Zmiana 1 z dnia 06.06.2024 r.

Zapytania z dnia 05.06.2024 r.

Zmienia się treść zapytania opublikowanego w dniu 05.06.2024 r. w ten sposób, że dotychczasową treść zamienia się na zmienioną treść jednolitą , bez wydłużenia terminu składania ofert, aby nie spowodować przypadkowego potraktowania przez Wykonawców wcześniejszej wersji jako obowiązującej, usuwa się treść opublikowaną dnia 05.06.2024 r., która traci ważność. Wykonawcy są zobowiązani do śledzenia strony zapytania , tak aby w swej ofercie uwzględnić aktualne wymagania zamówienia. Zmienia się stronę publikacji na PORTAL KONKURENCYJNOŚCI (BAZA KONKURENCYJNOŚCI) https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/

Uczestnicy postępowania są zobowiązani do zapoznania się z zasadami korespondencji i składania ofert w ramach tej bazy zamówień.

Podane w bazie konkurencyjności daty zawierania umów i końcowa realizacji dla zadanie 1 - są orientacyjne i będą zależeć od postępów w przebiegu wyłaniania wykonawcy, dla zadania 1 przewiduje się okres realizacji do 30 dni od podpisania umowy.

Zakres objęty niniejszym postępowaniem jest dofinansowany ze środków Unii Europejskiej w ramach projektu Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0719/FERC.02.02-CS.01-001/23/2024, realizowanego zgodnie z zasadami programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) , Priorytet II, działanie 2.2, konkurs grantowy „Cyberbezpieczny Samorząd” , FERC.02.02-CS.01-001/23.

Sokołów Małopolski, 6 czerwca 2024 r.

OA.136.14.2024

ZAPYTANIE OFERTOWE

Zmiana 1 Zapytania z dnia 06.06.2024 r. - wersja jednolita

Nazwa zamówienia:

Podniesienie funkcjonalności systemu antywirusowego

1. Zamawiający
   Gmina Sokołów Małopolski, ul. Rynek 1, 36 – 050 Sokołów Małopolski.

2. Przedmiot zamówienia:

Przedmiotem zamówienia jest realizacją następujących zadań:

1) Wymiana warstwy sprzętowej i programowej - Podniesienie funkcjonalności systemu antywirusowego z możliwością wykrywania zagrożeń i reagowania na nie – XDR

2) Szkolenia z zarządzania systemem antywirusowym wykorzystującym XDR oraz zdalną administrację

Szczegółowy opis przedmiotu zamówienia zawarty jest w załączniku nr 1 do zapytania (SWZ). Dopuszcza się rozwiązania równoważne opisanym w SWZ.
Wzór umowy stanowi załącznik nr 2.

Wykonawca, z którym podpisze się umowę - będzie realizował wszystkie zadania. Nie dopuszcza się składania ofert częściowych. Dopuszcza się podwykonawstwo w zakresie w/w zadań.

3. Termin realizacji zamówienia:
   1) System antywirusowy wraz z dokumentacją i licencjami do 30 dni od podpisania umowy, tj. orientacyjnie do dnia 19 lipca 2024
   2) Szkolenia realizowane do 30 grudnia 2024 roku

4. Kryteria oceny ofert: **najniższa cena**

   Zamawiający zastrzega sobie prawo do weryfikacji wiarygodności oferty i odrzucenia ofert , które nie rokują realnej możliwości ich realizacji (np. rażąco niska cena).

5. Miejsce i termin złożenia ofert.

   Oferty należy przesyłać wyłącznie za pośrednictwem Portalu Konkurencyjności **do 18 czerwca 2024 r. do godz. 12.00 Oferty, które wpłyną po oznaczonym terminie nie będą brane pod uwagę.**

   Uwaga: Składanie ofert, komunikacja i wymiana korespondencji tylko za pomocą Portalu Konkurencyjności, który jest jednocześnie stroną prowadzenia postępowania. Jako załącznik 3 udostępnia się wytyczne dotyczące komunikacji za pomocą Portalu Konkurencyjności.
   Z uwagi na powyższe możliwe jest składanie ofert i dokumentów wyłącznie w postaci cyfrowej z ważnym podpisem o postaci elektronicznej.

6. Termin otwarcia ofert:

Oferty zostaną otwarte w dniu 18 czerwca 2024 roku o godz. 12:05 w Urzędzie Gminy i Miasta Sokołów Małopolski, ul. Rynek 1, 36 – 050 Sokołów Małopolski, w pokoju nr 13.

Zamawiający nie przewiduje publicznego otwarcia ofert.

Gmina Sokołów Małopolski zastrzega sobie prawo unieważnienia niniejszego postępowania bez podania przyczyny.

Zapytanie nie jest równoznaczne z zobowiązaniem Gminy Sokołów do zawarcia umowy zakupu.

7. Warunki płatności:

   Płatność nastąpi na podstawie dwóch faktur dotyczących osobno każdej w części zamówienia, w terminie do 30 dni od wpływu prawidło wystawionej faktury do Urzędu Gminy i Miasta Sokołów Małopolski.

8. Osoby upoważniona do kontaktu z Wykonawcami:

   Jerzy Chorzępa – Kierownik Referatu Organizacyjno-Administracyjnego , tel. 17 7729 019 w. 50, email: informatyk@sokolow-mlp.pl

9. Sposób przygotowania oferty:

Oferty należy sporządzić w formie pisemnej, w języku polskim, według załączonego wzoru.
Koszty sporządzenia oferty ponosi wyłączenie wykonawca, nie przewiduje się zwrotu kosztów sporządzenia oferty i udziału w postępowaniu.

Burmistrz Gminy i Miasta Sokołów Małopolski

Andrzej Kraska

Wzór

OA.136.14.2024

ZAPYTANIE OFERTOWE
Nazwa zamówienia:
Podniesienie funkcjonalności systemu antywirusowego

Oferta

Oferta na wykonanie wymiany warstwy sprzętowej i programowej (Zadanie 1) oraz szkolenia z zarządzania systemem antywirusowym (Zadanie 2).

Nazwa Wykonawcy: ……..……....
Adres Wykonawcy: ……e- mail ……
NIP Wykonawcy: ……..
Numer konta do płatności: ……..

Dane osoby uprawnionej do podpisania umowy ze strony Wykonawcy:
Imię i Nazwisko: …….
Funkcja/Stanowisko: …….

Oferuję wykonanie:

Zadania 1 za:
Cenę netto: ……. zł (słownie złotych: ……..……..……..……..……)
Podatek VAT ……. zł (słownie złotych: ……..……..……..……)
Cenę brutto: ……. zł (słownie złotych: ……..……..……)
Producent/Nazwa systemu antywirusowego: ……...
Okres licencjonowania: ……

Zadania 2 za:
Cenę netto: ……. zł (słownie złotych: ……..……..……..……)

Zapoznałem się z aktualną wersją Zapytania, SWZ , wzorem umowy i wyrażam zgodę na warunki płatności określone w zapytaniu cenowym.

Dnia ……

Podpis Wykonawcy lub osoby upoważnionej

Pieczęć Wykonawcy

Załączniku nr 1 do zapytania

Zamówienie stanowi cześć projektu pn. „Cyberbezpieczny samorząd”

Zadanie 1

Kod CPV:

- 48761000-0 - Pakiety oprogramowania antywirusowego

(Zadanie 1.10) - Wymiana warstwy sprzętowej i programowej - Podniesienie funkcjonalności systemu antywirusowego z możliwością wykrywania zagrożeń i reagowania na nie – XDR

Celem postępowania jest podniesie funkcjonalności systemu antywirusowego poprzez aktualizację lub zakup nowego systemu dla Urzędu Gminy i Miasta w Sokołowie Małopolskim.

