FNR.271.1.14.2024 Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

zwana dalej **(OPZ)**

Cyberbezpieczny samorząd

1. Wspólny Słownik Zamówień:

Główny kod CPV – 48820000- 2 Serwery

72800000-8 Usługi audytu komputerowego i testowania komputerów

72810000-1 Usługi audytu komputerowego

80000000-4 Usługi edukacyjne i szkoleniowe

80533000-9 Usługi zapoznawania użytkownika z obsługą komputera i usługi szkoleniowe

80533100-0 Usługi szkolenia komputerowego

80550000-4 Usługi szkolenia w dziedzinie bezpieczeństwa

80532000-2 Usługi szkolenia w dziedzinie zarządzania

48821000-9 Serwery sieciowe

79417000-0 Usługi doradcze w zakresie bezpieczeństwa

48000000-8 Pakiety oprogramowania i systemy informatyczne

35100000-5 Urządzenia awaryjne i zabezpieczające

32420000-3 Urządzenia sieciowe

30200000-1 Urządzenia komputerowe

31122000-7 Jednostki prądotwórcze

32422000-7 Elementy składowe sieci

30230000-0 Sprzęt związany z komputerami

72263000-6 Usługi wdrażania oprogramowania

72541000-9 Usługi rozbudowy sprzętu komputerowego

2. Przedmiotem zamówienia jest: Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w odniesieniu do normy PN-EN ISO/IEC 27001, usługi z zakresu badania świadomości użytkowników, szkolenia z cyberbezpieczeństwa oraz weryfikacja nabytej wiedzy dla pracowników Zamawiającego oraz dostawa i wdrożenie narzędzia do prowadzenia procesu analizy ryzyka.

W ramach prac Wykonawca zobowiązany jest do:

1. Wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w odniesieniu do normy PN-EN ISO/IEC 27001:

A. Przeprowadzenia inwentaryzacji aktywów oraz określenia wymagań realizacji audytu wstępnego. Wraz z identyfikacją aktywów oraz inwentaryzacją zasobów zostanie opracowana klasyfikacja wagi aktywów w odniesieniu do standardu bezpieczeństwa informacji.

B. Przeprowadzenia audytu wstępnego, w którym przeprowadzi szczegółową analizę wdrożonej dokumentacji, procesów, polityk i procedur w organizacji. Analizie oprócz aspektów organizacyjnych należy poddać również systemy wchodzące w skład infrastruktury informatycznej w celu odniesienia wdrożonego standardu do możliwości technicznych. Wykonawca zidentyfikuje obszary wymagające usprawnienia oraz zaproponuje zmiany mające na celu poprawę standardu zarządzania bezpieczeństwem informacji w przedsiębiorstwie.

C. Przygotowania polityk bezpieczeństwa informacji i procedur operacyjnych zgodnych ze zdefiniowanymi celami, zakresami i działalnością organizacji. Wykonawca przeprowadzi analizę posiadanej dokumentacji pod kątem zgodności z wytycznymi.

Usługa będzie realizowana we współpracy z Zamawiającym. Wykonawca na każdym etapie realizacji usługi będzie w stałym kontakcie z zespołem wdrożeniowym po stronie Zamawiającego.

W ramach dokumentacji zostaną opracowanie i uwzględnione poniższe obszary:

a. Kroki podjęte w celu zapewnienia bezpieczeństwa informacji, a w tym:

- Cele bezpieczeństwa informacji, sposoby ich realizacji i odpowiedzialność za nie,
- Polityka Bezpieczeństwa informacji opracowana w oparciu o właściwe standardy i dobre praktyki,
- Zdefiniowana procedura przeglądu PBI,

b. Zasady, procedury i procesy zarządzania, monitorowania wymogów w zakresie regulacyjnym, prawnym, ryzyka, ochrony środowiska i operacyjnym w organizacji, szacowanie i zarządzanie ryzykiem, tolerancja ryzyk operacyjnych oraz we współpracy zewnętrznej:

- Identyfikacja kluczowych aktywów informacyjnych Jednostki (tj. zbiory danych/systemy/usługi), rejestr ryzyk oraz procedury zarządzania ryzykiem

