

Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa przedłużenia 750 licencji oprogramowania klasy EDR Palo Alto Networks Cortex XDR and Premium Partner Support wraz ze wsparciem technicznym na okres 12 miesięcy.
2. Zamawiający oświadcza, że posiada obecnie 750 licencji oprogramowania Palo Alto Networks Cortex XDR, numer seryjny 0220980000005745, ważnych do dnia 7.12.2024. Biorąc pod uwagę powyższe, Wykonawca może zaoferować Zamawiającemu dostawę licencji oprogramowania klasy EDR, jako przedłużenie obecnie posiadanych licencji Palo Alto Networks Cortex XDR lub równoważnych.
3. W okresie obowiązywania licencji Wykonawca musi zapewnić Zamawiającemu:
 - 3.1. prawo do pozyskania, instalacji i używania nowych wersji oprogramowania objętego licencjami w razie ich publikacji,
 - 3.2. dostęp do poprawek i uaktualnień oprogramowania,
 - 3.3. dostęp do materiałów producenta takich jak: dokumentacja techniczna, internetowa baza wiedzy, forum internetowe producenta oprogramowania.
4. Warunki wsparcia technicznego w okresie obowiązywania licencji:
 - 4.1. usługi wsparcia technicznego muszą być świadczone w oparciu o świadczenia gwarancyjne producenta oprogramowania lub autoryzowaną przez producenta do świadczenia takich usług firmę,
 - 4.2. możliwość zgłaszania nieograniczonej liczby zgłoszeń serwisowych,
 - 4.3. możliwość generowania zgłoszeń serwisowych za pomocą: e-mail, telefonu, strony internetowej,
 - 4.4. usługi wsparcia technicznego muszą być świadczone w systemie 24/7,
 - 4.5. czas odpowiedzi dla zgłoszeń awarii o statusie krytycznym „Critical” nie może przekroczyć 1 godziny. Za „awarię o statusie krytycznym” uważa się awarię oprogramowania objętego licencją w której produkt nie działa i uniemożliwia wykorzystywanie środowiska Zamawiającego, dla której nie ma rozwiązania tymczasowego,
 - 4.6. czas odpowiedzi dla zgłoszeń awarii o statusie wysokim „High” nie może przekroczyć 2 godzin. Za „awarię o statusie wysokim” uważa się taką awarię skutkującą niewłaściwym działaniem oprogramowania objętego licencją, która ma znaczący wpływ na środowiska Zamawiającego (np. spadek wydajności), lecz nie uniemożliwia korzystania z niego, dla której nie ma rozwiązania tymczasowego,
 - 4.7. czas odpowiedzi dla zgłoszeń awarii o statusie średnim „Medium” nie może przekroczyć 8 godzin. Za „awarię o statusie średnim” uważa się częściową, niekrytyczną awarię oprogramowania objętego licencją, która nie ma wpływu na środowisko Zamawiającego, dla której istnieją rozwiązania tymczasowe,
 - 4.8. czas odpowiedzi dla zgłoszeń o charakterze niskim „Low” nie może przekroczyć jednego dnia roboczego. Za „zgłoszenia o statusie niskim” oprogramowania objętego licencją uważa się inne niż opisane powyżej awarie, w tym błędy w dokumentacji.
5. Wymagane funkcjonalności stanowiące jednocześnie kryteria równoważności
 - 5.1. System bezpieczeństwa EDR musi być dostarczony w formie On-prem lub w formie SaaS. Jeśli system jest dostarczany w formie usługi SaaS to wówczas wymaga się, aby dane były przechowywane i przetwarzane (włącznie z sandboxingiem) na terenie Polski a producent systemu musi posiadać certyfikację SOC 2 type 2 lub ISO27001 oraz gwarantować dostępność usługi w ramach SLA co najmniej na poziomie 99,9%.
 - 5.2. Dokumentacja systemu musi być publikowana przez producenta na jego stronie internetowej w języku polskim lub/i angielskim.
