczych w tym przygotowania paczek instalacyjnych z oprogramowaniem klienckim.
10. Skonfiguruje logowanie zmian administracyjnych.
11. Skonfiguruje integrację z centralnym syslogiem.
12. Dokona integracji z posiadanym przez Zamawiającego sandboxem.
13. Opracuje scenariusze testowe i przeprowadzi testy akceptacyjne wdrożonego rozwiązania oraz przygotuje dane niezbędne do przeprowadzenia testów.
14. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza w terminie wyznaczonym przez Zamawiającego, nie później 7 dni przed zakończeniem wdrożenia, dochowując terminu wykonania Umowy.
15. Wykonawca opracuje **Dokumentację powykonawczą**, która będzie zawierać:
    a) opis architektury zaimplementowanego rozwiązania;
    b) szczegółowy opis instalacji i konfiguracji wykorzystywanego oprogramowania, ze wskazaniem poszczególnych opcji i ustawionych wartości;
    c) konfigurację urządzeń typu appliance, serwerów, modułów, komponentów i usług;
    d) zbiór zaimplementowanych polityk konfiguracyjnych dla poszczególnych modułów;

e) szczegółowe procedury eksploatacyjne oraz awaryjnego odtwarzania funkcjonalności systemu, opisujące krok po kroku niezbędne czynności umożliwiające Zamawiającemu samodzielne przywrócenie funkcjonalności systemu;
f) politykę i procedury wykonywania kopii zapasowych;
g) procedury aktualizacji systemu;
h) procedury i instrukcje bieżącego monitoringu oraz utrzymania i aktualizacji systemu.

Odbiór zadania 2

1. Zatwierdzona Dokumentacja techniczna zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru wdrożenia na urządzeniu typu pendrive w wersji edytowalnej i PDF oraz wydruk w 1 egzemplarzu.
2. Potwierdzeniem odbioru Zadania 2 będzie podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego, Protokół odbioru wdrożenia.

Zadanie 3 - Realizacja warsztatu szkoleniowego

1. Wykonawca przeprowadzi warsztat szkoleniowy w trybie zdalnym dla 4 osób, trwający minimum 3 dni.
2. Opracuje materiały warsztatowe w formie skryptu, w języku polskim lub angielskim, w wersji elektronicznej i udostępni dla każdego uczestnika.
3. Zakres warsztatów będzie obejmował zagadnienia dotyczące konfiguracji i działania systemu:
    a) Funkcjonalności dostępne w zaoferowanym rozwiązaniu;
    b) Konfigurację poszczególnych modułów i komponentów;
    c) Omówienie panelu administracyjnego;
    d) Konfigurację polityk;
    e) Tworzenie zapytań i filtrów umożliwiających zaawansowane wyszukiwanie zdarzeń;
    f) Identyfikowanie zagrożeń i analizę incydentów przy użyciu zaoferowanego rozwiązania;
    g) Wyszukiwanie IoC (indicators of compromise).
4. Czas trwania warsztatów: 3 dni, każdy dzień 8 godzin lekcyjnych, każda po 45 minut.
5. Liczba uczestników: 4
6. Warsztaty zostaną przeprowadzone przez osoby mające profesjonalną (zawodową) wiedzę z zakresu z zakresu zagadnień podejmowanych w tracie zajęć.
7. Wykonawca zapewni odpowiednie rozwiązania teleinformatyczne na potrzeby przeprowadzania warsztatu, tj. zdalny dostęp do środowiska laboratoryjnego umożliwiającego realizację programu warsztatu wraz z zainstalowanym, legalnym oprogramowaniem niezbędnym do przeprowadzenia warsztatu, a także zapewni kompleksową obsługę tych rozwiązań.
8. Wykonawca będzie odpowiedzialny za sprawdzenie czy całość zapewnionego przez niego sprzętu i oprogramowania działa prawidłowo.
9. Wykonawca przygotuje i przekaże uczestnikom warsztatu instrukcję dotyczącą sposobu logowania i korzystania z użytego przez Wykonawcę rozwiązania teleinformatycznego wykorzystanego do przeprowadzenia zajęć.
10. Warsztat będzie przeprowadzone w formie zajęć z elementami wykładu i opierać się będzie na ćwiczeniach wykonywanych w udostępnionym w trybie zdalnym środowisku.
11. Na początku warsztatów Wykonawca poinformuje uczestników, że po zakończeniu warsztatu zostaną poproszeni o elektroniczne wypełnienie arkuszy AIOS (Ankieta Indywidualnej Oceny Szkolenia), co ma na celu zebranie informacji na temat jakości warsztatów. Niedopuszczalne jest sugerowanie uczestnikom odpowiedzi na pytania zawarte w arkuszu.
12. Na koniec warsztatów Wykonawca przekaże do wypełnienia każdemu uczestnikowi Arkusz AIOS, w postaci dokumentu elektronicznego. Na podstawie wypełnionych elektronicznie i przesłanych Arkuszy AIOS Wykonawca przygotuje zbiorcze zestawienie zawierające analizę danych zawartych w ankietach, obrazującą stopień zadowolenia uczestników oraz użyteczność przeprowadzonego