- Identyfikacja podatności w środowisku Zamawiającego, szacowanie ryzyka związanego z zagrożeniami bezpieczeństwa informacji, identyfikacja zagrożeń zewnętrznych i wewnętrznych,
- Klasyfikacja zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutki,
- Procedury oceny dostawców i partnerów zewnętrznych w celu zwiększenia bezpieczeństwa łańcucha dostaw

D. Przeprowadzenia kompleksowej analizy ryzyk i bezpieczeństwa systemów informatycznych w oparciu o gotowe, dedykowane do tego celu narzędzie informatyczne spełniające poniższe wymagania:

a. Narzędzie umożliwi prowadzenie, aktualizację oraz eksport wyników analizy ryzyka,

b. Pełny interfejs aplikacji w języku polskim,

c. Narzędzie może być obsługiwane z poziomu przeglądarki internetowej,

d. Komunikacja będzie odbywać się z wykorzystaniem bezpiecznego, szyfrowanego połączenia SSL,

e. Architektura aplikacji nie będzie wymagać od Zamawiającego zapewnienia dodatkowych zasobów sprzętowych oraz wydajnościowych,

f. Aplikacja będzie zapewniała minimum poniższe funkcjonalności:

- możliwość definicji różnych poziomów dostępu do danych,
- powiadomienia uczestników analizy ryzyka o zbliżających się terminach i przypisanych do nich zadaniach,
- powiadomienia w postaci wiadomości e-mail i systemowych,
- gotowe słowniki czynności przetwarzania informacji dostosowane do organizacji,
- możliwość kategoryzacji ryzyk,
- możliwość realizacji procesu analizy ryzyka dla całości organizacji oraz dla wybranych jednostek organizacyjnych w wybranych obszarach czynności przetwarzania ryzyka
- możliwość automatycznego tworzenia podprocesów dla wybranych czynności przetwarzania analizy ryzyka dla każdej jednostki organizacyjnej,
- możliwość generowania raportów z analizy wraz z informacjami nt. postępowania z ryzykiem,
- możliwość zapisu wyników analizy ryzyka do pliku pdf i word
- moduł prowadzenia procesu zarządzania ryzykiem wraz z definicją i przydzieleniem zadań naprawczych do wybranych użytkowników systemu,

możliwość weryfikacji postępów prac naprawczych oraz definicji ich skuteczności,

- możliwość integracji z usługami katalogowymi Active Directory

2. Narzędzie informatyczne do prowadzenia procesu analizy ryzyka: W ramach dostarczonej licencji Zamawiający będzie posiadał dostęp do pełnej funkcjonalności oprogramowania w okresie minimum 12 miesięcy od zakończenia usługi wdrożenia SZBI.

Oprogramowanie zostanie udostępnione Zamawiającemu przez Wykonawcę w modelu usługowym (z ang. w modelu SaaS, Software as a Service).

Oprogramowanie oraz przetwarzane w nim dane będą udostępnione w bezpiecznym środowisku dedykowanym do świadczenia usług w modelu SaaS z zastosowanymi minimalnymi zabezpieczeniami:

- Wysoka dostępność zasobów zapewniona poprzez zastosowanie architektury wysokiej dostępności (HA) oraz zwielokrotnione łącze dostępowe do sieci Internet dostarczone przez minimum 3 operatorów przy użyciu minimum dwóch niezależnych ścieżek,

- Ośrodek danych powinien posiadać certyfikację ISO/IEC 27018 (ochrona danych osobowych w chmurze) oraz ISO/IEC 27017 (bezpieczeństwo przetwarzania w modelu chmurowym,

- Wykonawca musi być właścicielem ośrodka danych

3. Usługi z zakresu badania świadomości użytkowników, szkolenia z cyberbezpieczeństwa oraz weryfikacja nabytej wiedzy dla pracowników Zamawiającego:

Wykonawca wykona usługi z zakresu badania świadomości użytkowników, szkolenia z cyberbezpieczeństwa oraz weryfikacja nabytej wiedzy dla pracowników Zamawiającego w zakresie:

1. Zamawiający wymaga opracowania kampanii socjotechnicznej w formie symulowanego ataku:

a. Zamawiający dostarczy listę mailingową pracowników objętych badaniem.

b. Wykonawca powinien przeprowadzić proces badania świadomości użytkowników przy użyciu spreparowanej wiadomości email symulującej prawdziwy atak phishingowy.