Zamawiający posiada ochronę antywirusową firmy ESET (Identyfikator publiczny: 333-TKP-3XB) w wersjach:

- ESET PROTECT (Server), Wersja 10.0
- ESET PROTECT (Konsola internetowa), Wersja 10.0
- ESET SERVER SECURITY, Wersja 10.0
- ESET ENDPOINT ANTIVIRUS, Wersja 10.0 – Liczba licencji (stanowisk): 58

System antywirusowy po aktualizacji/zakupie powinien **obsłużyć 60 stanowisk – licencji (w tym maksymalnie 20 serwerów)** i ma mieć/spełniać poniższe wymagania i posiadać poniższe funkcjonalności:

Ochrona stacji roboczych – Windows

1. Rozwiązanie musi wspierać systemy Windows 10/Windows 11.
2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
3. Rozwiązanie musi wspierać architekturę ARM64.
4. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
5. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
6. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.
7. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives.

Ochrona antywirusowa i antyspyware

8. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

9. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
10. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
11. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
12. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
13. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
14. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu.
15. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak - nie wykonywało danego zadania.
16. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
17. Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
18. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
19. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
20. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
21. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
22. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
23. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
24. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
25. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
26. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
27. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
28. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
29. Rozwiązanie musi posiadać wbudowany konektor dla programu Microsoft Outlook.
30. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook.
31. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta

pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

32. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
33. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
34. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
35. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
36. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
37. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
38. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
39. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
40. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
41. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.
42. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
43. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
44. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
45. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
46. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
47. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
48. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
49. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
50. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

51. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
52. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.
53. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
54. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji - poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
55. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
56. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
57. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
58. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
59. Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
60. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
61. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
62. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
63. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
64. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
65. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
66. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
67. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje
    - reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku
    - wykrycia aktywności w systemie,

- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika.
  Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

68. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
69. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
70. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
71. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
72. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
73. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
74. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
75. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
76. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
77. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.
78. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
79. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
80. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
81. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
82. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
83. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.
84. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.

85. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
86. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
87. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
88. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
89. W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
90. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
91. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.
92. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
93. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
94. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
95. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
96. Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
97. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
98. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
99. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
100. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
101. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
102. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
103. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”
104. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
105. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
106. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

107. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
108. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
109. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.
110. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
111. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

Ochrona przed spamem

112. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
113. Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
114. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
115. Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
116. Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
117. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
118. Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
119. Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
120. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
121. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
122. Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

123. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    - tryb automatyczny - rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    - tryb interaktywny - rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    - tryb oparty na regułach - rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    - tryb uczenia się - rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
124. Rozwiązanie musi oceniać reguły zapory systemu Windows.
125. Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
126. Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
127. Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku

ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.

128. Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
129. Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
130. Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
131. Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
132. Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
133. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
134. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
135. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
136. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
137. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
138. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
    - z aplikacją lokalną, którą administrator wskazuje z listy,
    - z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

Kontrola dostępu do stron internetowych

139. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
140. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
141. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
142. Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
143. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
144. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być

automatycznie aktualizowana przez producenta.

145. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
146. Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
147. Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

Bezpieczna przeglądarka

148. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
149. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
150. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.
151. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.
152. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.
153. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

Ochrona stacji roboczych Linux

1. Rozwiązanie musi wspierać systemy operacyjne Debian, Ubuntu Desktop, Red Hat Enterprise Linux, SUSE Linux Enterprise Desktop oraz Linux Mint.
2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych.
3. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
6. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
10. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
11. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
12. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie.
13. Rozwiązanie musi posiadać możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz

wirusów.

14. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Administrator musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
15. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
16. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
17. Aktualizacje silnika detekcji muszą być dostępne z Internetu, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
18. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy.
19. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
20. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Kontrola dostępu do stron internetowych:

1. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli odwiedzanych stron internetowych.
2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
4. Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
5. Rozwiązanie musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii.
6. Podstawowe kategorie w jakie rozwiązanie musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
7. Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.
8. Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi wspierać system co najmniej Android 6.0.
2. Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3. Rozwiązanie musi wspierać procesory: ARM z obsługą ARMv7 lub x86 Intel Atom.
4. Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym.
5. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing”.

6. Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
7. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
8. Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia.
9. W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.
10. Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
11. Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

Skanowanie na żądanie:

12. Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji.
13. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
14. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
15. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.

Polityka ustawień:

16. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:
    - połączenie Wi-Fi,
    - GPS,
    - usługi lokalizacyjne,
    - pamięć,
    - roaming danych,
    - roaming połączeń,
    - nieznane źródła,
    - tryb debugowania,
    - komunikacja NFC,
    - szyfrowanie pamięci masowej,
    - urządzenie zrootowane.

Kontrola aplikacji:

17. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
18. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
19. Blokowanie aplikacji musi być możliwe w oparciu o:
    - nazwę aplikacji,
    - nazwę pakietu,
    - kategorię sklepu Google Play,
    - uprawnienia aplikacji,
    - pochodzenie aplikacji z nieznanego źródła.

Zabezpieczenia urządzenia:

20. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki

zabezpieczeń, w której może określić co najmniej:

- minimalny poziom zabezpieczeń i złożoność blokady ekranu,
- maksymalną dopuszczaną liczbę błędnych prób odblokowania,
- odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
- czas, po którym automatycznie nastąpi blokada ekranu,
- ograniczenie dostępu do kamery wbudowanej w urządzenie.

Aktualizacje modułów:

21. Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
22. Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
23. Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.

Konfiguracja i zdalne zarządzanie:

24. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
25. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.

Ochrona serwera – Linux

Architektura rozwiązania

1. Rozwiązanie musi posiadać skaner antywirusowy i antyspyware.
2. Rozwiązanie musi umożliwiać skanowanie plików, plików spakowanych i archiwów samorozpakowujących.
3. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
4. Rozwiązanie musi posiadać wbudowany mechanizm typu ,,watchdog". Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.
5. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikroserwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.
6. Rozwiązanie musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.
7. Rozwiązanie musi posiadać wsparcie dla SecureBoot-a.
8. Rozwiązanie musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.
9. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji

oprogramowania antywirusowego.

10. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.
11. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.
12. Rozwiązanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie ,,Permissive" jak i ,,Enforcing".
13. Rozwiązanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Centos 7.
14. Wszystkie mechanizmy bezpieczeństwa rozwiązania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.
15. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.
16. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
17. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
18. Rozwiązanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.
19. Rozwiązanie musi wspierać system plików zamontowany z flagą ,,noexec".
20. Rozwiązanie musi pozwalać na uruchamianie zadań skanowania działających ,,w tle", z możliwością ustawienia dla nich niskiego priorytetu.
21. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików.

Interfejs graficzny

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.
3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.
5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.
6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.
7. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.
8. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.
9. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najmniej języku: polskim, angielskim, niemieckim, francuskim, hiszpańskim, japońskim.

Skanowanie sieciowych systemów plików

1. Rozwiązanie musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.
2. Rozwiązanie nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP.
3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.
4. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

Instalacja

1. Rozwiązanie musi wspierać mechanizm instalacji zdalnej, realizowanej przez narzędzia do orkiestracji systemami operacyjnymi. Wspieranymi narzędziami muszą być co najmniej: Puppet, Chef, Ansible.
2. Rozwiązanie musi być wyposażone w mechanizm automatycznej aktualizacji komponentów programu.
3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
4. Rozwiązanie musi wspierać następujące systemy operacyjne: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux oraz Alma Linux.

Licencjonowanie

1. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
2. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji rozwiązania w trybie offline.

Ochrona serwera Windows

1. Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2012 i nowszych.
2. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
3. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
6. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
7. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
9. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do

skanowania, priorytet skanowania).

10. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
11. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
12. Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
13. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
14. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
15. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Rozwiązanie musi wspierać mechanizm klastrowania.
17. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
19. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
20. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
21. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
22. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
23. Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS.
24. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
25. Rozwiązanie musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
26. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
27. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

28. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
29. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
30. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
31. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
32. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
33. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
34. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
35. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
36. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
37. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
38. Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
39. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
40. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne -jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie.
41. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
42. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
45. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
46. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
47. Rozwiązanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
48. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
49. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji - poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.
50. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku,

których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.

51. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
53. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
54. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
55. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
56. Rozwiązanie musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
57. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
58. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
59. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
60. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
61. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
62. Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
63. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
64. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
65. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
66. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
67. Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
68. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
70. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

72. Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet.
73. Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
74. Rozwiązanie musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
77. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
78. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu

Ochrona usługi Microsoft 365

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
   - użytkowników, otrzymujących najwięcej spamu,
   - użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
   - użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
   - kont użytkowników, które mogę być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
   - jaka ilość wiadomości została przeskanowania,
   - wynik skanowania poszczególnej wiadomości,
   - czynność podjęta przez rozwiązanie.
   - Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
   - zagrożeniach, które zostały wykryte,
   - na jakim koncie zostały wykryte,
   - jakie zagrożenie zostało wykryte,
   - podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:

- wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
- wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online,
- dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.

14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
5. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
6. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.
7. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
9. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.
10. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.
11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
    - ilość znaków,
    - czy hasło ma zawierać wielkie litery,
    - czy hasło ma zawierać małe litery,
    - czy hasło ma zawierać cyfry,
    - czy hasło ma zawierać znaki specjalne,
    - okres ważności,
    - ilość nieudanych logowań,
    - możliwość zmiany hasła.
12. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
13. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    - Czysty,
    - Podejrzany,
    - Bardzo podejrzany,
    - Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Extended detection & response – Serwer (XDR)

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.
2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
7. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
8. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

9. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
10. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
11. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
12. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
13. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.
14. Serwer administracyjny musi oferować możliwość blokowania plików po sumachkontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
15. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
16. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnychna stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
17. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
18. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
19. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
20. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
21. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
22. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
23. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
24. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
25. Konsola administracyjna musi mieć możliwość tagowania obiektów.
26. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
27. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
28. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

29. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

Konektor

1. Pełne wsparcie dla systemu Windows 10/ Windows 11 oraz Windows Server 2012/2012R2/2016/2019/2022.
2. Pełne wsparcie dla systemów macOS 10.15 i nowszych.
3. Pełne wsparcie dla systemów Linux RHEL 7.6+/RHEL 8/RHEL 9/Ubuntu 18.04/Ubuntu 20.04/Ubuntu 22.04/Debian 10/Debian 11/Debian 12
4. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
5. Konektor musi współpracować z produktem antywirusowym tego samego producenta.
6. Konektor nie może działać bez produktu antywirusowego tego samego producenta.
7. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonane przez konektor.
8. Połączenie konektora do serwera zarządzającego musi być szyfrowane.
9. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.

Ochrona serwera pocztowego MS Exchange

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi umożliwiać Administratorowi na etapie instalacji wybór komponentów jakie mają być zainstalowane.
5. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
6. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
7. Rozwiązanie musi mieć możliwość zdefiniowania ilości wątków skanujących w celu optymalizacji pracy serwera. Liczba wątków skanowania musi wynosić od 1 do 21.
8. Rozwiązanie musi zapewnić skanowanie przed zapisaniem wiadomości w baziedanych przy pomocy transport agenta.
9. W przypadku wykrycia wirusa/blokowania wiadomości rozwiązanie musi umożliwić usunięcie wiadomości/ załącznika, podmianę załącznika na czysty plik zawierający jedynie informację o infekcji.
10. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
11. Rozwiązanie musi posiadać możliwość tworzenia białych i czarnych list domen/adresów IP, adresów e-mail.
12. Rozwiązanie musi posiadać możliwość akceptacji białych list stworzonych na poziomie serwera MS Exchange.
13. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.

14. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
15. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
16. Program ma posiadać mechanizm greylisting (szara lista).
17. Rozwiązanie musi posiadać możliwość tworzenia wyjątków dla mechanizmu szarej listy.
18. Rozwiązanie musi posiadać możliwość stworzenia kwarantanny poczty per użytkownik.
19. Kwarantanna musi być dostępna dla użytkownika końcowego za pośrednictwem przeglądarki WWW.
20. Pliki zapisywane w katalogu kwarantanny muszą być szyfrowane.
21. Użytkownik końcowy musi posiadać możliwość zarządzania wiadomościami znajdującymi się w kwarantannie w tym co najmniej, mieć możliwość uwolnienia wiadomości z kwarantanny, jej usunięcia lub pozostawienia w kwarantannie.
22. Administrator musi mieć możliwość wglądu w globalną kwarantannę z poziomu interfejsu aplikacji oraz przeglądarki WWW.
23. Rozwiązanie musi umożliwiać przesyłanie raportów dotyczących plików poddanych kwarantannie na wskazany adres e-mail.
24. Rozwiązanie musi umożliwiać pominięcie reguł kwarantanny podczas zwolnienia wiadomości e-mail w środowisku klastrowym.
25. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików serwera „na żądanie” lub według harmonogramu.
26. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
27. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
28. Rozwiązanie musi posiadać wbudowaną technologię ochrony przed atakami typu backscatter.
29. Rozwiązanie musi umożliwiać zaawansowane skanowanie przy użyciu interfejsu AMSI.
30. Rozwiązanie musi posiadać wbudowany skaner UEFI.
31. Rozwiązanie musi umożliwiać skonfigurowanie wyjątków ochrony przed atakami sieciowymi (IDS).
32. Rozwiązanie musi umożliwiać wykrywanie włamań wykorzystujących protokoły: SMB, RPC, RDP i informować użytkownika o wykryciu ataku.
33. Rozwiązanie musi wyświetlać powiadomienia po wykryciu ataku.
34. Rozwiązanie musi zezwalać na połączenia przychodzące do udziałów administracyjnych po protokole SMB.
35. Rozwiązanie musi odmawiać połączenia starym (nieobsługiwanym) dialektom protokołu SMB oraz zabezpieczeniom tego protokołu bez rozszerzeń zabezpieczeń.
36. Rozwiązanie musi umożliwiać komunikację z usługą menadżera konta zabezpieczeń, urząd zabezpieczeń lokalnych, rejestr zdalny, service control manager, usługą serwera i innymi usługami.
37. Rozwiązanie musi posiadać wbudowany skaner skryptów JavaScript, wykonywanych przez przeglądarki internetowe.
38. Rozwiązanie musi umożliwiać zdefiniowanie listy aplikacji, dla których jest przeprowadzane filtrowanie protokołu SSL/TLS.
39. Rozwiązanie musi umożliwiać określenie białej listy domen, dla których analiza protokoły SSL/TLS nie będzie wykonywana.
40. Rozwiązanie musi umożliwiać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
41. Rozwiązanie musi umożliwiać skanowanie plików spakowanych i skompresowanych.
42. Rozwiązanie musi posiadać wbudowaną technologię monitorowania zdarzeń bezpieczeństwa związanych z zagrożeniami typu malware, exploit, PUA, podłączenia do

sieci Botnet.

