

Zabrodzie, 20.05.2025r.

ZAPYTANIE OFERTOWE nr 8/SF/2025 NA ZAKUP OPROGRAMOWANIA

System wykrywania ataków i zagrożeń (XDR). Pełny monitoring sieci, threat hunting oraz automatyzacja działań w razie wykrycia zagrożenia

Oraz

System ochrony aplikacji Microsoft 365 przed szkodliwym oprogramowaniem, spamem i atakami phishingowymi, zarządzany za pomocą konsoli w chmurze

w ramach projektu:

„Budowa smart fabryki firmy DIJO III Sp. z o.o.”

Krajowy Plan Odbudowy i Zwiększania Odporności (KPO)

Komponent A „Odporność i konkurencyjność gospodarki”

Cel szczegółowy: A2. Rozwój narodowego systemu innowacji: wzmocnienie koordynacji, stymulowanie potencjału innowacyjnego oraz współpracy pomiędzy przedsiębiorstwami i organizacjami badawczymi, w tym w zakresie technologii środowiskowych

Reforma: A2.1. Przyspieszenie procesów robotyzacji i cyfryzacji i innowacji

Inwestycja: A2.1.1. Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach

1. Dane Zamawiającego:

Nazwa: DIJO III Sp. z o.o.

Adres: 52-327 Wrocław, Zabrodzie 28

NIP: 8961628212

2. Przedmiot zamówienia: Oprogramowanie – System DPL

Kod CPV:

48900000-7 · Różne pakiety oprogramowania i systemy komputerowe

Przedmiotem zamówienia jest: SYSTEM DLP - Data Loss Prevention

Aktualnie Zamawiający posiada licencję oprogramowania antywirusowego ESET Endpoint Security dla 220 urządzeń/użytkowników ważną do dnia 12.09.2025 r. Przedmiotem zamówienia jest rozbudowa oprogramowania do wersji ESET PROTECT Elite w okresie do dnia 12.09.2028r. obejmująca maksymalnie 230 użytkowników indywidualnych/urzędów lub dostawa równoważnej platformy bezpieczeństwa zgodnie z funkcjonalnymi kryteriami równoważności określonymi poniżej.

Ponadto zamawiający wymaga w przypadku dostarczenia oprogramowania przeprowadzenia autoryzowanego szkolenia dla dwóch osób z zespołu IT wskazanych przez zamawiającego

Minimalne wymagania (kryteria równoważności) określone dla równoważnej platformy zawiera załącznik nr 4

Jeżeli w opisie przedmiotu zamówienia lub załącznikach do zapytania ofertowego wskazano jakikolwiek znak towarowy, patent, rodzaj czy specyficzne pochodzenie, to należy przyjąć, że wskazane znaki towarowe, patenty, rodzaje czy pochodzenie określają parametry techniczne, eksploatacyjne, użytkowe i co oznacza,

że Zamawiający dopuszcza złożenie oferty w tej części przedmiotu zamówienia o równoważnych lub lepszych parametrach technicznych, eksploatacyjnych i użytkowych. Wszelkie wskazania określonego typu należy traktować jako przykładowe i pomocnicze.

Specyfikacja techniczna stanowi załącznik nr 4 do zapytania ofertowego.

3. Termin i miejsce realizacji zamówienia:

- Termin realizacji zamówienia : 30 dni od podpisania umowy z wykonawcą. Na etapie realizacji Umowy, Zamawiający dopuszcza zmianę wskazanego terminu, jednak z zastrzeżeniem wystąpienia uzasadnionych przyczyn, których nie dało się przewidzieć na etapie podpisywania Umowy, pomimo zachowania należytej staranności.

