Załącznik nr 2 do SWZ

Dotyczy: postępowania prowadzonego w trybie podstawowym bez negocjacji o wartości zamówienia nie przekraczającej progów unijnych o jakich stanowi art. 3 ustawy PZP, na ***podniesienia poziomu cyberbezpieczeństwa Szpitala,*** nr sprawy: **ZP/P/12/23**

OPIS PRZEDMIOTU ZAMÓWIENIA

Strony zgodnie stwierdzają, że na potrzeby niniejszego OPZ wraz z załącznikami i przyszłej Umowy dotyczącej opisanego zamówienia, wymienionym pojęciom nadają znaczenie określone poniżej, oraz że użyte w tekście poniżej wymienione pojęcia, rozumiane będą w sposób poniżej zdefiniowany. Dla podkreślenia, że pojęcia te rozumiane są w sposób zdefiniowany, ich pierwsze litery będą pisane w tekście wielką literą.
Strony ustalają następujące definicje:

1. **Zamawiający** – oznacza Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sulęcinie, ul. Witosa 7, 69-200 Sulęcin
2. **Wykonawca** - podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez prowadzenia negocjacji na podstawie art. 275 pkt 1 Ustawy z dnia 11 września 2019r – prawo zamówień publicznych (Dz.U. 2023 poz. 1605 ze zm.).
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania przetargowego.
4. **System informatyczny** - zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej.
5. **Infrastruktura sprzętowa -** znajdująca się w dyspozycji Zamawiającego, w tym stanowiąca jego własność oraz dostarczana w ramach realizacji przedmiotu zamówienia infrastruktura przetwarzania danych wszystkie połączenia, urządzenia fizyczne i oprogramowania aplikacyjne, które łącznie współpracując umożliwiają gromadzenie, przechowywanie, wytwarzanie danych i usług oraz udostępnianie danych i usług elektronicznych.
6. **Umowa** – umowa zawarta w ramach realizacji OPZ.
7. **SWZ –** Specyfikacja Warunków Zamówienia
8. **Gwarancja i Serwis** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie w oraz w projekcie umowy.
9. **Wada**- Należy przez to rozumieć Awarię, Błąd, Usterkę
10. **Awaria-** oznacza to Błąd, uniemożliwiający prawidłowe użytkowanie oprogramowania lub jego części, który nie prowadzi do zatrzymania eksploatacji oprogramowania.
11. **Błąd** - oznacza to powtarzalne działanie oprogramowania niezgodne z jego dokumentacją użytkową, uniemożliwiające wykonanie części jego funkcji.
12. **Usterka -** należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SWZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
13. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora infrastruktury sprzętowej.
14. **Zdalny Dostęp** – analogowe lub cyfrowe łącze wydajnej transmisji danych pomiędzy węzłem infrastruktury siedziby Wykonawcy, a węzłem infrastruktury zapewnianym przez Zamawiającego, umożliwiające realizować usługi serwisowe lub konfiguracyjne.
15. **Szczegółowy Harmonogram Realizacji Zadania** – szczegółowy terminarz realizacji przedmiotu Umowy wraz z podziałem na Etapy przygotowany przez Wykonawcę w terminie 14 dni roboczych od zawarcia umowy.

16. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
17. **Protokół Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów.
18. **Protokół Odbioru Końcowego-** Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego, stanowi potwierdzenie wykonania i odbioru Przedmiotu Zamówienia.
19. **Protokół Dostawy-** Protokół, w którym Zamawiający sprawdza ilości dostarczonego towaru i porównuje go ze stanem wykazanym w dokumentach towarzyszących dostawie.
20. **Protokół Usterek -** Protokół, w którym Zamawiający wskazuje zastrzeżenia co do zakresu i jakości wykonanych prac, które uniemożliwiają dokonanie odbioru wykonanych dostaw i prac.
21. **Protokół Uzgodnień** – dokument tworzony przez Wykonawcę i zatwierdzony przez Strony, na podstawie zapisu ze spotkania lub ustaleń zdalnych (mailowych, telefonicznych) z Zamawiającym. Dokument ten używany jest w trakcie prowadzenia analizy wymagań Zamawiającego i stanowi zobowiązanie obu Stron. Zamawiający zobowiązany jest, że wymagania zapisane w/w protokole nie zostaną zmienione, natomiast Wykonawca zobowiązany jest do realizacji zawartych w nim wymagań Zamawiającego. W przypadku zajścia konieczności wykonania zmian lub innych czynności niż te, które zostały opisane w Protokole Uzgodnień, należy utworzyć nowy Protokół Uzgodnień zawierający te zmiany. W Protokole Uzgodnień można zamieścić inne uzgodnienia, niezwiązane z wymaganiami projektu, tj. ustalenia organizacyjne.
22. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
23. **Godziny Robocze** – godziny od 7:30 do 14:30 w każdym Dniu Roboczym.
24. **Czas Reakcji** – okres liczony od zaewidencjonowania Zgłoszenia Serwisowego do zmiany jego statusu na zarejestrowane.
25. **Czas Naprawy** - czas pomiędzy Zgłoszeniem Serwisowym a usunięciem/rozwiązaniem przyczyny jego zgłoszenia.
26. **Kierownik Zamawiającego** – osoba wyznaczona przez Zamawiającego, koordynująca całość przedmiotu danego pakietu, posiadająca odpowiednie pełnomocnictwa. W szczególności odpowiedzialna ze strony Zamawiającego za realizację przedmiotu zamówienia.
27. **Kierownik Wykonawcy** - osoba wyznaczona przez Wykonawcę do koordynacji realizacji prac danego zadania. Upoważniona do podpisywania Dokumentacji Projektu z ramienia Wykonawcy.
28. **HelpDesk (HD)** – narzędzie posiadające interfejs WWW służące do rejestracji zgłoszeń (potencjalnych problemów, usterek) oraz kontroli ich cyklu życia (tzw. Issue Tracking System lub Defect Tracking System). System HD udostępniony zostanie przez Wykonawcę dla Zamawiającego na czas realizacji przedmiotu zamówienia oraz w okresie jego gwarancji.