 - 5.3. System musi obsłużyć co najmniej 750 stacji końcowych w tym:
 - 5.3.1. stacji roboczych z systemem Windows ,
 - 5.3.2. stacji roboczych z systemem macOS,
 - 5.3.3. stacji roboczych z systemem Linux,
 - 5.3.4. serwerów z systemem Windows Serwer,
 - 5.3.5. serwerów z systemem Linux.

- 5.4. System musi przechowywać informacje o alarmach i incydentach co najmniej przez 180 dni.
- 5.5. System musi posiadać możliwość analizy dynamicznej plików wykonywalnych Windows, Linux i MacOS w systemie sandbox tego samego producenta co producent oferowanego systemu i obsługiwać pliki o rozmiarze co najmniej 100MB. System musi umożliwiać pobranie raportu z analizy dynamicznej.
- 5.6. System musi umożliwiać zarządzania przez pojedynczy webowy interfejs graficzny z wykorzystaniem graficznej przeglądarki internetowej oraz przez API. Oba muszą być dostępne po https (co najmniej TLS 1.2). Nie dopuszcza się, aby webowy interfejs graficzny korzystał z technologii flash, silverlight lub java.
- 5.7. Wszystkie składniki systemu muszą być konfigurowalne i zarządzane przez jeden spójny interfejs a dostęp do nich realizowany jest przez pojedyncze logowanie (Single Sign-On). Nie dopuszcza się, aby składniki systemu posiadały oddzielne pulpity/konsole do zarządzania konkretnymi funkcjami bezpieczeństwa.
- 5.8. System musi posiadać możliwość ograniczenia logowania do systemu tylko ze wskazanych publicznych adresów IP.
- 5.9. System musi umożliwiać integrację z zewnętrznym katalogiem użytkowników via SAML 2.0 (ze wsparciem dla ADFS) oraz posiadać możliwość definiowania lokalnych użytkowników, których logowanie jest zabezpieczone hasłem oraz dodatkowym czynnikiem uwierzytelniającym w formie tokenu. System jako dodatkową metodę uwierzytelnienia musi wspierać co najmniej tokeny w formie jednorazowych kodów generowanych w aplikacji mobilnej lub przesyłanych poprzez email.
- 5.10. System musi umożliwiać przypisywanie użytkowników do grup użytkowników. Dodatkowo w przypadku użytkowników uwierzytelnionych via SAML 2.0 musi istnieć możliwość zmapowania grup SAML do lokalnie zdefiniowanych grup.
- 5.11. Każdy użytkownik systemu (administrator, operator, analityk) muszą posiadać indywidualne konta pozwalające na jego jednoznaczną identyfikację.
- 5.12. System musi umożliwiać określenie zakresu dostępu z wykorzystaniem ról i ich przypisanie do użytkownika lub do grupy użytkowników. Rola musi definiować dostęp do określonego obszaru administracyjnego systemu, jego rodzaju (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane stacje końcowe).
- 5.13. System w ramach roli musi umożliwiać określenie dostępu do co najmniej następujących obszarów:
 - 5.13.1. Ustawienia systemu
 - 5.13.2. Zarządzanie hostami
 - 5.13.3. Zarządzanie politykami
 - 5.13.4. Zarządzanie regułami detekcyjnymi
 - 5.13.5. Zarządzania wykluczeniami
 - 5.13.6. Zarządzanie incydentami
 - 5.13.7. Uruchamianie odpowiedzi na incydent
 - 5.13.8. Nawiązywanie połączenia do linii poleceń
 - 5.13.9. Uruchamianie skryptów python
 - 5.13.10. Zarządzanie kwerendami do danych
 - 5.13.11. Zarządzanie raportami
 - 5.13.12. Zarządzenie dashboardami/kokpitami
- 5.14. System musi posiadać możliwość definiowania własnych dopasowanych do potrzeb ról.
- 5.15. System musi posiadać zestaw dashboardów informujących co najmniej o:
 - 5.15.1. liczbie i powadze incydentów,
 - 5.15.2. liczbie incydentów przypisanych do analityków,
 - 5.15.3. hostach z największą liczbą incydentów,
 - 5.15.4. liczbie agentów z rozbiciem na wersję agenta,
 - 5.15.5. liczbie agentów z rozbiciem na agentów offline i online,
 - 5.15.6. liczbie agentów z rozbiciem na wersję aktualizacji podsystemów bezpieczeństwa,
 - 5.15.7. liczbie agentów z rozbiciem na status ochrony.