4. Opis warunków udziału w postępowaniu:

O realizację zamówienia mogą ubiegać się Oferenci spełniający łącznie następujące warunki:

- 1) **Posiadanie zdolności technicznej umożliwiającej realizację zamówienia:** Spełnienie warunku weryfikowane będzie na podstawie przedłożonych przez Oferenta dokumentów potwierdzających wykonanie co najmniej dwóch zamówień o podobnym charakterze – tzn. **dostawa na kwotę. min. 300 000,00 PLN netto** – w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie. Dokumentami potwierdzającymi wykonane dostawy mogą być referencje, protokoły odbioru lub inne dokumenty wystawione przez podmiot, na rzecz którego zamówienia były wykonywane, przy czym powinny one zawierać określenie przedmiotu umowy, datę wykonania i określenie podmiotu, na rzecz którego zostało ono wykonane wraz z informacją, czy zostały wykonane należyście.
- 2) Z udziału w postępowaniu wykluczone są podmioty powiązane osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru Oferenta, a Oferentem, polegające w szczególności na:
 - uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
 - posiadanie co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa);
 - pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
 - pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia;
 - pozostawanie z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.
- 3) Z udziału w postępowaniu wykluczone podmioty powiązane lub wspierające ze środków publicznych podmioty i osoby, które w bezpośredni lub pośredni sposób wspierają działania wojenne Federacji Rosyjskiej lub są za nie odpowiedzialne.

5. Kryteria i sposób oceny ofert:

Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga	Sposób oceny oferty
1.	Cena	100%	Całkowita cena Zamówienia netto (bez podatku VAT) tj. cena podana w ofercie winna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia oraz warunkami stawianymi przez Zamawiającego (w tym dostawę i uruchomienie)

Cena może być tylko jedna za cały zakres objęty przedmiotem zamówienia, nie dopuszcza się wariantowości cen. Podana cena będzie ceną ostateczną, jaką zapłaci Zamawiający. Cenę oferty należy podać w PLN, w EUR lub w USD (w przypadku ceny w EUR lub w USD przeliczenie na PLN nastąpi po średnim kursie NBP EUR lub USD na dzień porównania ofert). Maksymalna liczba punktów możliwych do uzyskania: 100 pkt. Za najkorzystniejszą zostanie uznana oferta, która spełni wszystkie wymagania i uzyska najwyższą ocenę.

6. Miejsce, termin i forma składania ofert

- Oferty należy złożyć w ciągu **7 dni kalendarzowych** od daty upublicznienia zapytania przez Zamawiającego, przy czym termin 7 dni kalendarzowych biegnie od dnia następnego po dniu upublicznienia zapytania ofertowego i kończy się z upływem ostatniego dnia, tj. **27.05.2025r. godz. 23.59** (decyduje moment wpływu oferty).
- Oferty złożone po wskazanym terminie nie będą rozpatrywane
- Oferty należy złożyć.
 - a) W systemie Baza Konkurencyjności.
- Oferta powinna zostać złożona na formularzu ofertowym stanowiącym Załącznik nr 1 do niniejszego zapytania. Należy do niej załączyć:
 - a) Oświadczenie o braku powiązań pomiędzy podmiotami współpracującymi – Załącznik nr 2 do zapytania ofertowego.
 - b) Oświadczenie o brak powiązań z Federacją Rosyjską – Załącznik nr 3 do zapytania ofertowego.
 - c) Dokumenty wymienione w punkcie 4.
 - d) Opis merytoryczny oferty umożliwiający ocenę rozwiązań proponowanych przez Oferenta, pod kątem ich zgodności z wymaganiami niniejszego Zapytania ofertowego. W przypadku wątpliwości lub braku opisów merytorycznych, Zamawiający zastrzega sobie prawo do przesłania dodatkowych pytań do Oferenta.
- Koszty przygotowania i dostarczenia Oferty pokrywa Oferent.