OPIS RÓWNOWAŻNOŚCI:

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy Pzp, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.

Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego.

Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ
Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.
Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.

DOSTAWA INFRASTRUKTURY OPROGRAMOWANIA

Przedmiotem zamówienia jest oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w SPZOZ w Sulęcinie .
Poniżej wyspecyfikowano minimalne oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.
Wymagania ogólne:

- Całość dostarczanego oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
- Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).
- Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:
    - posiadane środowisko domenowe,
    - posiadaną konfigurację sieci wraz z jednostkami podległymi,
    - posiadaną konfiguracją baz danych i backupów,
    - konfigurację stacji roboczych.

Opis parametrów minimalnych oprogramowania:
Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:

1. SYSTEM SIEM
Minimalne parametry techniczne
Użytkownicy: 1. Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. 2. Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.

Analiza logów systemowych:
1. Monitorowanie plików konfiguracyjnych
2. Skanowanie integralności plików
3. Analiza integralności rejestru
4. Analiza logów aplikacji systemowych
5. Analiza logów aplikacji internetowych
6. Analiza logów aplikacji na poziomie użytkownika
7. Analiza logów związanych z bazami danych
8. Analiza logów związanych z sieciami VPN
9. Analiza logów związanych z kontami użytkowników
10. Analiza logów związanych z kontami serwisowymi
11. Analiza logów związanych z kontami administratorów

Detekcja ataków i zagrożeń:
1. Wykrywanie prób włamania się (brute-force)
2. Wykrywanie prób ataku typu Man-in-the-Middle
3. Wykrywanie prób zmiany lub ataku na pliki systemowe
4. Wykrywanie prób wykorzystania podatności
5. Wykrywanie prób ataku typu SQL injection
6. Wykrywanie prób ataku typu Cross-Site Scripting (XSS)
7. Wykrywanie prób ataku typu zero-day
8. Wykrywanie prób ataku typu buffer overflow
9. Wykrywanie prób ataku typu DNS poisoning
10. Wykrywanie prób ataku typu DDoS (Denial-of-Service)

Zbieranie logów z wielu źródeł:
1. Zbieranie danych z systemów kontenerowych
2. Zbieranie danych z systemów wirtualizacji
3. Zbieranie danych z systemów kontroli wersji
4. Zbieranie danych z systemów monitorowania chmury
5. Zbieranie danych z systemów wirtualizacji
6. Zbieranie danych z systemów kontroli wersji
7. Zbieranie danych z platform IoT
8. Zbieranie danych z urządzeń mobilnych
9. Zbieranie danych z platform wirtualizacyjnych
10. Zbieranie danych z platform chmurowych

Monitorowanie aktywności użytkowników:
1. Monitorowanie aktywności użytkowników
2. Monitorowanie aktywności administratorów
3. Monitorowanie aktywności na poziomie portów i usług
4. Monitorowanie aktywności na poziomie interfejsów
5. Monitorowanie aktywności na poziomie protokołów

Monitorowanie urządzeń sieciowych:
1. Monitorowanie aktywności na poziomie protokołów sieciowych
2. Monitorowanie aktywności na poziomie protokołów aplikacji
3. Monitorowanie aktywności na poziomie protokołów transportowych
4. Monitorowanie aktywności na poziomie protokołów internetowych
5. Monitorowanie aktywności na poziomie protokołów telekomunikacyjnych

Integracja z systemami monitorowania:
1. Integracja z systemami monitorowania logów
2. Integracja z systemami monitorowania zachowań użytkowników
3. Integracja z systemami monitorowania aplikacji
4. Integracja z systemami monitorowania chmury
5. Integracja z systemami monitorowania IoT

Zdalne monitorowanie agentów:
1. Zdalne monitorowanie agentów w różnych środowiskach
2. Zdalne monitorowanie agentów na platformach IoT
3. Zdalne monitorowanie agentów w chmurze

Wykrywanie nieautoryzowanego dostępu:
1. Wykrywanie prób nieautoryzowanego dostępu
2. Wykrywanie prób podmiany binarnych
3. Wykrywanie prób podmiany tokenów uwierzytelniania
4. Wykrywanie prób podważenia integralności plików