43. Musi być możliwe uruchamianie modułu ochrony przed złośliwym oprogramowaniem w ramach usługi chronionej systemu Windows (dla systemów Windows Server 2012 R2 lub nowszych).
44. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
45. Rozwiązanie musi wykorzystywać technologię chmury w celu przyśpieszenia reakcji na nowe zagrożenia oraz optymalizacji samego procesu skanowania.
46. Rozwiązanie musi umożliwiać analizę zagrożeń przez porównanie skanowanych plików z białą i czarną listą obiektów w chmurze producenta.
47. Rozwiązanie musi umożliwiać wybór jakie typy podejrzanych próbek będą przesyłane do producenta. W tym co najmniej: pliki wykonywalne, archiwa, skrypty, możliwy SPAM.
48. Rozwiązanie musi umożliwiać określenie plików i folderów, które nigdy nie będą przesyłane do producenta w celu analizy, np. plików zawierających informacje poufne.
49. Rozwiązanie musi umożliwiać zapisywanie informacji diagnostycznych w dziennikach dla aparatu antyspamowego.
50. Rozwiązanie musi być wyposażone w mechanizm chroniący serwer przed exploitami i atakami typu 0-day.
51. Rozwiązanie musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera.
52. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
53. Rozwiązanie musi w natywny sposób wspierać środowiska klastrowe.
54. Rozwiązanie musi umożliwiać wskazanie zewnętrznych lokalizacji w których przechowywane będą moduły i aktualizacje programu.
55. Rozwiązanie musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM.
56. Rozwiązanie musi skanować i oczyszczać w czasie rzeczywistym pocztę przychodzącą i wychodzącą, która jest obsługiwana przy pomocy programu Microsoft Outlook zainstalowanego lokalnie na serwerze pocztowym.
57. Rozwiązanie musi posiadać wbudowaną ochronę przed atakami typu phishing w wiadomościach e-mail.
58. Rozwiązanie musi umożliwiać skanowanie w środowiskach hybrydowych opartych na MS Office 365.
59. Rozwiązanie musi umożliwiać ochronę dostępu do urządzeń według zdefiniowanych reguł w określonych przedziałach czasu.
60. Rozwiązanie musi tworzyć log ochrony protokołu SMTP.
61. Rozwiązanie musi mieć możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
62. Rozwiązanie musi umożliwiać aktualizację modułów ochrony bez konieczności re instalacji całego programu.
63. Rozwiązanie musi uruchamiać jeden skaner uruchamiany w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie.
64. Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach oraz procesów.
65. Administrator ma możliwość dodania wykluczenia ze skanowania po tzw. HASH'u, wskazującym bezpośrednio na określoną infekcję, a nie konkretny plik.
66. Rozwiązanie musi być wyposażone w dwa niezależnie pracujące mechanizmy analizy heurystycznej (standardowa i zaawansowana heurystyka).
67. Administrator musi posiadać możliwość używania jednego poziomu analizy heurystycznej

lub obu poziomów jednocześnie.

68. Rozwiązanie musi umożliwiać automatyczne wysyłanie nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy - nie wymaga ingerencji użytkownika.
69. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu rozwiązania i nie może do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie.
70. Rozwiązanie musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
71. W przypadku wykrycia wirusa, ostrzeżenie może zostać wysłane do administratora poprzez email.
72. Rozwiązanie musi posiadać wbudowany dziennik zdarzeń rejestrujący informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania.
73. Administrator musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
74. Możliwość zabezpieczenia hasłem musi obejmować wyłączenie rozwiązania antywirusowego oraz jego odinstalowanie.
75. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
76. Rozwiązanie musi być dostępne z Internetu, lokalnego zasobu sieciowego, nośnika CD/DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
77. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
78. Rozwiązanie musi wspierać aktualizacje za pośrednictwem serwera Proxy.
79. Administrator musi posiadać możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
80. Rozwiązanie musi rejestrować wszystkie dane transmitowane za pośrednictwem funkcji ochrony sieci w formacie PCAP.
81. Rozwiązanie musi umożliwiać zarejestrowanie dodatkowych informacji na temat systemu operacyjnego, na przykład dotyczące uruchomionych procesów, aktywności procesora o działania dysku.
82. Rozwiązanie musi rejestrować komunikację produktu z serwerami licencji producenta.
83. Rozwiązanie musi automatycznie przesyłać powiadomienia o zdarzeniach pocztą e-mail na wskazany adres e-mailowy.
84. Musi istnieć możliwość zdefiniowania wykorzystywanego zestawu znaków. W tym co najmniej: Unicode (UTF-8), Ascii (7-bit), Japanese (ISO-2022-JP), lokalne.
85. Rozwiązanie musi posiadać wsparcie dla RMM (Remote Monitoring and Management).
86. Rozwiązanie musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej.
87. Rozwiązanie musi posiadać wbudowany, dedykowany moduł command line umożliwiający konfigurację oraz uruchamianie zadań zainstalowanej aplikacji.
88. Rozwiązanie musi być wyposażone w narzędzie umożliwiające wygenerowanie raportu dotyczącego stanu komputera, w tym co najmniej zainstalowanych aplikacji, uruchomionych procesów, ważnych wpisów w rejestrze i uruchomionych usług.
89. Do administracji zdalnej musi być wykorzystywany dedykowany agent.
90. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji.
91. Skuteczność programu ma być potwierdzona nagrodami niezależnych organizacji (np. VB100, ISCA labs, Check Mark).
92. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego

dystrybutora autoryzowanego przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi być uruchomiony na sprzęcie Zamawiającego
2. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia przechowywanych danych.
3. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
4. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
5. Serwer Administracyjny musi obsługiwać przynajmniej 50 000 stacji roboczych/serwerów.
6. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
7. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".
8. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
9. Administrator musi posiadać możliwość zarządzania urządzeniami mobilnymi - MDM.
10. Administrator musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
11. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
12. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
13. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
14. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
15. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
16. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
17. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
18. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
19. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
20. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
21. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem,

zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

22. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
23. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie generowania raportów i usuwania stacji roboczych. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
24. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
25. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
26. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
27. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
28. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
29. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
30. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
31. Szablon grupy dynamicznej musi umożliwiać zdefiniowane przedziału czasowego kiedy grupa dynamiczna ma działać.
32. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
33. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
34. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
35. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
36. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
37. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
38. Serwer administracyjny musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
39. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
40. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
41. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
42. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny

znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.

43. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
44. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
45. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF i CSV.
46. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
47. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
48. Powiadomienia mailowe mają być wysyłane w formacie HTML.
49. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
50. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email.
51. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
52. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
53. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
54. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
55. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
56. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
57. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
58. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
59. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
60. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
61. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
62. Serwer musi wspierać wysyłanie logów do systemu SYSLOG.
63. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
64. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.

65. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
66. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

Ochrona poprzez dwuskładnikowe uwierzytelnianie

1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 /Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 /2016 /2019.
7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web A c-cess.
9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
11. Oprogramowanie musi integrować się z systemem Windows Server poprzez konsolę MMC (Microsoft Managment Console).
12. Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się z wbudowanym w systemie Windows Server modułem do zarządzania kontami użytkowników (ADUC) w postaci dodatkowej zakładki we właściwościach użytkownika.
13. Administrator musi mieć możliwość określenia z jakiej metody uwierzytelniania użytkownicy będą korzystać:
    - dwuskładnikowe uwierzytelnianie poprzez użycie aplikacji mobilnej zainstalowanej na urządzeniu mobilnym użytkownika
    - dwuskładnikowe uwierzytelnianie poprzez wiadomości SMS wysyłane do użytkowników
    - klasyczna uwierzytelnianie (przy użyciu nazwy użytkownika i hasła)
14. Administrator musi mieć możliwość wysłania w postaci wiadomości SMS odnośnika, za pomocą którego użytkownik może pobrać i zainstalować dedykowaną aplikację mobilną wspierającą systemy mobilne opisane w punkcie 28 niniejszej specyfikacji.
15. Dwuskładnikowe uwierzytelnianie nie może wymagać od użytkownika instalacji aplikacji mobilnej w telefonie - wówczas jednorazowe hasła muszą być przesyłane do użytkownika w postaci wiadomości SMS.
16. Dodatek w module ADUC musi wyświetlać informację co najmniej o dniu i godzinie ostatniej próby logowania oraz ostatniej nieudanej próby logowania użytkownika.
17. Oprogramowanie musi posiadać mechanizm zabezpieczający przed atakiem typu brute-

force, które po określonej liczbie prób nieudanego logowania musi automatycznie zablokować możliwość uwierzytelnienia się dla danego użytkownika.