- 5.16. System musi umożliwiać skonfigurowanie okresu czasu, po którym użytkownik zostanie automatycznie wylogowany z systemu oraz możliwość automatycznego zawieszania kont użytkowników, którzy nie logowali się dłużej niż określona liczba dni.
- 5.17. System musi co najmniej przez 365 dni przechowywać logi audytowe dokumentujące akcje podejmowane przez użytkowników zalogowanych do systemu oraz logi audytowe dotyczące funkcjonowania agentów.
- 5.18. System musi posiadać możliwość eksportu wybranych logów audytowych via syslog po ssl/tls w formacie CEF. W dokumentacji systemu musi być wskazany adres IP lub zakres adresów IP, z których nawiązywane będzie połączenie syslog.
- 5.19. System musi posiadać możliwość alarmowania o wskazanych zdarzeniach zapisanych w logach audytowych poprzez wysłanie emaila na wskazane skrzynki poczty elektronicznej.
- 5.20. System musi posiadać możliwość integracji z Microsoft Active Directory w zakresie synchronizacji struktury organizacyjnej katalogu AD zarówno z lokalnym AD jak również z Azure AD na potrzeby automatycznego wzbogacania informacji na temat stacji końcowych i użytkowników oraz tworzenia dynamicznych grup stacji końcowych celem różnicowania konfiguracji agentów.
- 5.21. System musi posiadać funkcjonalność wykrywania niezarządzanych stacji końcowych w sieci w oparciu o skanowanie obiektów kont komputerów Active Directory.
- 5.22. System po integracji z Active Directory, musi mieć możliwość wyświetlenia widoku wszystkich komputerów obsługiwanych przez Active Directory Zamawiającego z możliwością filtrowania per OU. Konsola zarządzająca oferowanego rozwiązania musi wykrywać serwery będące członkami domeny Active Directory, na których nie zainstalowano agenta Systemu EDR. Widok powinien być podzielony na maszyny chronione i nie chronione przez agenta. System co najmniej raz na dobę musi alarmować (co najmniej notyfikacja emailowa i via syslog), jeśli serwery w określonym OU nie są chronione przez agenta.
- 5.23. System musi posiadać możliwość określenia strefy czasowej wykorzystywanej do reprezentowania znaczników czasowych w interfejsie zarządzania oraz formatu tego znacznika co najmniej w takim zakresie, aby uwidaczniał on strefę czasową.
- 5.24. System musi posiadać oprogramowanie agenta co najmniej dla następujących systemów operacyjnych:
 - 5.24.1. Windows 10 i 11 (włącznie ze środowiskiem Persistent oraz Non-Persistent VDI)
 - 5.24.2. Windows Server 2012 R2, 2016 standard i core, 2019 standard i core oraz 2022,
 - 5.24.3. Linux
 - 5.24.3.1. Red Hat Enterprise Linux 7, 8 i 9
 - 5.24.3.2. Rocky Linux 8 i 9
 - 5.24.3.3. SUSE Linux Enterprise Server 11, 12 i 15
 - 5.24.3.4. Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS i 24.04 LTS
 - 5.24.3.5. Oracle Linux 6, 7, 8 i 9
 - 5.24.3.6. CentOS 7, 8 i 9
 - 5.24.3.7. Debian 8, 9, 10, 11 i 12
 - 5.24.4. macOS 11.x, 12.x, 13.x i 14.x, 15.x
- 5.25. System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:
 - 5.25.1. W formacie msi dla systemów Windows
 - 5.25.2. W formacie rpm, deb i sh dla systemów Linux
 - 5.25.3. W formacie pkg dla systemów macOS
- 5.26. Pakiet instalacyjny agenta dla systemów Windows, macOS, Linux musi posiadać możliwość:
 - 5.26.1. Przypisania do hosta nieusuwalnego znacznika, który może być wykorzystany do tworzenia dynamicznych grup stacji końcowych i określenia zakresu dostępu jaki posiada rola użytkownika.