Ostrzeganie przed atakami:
1. Ostrzeganie przed próbami włamania się na konta

2. Ostrzeganie przed próbami łamania haseł metodą bruteforce
3. Ostrzeganie przed próbami ataku typu SQL tampering
4. Ostrzeganie przed próbami ataku typu formjacking
5. Ostrzeganie przed próbami ataku typu clickjacking
6. Ostrzeganie przed próbami ataku typu formjacking
7. Ostrzeganie przed próbami ataku typu clickjacking
8. Ostrzeganie przed próbami ataku typu domain hijacking
9. Ostrzeganie przed próbami ataku typu URL poisoning
10. Ostrzeganie przed próbami ataku typu click injection
11. Ostrzeganie przed próbami ataku typu smart meter tampering
12. Ostrzeganie przed próbami ataku typu driverless car hacking
13. Ostrzeganie przed wykrytymi próbami ataku typu watering hole
14. Ostrzeganie przed wykrytymi próbami ataku typu zero-click exploit

Integracja z różnymi systemami:

1. Integracja z rozwiązaniami do zarządzania incydentami
2. Integracja z narzędziami do analizy ruchu sieciowego
3. Integracja z narzędziami do analizy zachowań malware'u
4. Integracja z narzędziami do analizy zachowań użytkowników
5. Integracja z narzędziami do analizy danych z urządzeń IoT
6. Integracja z narzędziami do analizy zachowań aplikacji
7. Integracja z narzędziami do analizy zachowań użytkowników na platformach chmurowych
8. Integracja z narzędziami do analizy zachowań użytkowników na platformach mobilnych
9. Integracja z narzędziami do analizy zachowań użytkowników na platformach IoT
10. Integracja z narzędziami do analizy zachowań użytkowników na platformach wirtualizacyjnych
11. Integracja z narzędziami do analizy zachowań użytkowników na platformach przemysłowych (OT)
12. Integracja z narzędziami do analizy zachowań użytkowników na platformach z systemami wbudowanymi
13. Integracja z narzędziami do analizy zachowań użytkowników na platformach autonomicznych pojazdów (AV)

Monitorowanie aktywności sieciowej:

1. Monitorowanie ruchu sieciowego
2. Monitorowanie aktywności na poziomie jądra systemu
3. Monitorowanie dostępów SSH
4. Monitorowanie aktywności sieciowych na poziomie interfejsów
5. Monitorowanie aktywności na poziomie protokołów
6. Monitorowanie aktywności na poziomie protokołu SMB/CIFS
7. Monitorowanie aktywności na poziomie protokołu RDP
8. Monitorowanie aktywności na poziomie protokołu POP3/IMAP
9. Monitorowanie aktywności na poziomie protokołu SMTP
10. Monitorowanie aktywności na poziomie protokołu DNS over HTTPS (DoH)
11. Monitorowanie aktywności na poziomie protokołu iSCSI (Internet Small Computer System Interface)
12. Monitorowanie aktywności na poziomie protokołu UPnP (Universal Plug and Play)
13. Monitorowanie aktywności na poziomie protokołu SIP-TLS (Session Initiation Protocol over Transport Layer Security)
14. Monitorowanie aktywności na poziomie protokołu DNS over HTTPS (DoH)
15. Monitorowanie aktywności na poziomie protokołu ICMPv6 (Internet Control Message Protocol version 6)
16. Monitorowanie aktywności na poziomie protokołu LLDP (Link Layer Discovery Protocol)
17. Monitorowanie aktywności na poziomie protokołu DHCP (Dynamic Host Configuration Protocol)
18. Monitorowanie aktywności na poziomie protokołu IGMP (Internet Group Management Protocol)
19. Monitorowanie aktywności na poziomie protokołu SCTP (Stream Control Transmission Protocol)
20. Monitorowanie aktywności na poziomie protokołu Thread (IPv6-based mesh networking protocol)
21. Monitorowanie aktywności na poziomie protokołu IPv6 over IPv4 tunneling
22. Monitorowanie aktywności na poziomie protokołu IP-in-IP (IP encapsulation)
23. Monitorowanie aktywności na poziomie protokołu SRTP (Secure Real-time Transport Protocol)
24. Monitorowanie aktywności na poziomie protokołu SAML (Security Assertion Markup Language)

Reagowanie na ataki:

1. Reagowanie na ataki w czasie rzeczywistym
2. Reagowanie na zablokowany dostęp do zasobów
3. Reagowanie na niepowodzenia uwierzytelniania
4. Reagowanie na zmiany uprawnień plików
5. Reagowanie na podejrzane aktywności na kontach użytkowników
6. Reagowanie na wykryte ataki typu phishing

7. Reagowanie na próby ataku typu Man-in-the-Middle
8. Reagowanie na próby manipulacji tokenami uwierzytelniania
9. Reagowanie na zmiany w konfiguracji firewalla
10. Reagowanie na podejrzane aktywności administratorów
11. Reagowanie na próby manipulacji logami zdarzeń
12. Reagowanie na wykryte próby ataku typu ransomware
13. Reagowanie na wykryte próby ataku typu drive-by download
14. Reagowanie na próby ataku typu cryptojacking
15. Reagowanie na wykryte próby ataku typu eavesdropping
16. Reagowanie na wykryte próby ataku typu steganografia
17. Reagowanie na wykryte próby ataku typu biometric data theft
18. Reagowanie na wykryte próby ataku typu data manipulation
19. Reagowanie na wykryte próby ataku typu supply chain attack
20. Reagowanie na wykryte próby ataku typu DNS poisoning
21. Reagowanie na próby ataku typu DDoS (Distributed Denial of Service)
22. Reagowanie na próby ataku typu DoS (Denial of Service)

