

Opis Przedmiotu Zamówienia

Dostawa systemu Web Proxy oraz Sandbox do zapewnienia bezpiecznego dostępu do sieci Internet wraz z wdrożeniem.

Przedmiotem zamówienia jest zakup i wykonanie wdrożenia „Systemu Bezpiecznego Dostępu do Sieci Internet” zwanym dalej Systemem.

Przedmiot zamówienia obejmuje 5 zadań:

1. Wykonanie projektu technicznego Systemu.
2. Dostawa licencji na okres 36 miesięcy oraz sprzętu z oprogramowaniem wraz z wdrożeniem Systemu.
3. Wykonanie Dokumentacji Powykonawczej Systemu.
4. Gwarancja i wsparcie producenta na dostarczony System.
5. Przeprowadzenie szkoleń dla administratorów.

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:

- 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;
- 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.

I. Opis środowiska Zamawiającego

1. Wspólne uwarunkowania dla zadań oraz opis środowiska Zamawiającego

Prace wdrożeniowe i konfiguracyjne będą realizowane w Podstawowym Centrum Przetwarzania Danych mieszczącym się w siedzibie Zamawiającego w Warszawie.

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

- 1.1. Zamawiający posiada domenę produkcyjną AD DS. (MS Active Directory) Windows Serwer 2019 o funkcjonalności lasu i domeny na poziomie Windows Server 2012R2.
- 1.2. Poczta korporacyjna statystyki publicznej działa w oparciu o MS Exchange 2019
- 1.3. Zamawiający dysponuje środowiskiem do wirtualizacji serwerów zbudowanym w oparciu o oprogramowanie VMware Cloud Foundation.
- 1.4. Do obsługi baz technicznych Zamawiający wykorzystuje oprogramowanie MS SQL Server oraz 2012 Standard Edition i 2019 Enterprise Edition.

2. Wymagania dotyczące bezpieczeństwa dostarczonego oprogramowania

2.1 Dostarczone oprogramowanie nie może być zabronione do stosowania przez administrację któregośkolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).

2.2 Oferowany system musi być w całości posadowiony w siedzibie Zamawiającego.

3 Opis infrastruktury Zamawiającego

Sieć teleinformatyczna w siedzibie Głównego Urzędu Statystycznego zbudowana jest z przełączników warstwy 3, z przełączników warstwy 2, routerów dostępowych oraz zapór sieciowych i podzielona jest na następujące segmenty:

1. Dostęp do Internetu

Strefa ta składa się z dwóch łączy do niezależnych operatorów oraz dwóch routerów, dwóch przełączników L2, redundantnego firewall'a brzegowego oraz systemu Symantec Proxy Web Security Gateway.

2. Strefy DMZ (strefa zdemilitaryzowana)

W strefie tej zainstalowane są serwery służące do komunikacji z systemami oraz użytkownikami zewnętrznymi. Poszczególne strefy DMZ są od siebie odseparowane na poziomie logicznym. Zabezpieczenia stref DMZ realizowane jest przez firewall brzegowy. Reguły na zaporze sieciowej pozwalają jedynie na konkretne połączenia pomiędzy DMZ a siecią wewnętrzną.

3. Sieci GUS-WAN

Sieć teleinformatyczna WAN zbudowana jest w oparciu o routery i firewall'e zlokalizowane w siedzibie GUS, w Urzędach statystycznych i ich Oddziałach.

4. Sieci GUS-LAN

Do tej strefy należą wszystkie zasoby znajdujące się w sieci LAN GUS, w tym: przełączniki szkieletowe, przełączniki agregacyjne, przełączniki dostępowe oraz komputery, laptopy, drukarki i urządzenia wielofunkcyjne.

5. Data Center

Sieć logiczna jest zbudowana w architekturze sieci programowalnych SDN. Zamawiający wykorzystuje oprogramowanie wirtualizacyjne VMware Cloud Foundation Advanced. Dodatkowo, na styku sieci DC, zainstalowany jest firewall wewnętrzny. Logicznie strefa ta jest podzielona na kilkadziesiąt podsieci. W skład tych podsieci wchodzi serwer aplikacji, serwery bazodanowe, serwery BackOffice oraz urządzenia balansujące ruch.

Zamawiający posiada wdrożone rozwiązanie typu SIEM, które zbiera, analizuje i koreluje logi zdarzeń z różnych źródeł infrastruktury Zamawiającego.

Zamawiający w swojej infrastrukturze posiada wdrożone rozwiązania typu EDR, Load balancer oraz firewall pocztowy współpracujące z obecnie wdrożonym systemem SWG.

Zamawiający realizuje kontrolę dostępu w sieci w oparciu o protokoły Radius, Tacacs oraz Active Directory.

II. Opis wymagań dla „Systemu Web Proxy oraz Sandbox do zapewnienia bezpiecznego dostępu do sieci Internet”.

Zamawiający wymaga dostarczenia sprzętu bądź wirtualnych appliance'ów. W przypadku zaoferowania sprzętu fizycznego urządzenia muszą spełniać następujące warunki:

1. fabrycznie nowego, nie używanego wcześniej w innych projektach (nie dopuszcza się rozwiązań typu „refurbished” itp.), były bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej,
2. objętego 3 letnią opieką gwarancyjną,
3. pochodzącego z autoryzowanego kanału sprzedaży producentów zaoferowanych urządzeń,
4. nieprzeznaczonego, w dniu składania ofert, przez producenta do wycofania z produkcji,
5. współpracującego z siecią energetyczną o parametrach: 230 V \pm 10%, 50 Hz, jednofazowo i wyposażonego w przewody zasilające,
6. posiadającego najnowszą rekomendowaną w dniu składania ofert wersję oprogramowania.

Wykonawca w treści złożonej oferty oświadczy, że Urządzenia dostarczone Zamawiającemu będą spełniały powyższe wymagania.

Opis wymaganych funkcjonalności dla modułów:

Wszystkie moduły systemu muszą posiadać:

1. Logowanie do systemu na bazie użytkowników lokalnych, LDAP i Radius.
2. Możliwość integracji z systemami typu SIEM do przekazywania logów.
3. Synchronizacja czasu z serwerem NTP.
4. Wysyłanie powiadomień o działaniu systemu przez SMTP.
5. Monitorowanie przy pomocy SNMP.