 - 5.26.2. Skonfigurowania komponentu pośredniczącego w komunikacji z systemem
 - 5.26.3. Wyłączenia opcji wykonywania skryptów python
 - 5.26.4. Wyłączenia opcji pobierania plików
 - 5.26.5. Wyłączenia opcji dostępu do linii poleceń

- 5.27. Pakiet instalacyjny agenta dla systemów Windows musi posiadać możliwość wskazania lokalnej kopii aktualizacji podsystemów bezpieczeństwa.
- 5.28. Instalacja agenta i jego aktywacja w systemie nie może wymagać restartu systemu operacyjnego.
- 5.29. Komunikacja pomiędzy agentem a systemem musi być zabezpieczona z wykorzystaniem https (co najmniej TLS 1.2) i w zależności od konfiguracji być realizowana w sposób bezpośredni lub pośredni via dedykowany komponent pośredniczący (dalej proxy) tego samego producenta, który:
 - 5.29.1. musi umożliwiać uruchomienie w formie maszyny wirtualnej
 - 5.29.2. musi obsługiwać funkcję proxy chaining dla http z uwierzytelnieniem
 - 5.29.3. musi umożliwiać cache'owanie aktualizacji oprogramowania agenta i aktualizacji podsystemów bezpieczeństwa agenta
- 5.30. Komunikacja pomiędzy proxy a systemem musi być zabezpieczona z wykorzystaniem https (co najmniej TLS 1.2). Proxy musi posiadać możliwość manualnej lub automatycznej aktualizacji. System musi umożliwiać centralne zarządzanie ustawieniami proxy.
- 5.31. W dokumentacji systemu muszą być wskazane publiczne adresy IP oraz adresy URL niezbędne do zapewnienia poprawnej komunikacji między agentami i systemem oraz pomiędzy proxy a systemem. Komunikacja musi być zawsze nawiązywana w kierunku od agenta/proxy do systemu.
- 5.32. System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup stacji końcowych. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:
 - 5.32.1. Dnia tygodnia i zakresu czasu, w którym wykonywana jest aktualizacja
 - 5.32.2. Maksymalnej liczby równoległe aktualizowanych agentów
 - 5.32.3. Zakresu: tylko minor release, tylko minor release w ramach wskazanego major release, najnowszy major.minor release, najnowszy przedostatni major.minor release
 - 5.32.4. Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowego release
 - 5.32.5. Źródła: bezpośrednio z systemu, z proxy, peer-to-peer
- 5.33. System musi posiadać możliwość skonfigurowania manualnej i automatycznej różnicowej aktualizacji podsystemów bezpieczeństwa agenta dla wskazanych grup stacji końcowych. Polityka automatycznej aktualizacji podsystemów bezpieczeństwa musi umożliwiać określenie:
 - 5.33.1. Zakresu: tylko major release, najnowszy major.minor release
 - 5.33.2. Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowego release
 - 5.33.3. Źródła: bezpośrednio z systemu, z komponentu pośredniczącego, peer-to-peer
 - 5.33.4. Globalnego limitu na wykorzystanie pasma przy bezpośrednim pobieraniu z systemu
- 5.34. System musi umożliwiać alarmowanie w przypadku, gdy:
 - 5.34.1. Podsystemy bezpieczeństwa agenta nie będą funkcjonowały poprawnie
 - 5.34.2. Agent zostanie odinstalowany
 - 5.34.3. Agent nie zgłosi się do systemu a równocześnie stacja końcowa zaloguje się w domenę Active Directory (dotyczy systemów Windows)
- 5.35. System musi umożliwiać różnicowanie konfiguracji agenta i podsystemów bezpieczeństwa poprzez przypisanie różnych profili konfiguracyjnych do wybranych grup stacji końcowych lub pojedynczych stacji końcowych.
- 5.36. System musi umożliwiać licencyjne rozszerzenie funkcjonalności o przetwarzanie i przechowywanie danych telemetrycznych i alarmów z urządzeń firewall co najmniej następujących producentów: Palo Alto Networks, Check Point, Fortinet i Cisco.