c. Wiadomość email powinna nakłaniać pracowników do kliknięcia w link, który będzie prowadził do pustej strony WWW.

d. Wykonawca powinien prowadzić ewidencję uwzględniającą liczbę kliknięć oraz pozwalać na identyfikację użytkownika bądź urządzenia z którego link został użyty.

e. Ewidencja i wyniki badania powinny zostać dostarczone w formie raportu maksymalnie 2 tygodnie po zakończeniu procesu.

f. Kampanie powinny zostać przeprowadzone przed szkoleniem opisanym w punkcie 2.

2. Zamawiający wymaga realizacji szkoleń z cyberbezpieczeństwa dla pracowników.

a. Sesja szkoleniowa powinna trwać maksymalnie 150 minut i powinna uwzględniać minimum jedną 15 minutową przerwę.

b. Szkolenie odbędzie się w formie stacjonarnej w ośrodku szkoleniowym posiadającym zaplecze w formie sali konferencyjnej umożliwiającej przeprowadzenie sesji szkoleniowej dla 26 osób.

c. Ewentualne koszty ośrodka szkoleniowego, wyżywienia, zakwaterowania pracowników w trakcie szkolenia oraz inne koszty logistyczne związane z szkoleniem pokryje Wykonawca.

d. Grupą docelową szkoleń będą pracownicy Zamawiającego korzystający z technologii informatycznych.

e. Zakres tematyczny szkolenia powinien obejmować minimum poniższe zagadnienia:

- Wprowadzenie do cyberbezpieczeństwa
- Typy zagrożeń i najczęstsze sposoby ataków
- Rola użytkownika w bezpieczeństwie
- Podpis cyfrowy
- Uwierzytelnianie i autoryzacja
- Poczta elektroniczna
- Bezpieczeństwo w Internecie
- Bezpieczeństwo sieci bezprzewodowej
- Bezpieczeństwo urządzeń mobilnych
- Bezpieczeństwo w mediach społecznościowych
- Postępowanie w przypadku naruszenia bezpieczeństwa
- Zastosowanie wdrożonych rozwiązań w zakresie zarządzania bezpieczeństwem informacji.
- Analiza przypadków zgłoszonych przez użytkowników

f. Wykonawca udostępni materiały szkoleniowe bezpośrednio przed sesją szkoleniową.

g. Szkolenie powinno przyjąć formę wykładu stacjonarnego wraz z prezentacją.

h. W ramach sesji szkoleniowej uczestnicy mają możliwość prowadzenia dyskusji z trenerem oraz zadawania pytań.

i. Wymaga się pokazu „na żywo” działającego systemu ochrony firewall z omówieniem logów oraz pokazem przykładowych reguł ochrony.

j. Jedna grupa szkoleniowa nie powinna przekraczać 26 osób.

k. Całkowita liczba pracowników objętych szkoleniem: 26 osób.

l. Zamawiający wymaga opracowania harmonogramu szkoleń umożliwiającego udział w sesji szkoleniowej każdemu pracownikowi.

m. Treści szkoleniowe powinny być odpowiednio dostosowane do stanowiska osób w nich uczestniczących, z uwzględnieniem trzech grup i rodzaju szkoleń:

- Szkolenie specjalistyczne dla pracowników IT i kadry kierowniczej – ilość osób: 5.
- Szkolenie ogólne z zakresu cyberbezpieczeństwo dla pracowników – ilość osób: 26.
- Szkolenie specjalistyczne dla pracowników odpowiedzialnych za politykę bezpieczeństwa informacji – ilość osób: 3.

n. Sesje powinny być zrealizowane w ciągu nie więcej niż 2 dni kalendarzowych, zgodnie z harmonogramem szkoleń ustalonym przez Strony,

o. Po zakończeniu szkoleń przeprowadzona zostanie dodatkowa weryfikacja wiedzy pracowników w formie testu wiedzy dostępnego online.

p. Wyniki testu wiedzy powinny zostać dostarczone w formie raportu maksymalnie 2 tygodnie po zakończeniu procesu.