Modułu proxy:

1. Realizować funkcję forward proxy w trybie explicit i transparent.
2. System ma analizować ruch do oraz z Internetu. Całkowite pasmo ruchu objęte ochroną powinno wynosić minimum: 2 Gbps, w tym co najmniej 70% ruchu HTTP/HTTPS oraz pozwalać na obsłużenie minimum 3000 użytkowników przy założeniu 80% udziału SSL/TLS w ruchu.
3. System musi obsługiwać w trybie proxy następujące protokoły: HTTP, HTTPS, FTP. Dla pozostałych protokołów musi być możliwość tunelowania ruchu.
4. Rozwiązanie musi umożliwiać identyfikację i kontrolę ruchu strumieniowego (audio/video streaming), w tym usług realizowanych w oparciu o protokół HTTPS.
5. Cachowanie ruchu i jego kontrole poprzez politykę – np. wyłączenie cachowania dla wybranej strony czy kategorii URL.
6. System musi umożliwiać definicję własnych serwisów nasłuchujących dla trybu explicit proxy dla różnych sieci na różnych portach i przypisanie polityk dla różnych serwisów.
7. Kategoryzację adresów URL opartą zarówno o bazę statyczną jak i automatycznie aktualizowaną (nie rzadziej niż 2 razy w ciągu doby) ze źródeł zewnętrznych.
8. Baza ma zawierać co najmniej 60 dostępnych kategorii URL i posiadać kategorie umożliwiające zapewnienie zgodności z obowiązującymi przepisami (np. zdrowie, finanse itp.).
9. Tworzenie własnych baz kategorii (minimum whitelist i blacklist).

10. Kategorie typu „Uncategorized”, która może być użyta w polityce na wypadek, gdyby mechanizm dynamicznej klasyfikacji nie był w stanie przypisać stronie żadnej kategorii.
11. Niezależnie od mechanizmu klasyfikacji w oparciu o kategorię strony musi istnieć mechanizm oceny reputacji danej strony uwzględniający przynajmniej 5 stopni ryzyka.
12. Każde zapytanie o reputację strony musi zwracać wynik w założonej przez producenta skali. Innymi słowy niedopuszczalna jest sytuacja, że mechanizm reputacji nie dostarcza żadnej informacji o ryzyku dla danej strony.
13. Rozwiązanie musi posiadać narzędzie graficzne do tworzenia polityk.
14. Zarządzanie urządzeniem musi być możliwe zarówno przez interfejs graficzny (lokalna lub centralna konsola) jak i przez linie poleceń.
15. System musi posiadać możliwość blokowania określonych typów plików na bazie ich zawartości np. plików wykonywalnych, plików PDF, obrazków itp.
16. Rozwiązanie musi uwierzytelniać użytkowników w oparciu o źródła takie jak: lokalny plik, NTLM lub Kerberos, LDAP, RADIUS i certyfikat.
17. System musi zapewniać możliwość kontroli popularnych webaplikacji z akcjami typu upload, download, post czy send. Minimalny zestaw webaplikacji: facebook, X (twitter), linkedin, youtube, vimeo, snapchat, google plus, gmail, google talk, google docs, sharepoint, evernote, dropbox, box, sugarsync, flickr, instagram, webex.
18. Możliwość deszyfrowania ruchu TLS oraz robienia wyjątków deszyfracji TLS w oparciu o adres źródłowy / podsieć i URL.
19. System musi umożliwiać selektywne wyłączenie funkcji deszyfracji dla wybranych kategorii.
20. W trybie rozszywania ruchu TLS system musi zapewnić możliwość sprawdzenia ważności certyfikatu serwera, do którego łączy się użytkownik tj. minimum sprawdzenia daty i łańcucha certyfikacji.
21. Wykrywanie i blokowanie tunelowania w protokołach HTTP/HTTPS np. blokowanie sesji SSH na porcie 443.
22. Możliwość zarządzania pasmem dla wybranych usług, wsparcie QoS/ToS.
23. Rozwiązanie musi wspierać komunikację z zewnętrznymi skanerami antywirusowymi/antymalware za pomocą protokołów ICAP/ICAPS.
24. Wsparcie protokołu WCCP v2 oraz możliwość współpracy z infrastrukturą wykorzystującą Policy Based Routing.
25. Możliwość trzymania plików konfiguracyjnych Proxy-Auto-Config (tzw. PAC) bezpośrednio na urządzeniu i wykorzystywania ich dla różnych podsieci.
26. Wsparcie IPv6 zarówno w zakresie analizy ruchu jak i systemu zarządzania.
27. System musi być w stanie obsłużyć min 125 tysięcy jednoczesnych połączeń.
28. System musi umożliwiać tworzenie i wykorzystanie w politykach obiektów opartych o grupy AD i źródłowe adresy IP.

Moduł analizy treści:

1. Analizę antymalware przy pomocy następujących mechanizmów:
 - a) baza reputacji plików na bazie hashy o różnym stopniu zaufania,

- b) minimum 2 silniki AV działające jednocześnie, pochodzące od różnych producentów.
Zamawiający dopuszcza rozwiązanie polegające na stosowaniu jednego silnika sygnaturowego oraz silnika do analizy bezsygnaturowej/behawioralnej w ramach jednego zunifikowanego procesu kontroli ruchu,
 - c) inline sandboxing bez infekcji pacjenta zerowego,
 - d) własnej bazy hash'y działającej na zasadzie białej / czarnej listy, przy czym wspierane muszą być hash'e tworzone za pomocą algorytmu MD5 i SHA256
2. Skanowanie przez mechanizm antymalware musi odbywać się po złożeniu pliku w całość.
 3. System musi skanować pod kątem malware wszystkie pliki bez wyjątków.
 4. Musi być możliwe skanowanie dużych plików powyżej 4GB i możliwość zablokowania plików większych niż zdefiniowane przez administratora systemu.
 5. Skanowanie plików antymalware musi ponadto uwzględniać:
 - a) blokowanie plików skompresowanych z hasłem z możliwością odblokowania dla wybranego użytkownika lub grupy użytkowników,
 - b) analizę wielokrotnie skompresowanych plików,
 - c) analizę ilości plików w archiwum,
 - d) blokowanie nieznanymi typów rozszerzeń plików i archiwów.
 6. Integracja poprzez ICAP(S) z dowolnym systemem w celu analizy treści z niego pochodzących.
 7. Możliwość integracji poprzez REST API.
 8. System musi być w stanie obsłużyć minimum 100 Mbps ruchu przy wykorzystaniu AV.