18. Administrator musi mieć możliwość odblokowania konta użytkownika w celu umożliwienia ponownego dostępu.
19. Administrator musi mieć możliwość wymuszenia zabezpieczenia aplikacji mobilnej za pomocą kodu PIN lub za pomocą danych biometrycznych - wówczas każdy użytkownik instalujący aplikację mobilną bez nadania kodu PIN nie będzie mógł generować jednorazowych haseł (OTP).
20. Administrator musi mieć możliwość podglądu informacji na temat:
    - aktualnego stanu licencji
    - ilości wykorzystanych licencji (użytkowników)
    - ilości pozostałych do wykorzystania wiadomości SMS.
21. Oprogramowanie przy użyciu serwera RADUIS musi umożliwiać dostęp do zabezpieczonych zasobów za pomocą klasycznej metody uwierzytelnienia (nazwa użytkownika i hasła).
22. Administrator musi mieć możliwość wyboru, którzy użytkownicy będą korzystać z dwuskładnikowego uwierzytelniania.
23. Administrator musi mieć możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji.
24. Jednorazowe hasło (OTP) generowane przez użytkowników powinno być unikalne i może być użyte tylko raz - nie dopuszcza się wielokrotnego użycia tego samego OTP.
25. Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM.
26. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania.
27. Wysyłanie wiadomości musi być możliwe w przypadku telefonów pracujących w roamingu.

API i SDK

28. Producent musi udostępnić API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu o usługę Active Directory.
29. Producent musi udostępniać SDK w celu umożliwienia programistom implementacji dwuskładnikowego uwierzytelniania dla środowisk nie wykorzystujących usługi Active Directory do uwierzytelniania użytkowników (np. wykorzystujących własną bazę danych z użytkownikami).
30. SDK musi być dostarczone zarówno dla platformy Microsoft .NET jak i języków programowania PHP i Java.

Aplikacja mobilna

28. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
29. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
30. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem - generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
31. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego użytkowników poprzez

dwuskładnikowe uwierzytelnianie.

32. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Zarządzanie podatnościami i aktualizacjami

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.
4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
   - nazwę aplikacji lub systemu operacyjnego
   - punktacje CVSS
   - opis wykrytej podatności
   - wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

Licencjonowanie:

1. Licencja nie mniej niż do 30 czerwca 2026 roku
2. Licencja obejmuje oprogramowanie, wsparcie oraz aktualizacje oprogramowania i sygnatur w całym okresie jej obowiązywania.

3. Oferowane licencje muszą pozwalać na użytkowanie systemu zgodnie z przepisami prawa oraz zapisami niniejszej specyfikacji wymagań przygotowanej przez Zamawiającego.
4. Licencja na system nie może ograniczać prawa Zamawiającemu do korzystania z oprogramowania w ramach wspólnej obsługi innych jednostek organizacyjnych gminy Sokołów Małopolski.
5. Licencja na system nie może ograniczać prawa licencjobiorcy do rozbudowy, zwiększenia ilości serwerów obsługujących oprogramowanie, przeniesienia oprogramowania na inny serwer, rozdzielenia funkcji serwera (osobny serwer bazy danych, osobny serwer aplikacji, osobny serwer plików).

Wdrożenie:

Dostawca (wykonawca) rozwiązania zobowiązany jest do przekazania oprogramowania, licencji, pełnej dokumentacji systemu i dot. administracji systemem oraz dokumentacji w języku polskim dot. instalacji w środowisku wirtualizacyjnym maszyn z: konsolą XDR i konsolą centralnej administracji systemu.
Ponadto dostawca przez okres 1 roku licząc od daty podpisania umowy świadczyć będzie pomoc, wsparcie w procesie konfiguracji systemu oraz wdrożenia i konfiguracji w/w maszyn wirtualnych, a także bieżącego użytkowania systemu na wniosek Zamawiającego .

Termin realizacji:

Do 30 dni od dnia podpisania umowy

Zadanie 2

Kod CPV:

- 80533100-0 - Usługi szkolenia komputerowego

Zadanie 2.7 Szkolenia - Szkolenie z zarządzania systemem antywirusowym wykorzystującym XDR oraz zdalną administrację

Przedmiotem zamówienia jest przeprowadzenie szkoleń autoryzowanych dla pracownika merytorycznego, tak aby umiał efektywnie instalować, konfigurować, administrować - wykorzystywać zakupione oprogramowanie w ramach zadania 1.10.

a) Szkolenie z technologii antywirusowej zgodnie z proponowanym rozwiązaniem, oraz wdrożeniem i konfiguracją zaproponowanego rozwiązania centralnego administrowania systemem dla jednej osoby

Szkolenie ma obejmować m.in. zagadnienia:

- Omówienie możliwości zaproponowanych rozwiązań
- Instalacja, konfiguracja i aktualizacja – klientów, agentów
- Kontrola dostępu do USB i stron www
- Filtrowanie treści
- Reagowanie na występujące incydenty
- Przeprowadzenie, analizowanie poszczególnych scenariuszy
- Optymalizacja i automatyzacja procesów związanych z zarządzeniem na stacjach roboczych i serwerach
- Zdalne zarządzanie rozwiązaniami na stacjach roboczych i serwerach
- Zarządzanie aktualizacjami elementów systemu
- Zarządzanie politykami
- Raportowanie

Informacje dodatkowe dot. szkolenia:

- szkolenie i materiały w języku polskim
- szkolenie w formie zdalnej
- czas trwania: min. 2 dzień, po min. 12 godzin
- uczestnik otrzyma dostęp do materiałów w wersji papierowej lub elektronicznej w języku polskim lub angielskim, a po ukończeniu certyfikat sygnowany prze producenta oprogramowania, certyfikat ukończenia

b) Szkolenie w formie warsztatów praktycznych adekwatne do zaproponowanego rozwiązania jednej osoby

Szkolenie ma obejmować m.in. zagadnienia:

- Wdrażanie i konfiguracja serwera centralnego zarządzania w postaci maszyn wirtualnych
- Instalacja i aktualizacja – agentów i konsoli do centralnego zarządzania
- Zaawansowane zarządzanie politykami
- Sandboxing chmurowy

- Szyfrowanie dysków
- Rozwiązywanie problemów

Informacje dodatkowe dot. szkolenia:

- szkolenie i materiały w języku polskim
- szkolenie w formie zdalnej
- czas trwania: min. 1 dzień, po min. 6 godzin
- uczestnik otrzyma dostęp do materiałów w wersji papierowej lub elektronicznej w języku polskim lub angielskim, a po ukończeniu certyfikat sygnowany prze producenta oprogramowania, certyfikat ukończenia

c) Kompleksowe szkolenie z narzędzia Extended Detection & Response (XDR) dla jednej osoby

Szkolenie ma obejmować m.in. zagadnienia:

- Wdrożenie i konfiguracja narzędzia XDR
- Diagnozowania nietypowych zachowań i naruszeń w sieci firmowej
- Ocena ryzyka, sposoby reakcji na zagrożenia, wdrażanie działań zaradczych
- Wykrywanie zagrożeń ATP
- Wykrywanie unikatowych plików w sieci
- Monitorowanie aplikacji
- Analiza powłamaniowa
- Ochrona przed ransomware
- Sposoby blokowania uruchomienia plików w sieci

Informacje dodatkowe dot. szkolenia:

- szkolenie i materiały w języku polskim
- szkolenie w formie zdalnej
- czas trwania: min. 1 dzień, po min. 6 godzin
- uczestnik otrzyma dostęp do materiałów w wersji papierowej lub elektronicznej w języku polskim lub angielskim, a po ukończeniu certyfikat sygnowany prze producenta oprogramowania, certyfikat ukończenia

Dla każdego ze szkoleń wykonawca zobowiązany jest zaproponować dwa gwarantowane terminy, z których zamawiający wybierze jeden.

Termin realizacji:

Do 30 grudnia 2024 r.