Wsparcie dla jednostek służby zdrowia:

1. Monitorowanie logów aplikacji medycznych: System SIEM może analizować logi z aplikacji medycznych, bazy danych i systemów informatycznych w jednostkach służby zdrowia. Pozwala to na wykrywanie nieprawidłowych aktywności, prób nieautoryzowanego dostępu i innych zagrożeń.
2. Detekcja ataków na systemy IT: System SIEM oferuje zaawansowane mechanizmy detekcji intruzów, które pozwalają na wykrywanie zaawansowanych ataków, prób wykorzystania luk w zabezpieczeniach i innych zagrożeń.
3. Monitorowanie integralności plików: System SIEM pozwala na monitorowanie zmian w plikach systemowych, co może być istotne dla ochrony danych medycznych i zapobiegania nieautoryzowanym zmianom.
4. Wdrażanie polityk bezpieczeństwa: System SIEM umożliwia definiowanie i egzekwowanie polityk bezpieczeństwa w organizacji, co pozwala na utrzymanie odpowiedniego poziomu bezpieczeństwa.
5. Analiza ruchu sieciowego: System SIEM oferuje funkcje analizy ruchu sieciowego, dzięki czemu można wykrywać podejrzane aktywności i ataki, takie jak próby skanowania portów czy ataki DDoS.
6. Reagowanie na incydenty: System SIEM pozwala na definiowanie planów reagowania na różne typy incydentów, dzięki czemu personel odpowiedzialny za bezpieczeństwo może skutecznie reagować na zagrożenia.
7. Powiadomienia i alerty: System SIEM generuje alerty w czasie rzeczywistym, informując personel o potencjalnych zagrożeniach. Możliwe jest również konfigurowanie powiadomień e-mail lub SMS
8. Monitorowanie logów medycznych: System SIEM może analizować logi z systemów klasy HIS (Hospital Information System), RIS (Radiology Information System) i PASC (Picture Archiving and Communication System) używanych w środowisku medycznym.
9. Wykrywanie naruszeń związanych z danymi pacjentów: Dzięki analizie logów medycznych, System SIEM może wykryć próby nieautoryzowanego dostępu do danych pacjentów, zmiany w medycznych zapisach pacjentów lub próby wykradzenia danych medycznych.
10. Ochrona danych medycznych: System SIEM umożliwia monitorowanie integralności i poufności danych medycznych, co pozwala na reagowanie na zagrożenia związane z ochroną danych medycznych i zapewnienie zgodności z przepisami regulującymi ochronę danych w sferze medycyny.
11. System monitoruje krytyczne elementy systemu HIS:
    - Komunikacja z platformą P1
    - Komunikacji bramek HL7
    - Komunikacja EWUŚ
    - Komunikacja KOWAL
    - Komunikacja AP-KOLCE
    - Funkcjonowanie Rejestru Zdarzeń Medycznych
    - Baza danych systemu HIS

Tworzenie reguł korelacji:

1. Możliwość definiowania reguł korelacji, które określają, jakie zdarzenia i logi mają być analizowane oraz w jaki sposób powiązywane, aby wykrywać zaawansowane zagrożenia i ataki.
2. Korelacja zdarzeń w czasie rzeczywistym: Silnik korelacji System SIEM działa w czasie rzeczywistym, co pozwala na wykrywanie ataków i zagrożeń w czasie rzeczywistym.
3. Korelacja wielu zdarzeń: Możliwość powiązania wielu zdarzeń i logów w celu identyfikacji bardziej złożonych aktywności i etapów ataków, które mogą obejmować różne komponenty infrastruktury.
4. Wykorzystywanie bazy wiedzy: Silnik korelacji wykorzystuje bazę wiedzy zawierającą informacje o znanych zagrożeniach i atakach, co pozwala na lepsze wykrywanie i identyfikację nowych incydentów.
5. Wykrywanie anomalii: Silnik korelacji może identyfikować anomalie w zachowaniach użytkowników, aplikacji i systemów, co może wskazywać na nieautoryzowany dostęp lub działania.