7. Wymagania odnośnie składanych ofert

- Nie dopuszcza się składania ofert częściowych;
- Minimalny termin ważności oferty: **60 dni** od dnia upływu terminu składania ofert;
- Oferta powinna zawierać:
 - Dane identyfikujące oferenta (adres, NIP lub równoważny nie obowiązujący w kraju, w którym podmiot jest zarejestrowany)
 - Imię i nazwisko oraz dane kontaktowe, telefon i adres e-mail, osoby wyznaczonej do kontaktów z Zamawiającym.
 - Datę sporządzenia oferty.
 - Termin ważności oferty.
 - Szczegółowy opis i specyfikację techniczną oferowanego przedmiotu zamówienia.
 - Odniesienie się do każdego z zamieszczonych w zapytaniu ofertowym kryteriów oceny oferty (cena, okres gwarancji).
 - Cenę całkowitą netto i brutto przedmiotu oferty.

- Podpis osoby upoważnionej do wystawienia oferty.
- Pieczęć firmową (jeśli podmiot posiada pieczęć).
- Dokumenty wymienione w pkt. 4 zapytania.

– Brak jakiegokolwiek z w/w elementów skutkuje odrzuceniem oferty.

8. Określenie warunków zmian umowy zawartej w wyniku przeprowadzonego postępowania

1. Zmiany istotnych warunków zawartej umowy można dokonać tylko i wyłącznie w przypadku:
 - 1) gdy możliwość zmiany została przewidziana w treści umowy;
 - 2) wystąpienia tzw. siły wyższej – jeżeli zamawiający działając z należytą starannością nie mógł przewidzieć zmian, a ich wartość nie przekracza 50% zamówienia.
2. Nie jest możliwe dokonywanie istotnych zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, chyba że:
 - 1) zmiany zostały przewidziane w umowie w postaci jasnych, precyzyjnych i jednoznacznych postanowień, które określają ich zakres i rodzaj oraz warunki wprowadzenia zmian;
 - 2) zmiany dotyczą realizacji dodatkowych dostaw, usług lub robót budowlanych od dotychczasowego wykonawcy, nieobjętych zamówieniem podstawowym, o ile stały się niezbędne i zostały spełnione łącznie następujące warunki:
 - a) zmiana wykonawcy nie może zostać dokonana z powodów ekonomicznych lub technicznych, w szczególności dotyczących zamienności lub interoperacyjności sprzętu, usług lub instalacji, zamówionych w ramach zamówienia podstawowego,
 - b) zmiana wykonawcy spowodowałaby istotną niedogodność lub znaczne zwiększenie kosztów dla Zamawiającego
 - c) wartość każdej kolejnej zmiany nie przekracza 50% wartości zamówienia określonej pierwotnie w umowie;
 - 3) zmiana nie prowadzi do zmiany charakteru umowy i zostały spełnione łącznie następujące warunki:
 - a) konieczność zmiany umowy spowodowana jest okolicznościami, których Zamawiający, działając z należytą starannością, nie mógł przewidzieć,
 - b) wartość zmiany nie przekracza 50% wartości zamówienia określonej pierwotnie w umowie;
 - 4) wykonawcę, któremu Zamawiający udzielił zamówienia, ma zastąpić nowy wykonawca:
 - a) na podstawie postanowień umownych,
 - b) w wyniku połączenia, podziału, przekształcenia, upadłości, restrukturyzacji lub nabycia dotychczasowego wykonawcy lub jego przedsiębiorstwa, o ile nowy wykonawca spełnia warunki udziału w postępowaniu o udzielenie zamówienia, nie zachodzą wobec niego podstawy wykluczenia oraz nie pociąga to za sobą innych istotnych zmian umowy,
 - c) w wyniku przejęcia przez OOW zobowiązań wykonawcy względem jego podwykonawców. W przypadku zmiany podwykonawcy, OOW może zawrzeć umowę z nowym podwykonawcą bez zmiany warunków realizacji zamówienia z uwzględnieniem dokonanych płatności z tytułu dotychczas zrealizowanych prac;
 - 5) zmiana nie prowadzi do zmiany ogólnego charakteru umowy i łączna wartość zamówienia jest mniejsza niż progi unijne oraz jest niższa niż 10% wartości pierwotnej umowy, w przypadku zamówień na usługi lub dostawy, albo 15%, w przypadku zamówień na roboty budowlane.

