Szacowanie wartości zamówienia

SIWZ - Specyfikacja Istotnych Warunków Zamówienia / OPZ – Opisz przedmiotu zamówienia

1. Gmina Istebna, Istebna 1000, 43-470 Istebna, NIP: 5482676134, zaprasza do składania ofert cenowych w ramach **szacowanie wartości zamówienia** na: **Dostawa oprogramowania i innych rozwiązań cyberbezpieczeństwa dla Gminy Istebna w ramach projektu pn. „Wzmocnienie poziomu cyberbezpieczeństwa w gminie Istebna” w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23”.**

   Postępowanie prowadzone jest w celu oszacowania wartości zamówienia.

2. Przedmiotem niniejszego zapytania jest:

   W szczególności wymagany zakres sprzętu obejmuje:

   Cześć I

   2.1. **Systemu NAC dla 150 IP - 1 sztuka – licencja bezterminowa**

Podstawowa funkcjonalność systemu NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
    - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
    - serwera RADIUS dla infrastruktury sieciowej,
    - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    - serwera SYSLOG,
    - serwera TACACS+,
    - serwera Monitoringu,
    - serwera DHCP,
    - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.

12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.

25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.

41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.

59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
    - Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
    - Czy włączony jest firewall
    - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
    - Czy jest włączone szyfrowanie dysku systemowego
    - Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
    - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
    - Czy w systemie są uruchomione procesy wskazane przez administratora
    - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
    - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
        - Wartości klucza rejestru
        - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    - Microsoft Windows
    - Mac OS
    - iOS
    - Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
    - MAC,
    - PAP/ASCII,
    - CHAP,
    - SNMP,
    - 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
    - Tożsamość/Urządzenie końcowe,
    - Grupa tożsamości/urządzeń końcowych,
    - Parametry urządzeń końcowych, min: system operacyjny, wersja,
    - Atrybuty Active Directory,
    - Jednostka organizacyjna tożsamości/urządzeń końcowych,
    - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
    - Grupy urządzeń sieciowych,
    - Porty urządzeń sieciowych,
    - Grupy portów urządzeń sieciowych,

- Jednostka organizacyjna portów,
- Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
- Data, czas ważności polityki,
- Wewnętrzny Captive Portal,
- Metoda autoryzacji.

8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.

20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
    - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
    - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
    - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
    - usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
    - Uruchamianie usługi dla wybranych podsieci,
    - Przypisanie ustalonego adresu IP dla adresu MAC.

- Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
- Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
- Możliwość określania braku dostępu dla wybranych adresów MAC,
- Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
- Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
- Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
- Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
- Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.

16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
    - Logowania, wylogowania z system w tym błędne logowania
    - Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
    - wiadomości e-mail,
    - Syslog,
    - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
    - Ilości obsługiwanych transakcji RADIUS,
    - Opóźnienie obsługi transkacji RADIUS,
    - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
    - badanie łączności IP za pomocą ping, traceroute,
    - tcpdump protokołów RADIUS, TACACS+,
    - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
        – nazwy użytkownika,
        – adresu MAC,
        – statusu uwierzytelnienia (udana lub nieudana),
        – powodu, jeżeli uwierzytelnienie nieudane,
        – zakresu czasowego, co do dnia, godziny i minuty,

- wykonanie zdalnego polecenia na urządzeniu sieciowym.

Szkolenia/warsztaty:

- Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC
- Warsztaty zostaną przeprowadzone dla maksymalnie 4 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC
- Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC
- Warsztaty odbędą się w formie zdalnej.
- Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
- Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym

Licencja wsparcia technicznego producenta oprogramowania:

Wykonawca dostarczy wraz **dożywotnią licencją systemu NAC** –licencja na wsparcie do 18 czerwca 2026

producenta oprogramowania. Licencja ta powinna obejmować minimum:

- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów do 24 godzin do zgłoszenia problemów krytycznych.

- Dostęp do dokumentacji i instrukcji na stronie internetowej.
- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

Zakres wdrożenia:

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku wirtualizacyjnym klienta.
- Podstawowa konfiguracja NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
- Konfiguracja urządzenia firewall (dodatnie VLAN, ustawienie polityk, etc.).
- Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
- Integracja posiadanych przez Zamawiającego urządzeń sieciowych (switche, AP) z NAC, w ramach funkcjonalności dostępnych na urządzeniach.
- Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na wszystkich urządzeniach końcowych, testy poprawności wdrożenia.
- Uruchomienie uwierzytelniania w oparciu o adres MAC oraz Certyfikaty na NAC, testy.
- Instalacja i konfiguracja serwera certyfikacji CA (Certificate Authority) do współpracy z NAC.
- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń.
- Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6h dziennie

Czas wdrożenia plus testy min 14 dni.
Przygotowanie dokumentacji powykonawczej zawierającej procedury włączenie poszczególnych funkcjonalności oraz odzyskiwania środowiska krok po kroku w jeżyku polskim z określeniem czasów RPO, RTO do 30 dni od zakończenia wdrożenia.
Wsparcie powdrożeniowe do 18 czerwca 2026 w ilości 20 godzin do wykorzystania na potrzeby Zamawiającego.