warsztatu. W terminie do 3 dni roboczych od dnia przeprowadzenia warsztatów, Wykonawca przekaże, w formie elektronicznej, Zamawiającemu wypełnione przez uczestników Arkusze AIOS wraz ze zbiorczym zestawieniem ocen z Arkuszy AIOS. W przypadku negatywnej oceny warsztatu (średnia z oceny trenera / trenerów poniżej 3) lub przeprowadzenia warsztatów niezgodnie z wymaganiami Zamawiającego, Wykonawca przeprowadzi dodatkowe warsztaty, dochowując terminu realizacji zamówienia. Organizacja dodatkowej edycji warsztatów będzie wymagała uzgodnienia z Zamawiającym terminu oraz osoby prowadzącej. Koszt ponownego zorganizowania i przeprowadzenia warsztatów ponosi Wykonawca.

13. Wykonawca po zakończeniu warsztatów przekaże Zamawiającemu, przygotowane w formie papierowej, wydane dla każdego uczestnika imienne zaświadczenie o ukończeniu warsztatów, które będzie zawierało następujące informacje: imię i nazwisko uczestnika, tytuł warsztatów, liczbę godzin, tematykę i datę przeprowadzenia warsztatów, pieczątkę Wykonawcy, identyfikowalny podpis osoby prowadzącej warsztaty. Warunkiem wydania zaświadczenia jest:
    a) potwierdzona obecność uczestnika w każdym dniu zajęć poprzez dokonane online przez uczestnika zgłoszenie uczestnictwa;
    b) przesłanie przez uczestnika wypełnionego elektronicznie arkusza AIOS.
14. W terminie 3 dni od dnia zakończenia warsztatów, Wykonawca przekaże Zamawiającemu na adres poczty elektronicznej, zeskanowane w formacie PDF wypełnione arkusze AIOS oraz dokumenty potwierdzające uczestnictwo osób biorących udział w warsztatach, w każdym z trzech dni zajęć, w postaci printscreena z platformy, na której uczestnicy szkolenia byli zalogowani.
15. Potwierdzeniem zrealizowania warsztatu, będzie podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego, Protokół odbioru warsztatów.
16. Protokół odbioru warsztatów Wykonawca dostarczy Zamawiającemu w terminie 5 dni roboczych od zakończenia warsztatów.

IV. Warunki gwarancji powdrożeniowej

1. Wykonawca obejmie wdrożony system gwarancją powdrożeniową przez okres 24 miesięcy, którego bieg rozpoczyna się od dnia aktywacji licencji.
2. W ramach gwarancji na wdrożony system, Wykonawca zapewni 200 bezpłatnych godzin asysty technicznej, w ramach której świadczyć będzie następujące usługi, w przypadku ich wystąpienia:
    a) usuwanie wad konfiguracyjnych systemu wdrożonego pojawiających się w trakcie użytkowania systemu przez Zamawiającego;
    b) przywracanie pełnej funkcjonalności działania komponentów systemu
    c) konsultacje w zakresie konfiguracji i eksploatacji systemu;
    d) pomoc w rozwiązywaniu problemów technicznych związanych z funkcjonowaniem powstałego systemu;
    e) rozbudowę lub modyfikację systemu;
3. Usługi asysty technicznej, zlecane będą, w miarę potrzeb Zamawiającego, drogą elektroniczną na adres poczty elektronicznej wskazany przez Wykonawcę.
4. Wykorzystanie liczby godzin asysty technicznej będzie udokumentowane Protokołem odbioru asysty technicznej sporządzonym nie później niż 14 dni przed końcem okresu gwarancyjnego.
5. W przypadku, jeżeli w wyniku dokonania istotnych zmian konfiguracyjnych, wystąpi konieczności zmiany Dokumentacji powykonawczej, Wykonawca dostarczy zaktualizowaną Dokumentację powykonawczą w terminie 30 dni roboczych po dokonaniu zmian konfiguracyjnych.
6. Wykonawca będzie miał prawo odmówić wykonania usług asysty technicznej w sytuacji gdy:
    a) Zamawiający wyczerpie przysługujący limit godzin asysty technicznej, o którym mowa w pkt 2;
    b) realizacja asysty techniczne we wnioskowanym zakresie spowodowałaby przekroczenie przysługującego Zamawiającemu limitu godzin, o którym mowa w pkt 2.
7. Świadczenie usług asysty technicznej będzie rozliczane z dokładnością do jednej godziny roboczej. Czas realizacji poszczególnych prac, zaokrąglany będzie w górę z dokładnością do jednej godziny roboczej.
8. W okresie gwarancji udzielonej na wdrożony system Wykonawca:

a) zapewni koordynatora obsługi gwarancyjnej, z którym będą prowadzone wszelkie bieżące uzgodnienia w zakresie realizacji napraw gwarancyjnych i asysty technicznej;
b) zapewni możliwość zdalnych konsultacji (np. e-mail, telefon), dotyczących rozwiązywania problemów występujących podczas obsługi lub funkcjonowania wdrożonego systemu;
c) uruchomi kanał kontaktowy w formie elektronicznej przez stronę www lub za pomocą poczty elektronicznej, umożliwiający zgłaszanie awarii;
d) zapewni realizację serwisu gwarancyjnego w języku polskim.