Moduł raportujący:

1. Predefiniowane raporty i możliwość dodawania własnych raportów.
2. Możliwość czyszczenia danych po założonym okresie np. 60 dni.
3. System musi przechowywać logi za okres minimum 90 dni.
4. Możliwość konfiguracji progów zajętości pamięci i dysków, dla których następuje powiadomienie SMTP.
5. Zarządzanie w oparciu o role, w tym możliwość definiowania własnych ról.
6. Minimalny zestaw raportów, które system ma oferować:
 - a) Najczęściej odwiedzane, spośród zarejestrowanych w czasie pracy urządzenia, kategorie URL.
 - b) Najczęściej odwiedzane, spośród zarejestrowanych w czasie pracy urządzenia, strony.
 - c) Zablokowane żądania per kategoria URL.
 - d) Zablokowane żądania per użytkownik.
 - e) Zablokowane żądania per strona.
 - f) Listę użytkowników ściągających najwięcej danych.
 - g) Aktywność w serwisach społecznościowych.
 - h) Listę wykorzystywanych aplikacji webowych.
 - i) Listę użytkowników odwiedzających zabronione kategorie np. pornografię.
 - j) Szczegółowy raport na temat danego użytkownika na podstawie IP lub nazwy użytkownika.
 - k) Listę użytkowników potencjalnie zainfekowanych przez malware.

- l) Listę zainfekowanych użytkowników, którzy łączą się ze znanymi serwerami C&C.
- m) Listę zidentyfikowanego malware z informacją o pochodzeniu i użytkowniku, który go ściągnął.
- n) Wszystkie raporty muszą dawać możliwość wygenerowania za żądany okres czasu – minimum 1 dzień, 30 dni, 90 dni.

Moduł centralnego zarządzania:

1. Graficzny interfejs zarządzania w oparciu o przeglądarkę WWW/HTTP i protokół TLS.
2. Monitorowanie stanu zdrowia urządzeń zarządzanych przez moduł centralnego zarządzania w tym co najmniej zużycie CPU, RAM i zajętości dysków.
3. Synchronizacja polityki między modułem zarządzania a dodanymi do niego urządzeniami.
4. Wersjonowanie polityk z możliwością porównania ze sobą różnych polityk znajdujących się w bazie konfiguracji z możliwością przywrócenie wcześniejszej wersji.
5. Backup konfiguracji urządzeń jak i samego systemu zarządzania w postaci cyklicznych zadań i na żądanie z możliwością szyfrowania.

Moduł Sandbox:

1. Wymagane jest aby system umożliwiał detonację plików z całości ruchu z systemu SWG.
2. Dwa niezależne mechanizmy dynamicznej analizy plików tj. emulacja i wirtualizacja.
3. Wymagane jest pełne dostosowywanie profili maszyn wirtualnych poprzez możliwość instalacji własnych aplikacji na potrzeby dostosowania środowiska odpowiadającego środowisku Zamawiającego.
4. System musi dawać możliwość podejrzenia opisu zachowań dla sygnatur dostarczanych przez producenta i ich modyfikacji – przynajmniej wyłączenia jeśli nie spełniają oczekiwań.
5. Wymagana jest detonacja plików w powiązaniu z dedykowanym interfejsem, tak że wszelka komunikacja z zainfekowanej maszyny odbywa się tylko i wyłącznie tym interfejsem.
6. Musi istnieć możliwość konfiguracji Firewalla na ruchu wychodzącym z wirtualnych maszyn, w tym całkowitego odcięcia malware od komunikacji ze światem zewnętrznym, nawet przez dedykowany interfejs.
7. System musi umożliwiać określenie maksymalnego czasu dynamicznej analizy / detonacji plików.
8. Pliki ściągane przez malware pierwszej fazy (dropper/loader) muszą być zapisywane w celu dalszej analizy.
9. Ruch generowany przez próbkę podczas procesu detonacji musi być zapisywany i dostępny w formacie PCAP w celu dalszej analizy.
10. Musi istnieć możliwość rozbudowy funkcjonalności systemu poprzez dodawanie pluginów, które wykonają się podczas procesu detonacji w celu wykonania jakiejś konkretnej czynności – np. dodatkowej interakcji z malware albo wyciągnięcia określonych danych z pamięci ulotnej.
11. System musi działać zarówno w trybie stand-alone jako dedykowany system analityczny jak i część większego systemu bezpieczeństwa działającego inline lub na kopii ruchu.

12. W trybie stand-alone system musi umożliwiać zarządzanie oparte o role RBAC, w tym minimum rola administratora systemowego, analityka, API i pełnego administratora.
13. Podczas procesu ręcznej detonacji system musi dawać możliwość określenia dodatkowych argumentów wykonania próbki i ścieżki w systemie, w której ma się wykonać.
14. Wsparcie mechanizmu YARA, w tym możliwość dodawania własnych sygnatur.
15. System musi umożliwiać analizę dynamiczną w oparciu o źródła reputacyjne – w tym reputacja URL i reputacja plików.
16. Wynik analizy reputacyjnej URL w procesie detonacji musi uwzględniać kategorię URL z którą łączy się malware np. Pornography czy Dynamic DNS.
17. Wymagana jest możliwość eksportu wyników detonacji pliku w formacie STIX w celu dalszej analizy przez inne systemy.
18. Wszystkie funkcje systemu dostępne z interfejsu graficznego muszą być również dostępne przez Remote API.
19. Połączenia za pomocą Remote API muszą być realizowane poprzez połączenie szyfrowane i wymagać uwierzytelnienia.
20. System musi umożliwiać analizę dynamiczną każdego pliku dla którego istnieje w systemie oprogramowanie go wykonujące, również po modyfikacji profili wirtualnych systemów.
21. Jako źródło detonacji wymagana jest możliwość wskazania URLa lub grupy URLi w celu ich analizy.
22. Musi być możliwe przynajmniej wykrywanie prób sprawdzania przez malware czy jest w piaskownicy. W szczególnych przypadkach np. dla wywołania funkcji sleep() system musi móc oszukać malware, że określony czas już minął.
23. System musi umożliwiać przeszukiwanie zbioru przanalizowanych plików min. w oparciu o hash MD5 lub SHA256 oraz Risk Score.
24. Wymagana jest możliwość integracji z systemami ochrony poczty elektronicznej oraz EDR.
25. Wymagana minimalna ilość jednocześnie uruchomionych maszyn wirtualnych w systemie to 25.
26. Możliwość analizy minimum 32000 plików na godzinę.
27. Każde z urządzeń musi mieć wydajność umożliwiającą przeprowadzenia analizy minimum 8000 próbek malware w ciągu 24h.
28. Możliwość analizy plików o rozmiarze co najmniej 200 MB
29. Możliwość skanowania stron www z linkami URL
30. System musi umożliwiać skanowanie plików na zasobach: SMB, NFS, SFTP, Microsoft OneDrive oraz Sharepoint z możliwością kwarantanny podejrzanych plików.
31. System musi umożliwiać skanowanie plików oraz URL z wykorzystaniem interfejsu API.
32. System musi umożliwiać interakcję analityka z badanym plikiem przez dostęp do konsoli maszyny wirtualnej uruchomionej na potrzeby analizy automatycznej. Funkcjonalność musi być dostępna z poziomu interfejsu WebUI i dotyczyć systemów operacyjnych Microsoft Windows oraz Linux.
33. System musi mieć możliwość integracji z regułami YARA firm trzecich.