2.2. System PAM – licencja bezterminowa

Ogólne - architektura

1. System PAM musi być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.
2. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze Hyper-V – środowisko posiadane przez Zamawiającego. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.

Licencjonowanie

1. System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 5 użytkowników, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:
    a. Ochrona kont uprzywilejowanych,
    b. Ochrona kluczy SSH,
    c. Zarządzanie i monitorowanie sesji uprzywilejowanych,
    d. Rejestrowanie sesji uprzywilejowanych
    e. Raportowanie wykorzystania kont uprzywilejowanych,
2. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo.
3. Dostarczone licencje na system PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych.
4. System powinien być dostarczony wraz z serwisem do 18 czerwca 2026 umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta.

Funkcjonalności

1) System PAM musi zapewniać możliwość zarządzania (w szczególności):
   a) Użytkownikami na systemach operacyjnych: Windows, Unix/Linux,
   b) Kontami domenowymi: MS Active Directory,
   c) Kontami lokalnymi: VMware ESX/ESXi,
   d) Kontami na urządzeniach m.in.: Cisco, Aruba, Alcatel, CheckPoint, Fortigate, Huawei, IBM AIX, Brocade,
   e) Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL
   f) Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC,
   g) Kontami aplikacji webowych: Facebook, Google, Twitter, Linkedin, Instagram, Openstack, AWS
   h) Kontami w innych nie wymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
2) System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
3) System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami:
   a) przeglądarka internetowa,
   b) klient RDP,
   c) klient protokołu SSH/Telnet (np. putty).
4) System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs Active Directory, OpenID.
5) System PAM powinien zapewniać możliwość dwuskładnikowego uwierzytelniania.
6) System PAM musi obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.
7) System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych.
8) System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.
9) System PAM musi posiadać log dla wszystkich zdarzeń systemowych.
10) System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera.
11) System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.
12) System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.
13) System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.

14) Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.
15) System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.
16) System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:
    a) umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne),
    b) generować automatycznie hasła kont systemów docelowych w sposób pseudo losowy,
    c) generować unikalne hasła dla konta systemów docelowych,
    d) wymuszać automatyczną zmianę hasła po jego podglądzie
17) System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
18) System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).
19) Audyt poleceń musi umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.
20) System PAM musi umożliwiać nagrywanie sesji wraz z podglądem sesji aktywnej oraz możliwość jej przerwania.
21) Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.
22) System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.
23) System PAM musi umożliwiać odtworzenie zarejestrowanych nagrań sesji.
24) Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski.
25) System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności:
    a) zarządzać kontami uprzywilejowanymi w ramach całej organizacji (około 100 użytkowników),
    b) monitorować wykorzystanie kont uprzywilejowanych,
    c) nagrywać i archiwizować sesje zdalne,
    d) gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług,
26) System PAM musi umożliwiać personalizację wyglądu aplikacji co najmniej po przez umieszczenie logo zamawiającego w głównym oknie aplikacji.

Zakres wdrożenia:

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku wirtualizacyjnym klienta.
- Podstawowa konfiguracja PAN (integracja z domeną, inne wymagane).
- Konfiguracja urządzenia firewall (VLAN-u, ustawienie polityk, etc.).
- Uruchomienie kontroli uwierzytelniania na urządzeniach końcowych, testy.
- Dostęp maszyny do serwerów w Internecie na portach 443 – dostarczenie i konfiguracja certyfikatu SSL na UG, instalacja certyfikatu i konfiguracja UTM.
- Dostęp z urządzenia PAM do urządzeń docelowych na wszystkich wymaganych portach (np. SSH, LDAP,
- HTTPS, HTTP)
- Lista użytkowników i ich uprawnień do systemów w przypadku konfigurowania Access Groups.
- Dostęp do zasobu sieciowego w przypadku konfiguracji backupu.
- Prawidłowo skonfigurowany LDAPS na serwerze AD (dla rotacji haseł LDAP).
- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji.

Czas wdrożenia plus testy min 3 dni.
Przygotowanie dokumentacji powykonawczej zawierającej procedury włączenie poszczególnych funkcjonalności oraz odzyskiwania środowiska krok po kroku w jeżyku polskim z określeniem czasów RPO, RTO do 30 dni od zakończenia wdrożenia.
Wsparcie powdrożeniowe do 18 czerwca 2026 w ilości 20 godzin do wykorzystania na potrzeby Zamawiającego.