9. Pozostałe informacje

- Dodatkowych informacji oraz wyjaśnień związanych z niniejszym zapytaniem ofertowym udzielane są w module Pytania w bazie konkurencyjności – osoba do kontaktu: Pani Katarzyna Kulesza, email: tender@dijo.pl,
- Jeżeli Oferent, którego oferta została wybrana, będzie uchylał się od zawarcia umowy Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert i zwrócić się o

zawarcie umowy z kolejnym podmiotem na liście uszeregowanej według najwyższej liczby uzyskanych punktów.

- Oferty, które nie spełniają wymagań określonych w zapytaniu ofertowym nie będą rozpatrywane.
- Żadne dokumenty wchodzące w skład oferty, nie podlegają zwrotowi przez Zamawiającego.
- Oferent ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty, które nie będą zwracane przez Zamawiającego.
- Pytania do postępowania należy przysyłać bezpośrednio w Bazie Konkurencyjności.
- Zamawiający może żądać od Oferentów wyjaśnień lub uzupełnień dotyczących złożonych ofert w terminie 3 dni roboczych od dnia wystosowania stosownego wezwania w tym zakresie.
- Zamawiający zastrzega sobie możliwość zmiany lub odwołania postępowania w dowolnym terminie bez podania przyczyny.

10. Załączniki do zapytania

1.	Formularz ofertowy
2.	Oświadczenie o braku powiązań pomiędzy podmiotami współpracującymi.
3.	Oświadczenie o braku powiązań z Federacją Rosyjską
4	Specyfikacja techniczna

Załącznik nr 1 – Formularz ofertowy

Nazwa podmiotu, w imieniu
którego składana jest oferta

Miejscowość, data

FORMULARZ OFERTOWY 8/SF/2025
DANE ZAMAWIAJĄCEGO:

Nazwa: DIJO III Sp. z o.o.

Adres: 52-327 Wrocław, Zabrodzie 28

NIP: 8961628212

DANE OFERENTA:

1.	Nazwa oferenta	
2.	Adres	
3.	Tel/fax	
4.	e-mail	
5.	NIP	
6.	Nr wpisu do ewidencji działalności gospodarczej/ KRS (jeżeli dotyczy)	

1. **SKŁADAMY OFERTĘ** na wykonanie przedmiotu zamówienia zgodnie z opisem zamówienia i oświadczamy, że wykonamy go na warunkach w niej określonych.
2. **OFERUJEMY** realizację przedmiotu zamówienia za:

Cena netto	Cena brutto:	Słownie cena brutto

3. **OŚWIADCZAMY**, że zapoznaliśmy się z opisem zamówienia i nie wnosimy do niego zastrzeżeń oraz przyjmujemy warunki w nim zawarte i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, w miejscu i terminie wskazanym przez Zamawiającego.
4. **UWAŻAMY SIĘ** za związanych niniejszą ofertą do dnia (minimum 60 dni od terminu składania ofert).
5. **OŚWIADCZAMY**, że niniejsza oferta jest jawna, za wyjątkiem informacji zawartych na stronach, które stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji i jako takie nie mogą być ogólnodostępne.
6. **WSZELKĄ KORESPONDENCJĘ** w sprawie niniejszego postępowania należy kierować do:

Imię i nazwisko

Adres:

Telefon:

Adres e-mail:

7. **OFERTĘ** niniejszą składamy na ____ kolejno ponumerowanych stronach, oraz dołączamy do niej następujące oświadczenia i dokumenty:

1)

2)

3)

Miejscowość, data

*podpis osoby uprawnionej
do reprezentowania podmiotu*

Załącznik nr 2 – Oświadczenie o braku powiązań pomiędzy podmiotami współpracującymi

*Nazwa podmiotu, w imieniu
którego składane jest oświadczenie*

Miejscowość, data

OŚWIADCZENIE O BRAKU POWIĄZANIA POMIĘDZY PODMIOTAMI WSPÓŁPRACUJĄCYMI

Oświadczam, iż podmiot składający ofertę nie jest powiązany osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu zamawiającego lub osobami wykonującymi w imieniu zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

- a) uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
- b) posiadanie co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa);
- c) pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
- d) pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia;
- e) pozostawanie z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

Pomiędzy Zamawiającym a Oferentem nie istnieją wymienione powyżej powiązania.