6. Wykorzystywanie heurystyk: Silnik korelacji System SIEM wykorzystuje zaawansowane heurystyki, aby identyfikować podejrzane aktywności i zachowania, nawet jeśli nie są to znane zagrożenia.
7. Personalizacja reguł i zapytań: Administratorzy mogą dostosowywać istniejące reguły i zapytania korelacji lub tworzyć własne, dopasowane do konkretnych potrzeb i wymagań organizacji.
8. Integracja z innymi źródłami danych: Możliwość integracji z dodatkowymi źródłami logów, co pozwala na analizę danych z różnych systemów i aplikacji, w tym również urządzeń IoT.
9. Generowanie alertów: Silnik korelacji może generować alerty i powiadomienia w czasie rzeczywistym, co pozwala na szybką reakcję na incydenty.
10. Raportowanie i analiza: Możliwość generowania raportów i analizy wykrytych zagrożeń oraz aktywności, co pozwala na lepsze zrozumienie sytuacji bezpieczeństwa i podejmowanie odpowiednich działań.
11. Ustalanie priorytetów: Możliwość przypisania priorytetów wykrytym incydentom na podstawie stopnia zagrożenia i znaczenia dla organizacji.
12. Uczenie maszynowe: Integracja z technologią uczenia maszynowego, która pozwala na automatyczną analizę danych i identyfikację nowych wzorców zachowań.
13. Korelacja zdarzeń między hostami: Możliwość powiązywania zdarzeń między różnymi hostami w celu wykrywania ataków na poziomie infrastruktury.
14. Filtracja zdarzeń: Możliwość definiowania reguł i filtrów, które pozwalają na wykluczenie zdarzeń bezpiecznych i skupienie się na tych bardziej podejrzanych.
15. Wielopoziomowa analiza: Możliwość przeprowadzania analizy na różnych poziomach infrastruktury, takich jak warstwa aplikacji, systemu operacyjnego, a także warstwa sieciowa.
16. Korelacja geolokacji: Możliwość powiązania zdarzeń z geolokacją, co pozwala na wykrywanie podejrzanych aktywności z różnych lokalizacji geograficznych.
17. Wsparcie dla różnych formatów logów: Silnik korelacji obsługuje różne formaty logów, co pozwala na integrację z wieloma aplikacjami i urządzeniami.
18. Detekcja ataków z wykorzystaniem wielu etapów: Możliwość wykrywania zaawansowanych ataków, które obejmują wiele etapów i etapów przeprowadzenia ataku.
19. Skalowalność: Silnik korelacji System SIEM jest skalowalny, co pozwala na analizę dużych ilości danych w środowiskach o dużej infrastrukturze.
20. Integracja z narzędziami SIEM: Możliwość integracji silnika korelacji System SIEM z innymi narzędziami SIEM, co pozwala na kompleksowe zarządzanie bezpieczeństwem i analizę zagrożeń.

Raportowanie:

1. Raporty na żądanie: Możliwość generowania raportów w czasie rzeczywistym na żądanie użytkownika w oparciu o określone zapytania i dane logów.
2. Automatyczne generowanie raportów: Możliwość zaplanowania i automatycznego generowania raportów na określone interwały czasowe, co pozwala na regularne monitorowanie i analizę aktywności.
3. Wybór zakresu czasowego: Możliwość wyboru zakresu czasowego dla raportu, aby skupić się na określonym przedziale czasowym.
4. Analiza zdarzeń bezpieczeństwa: Raportowanie i analiza zdarzeń bezpieczeństwa, które pozwalają na identyfikację podejrzanych aktywności, prób ataków i incydentów.
5. Wykrywanie anomalii: Raportowanie wykrytych anomalii w zachowaniach użytkowników, aplikacji czy systemów, co może wskazywać na nieprawidłowe lub nieautoryzowane działania.
6. Raporty o wydajności: Możliwość generowania raportów dotyczących wydajności i dostępności infrastruktury, które pozwalają na monitorowanie stanu systemów i urządzeń.
7. Raporty o atakach DDoS: Raportowanie prób ataków typu Distributed Denial of Service (DDoS) w celu zrozumienia potencjalnych ataków na infrastrukturę.
8. Raporty o próbach ataków brute-force: Generowanie raportów o próbach ataków brute-force na konta użytkowników czy aplikacje, które mogą wskazywać na próby złamania haseł.
9. Raporty o próbach ataków XSS i SQL injection: Raportowanie prób ataków typu Cross-Site Scripting (XSS) i SQL Injection, które mogą stanowić zagrożenie dla aplikacji webowych.
10. Raporty o próbach ataków RCE: Generowanie raportów o próbach ataków typu Remote Code Execution (RCE), które pozwalają na zdalne wykonanie kodu na systemie.
11. Personalizacja raportów: Możliwość personalizacji raportów, aby uwzględnić specyficzne wymagania i potrzeby organizacji.
12. Raportowanie na różnych poziomach: Możliwość generowania raportów na różnych poziomach abstrakcji, takich jak raporty ogólne, raporty szczegółowe czy raporty na poziomie hosta czy użytkownika.
13. Formatowanie raportów: Możliwość formatowania raportów, aby były czytelne i czytelnie przedstawiały wyniki analiz.
14. Raporty o zgodności: Generowanie raportów o zgodności z różnymi standardami i regulacjami dotyczącymi bezpieczeństwa, takimi jak GDPR, HIPAA, czy PCI-DSS.

15. Eksport danych: Możliwość eksportu danych z raportów do różnych formatów, takich jak PDF, CSV czy HTML.
16. Raporty na poziomie zarządczym: Możliwość generowania raportów na poziomie zarządczym, które pozwalają na przedstawienie kluczowych wskaźników i wyników dla kierownictwa.
17. Wykresy i diagramy: Możliwość przedstawienia wyników raportów za pomocą wykresów i diagramów, co ułatwia wizualizację danych i analizę trendów.
18. Raporty o monitorowaniu aktywności użytkowników: Generowanie raportów o aktywnościach użytkowników, co pozwala na kontrolę i audyt działań użytkowników.
19. Zautomatyzowane generowanie raportów bezpieczeństwa: Możliwość zautomatyzowanego generowania raportów dotyczących bezpieczeństwa w celu przestrzegania wymogów regulacji i standardów.