2.3. **Oprogramowanie przeciwdziałające wyciekowi danych DLP – 65 sztuk.**

Oprogramowanie na **licencji wieczystej z wsparciem do 18 czerwca 2026**.

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
4. Serwer administracyjny musi wspierać instalację w oparciu o bazę danych.
5. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
    a. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
    b. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:

a. logowanie oraz wylogowanie użytkownika,
b. włączenie oraz wyłączenie stacji roboczej,
c. blokada oraz odblokowanie stacji roboczej,
d. przejście w stan bezczynności stacji roboczej.

19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
20. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
21. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach
22. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
23. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
24. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
25. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
26. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
27. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
28. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
29. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania.
30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.

31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
a) aplikacje, z której zostały utworzone,
b) lokalizację,
c) adres URL,
d) format pliku,
e) zawartość pliku.
33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
a) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
b) blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
c) blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
d) blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
e) blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
f) blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
g) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
- Dropbox,
- Google Drive,
- SharePoint,
- OneDrive Business,
- OneDrive Personal.
- blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
- blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,

- blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
- uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,

35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:

a) numery kart kredytowych,
b) numer PESEL,
c) numer polskiego dowodu osobistego,
d) polski numer paszportu,
e) wyrażenia regularne,

f) określone ciągi znaków,
g) numer IBAN.

46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e- mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy").
50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
52. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania SIEM.
53. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
54. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
a) audyt i logowanie wiadomości e-mail,
b) audyt i logowanie operacji na plikach,
c) wprowadzanie polityk zabezpieczeń do wiadomości e-mail.
55. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
56. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
57. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
a) Bezpieczeństwo danych:
- Przegląd informacji o incydentach bezpieczeństwa.
- Przegląd danych przychodzących.
- Przegląd danych wychodzących.

- Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików. Podłączane/odłączane urządzenia przenośne.

b) Produktywność:

- Przegląd informacji na temat produktywności użytkowników.
- Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
- Trendy.

c) c. Eksploatacja sprzętu:

- Przegląd informacji na temat eksploatacji sprzętu komputerowego.
- Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
- Eksploatacja drukarek.
- Eksploatacji sieci.

58. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
59. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
60. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt:

- plików przenoszonych na nośniki USB i inne urządzenia przenośne,
- plików przesłanych za pomocą wiadomości e-mail,
- plików przesłanych za pomocą poczty webowej,
- plików przesłanych do Internetu,
- plików wysłanych za pomocą komunikatorów,
- plików przesłanych na dyski chmurowe,
- analiza sposobu korzystania z aplikacji,
- analiza korzystania z Internetu,
- analiza wykorzystania porali do poszukiwania pracy.

Wdrożenie oprogramowania przeciwdziałającemu wyciekowi danych.

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym

pod kontrolą systemu Windows Server co najmniej w wersji 2019 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

A. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.

B. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.

C. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.

D. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.

E. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.

F. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

G. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.

H. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.

I. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.

J. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

- Numery kart kredytowych
- Numery IBAN
- Numery dowodów osobistych
- Polski numer paszportu
- Numer PESEL

K. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.

L. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.

M. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.

N. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.

O. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.

P. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.

Q. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

2.4. Oprogramowania EDR oraz antywirusowe z centralna konsolą zarządzania dla 75 końcówek (65 stacji i 10 serwerów) licencja do 18 czerwca 2028 roku

Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.
Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

- Microsoft Windows 10
- Microsoft Windows 11

Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:

- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core
- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Essentials

- Microsoft® Windows Server 2022 Datacenter
- Microsoft® Windows Server 2022 Core

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.

Opis technologii

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware.
3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.

10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.

26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
27. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
30. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
31. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".
32. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
34. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
35. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
36. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.
37. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
38. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
39. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.

40. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
41. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
42. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
44. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
45. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
46. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
47. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
48. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
49. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
50. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
51. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
54. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
55. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.

56. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.

57. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.

58. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.

59. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).

60. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.

61. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.

62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.

63. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.

64. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.

65. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.

66. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.

67. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.

68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.

69. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.

70. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.

71. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.

72. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.

73. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.

74. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.

75. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.

76. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.

77. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.

78. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.

79. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.

80. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.

81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.

82. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker

83. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.

84. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.

85. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.

86. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.

87. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.

88. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)

89. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.

90. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.

91. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.

92. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.

93. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.

94. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.

95. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.

96. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.

97. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.

98. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.

99. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji

100. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.

101. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.

102. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.

103. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN

104. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu

Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania

konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)

105. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.

106. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).

107. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

Centralna administracja

1. Portal zarządzający jest dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.

7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.

22. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
30. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

Zakres wdrożenia:

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku wirtualizacyjnym klienta.
- Podstawowa konfiguracja EDR (integracja z domeną, inne wymagane).
- Uruchomienie kontroli na urządzeniach końcowych (65 stacji i 10 serwerów), testy.
- Konfiguracja konsoli zarzadzania i przygotowanie polityk zgodnie z wytycznymi Zamawiającego.
- Prawidłowo skonfigurowany z serwerem AD.
- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji.