34. System musi posiadać mechanizm rozpoznawania znaków (OCR) umożliwiający przetwarzanie obrazów i odczytywanie tekstów w celu efektywnego wykrywania zagrożeń – np. notatek z żądaniem okupu osadzonych w dokumentach.
35. System musi umożliwiać analizę plików pozyskiwanych z kopii ruchu sieciowego, analizę wiadomości e-mail w trybie BCC (Blind Carbon Copy) oraz integrację z wykorzystaniem protokołu ICAP.

Szczegółowa specyfikacja i opisy zadań do realizacji przez Wykonawcę

III. Zadanie 1. Wykonanie projektu technicznego Systemu.

1. Wykonawca opracuje i przekaże Zamawiającemu dokument pt. Projekt Techniczny „Systemu Bezpiecznego Dostępu do Sieci Internet” spełniający wymagania opisane w punkcie II.
Dokument powinien zawierać:
 - a. Koncepcję wdrożenia oraz schematy połączeń dostarczanych komponentów.
 - b. Wykaz dostarczanego sprzętu i licencji oprogramowania.
 - c. Wykaz planowanych do monitorowania systemów i aplikacji infrastruktury IT Zamawiającego.
 - d. Konfigurację i plan podłączenia wszystkich komponentów systemu do infrastruktury sieci LAN.
 - e. Zagadnienia bezpieczeństwa i zarządzania Systemem.
 - f. Zagadnienia archiwizacji i odtwarzania Systemu.
 - g. Plan rozmieszczenia sprzętu w szafie lub szafach „rack”, w pomieszczeniach serwerowni, udostępnionych przez Zamawiającego oraz wymagania dotyczące zasilania i wagi dostarczanych sprzętów.
 - h. Zestaw reguł filtrowania ruchu wychodzącego do Internetu, opracowany na podstawie istniejącego zestawu reguł na obecnie działającym SWG.
 - i. Zasady automatycznej konfiguracji klienta (PAC).
 - j. Zestaw testów odbiorczych uzgodnionych z Zamawiającym.
 - k. Harmonogram realizacji przedmiotu zamówienia uwzględniający wszystkie aspekty techniczne, organizacyjne oraz terminowe przedmiotowej umowy.
2. Projekt Techniczny „Systemu Bezpiecznego Dostępu do Sieci Internet” będzie podlegał procedurze odbioru, na następujących warunkach:
 - a. Wykonawca przekaże Zamawiającemu drogą elektroniczną do akceptacji Projekt Techniczny w terminie nie dłuższym niż 21 dni kalendarzowych od dnia zawarcia umowy.
 - b. Zamawiający w terminie nie dłuższym niż 5 dni kalendarzowych od dnia dostarczenia Projektu Technicznego, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian.
 - c. Wszystkie uwagi do Projektu Technicznego zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 3 dni kalendarzowe od dnia ich otrzymania.

- d. Zamawiający w terminie 3 dni kalendarzowe od dnia powtórnego dostarczenia przez Wykonawcę poprawionego Projektu Technicznego, poinformuje wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian.
 - e. Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w projekcie technicznym.
 - f. W przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia Projektu Technicznego nie później niż po 5 dniach kalendarzowych, po tym terminie Zamawiający ma prawo do odstąpienia od Umowy i zlecenia wykonawstwa zastępczego firmie trzeciej.
 - g. Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji Projektu Technicznego, następować będzie drogą mailową na adresy Wykonawcy i Zamawiającego wskazane w umowie.
3. Zatwierdzony Projekt Techniczny zostanie przekazany Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru Zadania I na pendrive w wersji edytowalnej i PDF.
 4. Potwierdzeniem odbioru Projektu Technicznego będzie Protokół odbioru Projektu Technicznego, podpisany z wynikiem pozytywnym, stanowiący załącznik nr ... do umowy.

IV. Zadanie 2. Dostawa licencji, sprzętu z oprogramowaniem i wdrożenie Systemu.

Dostawa

1. Zamawiający wymaga, aby Wykonawca dostarczył i wdrożył w ramach przedmiotu zamówienia kompletne środowisko sprzętowe i programowe (licencje) Systemu.
2. System powinien składać się z modułów oraz licencji opisanych w szczegółowo w rozdziale II.
3. Zamawiający wymaga, aby sprzęt:
 - a. spełniał przewidziane przez producenta rozwiązania parametry techniczne z uwzględnieniem wymagań określonych przez Zamawiającego,
 - b. był wyposażony w redundantne zasilacze,
 - c. był wyposażony w redundantne interfejsy sieciowe.
 - d. działał w klastrze HA trybie active-passive z możliwością przełączenia na tryb active-active.
4. Zaoferowany sprzęt, musi być przystosowany do instalacji w posiadanych przez Zamawiającego szafach rack 19 cali.
5. Wszystkie urządzenia muszą zawierać osprzęt wymagany przez producentów oferowanego rozwiązania (na przykład: okablowanie energetyczne, urządzenia zasilające) oraz niezbędny do jego prawidłowego podłączenia z dedykowaną siecią energetyczną Zamawiającego o parametrach: 230V \pm 10%, 50Hz oraz siecią logiczną. W szafach rack Zamawiającego są dostępne listwy zasilające z gniazdami C13 lub istnieje możliwość dedykowanego zasilania.
6. Wszystkie dostarczane urządzenia muszą zawierać sieciowe okablowanie logiczne. Zamawiający udostępni przełączniki sieciowe do podłączenia Systemu do infrastruktury sieciowej poprzez interfejsy fizyczne miedziane RJ45 lub światłowodowe w standardzie SFP/SFP+ 1Gbps oraz 10Gbps. Wykonawca dostarczy do posiadanych przez Zamawiającego przełączników sieciowych

odpowiednią ilość kompatybilnych wkładek, nie powodujących utraty gwarancji producenta na te przełączniki, niezbędnych do prawidłowego funkcjonowania systemu oraz kable umożliwiające połączenie dostarczonych urządzeń do infrastruktury sieciowej Zamawiającego.