Załączniku nr 2 do zapytania

WZÓR UMOWY

Umowa nr ……

zawarta w dniu …… 2024 roku

Strony umowy:

Gmina Sokołów Małopolski

ul. Rynek 1, 36-050 Sokołów Małopolski, NIP 517-01-21-981

zwana w dalszej części umowy „Zamawiającym”

reprezentowana przez;

Pana Andrzeja Kraska – Burmistrza Gminy i Miasta Sokołów Małopolski,

przy kontrasygnacie Pani Moniki Lichota - Skarbnika Gminy Sokołów Małopolski, a

…….

zwany w dalszej części umowy „Wykonawcą”

reprezentowany przez;

……,

……,

W rezultacie dokonania przez Zamawiającego wyboru oferty Wykonawcy na podstawie art. 2 ust. 1 pkt 1 ustawy Prawo zamówień publicznych i na podstawie Zarządzenia Burmistrza nr 404/2021 w zapytaniu OA.136.14.2024 pn.: „**Podniesienie funkcjonalności systemu antywirusowego**” została zawarta umowa następującej treści:

§ 1

1. Zamawiający zleca, a Wykonawca przyjmuje do wykonania zadanie pn.: „Podniesienie funkcjonalności systemu antywirusowego”
2. Zakres umowy to:

    1) Wymiana warstwy sprzętowej i programowej - Podniesienie funkcjonalności systemu antywirusowego z możliwością wykrywania zagrożeń i reagowania na nie – XDR

    2) Szkolenia z zarządzania systemem antywirusowym wykorzystującym XDR oraz zdalną administrację

3. Szczegółowy opis, zakres i sposób wykonania dostaw znajduje się w załączonej do zapytania dokumentacji (SWZ) i w ofercie Wykonawcy, które to dokumenty stanowią integralną część niniejszej umowy.
4. Zamawiający i Wykonawca obowiązani są współdziałać przy wykonaniu umowy w sprawie zamówienia publicznego, zwanej dalej "umową", w celu należytej realizacji zamówienia.

§ 2

1. Wykonawca zobowiązuje się wykonać przedmiot umowy z najwyższą starannością, zgodnie z treścią umowy, zakresem, specyfikacją warunków zamówienia oraz zgodnie z obowiązującymi przepisami prawa.
2. Wykonawca wyraża zgodę na przetwarzanie danych osobowych osób uczestniczących ze strony Wykonawcy w realizacji niniejszej umowy dla potrzeb niezbędnych do realizacji umowy (zgodnie z Ustawą o Ochronie Danych Osobowych Dz.U.2019.1781). Wykonawca poinformuje te osoby o uprawnieniach i obowiązkach w zakresie przetwarzanie danych osobowych.
3. Wykonawca jest zobowiązany do współpracy z zamawiającym w zakresie tworzenia, kompletowania dokumentacji rozliczeniowej, zarówno na etapie realizacji umowy jak i po jej zakończeniu, tak aby możliwe było prawidłowe rozliczenie dofinansowania przypisanego do zakresu objętego niniejszą umową, zgodnie z wytycznymi darczyńcy: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

§ 3

Termin wykonania umowy ustala się dla zadań:

1) System antywirusowy wraz z dokumentacją i licencjami - 30 dni od podpisania umowy, tj.: ……*(orientacyjnie do dnia 19 lipca 2024 r.)*

2) Szkolenia realizowane do 30.12.2024 roku

§ 4

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy i dalszemu podwykonawcy.
2. Powierzenie wykonania części zamówienia podwykonawcom, nie zwalnia wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.

§ 5

1. Za realizację przedmiotu umowy strony ustalają **wynagrodzenie całkowite**, które zgodnie z złożoną w przetargu ofertą wyniesie - łącznie:

Wartość netto: ……zł

Podatek VAT: ……zł, według obowiązującej stawki.

Wartość brutto: ……..zł

(słownie ……złotych)

W tym:

Zadanie 1 (oprogramowanie):

Wartość netto: ……zł

Podatek VAT: ……zł, według obowiązującej stawki (23%).

Wartość brutto: ……..zł

(słownie ……złotych)

Zadanie 2 (szkolenie):

Wartość netto: ……zł

Podatek VAT: ……zł, według obowiązującej stawki (0%).

Wartość brutto: ……..zł

(słownie ……złotych)

2. Wynagrodzenie stanowi sumę wynagrodzenia ryczałtowego za każdy wyceniony w ofercie element zamówienia. Zapłata należy się tylko za elementy ujęte w ofercie, które zostały faktycznie wykonane/zrealizowane prawidłowo i odebrane przez zamawiającego.

§ 6

1. Zamawiający przystąpi do odbioru w terminie do 7 dni od daty wpływu do Zamawiającego pisemnego zgłoszenia zakończenia realizacji zadania 1 i Zadania 2 i całej umowy i po przedłożeniu kompletnej dokumentacji powykonawczej.
2. Kompletną dokumentację powykonawczą stanowi: licencja, pełna dokumentacja systemu i dot. administracji systemem oraz dokumentacja w języku polskim dot. instalacji w środowisku wirtualizacyjnym maszyn z: konsolą XDR i konsolą centralnej administracji systemu.
3. W przypadku nieprawidłowości, w odniesieniu do wszystkich elementów dokumentacji powykonawczej Zamawiający może żądać wyjaśnień, korekt, uzupełnień a Wykonawca będzie zobowiązany je dokonać we wskazanym przez Zamawiającego terminie- nie krótszym niż 5 dni roboczych.
4. Nieprawidłowości w dokumentacji powykonawczej zwalniają Zamawiającego z zobowiązań dotyczących terminu płatności o którym mowa w § 7 ust.3 .

§ 7

1. Zapłata za wykonanie dostawy nastąpi w oparciu o faktury za wykonanie usług, tj. odrębna faktura za zadanie 1 i zadanie 2
2. podstawę do wystawienia faktur stanowić będzie protokół odbioru częściowego i protokół odbioru końcowego.
3. Termin zapłaty faktur Wykonawcy (licząc od daty dostarczenia Zamawiającemu prawidłowych faktury wraz z dokumentami rozliczeniowymi) wynosi do 30 dni i nastąpi przelewem na konto Wykonawcy …….. w banku ……..
4. W razie opóźnienia w zapłacie faktur, Wykonawcy przysługuje prawo naliczenia ustawowych odsetek liczonych od wartości nieterminowo zapłaconej faktury, chyba, że opóźnienie wynika z niedopełnienia postanowień niniejszej umowy przez Wykonawcę.
5. Wszelkie zmiany zakresu lub specyfiki dostaw mogą być wykonane (lub „zaniechane”) na podstawie protokołów konieczności potwierdzonych przez Wykonawcę i zatwierdzonych przez Zamawiającego.
6. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy KC .

§ 8

1. **Wykonawca ustanawia osobę do kontaktów w sprawie realizacji zamówienia: ……**

2. **Wykonawca podaje kontakt e-mailowy do celów realizacji niniejszej umowy: ……** i o jego zmianie Wykonawca poinformuje najpóźniej 3 dni od tego faktu Zamawiającego bez wezwania.
3. Zamawiający podaje osobę do kontaktu w sprawie realizacji zamówienia, tj.: ……., e mail …….

§ 9

Do obowiązków Wykonawcy należy realizacja zadania zgodnie z postanowieniami specyfikacji i wymogów technicznych zamieszczonych wraz z ogłoszeniem o zamówieniu i zgodnie z ofertą a w szczególności:

1. Przedłożenie przed wszczęciem realizacji zadania bez żądania Zamawiającego dokumentacji potwierdzającej zgodność oferowanych dostaw , usług z SWZ. Zamawiający po przedłożeniu dokumentów dokonuje zatwierdzeń w ciągu 3 dni roboczych, lub wnosi o wydłużenie czasu na dokonanie weryfikacji i zatwierdzeń z jednoczesnym zastosowaniem wydłużenia terminu realizacji umowy, o którym mowa w paragrafie 3).
2. Zapewnienie ciągłości kontaktu z Zamawiającym,
3. Przestrzeganie przepisów prawa z zakresu RODO i dostępu do danych osobowych,
4. Naprawienie na swój koszt szkód powstałych z przyczyn leżących po stronie Wykonawcy,
5. Informowanie Zamawiającego o zagrożeniach dotrzymania terminu realizacji zadania.
6. Zabezpieczenie we własnym zakresie i na własny koszt organizacji realizacji umowy.
7. Przyjmowanie i korespondencji listownej i mailowej i niezwłoczne odpowiadanie na pisma Zamawiającego oraz niezwłoczne informowanie Zamawiającego o zmianie adresu siedziby i danych kontaktowych.
8. Dokonywanie w ustaleń szczegółowych w zakresie oferowanych rozwiązań, wykonanie całego przedmiotu umowy zgodnie z wymogami SWZ.