Czas wdrożenia plus testy min 2 dni.
Przygotowanie dokumentacji powykonawczej zawierającej procedury włączenie poszczególnych funkcjonalności EDR do 30 dni od zakończenia wdrożenia.
Wsparcie powdrożeniowe do 18 czerwca 2026 w ilości 20 godzin do wykorzystania na potrzeby Zamawiającego.

Cześć II

2.6 SYSTEM SIEM 1 sztuka – licencja open source

1. Wprowadzenie

Celem zamówienia jest nabycie i wdrożenie systemu SIEM, który zapewni skuteczne zarządzanie bezpieczeństwem informacji oraz monitorowanie zdarzeń bezpieczeństwa w organizacji.

2. Zakres Zamówienia

Zamówienie obejmuje dostawę, instalację, konfigurację i uruchomienie systemu SIEM, a także szkolenie personelu oraz wsparcie techniczne i serwisowe.

3. Wymagania Funkcjonalne

- System musi bazować na rozwiązaniu open source i być całkowicie darmowy
- System musi umożliwiać gromadzenie, korelację zdarzeń przesyłanych lub pobieranych z innych systemów
- Monitorowanie zdarzeń bezpieczeństwa
- Analiza logów i detekcja anomali
- Reakcja na zagrożenia i alertowanie personelu odpowiedzialnego za bezpieczeństwo
- Kompatybilność z istniejącą infrastrukturą IT
- Możliwość łatwego rozszerzenia funkcjonalności w przyszłości

- Zapewnienie zgodności z obowiązującymi regulacjami takimi jak: PCI DSS, HIPAA, NIST 800-53, TSC GDPR
- Skonfigurowanie zbierania logów z różnych źródeł
- Analiza zachowań i detekcja anomalii
- Zdefiniowanie zestawu reguł detekcji zgodnych z branżowymi standardami
- Generowanie alertów na podstawie wykrytych zagrożeń
- Skonfigurowanie reakcji automatycznych na określone zdarzenia
- Integracja z systemami ticketingowymi
- Analiza trendów i podejrzanych wzorców
- Mechanizmy szyfrowania dla komunikacji między komponentami.
- Odpowiednie zabezpieczenia dostępu do systemu.
- Intuicyjny interfejs do konfiguracji i zarządzania systemem.
- Możliwość łatwej aktualizacji i rozbudowy.
- Oprogramowanie SIEM zostanie dostosowane na potrzeby zbierania informacji i informowania o incydentach z systemów oraz urządzeń
- System SIEM będzie wspierać integrację z różnymi systemami i narzędziami, w tym serwerami, firewallami, systemami IDS, systemami NAC, systemami kontroli dostępu, systemami zarządzania tożsamością w tym Active Directory
- SIEM będzie obsługiwać różne protokoły transmisji logów, takie jak Syslog, SNMP, WMI i inne
- SIEM umożliwi zbieranie, normalizację i korelację logów z różnych źródeł w jednolitym formacie
- System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów
- System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK

- System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email.
- Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.
- Wbudowane mechanizmy detekcji zagrożeń pozwalają na szybkie reagowanie na potencjalne ataki.
- integracja się z różnymi źródłami logów, zarówno systemowymi, jak i aplikacyjnymi.
- Zapewnia normalizację logów, co ułatwia analizę i porównywanie informacji pochodzących z różnych źródeł.
- Posiadanie system detekcji włamań (HIDS), który monitoruje aktywność systemu operacyjnego i aplikacji na poziomie hosta
- Wykrywanie podejrzanych aktywności, takich jak próby włamań, ataki brute-force czy nieautoryzowane zmiany w plikach systemowych
- Posiadanie funkcji detekcji na poziomie sieci (NIDS), które monitorują ruch sieciowy i identyfikują potencjalne zagrożenia.
- Analizowanie ruchu w czasie rzeczywistym, a także przeszukiwanie archiwalnych danych.
- centralne zarządzanie konfiguracją i politykami bezpieczeństwa.
- Umożliwia jednolitą konfigurację dla wielu agentów w środowisku.
- Integracja z narzędziami Elastic Stack (Elasticsearch, Logstash, Kibana), co umożliwia zaawansowaną analizę i wizualizację danych bezpieczeństwa.
- funkcje raportowania i wizualizacji, które pozwalają na szybkie zrozumienie stanu bezpieczeństwa w organizacji.
- Możliwość tworzenia niestandardowych raportów i widoków.