- 5.37. System musi umożliwiać licencyjne rozszerzenie funkcjonalności o przetwarzanie i przechowywanie danych telemetrycznych co najmniej z następujących systemów: Microsoft Office 365, Amazon Web Services, Azure Event Hub, Google Cloud Platform.
- 5.38. System musi umożliwiać licencyjne rozszerzenie funkcjonalności o przetwarzanie i przechowywanie danych telemetrycznych w formacie NetFlow v9 i IPFIX.
- 5.39. System musi umożliwiać licencyjne rozszerzenie funkcjonalności o przetwarzanie i przechowywanie danych telemetrycznych przesyłanych przez syslog w formacie CEF

- i LEEF a w przypadku nieustrukturyzowanych danych umożliwiać ich analizę i mapowanie.
- 5.40. System musi umożliwiać licencyjne rozszerzenie funkcjonalności o przetwarzanie i przechowywanie danych telemetrycznych przesyłanych w ramach mechanizmu Windows Event Forwarding.
 - 5.41. Wszystkie dane telemetryczne muszą być przechowywane przez system w centralnym i przeszukiwalnym repozytorium danych.
 - 5.42. System musi umożliwiać przeszukiwanie danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Kwerendy muszą umożliwiać łączenie danych telemetrycznych z różnych źródeł, ich filtrowanie i przekształcanie wyników. Reguły tworzenia kwerend muszą być opisane w dokumentacji systemu.
 - 5.43. System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do prywatnej biblioteki kwerend danego użytkownika lub do globalnej biblioteki kwerend dostępnej dla wszystkich innych użytkowników.
 - 5.44. System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via REST API.
 - 5.45. System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.
 - 5.46. System musi umożliwiać uruchamianie kwerendy cyklicznie zgodnie z podanym harmonogramem lub jeden raz o określonym czasie.
 - 5.47. System musi umożliwiać wizualizację wyników kwerendy do danych telemetrycznych w formie tabelarycznej i w formie wykresu: liniowego, słupkowego i kołowego.
 - 5.48. System musi umożliwiać wykorzystanie wyników kwerendy do tworzenia okresowo generowanych raportów.
 - 5.49. System musi umożliwiać wykorzystanie wyników kwerend do wizualizacji danych w dashboardach.
 - 5.50. System musi umożliwiać globalne blokowanie uruchamiania/ładowania plików binarnych o określonych SHA256.
 - 5.51. System w ramach odpowiedzi na incydent musi umożliwiać:
 - 5.51.1. Remediację ze wskazaniem kroków, które mogą być podjęte automatycznie i kroków, które należy zrealizować manualnie. Musi istnieć możliwość wyboru kroków remediacyjnych, które zostaną wykonane automatycznie.
 - 5.51.2. Uruchomienie skryptu python na stacji końcowej.
 - 5.51.3. Nawiązanie interaktywnego połączenia do linii poleceń na stacji końcowej.
 - 5.51.4. Wstrzymanie procesu na stacji końcowej.
 - 5.51.5. Wyłączenie procesu na stacji końcowej.
 - 5.51.6. Izolację sieciową hosta.
 - 5.51.7. Dodanie adresu IP do listy publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa.
 - 5.51.8. Dodanie nazwy domenowej do publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa.
 - 5.51.9. Zmianę w rejestrze (tylko systemy Windows).
 - 5.51.10. Usunięcie pliku na stacji końcowej.
 - 5.51.11. Przeniesienie pliku na stacji końcowej do kwarantanny.
 - 5.51.12. Wyszukanie pliku na innych hostach.
 - 5.51.13. Zrzucenie pamięci procesu na stacji końcowej.
 - 5.52. System musi obsługiwać co najmniej następujące poziomy powagi alarmów: informacyjny, niski, średni, wysoki i krytyczny.
 - 5.53. System musi automatycznie grupować powiązane alarmy w celu przyspieszenia i ułatwienia triażu i analizy incydentu.