3. Opis przedmiotu zamówienia z podziałem na zadania:

1. ZADANIE:

1.1. Zakup i dostarczenie zasilaczy UPS do komputerów stacjonarnych,
1.2. Zakup i dostarczenie zasilaczy do serwera i urządzenia sieciowego,
1.3. Zakup i wdrożenie oprogramowania antywirusowego,
1.4. Zakup i wdrożenie systemu wykrywania złośliwego oprogramowania,
1.5. Zakup i dostarczenie agregatu prądotwórczego 10000 W,
– w terminie do 27.12.2024

2. ZADANIE:

2.1. Zakup i wzdrożenie systemu do zarządzania kopią bezpieczeństwa,
2.2. Szkolenia specjalistyczne dla pracowników IT kadry kierowniczej,
2.3. Szkolenia ogólne z zakresu cyberbezpieczeństwa dla pracowników,
2.4. Szkolenia ogólne z zakresu cyberbezpieczeństwa dla pracowników odpowiedzialnych za politykę bezpieczeństwa informacji,

2.5. Opracowanie, aktualizacja i wdrożenie Systemu Zarządzania Bezpieczeństwem informacji
– w terminie do 6 miesięcy od podpisania umowy.

4. Opis wymagań sprzętu:

4.1. Serwer + szyny rack

Typ urządzenia	Serwer NAS
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 3,35 GHz (z przyspieszeniem do 3.6 GHz)
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 8 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 24 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń Infiniband
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 gniazdo rozszerzenia
Porty sieciowe	Minimum: • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) • 1 port 10GbE RJ45 • Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 4-liniowe gniazdo x8 Gen. 3
Wentylator obudowy	Min. 3 wentylatory 60 mm x 60 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: o 200 TB (wymagana pamięć 32 GB) o 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN

Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2 048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 2 000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać

	udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Konserwacja	• Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack
Gwarancja	Wykonawca udzieli gwarancji: • 3 lata na urządzenie główne • 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack

4.2. **System EDR**

System EDR zarządzany 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.

Ten sam agent zainstalowany na systemach Windows powinien umożliwić rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Rozwiązanie powinno posiadać możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:

- Microsoft Windows 10
- Microsoft Windows 11
- macOS version 14 "Sonoma"
- macOS version 13 "Ventura"
- macOS version 12 "Monterey"

Rozwiązanie powinno posiadać możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:

- 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:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Rozwiązanie powinno posiadać polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.

4.3. **Ochrona antywirusowa**

Wymagana jest 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 powinno wspierać następujące systemy operacyjne:

- Microsoft Windows 10

- Microsoft Windows 11
- macOS version 14 "Sonoma"
- macOS version 13 "Ventura"
- macOS version 12 "Monterey"

Rozwiązanie dla ochrony antywirusowej systemów serwerowych powinno wspierać 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 powinno posiadać Polski interfejs użytkownika.

Ten sam agent zainstalowany na systemach Windows powinien umożliwić rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Chronione platformy powinny być zarządzane z tej samej konsoli zarządzającej

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

4.4. **Agregat prądotwórczy 10000W.**

Instalacja agregatu wraz z pierwszym uruchomieniem.
Wymagane minimalne parametry agregatu:
Silnik wysokoprężny 1100FA
Moc znamionowa 9KW/11,25
Moc maksymalna 10 KW / 12,5 kVA
Napięcie 220-480V
Częstotliwość 50 Hz / 60 Hz
Szybkość 3000/3600 obr./min
Rodzaj chłodzenia: powietrze
Kontroler Cyfrowy
Rozruch: elektryczny
+ zgodny system ATS

4.5. **Zasilacze UPS do komputerów stacjonarnych**

Wymagane minimalne parametry UPS serwer/urządzenie sieciowe:

Moc pozorna 1000VA
Moc czynna 1000W
Pojemność akumulatora: 9 Ah
Czas podtrzymania (obciążenie 100%) 5 min
Czas ładowania 6 h
Typ obudowy: Rack

Dla komputerów:
Moc pozorna 900 VA
Moc czynna 480 W
Czas ładowania 8 h
Typ obudowy: Tower

Zatwierdzono w dniu:

28.11.2024

Przemysław Krzyczmanik

Elektronicznie podpisany przez Przemysław Krzyczmanik
Data: 2024.11.28 14:12:01 +01'00'