Aktywny parser logów z rożnych systemów :

1. Zbieranie logów w czasie rzeczywistym: System SIEM posiada agenty logowania (System SIEM Agents), które mogą zbierać logi z różnych systemów i aplikacji. Te agenty mogą działać w czasie rzeczywistym, pozwalając na monitorowanie aktywności na bieżąco.
2. Normalizacja logów: System SIEM normalizuje logi z różnych źródeł do jednolitego formatu, co ułatwia analizę i detekcję zagrożeń. Dzięki temu, nawet jeśli logi pochodzą z różnych systemów i mają różne formaty, System SIEM pozwala na ich spójną analizę.
3. Wykorzystanie reguł i detekcja w czasie rzeczywistym: System SIEM pozwala na konfigurację zaawansowanych reguł detekcji, które pozwalają na identyfikację niebezpiecznych aktywności w czasie rzeczywistym. Kiedy zdarzenie spełnia kryteria reguły, System SIEM generuje alert, który może być natychmiastowo obsłużony przez personel bezpieczeństwa.
4. Integracja z Elastic Stack: System SIEM można zintegrować z Elastic Stack, co pozwala na zaawansowaną analizę logów przy użyciu narzędzi takich jak Elasticsearch, Logstash i Kibana. Elastic Stack jest w stanie przetwarzać ogromne ilości logów w czasie rzeczywistym i umożliwia zaawansowane filtrowanie, sortowanie i analizę danych.
5. Skalowalność: System SIEM jest skalowalne, co oznacza, że można go rozbudować, aby obsługiwać duże ilości logów z różnych źródeł w czasie rzeczywistym.

Poczta elektroniczna:

1. Analiza logów serwera poczty elektronicznej: System SIEM jest w stanie monitorować logi generowane przez serwery pocztowe, takie jak Microsoft Exchange, Postfix, czy Sendmail. Dzięki temu możliwe jest wykrycie podejrzanych aktywności, takich jak próby nieudanych logowań, wysyłania dużej ilości e-maili w krótkim czasie (możliwe znaki kompromitacji konta), czy ataki typu "brute-force" mające na celu przejęcie konta pocztowego.
2. Wykrywanie prób phishingu: System SIEM może analizować zawartość e-maili i załączników w poszukiwaniu potencjalnie szkodliwych linków, które mogą prowadzić do stron phishingowych. Jeśli wykryte zostaną podejrzane adresy URL, System SIEM może generować alert, umożliwiając administratorowi podjęcie odpowiednich działań.
3. Monitorowanie zmian konfiguracji: System SIEM pozwala monitorować zmiany w konfiguracji serwera poczty elektronicznej. W przypadku nieautoryzowanych zmian, takich jak dodawanie nowych kont użytkowników lub zmiana ustawień przekierowań, System SIEM może wygenerować alert, informując o potencjalnym naruszeniu bezpieczeństwa.

Sandbox:

1. Analiza zachowania plików: System SIEM może integrować się z rozwiązaniami do analizy zachowania plików w sandboxie. Po uruchomieniu podejrzanego pliku w bezpiecznym środowisku, dane z analizy w sandboxie są przesyłane do System SIEM w celu identyfikacji podejrzanych aktywności.
2. Wykrywanie zaawansowanych zagrożeń: Dzięki analizie zachowania plików, System SIEM może wykryć nowe, nieznane wcześniej zagrożenia, które omijają tradycyjne metody wykrywania, takie jak sygnatury antywirusowe.

Skanery podatności:

1. Integracja z narzędziami do skanowania podatności: System SIEM może integrować się z różnymi narzędziami do skanowania podatności, takimi jak Nessus czy OpenVAS. Po przeprowadzeniu skanowania podatności, wyniki są przesyłane do System SIEM w celu analizy i identyfikacji słabych punktów w infrastrukturze.
2. Wykrywanie zagrożeń wynikających z podatności: System SIEM może analizować wyniki skanowania podatności w celu identyfikacji potencjalnych zagrożeń i generowania alertów w przypadku wystąpienia znanych podatności, które mogą być wykorzystane przez atakujących.

Możliwe działania proaktywne w ramach SIEM (na podstawie dodatkowych zamówień):

1. Wykonywanie skanów podatności
2. Stałe aktualizacje zabezpieczeń i łatek oprogramowania
3. Wdrażanie mechanizmów zwiększających odporność na ataki
4. Edukacja użytkowników w zakresie bezpieczeństwa informatycznego
5. Analiza trendów i nowych zagrożeń w cyberprzestrzeni

6. Wdrażanie technologii zwiększających wykrywalność ataków
7. Ocena ryzyka i zarządzanie bezpieczeństwem informacji
8. Tworzenie planów reagowania na incydenty i awarie
9. Wdrażanie polityk bezpieczeństwa w organizacji
10. Monitorowanie mediów społecznościowych pod kątem zagrożeń
11. Współpraca z innymi organizacjami w celu wymiany informacji o zagrożeniach
12. Tworzenie świadomości kultury bezpieczeństwa w całej organizacji
13. Opracowanie strategii audytów bezpieczeństwa i weryfikacji zgodności
14. Zarządzanie i zapewnienie bezpieczeństwa informacji to proces ciągły, który wymaga podejmowania działań zarówno reaktywnych, jak i proaktywnych. Wszystkie te obszary funkcjonalne wspólnie tworzą całościowe podejście do zapobiegania incydentom bezpieczeństwa i minimalizowania ryzyka wystąpienia zagrożeń w środowisku informatycznym.