 - 5.53.1. W ramach incydentu system musi grupować:
 - 5.53.2. Powiązanych z incydem użytkowników
 - 5.53.3. Stacje końcowe
 - 5.53.4. Pliki
 - 5.53.5. Domeny
 - 5.53.6. Adresy IP

- 5.54. System musi umożliwiać wgląd w raport z sandboxa dla plików powiązanych z incydem i eksport tego raportu.
- 5.55. Agent nie może wykorzystywać Oracle Java JRE/JDK.
- 5.56. Agent dla systemów Windows:
 - 5.56.1. Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:
 - 5.56.1.1. Bezpośrednio z systemu
 - 5.56.1.2. Z komponentu pośredniczącego
 - 5.56.1.3. Od innych stacji końcowych w tej samej podsieci (peer-to-peer)
 - 5.56.2. Musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie podsystemów bezpieczeństwa i odinstalowanie agenta musi wymagać podania hasła, które może być skonfigurowane per grupa stacji końcowych lub indywidualnie dla danego hosta po stronie systemu. Nie dopuszcza się rozwiązań, w których hasło jest statyczne i podawane w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.
 - 5.56.3. Musi być procesem chronionym w trybie PPL dla oprogramowanie anty-malware'owego.
 - 5.56.4. Musi posiadać sterownik ELAM (Early Launch Anti-Malware).
 - 5.56.5. Musi umożliwiać:
 - 5.56.5.1. Ukrycie ikony agenta w zasobniku systemowym
 - 5.56.5.2. Wyłączenie powiadomień o zablokowanych zagrożeniach
 - 5.56.5.3. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej
 - 5.56.5.4. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego
 - 5.56.5.5. Spolszczenie komunikatów powiadomień
 - 5.56.5.6. Zarządzanie host firewallem hosta z wykorzystaniem Windows Filtering Platform
 - 5.56.5.7. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu
 - 5.56.5.8. Weryfikację stanu szyfrowania dysków
 - 5.56.6. Musi integrować się z Windows Security Center
 - 5.56.7. Musi posiadać możliwość blokowania uruchamiania programów z zewnętrznej pamięci masowej podłączonej na porcie USB i z napędów optycznych.
 - 5.56.8. Musi posiadać możliwość blokowania uruchamiania programów ze wskazanych lokalizacji w systemie plików.
 - 5.56.9. Musi posiadać możliwość blokowania uruchamiania programów z zasobów sieciowych poza wybranymi ścieżkami.
 - 5.56.10. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technik eksploatacji:
 - 5.56.10.1. Przekierowanie APC
 - 5.56.10.2. Obejście Data Execution Prevention
 - 5.56.10.3. DLL Hijacking
 - 5.56.10.4. Exploit Kit Fingerprinting
 - 5.56.10.5. JIT
 - 5.56.10.6. Null Dereference
 - 5.56.10.7. ROP
 - 5.56.10.8. Structures exception handler hijackings
 - 5.56.10.9. Heap Spray
 - 5.56.10.10. Kernel Privilege Escalation
 - 5.56.11. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi umożliwiając skonfigurowanie co najmniej następujących mechanizmów:
 - 5.56.11.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu

- 5.56.11.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym gościu)
- 5.56.11.3. Lokalna analiza statyczna
- 5.56.11.4. Weryfikacja podpisu pliku binarnego
- 5.56.11.5. Przeniesienie pliku binarnego do kwarantanny
- 5.56.11.6. Zablokowanie uruchomienia/załadowania złośliwego pliku binarnego
- 5.56.11.7. Zablokowanie uruchomienia pliku z przenośnej pamięci masowej USB
- 5.56.11.8. Zablokowanie uruchomienia pliku z innych lokalizacji sieciowych niż wskazane
- 5.56.11.9. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego
- 5.56.11.10. Wykrywanie shellcodu'u ładowanego do pamięci
- 5.56.11.11. Wykrycie i przerwanie próby szyfrowania plików na dysku (ochrona przeciw ransomware).
- 5.56.12. Musi wykrywać i blokować próbę wyłączenia Volume Shadow Copy Service (VSS).