7. Zamawiający wymaga aby każde urządzenie typu Web Gateway było połączone z siecią LAN Zamawiającego czterema (4) interfejsami o przepustowości 10 Gbps.
8. Zamawiający wymaga aby każde urządzenie typu Sandbox było połączone z siecią LAN Zamawiającego dwoma (2) interfejsami o przepustowości minimum 1 Gbps.
9. Zamawiający wymaga aby interfejsy do zarządzania (management) dostarczonymi urządzeniami były połączone z siecią LAN Zamawiającego interfejsem o przepustowości minimum 1 Gbps.
10. Wykonawca gwarantuje, że wszystkie dostarczane produkty (dotyczy to zarówno sprzętu jak i oprogramowania) są ze sobą kompatybilne w zakresie, w jakim wymagana jest ich wzajemna współpraca.
11. Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (tzn. bez śladów użytkowania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej).
12. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania. Zamawiający wymaga, aby urządzenia były rozpakowane i uruchomione wyłącznie przez Wykonawcę lub podmioty przez niego uprawnione.
13. Dostawa sprzętu i oprogramowania zostanie zrealizowana zgodnie z wymaganiami:
 - a. Wykonawca dostarczy całość sprzętu wraz z oprogramowaniem do siedziby Zamawiającego.
 - b. Wykonawca dostarczy sprzęt w godzinach od 10:00 do 14:00 w dni robocze od poniedziałku do piątku.
 - c. Wykonawca zapewni we własnym zakresie środki transportu umożliwiające rozładunek i przewóz sprzętu z samochodu do serwerowni w budynku GUS, które są zlokalizowane na parterze oraz na pierwszym piętrze.

Wdrożenie

1. Wszystkie prace instalacyjne oraz wdrożeniowe będą uzgadniane i realizowane we współpracy z administratorami Zamawiającego.
2. Montaż sprzętu, podłączenie okablowania, instalacja oprogramowania oraz inne czynności konieczne do uruchomienia przedmiotu zamówienia, zostaną wykonane przez Wykonawcę w ramach ceny za przedmiot zamówienia.
3. Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie komponenty przedmiotu zamówienia zgodnie z opracowanym Projektem Technicznym Systemu.
4. Wykonawca dostarczy licencje oprogramowania, których liczba oraz zasady instalacji oprogramowania umożliwią eksploatację systemu w infrastrukturze IT Zamawiającego i zostały określone ilościowo i jakościowo w projekcie technicznym Systemu.
5. Wykonawca zainstaluje dostarczane urządzenia w serwerowni GUS w posiadanych przez Zamawiającego szafach rack 19".

6. Wykonawca dostarczy wszelkie niezbędne elementy do wykonania prac w szczególności kable elektryczne, światłowody, patchcordy - kable Ethernet kat. 6, bezpieczniki, gniazda zasilające, moduły PDU do szaf rack, organizery okablowania, peszle itp. w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich urządzeń dostarczanych w ramach przedmiotowego postępowania zgodnie z opracowanym Projektem Technicznym Systemu.
7. Wykonawca wykona konieczne połączenia sieciowego okablowania logicznego pomiędzy dostarczonymi urządzeniami, a przełącznikami sieciowymi zamontowanymi w serwerowni Zamawiającego.
8. Wykonawca oznaczy każdy kabel w sposób umożliwiający jego jednoznaczną identyfikację zgodnie z przyjętą konwencją nazewniczą.
9. Wykonawca dokona podłączenia dostarczonych urządzeń do sieci energetycznej Zamawiającego w sposób zgodny z obowiązującymi przepisami, zapewniający właściwe bezpieczeństwo użytkownika.
10. Jeżeli będzie to konieczne, Wykonawca wykona niezbędne otwory w podłodze technicznej w celu doprowadzenia okablowania.
11. Wykonawca ułoży okablowanie instalowanego sprzętu w przeznaczonych do tego celu korytkach, peszlach, organizacjach okablowania.
12. Wszystkie nośniki danych dostarczane wraz z urządzeniami pozostają w siedzibie Zamawiającego i przechodzą na jego własność. Wykonawca dostarczy na płytach CD/DVD lub pamięci Flash (pendrive) komplet sterowników systemowych i niezbędne oprogramowanie narzędziowe producenta.
13. Wszelkie koszty związane z wdrożeniem Systemu do środowiska Zamawiającego pokryje Wykonawca.
14. Wykonawca jest zobowiązany do posprzątania i wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania.
15. Wykonawca dokona uruchomienia i wstępnej konfiguracji dostarczanego sprzętu wraz z oprogramowaniem w infrastrukturze IT zgodnie z opracowanym Projektem Technicznym Systemu.
16. Wykonawca dokona aktualizacji oprogramowania firmware, wszystkich dostarczonych urządzeń do najnowszych rekomendowanych wersji.
17. Wykonawca uruchomi wszystkie komponenty i dokona konfiguracji komponentów Systemu zgodnie z opracowanym Projektem Technicznym w tym:
 - a. Wykonanie integracji wdrożonego systemu z systemem Active Directory Zamawiającego przynajmniej w zakresie identyfikacji użytkowników.
 - b. Wdrożenie zestawu reguł filtrowania ruchu wychodzącego do Internetu.
 - c. Wdrożenie rozszywania ruchu tunelowanego SSL wraz przygotowanym zestawem reguł
 - d. Wdrożenie zasad automatycznej konfiguracji klienta (PAC).
 - e. Wykonanie integracji SWG, modułu zawansowanej analizy treści z Sandboxem
 - f. Przeprowadzi wdrożenie pilotażowe na wybranej grupie użytkowników.
 - g. Przeprowadzi migrację użytkowników z istniejącego rozwiązania SWG na dostarczony

system.

18. Wykonawca przeprowadzi testy sprawdzające komponenty systemu w zakresie:
 - a. sprawdzenia statusów stanu sprzętu lub testów fabrycznych (producenta),
 - b. sprawdzenia poprawności działania HA, poprzez zasymulowanie uszkodzenia jednego z urządzeń,
 - c. sprawdzenia wydajności systemu.
19. Wykonawca przeprowadzi z Zamawiającym procedurę tworzenia kopii zapasowej oraz przywracania systemu z kopii zapasowej.
20. Realizacja Zadania 2, potwierdzone zostanie podpisanym z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego, Protokołem odbioru Zadania 2 nie później niż 14 tygodni od daty podpisania umowy.