- Wbudowany system monitorowania integralności plików (FIM) sprawdza, czy pliki systemowe i konfiguracyjne nie uległy nieautoryzowanym zmianom.
- Możliwość konfiguracji zautomatyzowanych reakcji na wykryte zagrożenia, co przyspiesza proces reagowania na incydenty.
- Obsługa różne protokoły bezpieczeństwa, takie jak Syslog, SNMP, czy JSON, co ułatwia integrację z różnymi systemami.
- moduły i rozszerzenia, które umożliwiają dostosowanie systemu do specyficznych potrzeb organizacji.
- System musi umożliwiać generowanie raportów na żądanie oraz raportów okresowych.
- Raporty powinny być konfigurowalne i dostosowane do potrzeb różnych grup odbiorców (np. zarząd, dział IT, audyt).
- System musi zapewniać bezpieczne przechowywanie zebranych logów i zdarzeń przez określony czas (np. 1 rok).
- Dane powinny być chronione przed nieautoryzowanym dostępem i modyfikacją.

4. Wymagania Niefunkcjonalne

4.1 **Wydajność**

- System musi zapewniać wysoką wydajność i skalowalność, aby obsłużyć dużą ilość danych i zdarzeń.

4.2 **Bezpieczeństwo**

- System musi spełniać wysokie standardy bezpieczeństwa, w tym szyfrowanie danych w tranzycie i w spoczynku.
- System powinien być odporny na ataki typu DDoS oraz inne próby naruszenia jego integralności.

4.3 **Łatwość Użycia**

- Interfejs użytkownika powinien być intuicyjny i łatwy w obsłudze

I. Szczegółowa specyfikacja zamówienia i opisy zadań do realizacji przez Wykonawcę

Zadanie I – Wykonanie Projektu technicznego obejmującego całość wdrożenia w oparciu o analizę istniejącego środowiska Zamawiającego

1) Wykonawca opracuje Projekt techniczny realizacji uzgodnionej koncepcji, uwzględniający najlepsze praktyki i rekomendacje publikowane wdrożenia SIEM. W projekcie technicznym muszą być zawarte:
   - Architektura wdrożenia
   - Usługi i systemy monitorowanie przez SIEM
   - Wykaz logów zbieranych przez SIEM
   - Wykaz wymaganych przez SIEM portów
   - Opcje instalacji agentów SIEM
   - Opcje podłączenia urządzeń sieciowych do SIEM
   - szczegółowy harmonogram realizacji prac migracyjnych, uwzględniający specyfikę organizacji Zamawiającego

   Projekt musi zostać przedstawiony do analizy Zamawiającemu który decyduje o jego akceptacji lub zwraca do uzupełnienia z pisemnym wskazaniem obszarów do uzupełnienia. Zamawiający ma 7 dni pracujących na zaakceptowanie projektu lub przesłanie do poprawy – uzupełnienia. Wykonawca ma 5 dni pracujących na uzupełnienie projektu zwróconego do poprawy. Po uzupełnienia Wykonawca ponownie przedstawia projekt do akceptacji przez Zamawiającego. W przypadku przedstawienia dwukrotnie nieuzupełnionego odpowiednio projektu – brak uzyskania akceptacji Zamawiającego – Zamawiający ma możliwość wypowiedzenia umowy z winy Wykonawcy w terminie 7 dni po przedstawieniu pisemnego uzasadnienia Wykonawcy.

Zadanie II – Wdrożenie i dostosowanie SIEM oraz wykonanie dokumentacji powykonawczej.

W ramach Zadania II, Wykonawca:

2) wykona instalację i konfigurację rozwiązania SIEM w tym:

- Instalacja SIEM
- Konfigurację portów wymaganych przez SIEM
- Instalację agenta SIEM na systemach Windows
- Instalację agenta SIEM na Hyper-V
- Instalację agenta SIEM na systemach Linux
- Utworzy reguły dla poszczególnych grup agentów
- Podłączy urządzenia sieciowe do SIEM
- Dostosuje reguły zbierania logów z urządzeń
- Dostosuje reguły zbierania logów z systemów Windows
- Dostosuje reguły zbierania logów z systemów Linux
- Utworzy reguły normalizacji logów, jeśli będzie taka potrzeba
- Skonfiguruje moduł integralności plików oraz rejestru na systemach Windows monitorowanych przez SIEM
- Utworzy reguły wykrywania ataków
- Utworzy reguły wykrywania ataków Pass-the-Hash
- Utworzy reguły wykrywania ataków Pass-the-ticket
- Utworzy reguły wykrywania ataków DCSync