Miejscowość, data

*podpis osoby uprawnionej
do reprezentowania podmiotu*

Załącznik nr 3 – Oświadczenie o braku powiązań z Federacją Rosyjską

*Nazwa podmiotu, w imieniu
którego składane jest oświadczenie*

Miejscowość, data

OŚWIADCZENIE

**o niepodleganiu wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r.
o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących
ochronie bezpieczeństwa narodowego**

podmiot, który reprezentuję nie podlega wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835), dalej jako „ustawa”. Zgodnie z treścią ww. przepisu, z postępowania o udzielenie zamówienia wyklucza się:

- 1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
- 2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
- 3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

Miejscowość, data

*podpis osoby uprawnionej
do reprezentowania podmiotu*

Załącznik nr 4 – Specyfikacja techniczna

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnień: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. 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.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych – Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi posiadać funkcjonalność przywrócenie plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
6. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
7. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
11. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
12. Rozwiązanie musi zapewniać 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).

13. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
14. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
15. Rozwiązanie musi zapewniać 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.
16. Rozwiązanie musi posiadać funkcję 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.
17. 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.
18. 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.
19. 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.
20. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
21. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
22. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
23. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
24. 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.
25. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
26. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
27. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

28. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
29. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
30. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
31. 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.

Ochrona stacji roboczych - macOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) lub nowszych.
2. Rozwiązanie musi wspierać architekturę Apple Silicon (ARM)
3. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
4. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
5. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
7. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań.
8. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
9. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej.
10. 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).

Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop, Red Hat Enterprise Linux oraz Linux Mint.
2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych.
3. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
6. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
10. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody

heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać 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.
14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
5. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO).

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
 - Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia,
 - przywrócenie urządzenia do ustawień fabrycznych,
 - zablokowania urządzenia,
 - uruchomienie sygnału dźwiękowego,
 - lokalizację GPS.
5. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
6. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - nazwę aplikacji,
 - nazwę pakietu,
 - kategorię sklepu Google Play
 - uprawnienia aplikacji
 - pochodzenie aplikacji z nieznanego źródła

Ochrona serwera pocztowego MS Exchange

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.

9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
 - a) Czysty,
 - b) Podejrzany,
 - c) Bardzo podejrzany,
 - d) Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Ochrona usług chmurowych

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint, Teams oraz ochroną usługi Google Workspace, takie jak Gmail oraz Dysk Google.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365 oraz Google Workspace.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
 - użytkowników, otrzymujących najwięcej spamu,
 - użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
 - użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
 - kont użytkowników, które mogą być podejrzane
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online, Onedrive, zespoły Teams, lokalizacje SharePoint, Gmail i OneDrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
 - jaka ilość wiadomości została przeskanowana,
 - wynik skanowania poszczególnych wiadomości,
 - czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
 - zagrożeniach, które zostały wykryte,
 - na jakim koncie zostały wykryte,
 - jakie zagrożenie zostało wykryte,
 - podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online, Onedrive, zespoły Teams, lokalizacje SharePoint, Gmail i OneDrive.
11. Rozwiązanie musi umożliwiać tworzenia reguł filtrowania w oparciu o co najmniej: DKIM, SPF, DMARC.

12. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
13. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
14. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
 - o Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej: wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
 - o wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online,
 - o dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
15. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
16. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
17. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
18. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
19. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

Moduł zarządzania podatnościami i aktualizacjami

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

14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. 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.
10. 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.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. 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.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. 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.
15. 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, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Ochrona poprzez dwuskładnikowe uwierzytelnianie

1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjny Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.

6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
11. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
12. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
13. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
14. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
15. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
16. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego
17. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.