V. Zadanie 3. Wykonanie dokumentacji powykonawczej Systemu.

1. Wykonawca jest zobowiązany do wykonania i dostarczenia Zamawiającemu, w ramach zapłaty za przedmiot zamówienia, Dokumentacji Powykonawczej, bazującej na Projekcie Technicznym „Systemu Bezpiecznego Dostępu do Sieci Internet”, zawierającej dokładny opis montażu, instalacji i konfiguracji zainstalowanych komponentów, schematy logiczne, konfiguracje dot. urządzeń i oprogramowania będącego obiektem prac podczas realizacji przedmiotu zamówienia oraz zawierający „Dokumentację administratora”.
2. „Dokumentacja administratora”, stanowiąca integralną część Dokumentacji Powykonawczej, musi zawierać, co najmniej:
 - a. Procedury działań administracyjnych takich jak np. wykonanie aktualizacji oprogramowania typu firmware, wykonanie aktualizacji oprogramowania aplikacyjnego, kolejność wykonywania aktualizacji poszczególnych komponentów Systemu.
 - b. Metody i narzędzia diagnostyki poprawności działania Systemu.
 - c. Procedury okresowych/planowanych działań administracyjnych, takich jak backup i archiwizacja danych.
 - d. Procedurę włączenia i wyłączenia całości dostarczanego sprzętu w przypadku prac planowych.
 - e. Procedurę przywracania całości Systemu z kopii zapasowej.
 - f. Dokumenty muszą posiadać spis treści, metrykę dokumentu oraz będą napisane w języku polskim.
3. Dokumentacja Powykonawcza podlegała będzie procedurze odbioru, na następujących warunkach:
 - a. Wykonawca przekaze Zamawiającemu drogą elektroniczną do akceptacji dokumentację powykonawczą, co najmniej na 15 dni roboczych przed terminem zakończenia realizacji umowy;
 - b. Zamawiający w terminie nie dłuższym niż 2 dni roboczych od dnia dostarczenia przez Wykonawcę dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian;
 - c. Wszystkie uwagi do dokumentacji powykonawczej zgłoszone przez Zamawiającego zostaną

- wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 2 dni robocze od dnia ich otrzymania;
- d. Zamawiający w terminie 2 dni robocze od dnia powtórnego dostarczenia przez Wykonawcę poprawionej dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian;
 - e. Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w dokumentacji powykonawczej;
 - f. W przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo wskazania ostatecznego terminu dostarczenia dokumentacji nie dłużej niż 5 dni robocze, w przeciwnym razie Zamawiający ma prawo do odstąpienia od Umowy i przekazanie wykonawstwa firmie trzeciej;
 - g. Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji Dokumentacji Powykonawczej, następować będzie drogą mailową na adresy Wykonawcy i Zamawiającego wskazane w umowie;
 - h. Zatwierdzona Dokumentacja Powykonawcza zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania Protokołu Odbioru Dokumentacji Powykonawczej na pendrive w wersji edytowalnej i PDF oraz wydruk papierowy w 2 egzemplarzach,
4. Zadanie 3 zostaje zakończone po podpisaniu Protokołu Odbioru Dokumentacji Powykonawczej bez zastrzeżeń.

VI. Zadanie 4. Gwarancja i wsparcie producenta na dostarczony system

- 1. Zamawiający wymaga, aby wszystkie dostarczone komponenty Systemu, w ramach ceny za przedmiot zamówienia, były objęte opieką gwarancyjną na okres 36 miesięcy.
- 2. Termin biegu gwarancji liczony będzie od dnia podpisania z wynikiem pozytywnym Końcowego Protokołu Odbioru.
- 3. Udzielona przez Wykonawcę gwarancja nie wyłącza prawa Zamawiającego do gwarancji udzielonych przez producentów elementów zaimplementowanego w ramach Umowy rozwiązania.
- 4. Niezależnie od udzielonej gwarancji Zamawiającemu przysługuje rękojmia w zakresie przedmiotu zamówienia.
- 5. Gwarancja powinna zawierać co najmniej wsparcie techniczne świadczone przez Producenta oraz jego autoryzowanego polskiego przedstawiciela, dostęp do nowych wersji oprogramowania a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
- 6. Wykonawca udzieli Zamawiającemu gwarancji na wykonaną usługę wdrożenia z istniejącą infrastrukturą obejmującą poprawę wykrytych ewentualnie błędów konfiguracji realizowanych wg założeń Zamawiającego na okres 36 miesięcy od daty podpisania protokołu odbioru wdrożenia.
- 7. Wykonawca zobowiązuje się do świadczenia usług gwarancji i asysty technicznej z należytą starannością, z uwzględnieniem ogólnie przyjętych i stosowanych standardów i procedur przy

tego rodzaju usługach, a także zaleceń lub procedur określonych przez Producenta.

8. Wykonawca zobowiązuje się świadczyć usługi gwarancyjne i asystę techniczną w miejscu użytkowania sprzętu, z możliwością naprawy w serwisie Wykonawcy, jeżeli naprawa sprzętu w miejscu użytkowania okaże się niemożliwa. W przypadku braku możliwości dokonania naprawy w miejscu użytkowania sprzętu i konieczności jego dostarczenia do punktu serwisowego wskazanego przez Wykonawcę, koszty dostarczenia uszkodzonego sprzętu do punktu serwisowego oraz z punktu serwisowego do miejsca użytkowania pokrywa Wykonawca.
9. Nośniki informacji takie jak, np. dyski twarde, pamięci flash, mogą być naprawiane jedynie w miejscu ich użytkowania, a w przypadku konieczności wymiany uszkodzonych nośników na nowe, wolne od wad, nośniki informacji pozostają u Zamawiającego. W przypadku konieczności dokonania naprawy sprzętu wyposażonego w nośniki informacji poza miejscem użytkowania, nośniki pozostają w siedzibie Zamawiającego.
10. Wykonawca zobowiązuje się do ponoszenia wszelkich kosztów naprawy, w tym kosztów transportu, instalacji, konfiguracji i uruchomienia Urządzenia.
11. 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.
12. 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.
13. W przypadku awarii wymagającej wymiany sprzętu, Wykonawca dostarczy Zamawiającemu sprzęt wolny od wad, równoważny jakościowo i funkcjonalnie w ciągu 72 godzin od zgłoszenia problemu.
14. Do dostarczonego rozwiązania będą dołączone karty gwarancyjne zawierające numery seryjne, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
15. Wykonawca zobowiązuje się przyjmować zgłoszenia gwarancyjne poprzez stronę www Wykonawcy dostępną przez całą dobę, 365 dni w roku. Wykonawca dostarczy dane niezbędne do autoryzacji na stronie www Wykonawcy w celu dokonywania zgłoszeń serwisowych przez Zamawiającego. Zamawiający wymaga również zapewnienia możliwości dokonywania zgłoszeń serwisowych poprzez e-mail w przypadku braku możliwości dokonania zgłoszenia serwisowego przez stronę www (np. w przypadku braku dostępności dedykowanej strony www). Wzór formularza zgłoszenia serwisowego będzie stanowił załącznik do umowy. Wykonawca potwierdzi otrzymanie zgłoszenia serwisowego poprzez wysłanie wiadomości e-mail na adres Zamawiającego wskazany w umowie. Wszelkie wykonane przez Wykonawcę lub jego przedstawicieli czynności serwisowe wymagają dokumentowania w formie pisemnej.
16. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do współpracy z Zamawiającym w zakresie wykrytych przez Zamawiającego bądź podmiot trzeci podatności i luk w systemie oraz zobowiązuje się do niezwłocznego wprowadzania zmian i poprawek w systemie, które wynikać będą z rekomendacji po wykonanym teście, przy uwzględnieniu racjonalnych możliwości

wdrożenia rekomendacji.