- Utworzy reguły wykrywania ataków Golden Ticket
- Utworzy reguły wykrywania ataków Kerberoasting
- Utworzy reguły wykrywania ataków na poświadczenia Windows
- Utworzy reguły wykrywania ataków na bazę haseł z Ntds.dit
- Utworzy reguły wykrywania połączeń PsExec w systemach Windows
- Utworzy reguły wykrywania ataków Ransomware
- Skonfiguruje listy IP allow i IP block dla SIEM
- Skonfiguruje moduł blokujący połączenia do hostów monitorowanych przez SIEM
- Uruchomi moduł wykrywający podatności CVE na systemach monitorowanych przez SIEM
- Skonfiguruje moduł wykrywający poziom bezpieczeństwa na systemach monitorowanych przez SIEM
- Utworzy raporty wskazane przez zamawiającego
- Skonfiguruje backup rozwiązania SIEM oraz procedury Disaster Recovery

5. **Wsparcie i Serwis**

- Dostawca powinien zapewniać wsparcie techniczne oraz serwis systemu do 18 czerwca 2026 roku w ilości 40 godzin.
- Wsparcie powinno obejmować dostęp do aktualizacji oprogramowania oraz pomoc w rozwiązywaniu problemów i dostosowywaniu systemu
- Wsparcie będzie świadczone przez architekta posiadającego referencje z uczestnictwa w projektach opisanych w pkt 7.

- Warunkiem koniecznym jest, aby architekt świadczący usługę wsparcie uczestniczył w procesie wdrożenia całości usług SIEM, wraz z integracją Active Directory u zamawiającego (posiadał niezbędną wiedzę w infrastrukturze zamawiającego).

6. **Dokumentacja**

- System musi być dostarczony z pełną dokumentacją użytkownika, administracyjną oraz techniczną.
- Dokumentacja powinna być dostępna w języku polskim.

7. **Wymagania względem członków zespołu wdrożeniowego.**

Wykonawca oddeleguje do przeprowadzenia usług wdrożeniowych oraz wsparcia technicznego zespół w składzie co najmniej:

a) architekt rozwiązań Security/Architekt ds. bezpieczeństwa:
   - przynajmniej 5 lat doświadczenia na stanowisku architekta systemów IT oraz bezpieczeństwa IT;
   - udział w ciągu 3 lat ostatnich lat w minimum 4 projektach IT wykorzystujących Windows oraz Active Directory i SIEM
   - udział w ciągu 3 lat ostatnich lat w minimum 4 projektach IT wykorzystujących integrację SIEM z Microsoft LAPS
   - posiada certyfikat Cybersecurity Architect Expert
   - ukończył szkolenie Mastering SIEM min. z zakresy integracji SIEM z Active Directory w wykrywaniu ataków: pass-the-hash, pass-the-ticket, golden ticket, kerberoasting
   - ukończył szkolenie Bezpieczeństwo Windows i informatyka śledcza
   - posiada kompetencje trenerskie poparte referencjami z minimum 4 przeprowadzonych szkoleń Mastering SIEM niezbędne do przeprowadzenia szkolenia po wdrożeniu

- ukończył autoryzowane szkolenie Microsoft 40366 Networking Fundamentals
- ukończył autoryzowane szkolenie Microsoft 40367 Security Fundamentals

8. Wymagania Dotyczące Szkolenia

- Dostawca musi przeprowadzić szkolenie dla personelu administracyjnego i technicznego organizacji.
- Szkolenie powinno obejmować zarówno aspekty teoretyczne, jak i praktyczne związane z obsługą i zarządzaniem systemem SIEM.
- Szkolenie ma obejmować integrację SIEM z Active Directory w wykrywaniu ataków: pass-the-hash, pass-the-ticket, golden ticket, kerberoasting
- integracji SIEM z Active Directory i LAPS
- Czas trwania szkolenia 3 dni robocze po 8 godzin lekcyjnych – zdalne.

2.7Skaner podatności dla minimum 110 urządzeń

Przedmiotem zamówienia jest wdrożenie skanera podatności w infrastrukturze informatycznej Zamawiającego. Celem wdrożenia jest zwiększenie bezpieczeństwa systemów informatycznych poprzez identyfikację i zarządzanie podatnościami.

Zakres Przedmiotu Zamówienia

1. **Dostarczenie oprogramowania:**
   - Oprogramowanie ma być dostarczone w darmowej wersji **Open Source**
   - Zapewnienie, że dostarczona wersja jest najnowsza i stabilna
2. **Instalacja i konfiguracja:**
   - Instalacja oprogramowania na wskazanym przez Zamawiającego serwerze
   - Konfiguracja skanera zgodnie z wymaganiami bezpieczeństwa Zamawiającego
   - Integracja z istniejącą infrastrukturą sieciową i systemami zarządzania IT w tym Active Directory oraz SIEM
3. **Testowanie i walidacja:**
   - Przeprowadzenie testowych skanów bezpieczeństwa
   - Walidacja wyników skanów oraz dostosowanie konfiguracji w razie konieczności

- Sporządzenie raportu z wynikami testów oraz ewentualnymi rekomendacjami

4. **Szkolenie personelu oraz dokumentacja**
   - Przeprowadzenie zaawansowanego szkolenia dla administratorów IT
   - Opracowanie szczegółowej dokumentacji rozwiązania
   - Opracowanie procedur administracyjnych i operatorskich obejmujących obsługę i konfigurację
5. **Wsparcie techniczne:**
   - Zapewnienie wsparcia technicznego do 18 czerwca 2026 od zakończenia wdrożenia w ilości 50 godzin zegarowych rozliczanych do minuty.