Gwarancja i serwis

1. Oprogramowanie ma być objęte minimum 12 miesięcznym gwarancją (kryterium oceny oferty) dla wszystkich funkcji.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
3. Aktualizacje dostarczonego Systemu SIEM do nowych wersji oprogramowania.
4. Szkolenia administratorów on-line z nowych funkcjonalności,
5. Usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem, bieżące aktualizacje dokumentacji technicznej dla Systemu,
6. Przyjmowania zgłoszeń serwisowych przez dedykowany serwisowy moduł internetowy oraz mail 24/7
7. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24 /7/365, zgodnie z określonymi poniżej warunkami SLA
8. Zgłoszenia i Incydenty są klasyfikowane na podstawie potencjalnego wpływu na Klienta. wykorzystywane są 4 poziomy klasyfikacji, jak przedstawiono w poniższej tabeli:

Poziom	Opis	Zagrożenie	Przykład
Krytyczny	Niezbędne natychmiastowe działanie	– Przerwa w działaniu serwera/systemu	Wyciek danych
	złagodzić obecne złośliwe oprogramowanie	– Brak odbioru danych z lokalizacja klienta	
	Działalność		
3	Wysokie prawdopodobieństwo incydentu, jeśli	– Znaczące zmiany w SIEM	Brak potwierdzenia
	nie podejmuje się działań zapobiegawczych	– wskazanie natężenia ruchu danych obniżona wydajność potencjał	
2	Niski potencjalny incydent	– Użytkownik nie zaktualizował hasła w wymaganym odstępie czasu	Znaleziony wirus na stacji roboczej
1	Aktywności utrzymaniowe lub informacyjne	-	Raport

w oparciu o klasyfikację i rodzaj zdarzenia/zgłoszenia wsparcie reaguje zgodnie z poniższymi interwałami.

Poziom	Opis	Zagrożenie	SLA
Krytyczny	1 godzina	1 godzina	96%
3	24 godziny	2 godziny	96%
2	72 godziny	8 godzin	96%
1	5 dni	24 godzin	96%

Dodatkowe wymagania:

1. Producent Systemu SIEM musi posiadać certyfikacje w zakresie: ŚWIADCZENIA USŁUGI SECURITY OPERATION CENTER - REAGOWANIE NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA, zgodnie z normą ISO ISO/IEC 27001:2017 – załączyć do oferty.
2. W celu zabezpieczenia danych krytycznych przetwarzanych w systemie HIS Zamawiającego (system Eskulap, którego producentem jest Nexus Polska Sp. z o.o.), Wykonawca zobowiązany jest dołączyć do oferty potwierdzenie, że posiada uprawnienia lub autoryzację Nexus Polska lub zrealizuje przedmiot zamówienia w obszarze dotyczącym ingerencji w dane przetwarzane przez system Eskulap, nie naruszając postanowień licencyjnych i gwarancyjnych dla systemu medycznego Eskulap i będzie gwarantował jego poprawne monitorowanie po zakończeniu prac integracyjnych – załączyć do oferty.

<u>System EDR – 50 stanowisk (rozbudowa posiadanego systemu EDR ESET do 200 stanowisk).</u> **Wymagane minimalne parametry techniczne**	
Ochrona stacji roboczych – Windows	
1.	▪ Rozwiązanie musi wspierać systemy operacyjne Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11. ▪ Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. ▪ Rozwiązanie musi wspierać architekturę ARM64. ▪ Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. ▪ Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. ▪ Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim. ▪ Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives.
Ochrona antywirusowa i antyspyware	
1.	▪ Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. ▪ Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. ▪ Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. ▪ Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. ▪ Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. ▪ Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. ▪ 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. ▪ 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). ▪ Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. ▪ Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. ▪ Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. ▪ Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. ▪ Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. ▪ Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. ▪ Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. ▪ Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. ▪ Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.

	▪ W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. ▪ Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. ▪ 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. ▪ Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. ▪ Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. ▪ 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). ▪ Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. ▪ Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. ▪ Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. ▪ 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. ▪ Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. ▪ Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. ▪ Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. ▪ Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. ▪ Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. ▪ Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego. ▪ Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. ▪ Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. ▪ Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. ▪ 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. ▪ 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. ▪ 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. ▪ Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. ▪ Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. ▪ Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik

	przy próbie dostępu do konfiguracji, był proszony o jego podanie. ▪ 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. ▪ Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. ▪ Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. ▪ 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. ▪ 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. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. ▪ 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. ▪ 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. ▪ Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. ▪ 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. ▪ Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. ▪ W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. ▪ Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika. ▪ Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). ▪ 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. ▪ Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. ▪ Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. ▪ Rozwiązanie musi posiadać zaawansowany skaner pamięci. ▪ Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.

	▪ 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. ▪ 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. ▪ Rozwiązanie musi posiadać posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. ▪ Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. ▪ 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. ▪ Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji. ▪ Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. ▪ Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. ▪ Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). ▪ Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). ▪ Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. ▪ W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania. ▪ Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. ▪ Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń. ▪ Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. ▪ 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. ▪ Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie. ▪ 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. ▪ W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. ▪ Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej. ▪ Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. ▪ Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. ▪ Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. ▪ Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. ▪ 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. ▪ Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.

	▪ Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. ▪ Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. ▪ Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia. ▪ Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. ▪ Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. ▪ Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść". ▪ Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. ▪ Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. ▪ Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. ▪ Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. ▪ Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet. ▪ Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB. ▪ Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. ▪ Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
Ochrona przed spamem	
1.	▪ Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. ▪ Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. ▪ Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. ▪ Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego. ▪ Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego. ▪ Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam. ▪ Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam. ▪ Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook. ▪ Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana" ▪ Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana". ▪ Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
Zapora osobista (personal firewall)	
1.	▪ 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. ▪ Rozwiązanie musi oceniać reguły zapory systemu Windows. ▪ Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych. ▪ Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie. ▪ 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. ▪ Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj. ▪ Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji. ▪ 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. ▪ Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu. ▪ Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. ▪ Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. ▪ Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. ▪ 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. ▪ 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. ▪ 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. ▪ 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	
1.	▪ Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. ▪ Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. ▪ Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. ▪ 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. ▪ Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych. ▪ Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta. ▪ Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. ▪ Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.