§ 10

Wykonawca przejmuje na siebie obowiązki skompletowania , usystematyzowania i dostarczenia Zamawiającemu dokumentacji odbiorowej.

§ 11

Wykonawca ponosi pełną odpowiedzialność za należyte wykonanie obowiązków określonych w niniejszej umowie wobec Zamawiającego jak również wobec osób trzecich, którym wyrządził szkodę.

§ 12

1. Wykonawca zapłaci Zamawiającemu kary umowne w następujących przypadkach:
   a) za zwłokę w wykonaniu Zadania 1 w wysokości 0,1 % wynagrodzenia brutto, określonego dla zadania 1 w § 5 za każdy dzień zwłoki licząc od umownego terminu zakończenia realizacji zadania 1 (§3 pp 1)) do dnia wpływu do Zamawiającego pisemnego zgłoszenia do odbioru lub ponownego zgłoszenia do odbioru zadania 1.
   b) za zwłokę w wykonaniu Zadania 2 w wysokości 0,1 % wynagrodzenia brutto, określonego dla zadania 2 w § 5 za każdy dzień zwłoki licząc od umownego terminu zakończenia realizacji zadania 2 (§3 pp 2)) do dnia wpływu do Zamawiającego pisemnego zgłoszenia do odbioru lub ponownego zgłoszenia do odbioru zadania 2 i całej umowy.
   Zgłoszenie do odbioru kończy bieg okresu naliczania kar umownych tylko wówczas, gdy przedmiot zgłoszenia zostanie zaakceptowane przez Zamawiającego, co zostanie potwierdzone protokołem odbioru lub odbioru końcowego.
   c) za uchybienie wykonywania świadczenia przez okres 1 roku licząc od daty podpisania umowy, o którym mowa w dziale wdrożenie z SWZ Zadania 1, w wysokości 0,1 % całkowitego wynagrodzenia umownego brutto za każdy przypadek uchybienia, tj.: za brak reakcji Wykonawcy przez minimum 4 dni robocze od przesłania wniosku od Zamawiającego.
   d) za brak współpracy w zakresie dokumentacji rozliczeniowej o której mowa w §2 ust.3, do wysokości utraconego dofinansowania.
2. Strony zastrzegają sobie prawo do dochodzenia odszkodowania uzupełniającego, przenoszącego wysokość kar umownych, do wysokości rzeczywiście poniesionej szkody.
3. Wykonawca wyraża zgodę na potrącenie z wynagrodzenia wszelkich kar umownych oraz roszczeń opisanych w niniejszym paragrafie bez zastosowania innych szczególnych procedur , tj.: po uprzednim przekazaniu przez Zamawiającego do Wykonawcy oświadczenia o zamiarze dokonania potrącenia. Potrącenia można dokonać nie wcześniej niż po upływie 5 dni od przesłania oświadczenia na e-mail, o którym mowa w § 8 ust. 2 lub na e-mail Wykonawcy .
4. Gdy pomimo dwukrotnego wezwania pisemnego lub mailowego Wykonawca nie przystąpi do usuwania wad w przedmiocie umowy w terminie 5 dni od daty przesłania ostatniego wezwania lub pomimo dwukrotnego przystąpienia do usuwania wad, wady te nie zostaną prawidłowo usunięte, to wówczas Wykonawca wyraża zgodę na zastępcze usunięcie wad na koszt Wykonawcy - zarówno w okresie realizacji umowy (wady przedmiotu dostawy i usługi) jak i w okresie 1 roku, o którym mowa w dziale WDROŻENIE w SWZ Zadania 1 (wady usług w okresie 1 roku , o których mowa w dziale WDROŻENIE w SWZ Zadania 1).
5. Zamawiający może wstrzymać wypłatę należnego wynagrodzenia za wadliwe produkty i usługi, nawet w przypadku powzięcia informacji o nieprawidłowościach po dokonaniu odbioru. Wówczas nie mają zastosowania zapisy paragrafu 7 ust. 3 i 4 w zakresie wadliwych produktów i usług i Wykonawcy nie przysługują żadne roszczenia tytułem opóźnienia zapłaty za wadliwe produkty/usługi. Wstrzymanie zapłaty kończy się z dniem następującym po dacie protokołu z usunięcia wad – jeśli te usunął na swój koszt Wykonawca, jeśli , wystąpiło usunięcie zastępcze wad, to koszty zastępczego usunięcia oszacuje się lub przyjmie od wykonawcy zastępczego i potrąci się z wynagrodzenia Wykonawcy.
6. Za szkody wyrządzone osobom trzecim Wykonawca odpowiada samodzielnie.

7. Łączną maksymalną wysokość kar umownych, których mogą dochodzić strony to 10 % pierwotnej wartości umowy netto.

§ 16

1. Dopuszcza się wprowadzenie w umowie zmian obejmujących zmianę terminu, zakresu, specyfiki, wartości dostaw w następujących przypadkach adekwatnie:
   1) W przypadku ujawnienia się nieprawidłowości i niedokładności SWZ, lub błędów przypadkowych lub pisarskich w SWZ lub umowie , w tym wystąpienia błędnych opisów parametrów produktów (przedmiotu dostawy), co skutkowałoby niemożnością zrealizowania dostawy zgodnie z zamierzonym celem –wówczas dokona się zmiany umowy uwzględniając cel wprowadzonego zapisu.
   2) W przypadku zmiany wymogów zabezpieczeń stawianych dla Zamawiającego przepisami prawa.
   3) W przypadku zaistnienia sytuacji nagłych i nieprzewidzianych, które skutkowałyby niemożnością dokonania odbiorów lub dostaw, np. działań związanych z sytuacją kryzysową .
   4) W przypadku wystąpienia konieczności zwiększenia zakresu umowy o elementy nie wycenione w kalkulacji cenowej, to wówczas cena dodatkowych elementów będzie podlegać negocjacjom, a Wykonawca będzie musiał wykazać dokumentami, że oferowana cena jest ceną rynkową , nie droższą niż ogólnie dostępne na rynku oferty. Zamawiający będzie mógł wskazać do uwzględnienia wyszukane przez siebie oferty.
   5) Strajki, protesty, załamanie rynkowe, z wyłączeniem strajków pracowników Wykonawcy, działanie sił przyrody lub osób trzecich, wystąpienia zagrożenia dla: mienia, zdrowia i życia w pobliżu miejsc planowanej realizacji dostawy, zdarzeń nadzwyczajnych - np. katastrofy, wojny, działań wojennych, powodzi- o czas niemożliwości wykonywania dostaw.
2. Dopuszcza się również w Umowie wprowadzenie zmiany osób wyznaczonych do kontaktów przez Wykonawcę- bez konieczności aneksowania umowy.
3. Strona powołująca się na zaistnienie ww. zdarzeń jest zobowiązana do niezwłocznego pisemnego powiadomienia o powyższym drugiej Strony, a następnie do udokumentowania zaistnienia tego stanu.
4. Po ustąpieniu przeszkód w realizacji niniejszej Umowy, spowodowanych zaistnieniem siły wyższej, lub z innych przyczyn Wykonawca zobowiązany jest dołożyć starań dla nadrobienia zaległości powstałych w wyniku ww. nieprzewidzianych zdarzeń.
5. Wszelkie zmiany i uzupełnienia Umowy wymagają dla ich ważności uprzedniej akceptacji Stron i formy pisemnego aneksu, pod rygorem nieważności muszą być dokonane przez umocowanych do tego przedstawicieli obu Stron. Podpisanie aneksu do umowy powinno być poprzedzone sporządzeniem protokołu konieczności zawierającego min.: istotne okoliczności potwierdzające konieczność zawarcia aneksu oraz przedstawienie ewentualnych zmian w wynagrodzeniu umownym. Błędy przypadkowe i pisarskie w umowie będą poprawiane z uwzględnieniem celu zapisu i nie wymagają sporządzania protokołów konieczności.