- 5.56.13. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami co najmniej w plikach Microsoft Word i Microsoft Excel umożliwiając skonfigurowanie co najmniej następujące mechanizmy:
 - 5.56.13.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu
 - 5.56.13.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym gościu)
 - 5.56.13.3. Lokalna analiza statyczna
- 5.56.14. Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.
- 5.56.15. Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu.
- 5.56.16. Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każda stacja końcowa musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.
- 5.57. Agent dla systemów macOS:
 - 5.57.1. Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:
 - 5.57.1.1. Bezpośrednio z systemu
 - 5.57.1.2. Z komponentu pośredniczącego
 - 5.57.1.3. Od innych stacji końcowych w tej samej podsieci (peer-to-peer)
 - 5.57.2. Musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie podsystemów bezpieczeństwa i odinstalowanie agenta musi wymagać podania hasła, które może być skonfigurowane per grupa stacji końcowych lub indywidualnie dla danego hosta po stronie systemu. Nie dopuszcza się rozwiązań, w których hasło jest statyczne i podawana w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.
 - 5.57.3. Musi umożliwiać:
 - 5.57.3.1. Ukrycie ikony agenta w zasobniku systemowym
 - 5.57.3.2. Wyłączenie powiadomień o zablokowanych zagrożeniach
 - 5.57.3.3. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej
 - 5.57.3.4. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego
 - 5.57.3.5. Spolszczenie komunikatów powiadomień

- 5.57.3.6. Zarządzanie host firewallem hosta
- 5.57.3.7. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu
- 5.57.3.8. Weryfikację stanu szyfrowania dysków
- 5.57.4. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technik eksploatacji:
 - 5.57.4.1. Dylib Hijacking
 - 5.57.4.2. JIT
 - 5.57.4.3. ROP
- 5.57.5. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
 - 5.57.5.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu
 - 5.57.5.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym gościu)
 - 5.57.5.3. Lokalna analiza statyczna
 - 5.57.5.4. Weryfikacja podpisu pliku binarnego
 - 5.57.5.5. Przeniesienie pliku binarnego do kwarantanny
 - 5.57.5.6. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego
- 5.57.6. Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.
- 5.57.7. Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacja sieciowa) poza połączeniem do systemu.
- 5.57.8. Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każda stacja końcowa musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.
- 5.58. Agent dla systemów Linux:
 - 5.58.1. Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:
 - 5.58.1.1. Bezpośrednio z systemu
 - 5.58.1.2. Z komponentu pośredniczącego
 - 5.58.1.3. Od innych stacji końcowych w tej samej podsieci (peer-to-peer)
 - 5.58.2. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.
 - 5.58.3. Musi posiadać wsparcie dla rozszerzenia eBPF.
 - 5.58.4. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technik eksploatacji:
 - 5.58.4.1. Java Deserialization
 - 5.58.4.2. SO Hijacking
 - 5.58.4.3. Heap spray
 - 5.58.4.4. ROP
 - 5.58.4.5. Kernel Privilege Escalation
 - 5.58.5. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
 - 5.58.5.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu
 - 5.58.5.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym gościu)
 - 5.58.5.3. Lokalna analiza statyczna

- 5.58.5.4. Przeniesienie pliku binarnego do kwarantanny
 - 5.58.5.5. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego
 - 5.58.5.6. Wykrywanie webshell
 - 5.58.6. Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.
 - 5.58.7. Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu.
 - 5.58.8. Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każda stacja końcowa musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.
6. Kryteria równoważności – wymagania
- 6.1. Przedmiot zamówienia został opisany przez Zamawiającego przez wskazanie nazwy, znaku towarowego lub producenta, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę z uwagi na fakt, że Zamawiający nie może opisać przedmiotu zamówienia w tym zakresie w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu temu towarzyszą wyrazy „lub równoważny”.
 - 6.2. Wszędzie tam, gdzie przedmiot zamówienia został opisany przez wskazanie nazw, znaków towarowych lub producenta, Zamawiający dopuszcza zaoferowanie przez Wykonawcę licencji oprogramowania równoważnego na warunkach określonych w niniejszym opisie przedmiotu zamówienia.