9. Usługi gwarancyjne w zakresie usuwania zgłaszanych przez Zamawiającego problemów z funkcjonowaniem systemu, klasyfikowanych jako awarie, świadczone będą w miejscu instalacji na następujących warunkach:
   a) przez awarię rozumie się wadę systemu, zdarzenie, w wyniku którego uszkodzeniu uległ jeden (lub więcej) element, ograniczający jego wydajność i funkcjonalność lub uniemożliwiający Zamawiającemu korzystanie z systemu zgodnie z jego specyfikacją techniczną/instrukcją użytkowania lub zmniejszając bezpieczeństwo;
   b) zgłoszenie awarii systemu będzie możliwe przez 5 dni w tygodniu, w dni robocze od poniedziałku do piątku, w godzinach 8:00 -17:00 poprzez stronę www lub za pomocą poczty elektronicznej;
   c) czas reakcji (rozumiany jako maksymalny czas, jaki może upłynąć pomiędzy zgłoszeniem awarii a reakcją serwisu) na podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nie może przekroczyć 4 godzin od momentu gwarancyjnego zgłoszenia awarii przez Zamawiającego, jeżeli do zgłoszenia doszło do godziny 14:00. W przypadku gwarancyjnego zgłoszenia awarii w dzień roboczy (poniedziałek-piątek) po godzinie 14:00 lub w dzień ustawowo wolny od pracy podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nastąpi następnego dnia roboczego (poniedziałek-piątek) w godzinach od 8:00 do 12:00;
   d) usunięcie awarii i przywrócenie pełnej funkcjonalności systemu zostanie wykonane w terminie 48 godzin od zgłoszenia awarii, z zastrzeżeniem, że diagnoza problemu wliczana jest w wymagany czas naprawy;
   e) wszelkie koszty związane z naprawami gwarancyjnymi, usuwaniem awarii, włączając w to koszt transportu do siedziby Zamawiającego ponosi Wykonawca;
   f) w przypadku, jeżeli Wykonawca nie wywiązuje się ze zobowiązań wynikających z gwarancji, Zamawiający może dokonać czynności naprawy we własnym zakresie lub zlecić jej wykonanie osobie trzeciej, a kosztami obciążyć Wykonawcę z wykorzystaniem kwoty zabezpieczenia należytego wykonania umowy;
   g) w przypadku awarii wymagającej wymiany sprzętu, Wykonawca dostarczy Zamawiającemu sprzęt wolny od wad, równoważny jakościowo i funkcjonalnie w ciągu 72 godzin od zgłoszenia problemu;
   h) w przypadku uszkodzenia dysku (nośnika pamięci), Wykonawca dostarczy nowy dysk wolny od wad równoważny jakościowo i funkcjonalnie;
   i) dysk uszkodzony przechodzi na własność Zamawiającego;
10. Wykonawca w okresie gwarancji jest zobowiązany do jednokrotnego wykonania wspólnie z Zamawiającym bezpłatnego przeglądu Systemu, w ramach którego Wykonawca wykona:
    a) aktualizacje wymaganych lub rekomendowanych przez producenta lub producentów komponentów Systemu;
    b) uruchomienie nowych, dostępnych w ramach aktualizacji funkcjonalności istotnych dla bezpieczeństwa teleinformatycznego.
11. Dla realizacji świadczeń gwarancyjnych Zamawiający dopuszcza połączenie zdalne do sieci informatycznej Zamawiającego, kontakt mailowy i telefoniczny, pod warunkiem, że powyższe nie wpłynie one na obniżenie jakości świadczenia usług gwarancyjnych.
12. Zamawiający zastrzega sobie prawo do dokonywania rozbudowy Systemu powstałego w trakcie realizacji Umowy o nowe elementy przez wykwalifikowanych pracowników.
13. W przypadku stwierdzenia niezgodności w sposobie realizacji przez Wykonawcę zobowiązań gwarancyjnych, Zamawiający zastrzega sobie prawo do naliczenia kar umownych i potrącenia ich z Zabezpieczenia należytego wykonania umowy.

14. Udzielona przez Wykonawcę gwarancja nie wyłącza prawa Zamawiającego do gwarancji udzielonych przez producentów elementów wdrożonego w ramach Umowy Systemu.
15. Okres rękojmi za wady, którego bieg rozpoczyna się w stosunku do przedmiotu Umowy od dnia aktywacji licencji równy będzie okresowi udzielonej przez Wykonawcę gwarancji. Zamawiający będzie mógł dochodzić roszczeń z tytułu rękojmi także po terminie określonym w zdaniu pierwszym, jeżeli zgłosił Wykonawcy wadę w ww. terminie.