§ 17

1. Zamawiającemu przysługuje prawo odstąpienia od umowy bez żadnych kar umownych na rzecz Wykonawcy jeżeli:
   a) zostanie ogłoszona upadłość lub rozwiązanie firmy Wykonawcy,
   b) Wykonawca nie rozpoczął realizacji zadania przez 14 dni od podpisania umowy lub go nie kontynuuje lub gdy nie odpowiada na korespondencję bez uzasadnionych przyczyn, pomimo 2 krotnego przesłania wezwania od Zamawiającego. Przez rozpoczęcie realizacji zadania rozumie się okazanie Zamawiającemu do zatwierdzenia dokumentacji potwierdzającej zgodność oferowanych dostaw z OPZ.
2. Zamawiający w razie odstąpienia od umowy z przyczyn, za które Wykonawca nie odpowiada obowiązany jest przeprowadzić odbiór Zadania oraz do zapłacić wynagrodzenie za elementy zrealizowane i odebrane do dnia odstąpienia od umowy.

§ 18

Spory wynikłe na tle niniejszej umowy strony poddają rozstrzygnięciu Sądu właściwego rzeczowo i miejscowo ze względu na siedzibę Zamawiającego.

§ 19

W sprawach nie uregulowanych niniejszą umową stosuje się w szczególności przepisy Kodeksu Cywilnego i przepisy dotyczące wymogów wynikających ze specyfiki przedmiotu zamówienia .

§ 20

Umowę sporządzono w trzech jednobrzmiących egzemplarzach; 2 dla Zamawiającego i 1 dla Wykonawcy.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 3 do zapytania

Link do wytycznych (zaleceń): https://www.gov.pl/attachment/49d7f2bb-69a6-43f1-aadd-c41010f72d3d

Komunikacja w postępowaniu o udzielenie zamówienia przez Bazę Konkurencyjności (oraz poza Bazą Konkurencyjności)

Zgodnie z sekcją 3.2.3 pkt. 1 Wytycznych dotyczących kwalifikowalności wydatków na lata 2021-2027 (dalej zwanymi: Wytycznymi), komunikacja w postępowaniu o udzielenie zamówienia, w tym ogłoszenie zapytania ofertowego, składanie ofert, wymiana informacji między Zamawiającym a Wykonawcą oraz przekazywanie dokumentów i oświadczeń odbywa się pisemnie za pomocą Bazy Konkurencyjności (dalej zwanej: BK2021).

Zgodnie z sekcją 3.2.3 pkt. 2 Wytycznych, wyjątkowo, możliwe jest odstąpienie od komunikacji określonej w pkt. 1, o czym Zamawiający informuje Wykonawców w zapytaniu ofertowym upublicznianym w BK2021, jeżeli:

- charakter zamówienia wymaga użycia narzędzi, urządzeń lub formatów plików, które nie są obsługiwane za pomocą BK 2021, lub
- aplikacje do obsługi formatów plików, które nadają się do przygotowania ofert lub prac konkursowych, korzystają z formatów plików, których nie można obsługiwać za pomocą żadnych innych aplikacji otwarto źródłowych lub ogólnie dostępnych, lub są one objęte licencją i nie mogą zostać udostępnione do pobierania lub zdalnego wykorzystania przez Zamawiającego, lub
- Zamawiający wymaga przedstawienia modelu fizycznego, modelu w skali lub próbki, których nie można przekazać za pośrednictwem BK2021, lub
- jest to niezbędne z uwagi na potrzebę ochrony informacji szczególnie wrażliwych, której nie można zagwarantować w sposób dostateczny przy użyciu BK2021.

Odstąpienie od komunikacji określonej w pkt 1 jest dopuszczalne w zakresie, w jakim nie jest możliwe dotrzymanie sposobu komunikacji w BK2021. Zamawiający określa w zapytaniu

ofertowym sposób komunikacji w postępowaniu o udzielenie zamówienia wynikający z zakresu odstąpienia od komunikacji w BK2021.

Zgodnie z sekcją 3.2.3 pkt. 3 Wytycznych, w przypadku zawieszenia działalności BK2021 potwierdzonego odpowiednim komunikatem w BK2021, Zamawiający kieruje zapytanie ofertowe do co najmniej trzech potencjalnych Wykonawców, o ile na rynku istnieje trzech potencjalnych Wykonawców danego zamówienia, oraz ogłasza zapytanie ofertowe co najmniej na swojej stronie internetowej, o ile posiada taką stronę. W takim przypadku Zamawiający określa w zapytaniu ofertowym sposób komunikacji w postępowaniu o udzielenie zamówienia.

Zgodnie z technicznymi uwarunkowaniami BK2021, komunikacja poprzez BK2021 jest obowiązkowa od momentu opublikowania postępowania do upływu terminu składania ofert (np. wyjaśnienie treści ogłoszenia). Po upływie terminu składania ofert, komunikacja między Zamawiający a Wykonawcą za pośrednictwem BK2021 nie jest wymagana. Na tym etapie można się kontaktować z Wykonawcą np. za pomocą danych kontaktowych dostępnych w sekcji „Osoby do kontaktu" w ogłoszeniu. Zamawiający powinien jednak pamiętać, że kontaktując się z Wykonawcami powinien czynić to z poszanowaniem zasady uczciwej konkurencji i równego traktowania Wykonawców.

Wytyczne nie dopuszczają innej formy i sposobu składania ofert niż za pośrednictwem BK2021. Niespełnienie tego wymogu oznacza niezgodność oferty z ogłoszeniem. Potencjalne oferty składane poza BK2021 powinny zostać odrzucone przez Zamawiającego. Dopuszczenie oferty złożonej poza BK 2021 do oceny jest niezgodne z Wytycznymi, czyli procedurami, o których mowa w art. 184 UFP.

W przypadku braku miejsca na dodanie załączników przez Zamawiającego do postępowania (w związku z występującym limitem miejsca na załączniki w ogłoszeniu), Zamawiający może zamieścić je poza BK2021 – np. na swojej stronie internetowej – a link do nich (dokładny) zamieścić w ogłoszeniu w BK2021.

W przypadku dużej ilości załączników przekazywanych przez Oferenta, Zamawiający może poinformować o odstąpieniu od komunikacji przez BK2021 jeśli liczba lub rozmiar plików przekroczą techniczne możliwości BK2021 – jako że w ten sposób, tzn. przekraczając techniczne możliwości BK2021, pliki te również nie są obsługiwane przez BK2021. Sugerujemy, aby pliki które przekraczają techniczne możliwości BK2021, w pierwszej kolejności próbować przesłać przez pocztę elektroniczną (np. na adres ogłoszeniodawcy wskazany w sekcji "Osoby do kontaktu" na ogłoszeniu). Korzystanie przez Oferentów z zewnętrznych linków rekomendujemy jako możliwość z której należałoby korzystać po wyczerpaniu się innych możliwości przesłania przez nich załączników do swojej oferty do ogłoszenia. Pamiętać należy bowiem o konieczności zachowania śladu audytowego, co w przypadku wielu linków (od wielu Oferentów) może być utrudnione – niemniej jednak rozwiązanie to może być zastosowane po wyczerpaniu innych możliwości.

Wymagania, w zakresie komunikacji za pośrednictwem BK 2021, będą miały znaczenie dla kwalifikowalności wydatków w projektach realizowanych z programów perspektywy finansowej 2021-2027.