 - 6.3. W opisie przedmiotu zamówienia (w ust. 5) Zamawiający wskazał kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania przez Wykonawcę rozwiązania (oprogramowania) równoważnego, na Wykonawcy spoczywa obowiązek wykazania równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez rozwiązanie (oprogramowanie) równoważne wszystkich wskazanych przez Zamawiającego kryteriów równoważności.
 - 6.4. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie (oprogramowanie) równoważne nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.
 - 6.5. Zastosowanie rozwiązania (oprogramowania) równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązania opisanego jako rozwiązanie referencyjne po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.
 - 6.6. W przypadku zaoferowania przez Wykonawcę rozwiązania (oprogramowania) równoważnego, Wykonawca na swój koszt zapewni inżyniera wsparcia technicznego certyfikowanego przez producenta zaoferowanych przez Wykonawcę licencji systemu zaawansowanej ochrony urządzeń końcowych, który przeprowadzi:
 - 6.6.1. Wdrożenie: Zakres wdrożenia musi obejmować wszystkie elementy systemu zaawansowanej ochrony dla stacji końcowych i serwerów, w szczególności zaś:
 - 6.6.1.1. konfigurację konsoli centralnej, w tym raportów,
 - 6.6.1.2. integrację systemu z systemami centralnymi Zamawiającego: AD, DNS, NTP, Poczta elektroniczna,
 - 6.6.1.3. przygotowanie ustawień agentów i przypisanie ich do grup chronionych systemów,
 - 6.6.1.4. próbną instalację, konfigurację i sprawdzenie poprawności działania agentów na maksymalnie 15 urządzeniach,
 - 6.6.1.5. konfigurację monitoringu i raportowania,
 - 6.6.1.6. testy poprawności działania całego systemu,

- 6.6.1.7. stworzenie dokumentacji powdrożeniowej.
- 6.6.2. Szkolenie:
 - 6.6.2.1. zakres szkolenia musi odnosić się bezpośrednio do przedmiotowego wdrożenia i obejmować minimum:
 - 6.6.2.1.1. zarządzanie systemem,
 - 6.6.2.1.2. tworzenie reguł bezpieczeństwa i wyjątków od nich,
 - 6.6.2.1.3. zarządzanie grupami chronionych urządzeń, przypisywanie do nich reguł,
 - 6.6.2.1.4. zarządzanie agentami chronionych urządzeń,
 - 6.6.2.1.5. obsługę wykrytych incydentów,
 - 6.6.2.1.6. utrzymanie systemu,
 - 6.6.2.2. czas szkolenia: minimum 8 godzin,
 - 6.6.2.3. językiem szkolenia musi być język polski,
 - 6.6.2.4. Wykonawca zobowiązany jest przeprowadzić szkolenie dla maksymalnie 5 osób wskazanych przez Zamawiającego,
 - 6.6.2.5. szkolenie musi odbyć się w formie zdalnej,
 - 6.6.2.6. Wykonawca przygotowuje na potrzeby przeprowadzenia szkolenia wszelkie niezbędne zaplecze techniczne, tj. środowiska informatyczne dla poszczególnych uczestników, wirtualną salę laboratoryjną, oprogramowanie, licencje,
 - 6.6.2.7. po zakończeniu szkolenia Wykonawca przekaze uczestnikom certyfikaty uczestnictwa.
- 6.7. W przypadku zaoferowania przez Wykonawcę rozwiązania (oprogramowania) równoważnego, czas wdrożenia musi być tak dobrany, aby Zamawiający nie pozostał bez ochrony stacji końcowych przy użyciu obecnie posiadanego systemu i systemu zaoferowanego przez Wykonawcę.
- 6.8. W przypadku zaoferowania przez Wykonawcę rozwiązania (oprogramowania) równoważnego, wdrożenie ochrony na stacjach końcowych musi być zrealizowane zdalnie bez konieczności bezpośredniego działania służb technicznych Zamawiającego na stacjach końcowych. Wykonawca zapewni również zdalne odinstalowanie agentów obecnie posiadanego przez Zamawiającego systemu EDR ze stacji końcowych.