Wymagania Techniczne

1. **Serwer:**
   - System operacyjny: Linux (preferowany Debian, Ubuntu lub CentOS) w aktualnej wersji.
   - Minimalne wymagania sprzętowe: 8 GB RAM, 100 GB wolnego miejsca na dysku, procesor z 4 rdzeniami
2. **Sieć:**
   - Dostępność sieciowa serwera do skanowania różnych segmentów sieci.
   - Konfiguracja firewalli i routerów umożliwiająca swobodny przepływ danych niezbędnych do skanowania – wykonawca musi odpowiednio skonfigurować infrastrukturę Zamawiającego w celu przeprowadzenia testów podatności – infrastruktura oparta na UTM FortiGate.
3. **Bezpieczeństwo:**
   - Zastosowanie odpowiednich polityk bezpieczeństwa na serwerze skanera
   - Regularne aktualizacje oprogramowania i baz podatności

4. Wymagania Funkcjonalne

1. **Skalowalność:**
   - Możliwość skanowania małych, średnich i dużych sieci
   - Obsługa wielu jednoczesnych skanów
2. **Baza danych podatności:**
   - Regularne aktualizacje bazy danych podatności
   - Możliwość dodawania własnych definicji podatności
3. **Raportowanie:**

- Generowanie szczegółowych raportów z wynikami skanów
- Wykaz zidentyfikowanych podatności wraz z odpowiadającym im kodem CVE (Common Vulnerability Enumaration) oraz odnośnikiem do opisu luki. Podatności muszą być pogrupowane według ryzyka zgodnie ze standardem CVSS (Common Vulnerability Scoring System),
- Możliwość eksportu raportów

4. **Interfejs użytkownika:**
   - Przyjazny dla użytkownika interfejs webowy.
   - Możliwość zarządzania skanami, harmonogramami i wynikami przez przeglądarkę internetową.
5. **Integracja:**
   - Integracja z SIEM np. WAZUH
   - Obsługa API umożliwiającego automatyzację zadań skanowania i raportowania.
6. **Alertowanie:**
   - Konfiguracji powiadomień e-mailowych o wynikach skanów i wykrytych podatnościach zgodnie z zaleceniami Zmawiającego.
7. **Zarządzanie użytkownikami:**
   - Obsługa wielu użytkowników z różnymi poziomami uprawnień.
   - Logowanie i monitorowanie aktywności użytkowników.
8. **Harmonogramowanie:**
   - Przygotowanie planów - regularnych skanów.
   - Opcja skanowania na żądanie oraz według ustalonego harmonogramu.
9. **Dokładność i wydajność skanowania:**
   - Wysoka dokładność wykrywania podatności.
   - Minimalny wpływ na wydajność skanowanych systemów.

5. Szczegółowa specyfikacja zamówienia i opisy zadań do realizacji przez Wykonawcę

Zadanie I – Wykonanie Projektu technicznego obejmującego całość wdrożenia w oparciu o analizę istniejącego środowiska Zamawiającego

1) Wykonawca opracuje Projekt techniczny realizacji uzgodnionej koncepcji, uwzględniający najlepsze praktyki i rekomendacje publikowane wdrożenia. W projekcie technicznym muszą być zawarte:

- Architektura wdrożenia
- Konfiguracja skanów

- Integracja z infrastruktura
- Integracja z SIEM np. WAZUH
- Disaster recovery
- szczegółowy harmonogram realizacji prac migracyjnych, uwzględniający specyfikę organizacji Zamawiającego

Projekt musi zostać przedstawiony do analizy Zamawiającemu który decyduje o jego akceptacji lub zwraca do uzupełnienia z pisemnym wskazaniem obszarów do uzupełnienia. Zamawiający ma 7 dni pracujących na zaakceptowanie projektu lub przesłanie do poprawy – uzupełnienia. Wykonawca ma 5 dni pracujących na uzupełnienie projektu zwróconego do poprawy. Po uzupełnienia Wykonawca ponownie przedstawia projekt do akceptacji przez Zamawiającego. W przypadku przedstawienia dwukrotnie nieuzupełnionego odpowiednio projektu – brak uzyskania akceptacji Zamawiającego – Zamawiający ma możliwość wypowiedzenia umowy z winy Wykonawcy w terminie 7 dni po przedstawieniu pisemnego uzasadnienia Wykonawcy.