	▪ Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.
Bezpieczna przeglądarka	
1.	▪ Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. ▪ Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. ▪ Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki. ▪ Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. ▪ Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki. ▪ Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
Ochrona serwera Windows	
1.	▪ Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2008 R2 i nowszych. ▪ Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. ▪ Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. ▪ Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. ▪ Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. ▪ Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. ▪ Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. ▪ Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu. ▪ 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). ▪ Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. ▪ Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. ▪ Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. ▪ Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. ▪ Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. ▪ Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. ▪ Rozwiązanie musi wspierać mechanizm klastrowania. ▪ Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). ▪ 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. ▪ Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. ▪ Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. ▪ Rozwiązanie musi posiadać zaawansowany skaner pamięci. ▪ Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. ▪ Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS. ▪ Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze. ▪ 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. ▪ 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. ▪ Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. ▪ 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. ▪ Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. ▪ Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. ▪ W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. ▪ Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. ▪ Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. ▪ Dodanie automatycznych wyłączeń nie wymaga restartu serwera. ▪ Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. ▪ Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. ▪ Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. ▪ Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). ▪ 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. ▪ 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. ▪ 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. ▪ 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. ▪ Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. ▪ Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium

	producenta. ▪ W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. ▪ 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. ▪ Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. ▪ Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji. ▪ 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. ▪ 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. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. ▪ 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. ▪ 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. ▪ 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. ▪ Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. ▪ 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. ▪ Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. ▪ Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. ▪ Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. ▪ Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). ▪ Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). ▪ Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. ▪ Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. ▪ Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania. ▪ Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”. ▪ Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. ▪ Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia. ▪ Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci

	oraz wykrywaniem aktywności wirusów sieciowych. ▪ Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. ▪ Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet. ▪ Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. ▪ 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. ▪ Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. ▪ Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. ▪ Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. ▪ Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
Administracja zdalna	
1.	▪ Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux. ▪ Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD. ▪ Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. ▪ Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. ▪ Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. ▪ Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. ▪ Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy. ▪ Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6. ▪ Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs. ▪ Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji. ▪ Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. ▪ Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym. ▪ Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. ▪ Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. ▪ Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. ▪ Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image". ▪ Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów. ▪ Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy. ▪ Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. ▪ Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. ▪ Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS. ▪ Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak:

	ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11. ▪ Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap. ▪ Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych. ▪ Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów. ▪ Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. ▪ Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android. ▪ Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS. ▪ 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. ▪ Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. ▪ Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające. ▪ 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. ▪ Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. ▪ Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny. ▪ W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play. ▪ 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. ▪ Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego. ▪ Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi. ▪ Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. ▪ Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. ▪ Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. ▪ Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany. ▪ Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera

	muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. ▪ 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. ▪ Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych. ▪ Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. ▪ Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej. ▪ 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. ▪ Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. ▪ 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. ▪ Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania. ▪ Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. ▪ Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta. ▪ Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej. ▪ Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji. ▪ Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce. ▪ Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta. ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów. ▪ Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie. ▪ Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy. ▪ Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania. ▪ Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. ▪ Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny. ▪ 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 lub CSV. ▪ Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów. ▪ Powiadomienia mailowe mają być wysyłane w formacie HTML. ▪ Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń. ▪ Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. ▪ Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień

	występujących w zadanym przez administratora okresie czasu. ▪ Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji. ▪ Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami. ▪ Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych. ▪ W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu. ▪ Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. ▪ Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan. ▪ Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. ▪ Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli. ▪ 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. ▪ Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta. ▪ Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli. ▪ Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania. ▪ Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie. ▪ Konsola administracyjna musi umożliwiać personalizację interfejsu webowego. ▪ Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych. ▪ 9Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault). ▪ Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk. ▪ Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal). ▪ Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.
Sandbox w chmurze	
1.	▪ Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. ▪ Rozwiązanie musi wykorzystywać do działania chmurę producenta. ▪ 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. ▪ Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. ▪ Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. ▪ Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. ▪ Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. ▪ Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. ▪ Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

	▪ Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. ▪ 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. ▪ Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: – Czysty, – Podejrzany, – Bardzo podejrzany, – Szkodliwy. ▪ 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. ▪ 1W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
Endpoint Detection and Response	
	Serwer ▪ Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych. ▪ Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. ▪ System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. ▪ Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. ▪ Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. ▪ Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. ▪ Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. ▪ Wykluczenia muszą dotyczyć procesu lub procesu „rodzica". ▪ Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. ▪ Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. ▪ Serwer musi posiadać ponad 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. ▪ Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne. ▪ Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. ▪ Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali. ▪ Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na 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. ▪ Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. ▪ 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. ▪ W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. ▪ 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. ▪ Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy. ▪ 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. ▪ Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal). ▪ Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. ▪ Konsola administracyjna musi mieć możliwość tagowania obiektów. ▪ Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli. ▪ Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci. ▪ Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. ▪ Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł. **Agent** ▪ Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10 oraz Windows Server 2008/2012/2016/2019. ▪ Pełne wsparcie dla systemów macOS 10.12 i nowszych. ▪ Wsparcie dla 32 i 64-bitowej wersji systemu Windows. ▪ Agent musi współpracować z produktem antywirusowym tego samego producenta. ▪ Agent nie może działać bez produktu antywirusowego tego samego producenta. ▪ W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta. ▪ Połączenie agenta do serwera zarządzającego musi być szyfrowane. ▪ Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.

UWAGA: do oferty należy dołączyć materiały pozwalające Zamawiającemu zapoznać się z oferowanymi produktami.
Dokument należy uzupełnić, podpisać elektronicznie i załączyć do oferty.