17. Wykonawca zapewni świadczenie usługi asysty technicznej w ramach której zapewni:
 - a. stabilną pracę zaimplementowanego rozwiązania,
 - b. dodawanie nowych, określonych przez Zamawiającego funkcjonalności,
 - c. porady eksperckie,
 - d. dodatkowe integracje z systemami wewnętrznymi,
 - e. aktualizację oprogramowania;
 - f. cykliczny bezpłatny przegląd Systemu nie rzadziej niż raz w roku
18. Jeśli błąd dotyczy oprogramowania i Wykonawca uzyska diagnozę problemu wskazującą, że naprawa wymaga instalacji nowej wersji oprogramowania, Wykonawca zobowiązany jest przekazać Zamawiającemu treść diagnozy i zastosować rozwiązanie problemu z zastrzeżeniem, że nowa wersja oprogramowania istnieje. Jeżeli Producent nie dostarczył wersji oprogramowania pozbawionej błędu, czas realizacji zgłoszenia zostanie wstrzymany do czasu powstania nowej wersji oprogramowania.
19. Zamawiający wymaga udostępnienia przez Wykonawcę Zamawiającemu, na jego prośbę, dostępu do informacji o zgłoszeniach.
20. Usługi asysty technicznej będą świadczone w wymiarze 180 roboczogodzin na czas trwania umowy (w roboczogodzinę wsparcia nie wlicza się czasu dojazdu oraz ilości osób świadczących usługę, tzn. nie ma znaczenia, ile osób jednocześnie będzie świadczyło usługę w ramach jednej roboczogodziny). Usługa będzie świadczona dla infrastruktury Zamawiającego (sprzętu i oprogramowania).
21. W przypadku, jeżeli w wyniku dokonania istotnych zmian konfiguracyjnych, wystąpi konieczność zmiany Dokumentacji powykonawczej, Wykonawca dostarczy zaktualizowaną Dokumentację powykonawczą w formie elektronicznej w terminie 30 dni roboczych po dokonaniu zmian konfiguracyjnych.
22. Wykonawca będzie miał prawo odmówić wykonania usług asysty technicznej w sytuacji gdy:
23. Zamawiający wyczerpie przysługujący limit godzin asysty technicznej, o którym mowa w pkt 20;
24. Realizacja asysty technicznej we wnioskowanym zakresie spowodowałaby przekroczenie przysługującego Zamawiającemu limitu godzin, o którym mowa w pkt 20 .
25. Asysta techniczna będzie świadczona w języku polskim i realizowana zdalnie lub lokalnie w zależności od metodyki właściwej dla zdefiniowanego problemu według decyzji Wykonawcy. Na wyraźne wezwanie Zamawiającego inżynier wsparcia technicznego ma obowiązek przybyć do siedziby Zamawiającego i tam realizować zgłoszenie.
26. W ramach wsparcia technicznego Wykonawca zapewni, zgodnie z potrzebami Zamawiającego, co najmniej jednego inżyniera, posiadającego minimum 3 letnie doświadczenie w administrowaniu systemem w zakresie zaimplementowanego rozwiązania oraz posiada certyfikat obejmujący podstawy sieci, bezpieczeństwa i serwerów webowych.
27. Zakres czynności wykonywanych w ramach wsparcia technicznego nie może być tożsamy z zakresem objętym serwisem gwarancyjnym. W przypadku, gdy Zamawiający zleci Wykonawcy prace, które powinny być zrealizowane w ramach serwisu gwarancyjnego, Wykonawca ma obowiązek poinformowania o tym fakcie Zamawiającego.

28. Zamawiający będzie przekazywać Wykonawcy zlecenia w ramach asysty technicznej, w których określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
29. Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą w szczególności zakres prac zawartych w zleceniu oraz proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
30. Zamawiający może zaakceptować propozycję wykonania zlecenia albo odrzucić propozycję, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, w wyznaczonym terminie, dodatkowych wyjaśnień, informacji do przedstawionej propozycji wykonania zlecenia.
31. W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, termin wykonania prac.
32. 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.
33. Rozliczenie godzin w ramach wsparcia technicznego inżyniera odbywać się będzie na podstawie podpisanego bez zastrzeżeń, przez Wykonawcę i Zamawiającego dokumentu „Protokół odbioru usługi gwarancyjnej/wsparcia technicznego” – Załącznik do Umowy.
34. Wymagany czas na usunięcie awarii wynosi 24 godziny od momentu potwierdzenia zgłoszenia telefonicznego, drogą mailową lub pisemnie do siedziby serwisu, natomiast działania serwisowe należy podjąć w ciągu 4 godzin w siedzibie Zamawiającego lub zdalnie od momentu zgłoszenia telefonicznego, drogą mailową lub pisemnie do siedziby serwisu.
35. W razie wątpliwości uznaje się, że zgłoszenie zostało dokonane w chwili wystąpienia informacji w formie mailowej lub za pomocą dedykowanego narzędzia. Ryzyko nieotrzymania prawidłowo przekazanego zgłoszenia spoczywa na Wykonawcy, z wyjątkiem sytuacji, gdy Wykonawca udowodni, że nie otrzymał wiadomości z przyczyn od niego niezależnych.
36. Wskazane powyżej czasy liczone są od chwili dokonania zgłoszenia w sposób ciągły w odniesieniu do pojedynczego zgłoszonego problemu.
37. Przez usunięcie awarii należy rozumieć przywrócenie funkcjonalności systemu z przed awarii we wszystkich modułach i zaprzestaniu stosowania przez obsługę w bieżącej pracy zastępczego sprzętu i/lub Procedur Zastępczych.
38. Czas trwania Procedur Zastępczych nie może być dłuższy niż 30 dni kalendarzowych od chwili zgłoszenia awarii.
39. W przypadku braku możliwości dochowania terminu o którym mowa w pkt 36, Wykonawca dostarczy Zamawiającemu fabrycznie nowy sprzęt wolny od wad, równoważny funkcjonalnie. Dostawa przedmiotowego sprzętu nastąpi nie później niż w pierwszym dniu roboczym po terminie o którym mowa jest w pkt 36.
40. Po usunięciu każdej awarii, Wykonawca zobowiązuje się do doprowadzenia całego sprzętu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych modułów.
41. Czas usunięcia awarii liczony będzie w godzinach, od momentu wystąpienia przez Zamawiającego

do Wykonawcy formularza „Zgłoszenie o świadczenie usługi gwarancyjnej /wsparcia technicznego” – Załącznik do umowy.