Zadanie II – Wdrożenie i dostosowanie skanera oraz wykonanie dokumentacji powykonawczej.

W ramach Zadania II, Wykonawca:

2) wykona instalację i konfigurację rozwiązania w tym:
   - Instalacja skaner
   - Konfigurację portów wymaganych przez skaner
   - Utworzy zadań skanów
   - Utworzy zadań skanów z uwierzytelnieniem
   - Utworzy role użytkowników
   - Wykona skany podatności w infrastrukturze
   - Utworzy raporty wskazane przez zamawiającego
   - Skonfiguruje backup rozwiązania oraz procedury Disaster Recovery
   - Sporządzi szczegółową dokumentację rozwiązania
   - Utworzy procedury administratorskie i operatorskie

Termin realizacji:

- Wdrożenie powinno zostać zakończone w ciągu 60 dni od dnia podpisania umowy.

Wymogi dokumentacyjne:

- Dokumentacja techniczna obejmująca szczegółowy opis konfiguracji oraz procesów skanowania.
- Raport z przeprowadzonych testów i skanów bezpieczeństwa.
- Instrukcje obsługi oraz materiały szkoleniowe.

Gwarancje i serwis:

- Gwarancja poprawności działania skanera 48 miesięcy od zakończenia wdrożenia.
- Wsparcie wykonawcy do 18 czerwca 2026 roku. Reakcja na zgłoszenia serwisowe w okresie wsparcia w czasie nie dłuższym niż 24 godziny – maksymalna liczba godzin wsparcia do 18 czerwca 2026 roku wynosi 40 godzin zegarowych rozliczanych do 15 minut.

Doświadczenie i kompetencje zespołu wdrażającego:

Wykonawca oddeleguje do przeprowadzenia usług wdrożeniowych oraz wsparcia technicznego zespół w składzie co najmniej:

- architekt rozwiązań Security/Architekt ds. bezpieczeństwa:
  - przynajmniej 5 lat doświadczenia na stanowisku architekta systemów IT oraz bezpieczeństwa IT;
  - udział w ciągu 3 lat ostatnich lat w minimum 4 projektach IT wykorzystujących Windows oraz Active Directory i SIEM
  - udział w ciągu 3 lat ostatnich lat w minimum 4 projektach IT wykorzystujących integrację SIEM z Microsoft LAPS
  - posiada certyfikat Cybersecurity Architect Expert
  - ukończył szkolenie Mastering SIEM min. z zakresy integracji SIEM z Active Directory w wykrywaniu ataków: pass-the-hash, pass-the-ticket, golden ticket, kerberoasting
  - ukończył szkolenie Bezpieczeństwo Windows i informatyka śledcza
  - posiada kompetencje trenerskie poparte referencjami z minimum 4 przeprowadzonych szkoleń Mastering SIEM niezbędne do przeprowadzenia szkolenia po wdrożeniu

- ukończył autoryzowane szkolenie Microsoft 40366 Networking Fundamentals
- ukończył autoryzowane szkolenie Microsoft 40367 Security Fundamentals

3. Termin realizacji zamówienia:

3.6 Realizacja każdego zadania wynosi 45 dni kalendarzowych.

4. Okres gwarancji: określone dokładnie przy danej pozycji
5. Warunki płatności:

Zamawiający przewiduje płatności po wykonaniu każdej zadania w ramach realizacji zamówienia zgodnie z zaoferowaną stawką.

Płatność przelewem 30 dni od dnia otrzymania prawidłowo wystawionych faktury VAT wraz z protokołem odbioru konkretnego zadania – protokół potwierdzony przez przedstawiciela Zamawiającego.

6. Inne istotne warunki zamówienia:

Wymagania dla wdrożenia zostały opisane pod danym zadaniem.

7. Kryterium oceny ofert: cena 100%.
8. Zamawiający informuje, że:

1.1. W toku badania i oceny ofert może żądać od Wykonawcy pisemnych wyjaśnień dotyczących treści złożonej oferty lub innych składanych dokumentów lub oświadczeń. Wykonawca będzie zobowiązanych do przestawienia wyjaśnień w terminie określonym przez Zamawiającego pod rygorem odrzucenia oferty.

9. Sposób przygotowania oferty:

9.6 Ofertę należy sporządzić w języku polskim, na formularzu określonym w załączniku nr 1 do niniejszego szacowania zapytania ofertowego i złożyć za pośrednictwem bazy konkurencyjności.

9.7 formularz oferty oraz załączniki muszą być podpisane elektronicznie przez osobę upoważnioną do reprezentowania Wykonawcy.

10. Ofertę należy złożyć w terminie do dnia 21 września 2024 r. do godz. 12:00.

Stanisław Józef Legierski

Elektronicznie podpisany przez Stanisław Józef Legierski
Data: 2024.09.16 15:12:22 +02'00'