42. Zamawiający zastrzega sobie prawo dokonywania modyfikacji konfiguracji wdrożonego rozwiązania.
43. Wykonawca ma obowiązek w okresach rocznych rozliczania wykorzystanych godzin opieki gwarancyjnej oraz przekazywania raportów z liczbą godzin wykorzystanych i liczbą godzin pozostałych do wykorzystania.

VII. Zadanie 5. Warsztaty szkoleniowe

Przeprowadzenie warsztatów szkoleniowych dla administratorów.

Wykonawca przeprowadzi szkolenia w formie warsztatów z zakresu obsługi, konfiguracji oraz administracji dostarczonego rozwiązania. Szkolenie powinno trwać minimum 5 dni.

1. Program szkoleń powinien zawierać informacje dotyczące tematyki prowadzonych warsztatów, informacje dotyczące wiedzy i umiejętności jakie zdobędą uczestnicy po zakończeniu warsztatów. Zamawiający zastrzega sobie prawo do korekty programu warsztatów w zakresie nieograniczonym regulacjami prawnymi.
2. Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy – z rozpisaniem na dni i godziny - oraz programy szkoleń i dostarczy je Zamawiającemu.
3. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu. Harmonogram powinien zostać wydrukowany i rozdany uczestnikom szkolenia na pierwszym spotkaniu.
4. Wykonawca, zgodnie z planem szkoleń i w terminie przewidzianym w zatwierdzonym Harmonogramie przeprowadzi szkolenie w certyfikowanym ośrodku szkoleniowym na terenie Warszawy dla 6 osób, w dwóch nie nakładających się turach - w każdej turze zostanie przeszkolonych 3 pracowników Zamawiającego.
5. W przypadku szkoleń przeprowadzanych poza terenem Warszawy, Wykonawca poniesie całkowite koszty zakwaterowania i wyżywienia uczestników szkolenia.
6. Wykonawca zobowiązany jest do zrealizowania szkoleń w terminie do dnia podpisania protokołu odbioru końcowego.
7. Wykonawca musi dysponować lub zapewnić na cele realizacji przedmiotu zamówienia odpowiednio wykwalifikowaną kadrę, której powierzy realizację przedmiotu zamówienia w zakresie szkoleń. Wymagane jest, aby kadra trenerska posiadała udokumentowane co najmniej 2 letnie doświadczenie w przedmiocie szkolenia.
8. W pobliżu sali wykładowej (w tym samym budynku) powinna znajdować się toaleta z węzłem sanitarnym.
9. Zajęcia powinny odbywać się w dni powszednie od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin dziennie.

10. Wykonawca przygotowuje i zapewni materiały szkoleniowe dla każdego uczestnika pozwalające na samodzielną edukację z zakresu tematyki szkoleń (opracowania, wydruki materiałów szkoleniowych).
11. Wykonawca zapewni na potrzeby wyżywienia uczestników szkoleń odpowiednie pomieszczenie oraz niezbędną liczbę stołów i krzeseł. Zamawiający nie dopuszcza serwowania posiłków w tej samej sali, w której odbywają się szkolenia.
12. Miejsce posiłku nie powinno być oddalone dalej niż 10 minut drogi pieszo od miejsca szkolenia.
13. Wykonawca zapewni min. 2 przerwy kawowe podczas jednego dnia szkoleniowego
14. Czas na przerwy kawowe i obiadowe należy doliczyć do założonej liczby godzin warsztatów.
15. Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.
16. Szkolenia muszą być prowadzone w języku polskim.
17. Każdy uczestnik szkoleń otrzyma imienne zaświadczenia jego ukończenia potwierdzające, że nabyli wiedzę zgodną z celem szkolenia.
18. Potwierdzeniem prawidłowej realizacji szkoleń będzie podpisany bez zastrzeżeń przez Zamawiającego „Protokół odbioru szkoleń” (w czterech jednobrzmiących egzemplarzach) wraz z dołączonymi załącznikami:
 - a) oryginalną listą obecności,
 - b) harmonogramem i programem szkoleń (nazwę, tematykę i czas trwania szkoleń, datę i miejsce szkoleń, imię i nazwisko oraz specjalizację osób prowadzących szkolenia),
 - c) ankiety oceny szkoleń przeprowadzonej wśród uczestników szkoleń.
19. W przypadku negatywnej oceny szkoleń (średnia z oceny trenera / trenerów poniżej 3), Wykonawca przeprowadzi dodatkowe szkolenia na koszt własny, dochowując terminu realizacji Zadania. Organizacja dodatkowego szkoleń będzie wymagała uzgodnienia z Zamawiającym terminu oraz osoby prowadzącej zajęcia. Ponowne przeprowadzenie szkoleń musi się odbyć nie później niż 5 dni przed terminem zakończenia Zadania. Koszt ponownego zorganizowania i przeprowadzenia szkoleń ponosi Wykonawca.

Minimalny zakres szkoleń:

Zakres szkoleń będzie obejmował zagadnienia podstawowe i zaawansowane dotyczące systemu:

- a. Web Gateway wraz z modułami zaawansowanej analizy treści, raportowania i centralnego zarządzania oraz systemu Sandbox,
- b. Informacje i funkcjonalności dostępne w zaoferowanym systemie.
- c. Konfiguracja poszczególnych modułów i komponentów.
- d. Omówienie panelu administracyjnego.
- e. Konfiguracja polityk.
- f. Konfiguracja load balancingu.
- g. Tworzenie backupów i przywracanie z kopii zapasowych.
- h. Zarządzanie bezpieczeństwem Systemu.
- i. Obsługa błędów Systemu.
- j. Modyfikacja, rozbudowa i aktualizacja Systemu.

Po ukończeniu szkolenia uczestnik będzie potrafił:

1. Dobrać odpowiednią architekturę i model implementacji
2. Samodzielnie zainstalować i skonfigurować dostarczone rozwiązanie
3. Tworzyć, zarządzać i optymalizować polityki ochrony ruchu webowego
4. Monitorować system i analizować zdarzenia bezpieczeństwa
5. Diagnozować problemy i skutecznie je rozwiązywać
6. Stosować dobre praktyki administracyjne i eksploatacyjne.