

## OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiotem zamówienia jest:

Dostawa subskrypcji ważnej przez 12 miesięcy dla systemu do wykrywania zagrożeń w plikach przesyłanych do systemów Zamawiającego wraz instalacją i konfiguracją powyższego systemu w infrastrukturze Zamawiającego w terminie 14 dni od daty zawarcia Umowy.

II. Przedmiot Umowy obejmuje dostawę subskrypcji oraz kontraktów serwisowych udostępnionych Zamawiającemu na wyłączność kluczy autoryzacyjnych wraz z doręczeniem wymaganych dokumentów, wystawionych przez producenta oprogramowania, uprawniających do korzystania ze wskazanych subskrypcji zgodnie z prawem. Dostarczenie wskazanych kluczy autoryzacyjnych oraz kontraktów serwisowych nastąpi w nieprzekraczalnym terminie 14 dni od dnia zawarcia Umowy.

Wykonawca dostarczy klucze autoryzacyjne na nośnikach danych bądź za pośrednictwem dedykowanego portalu producenta bądź udostępni w postaci elektronicznej na adres poczty elektronicznej Zamawiającego: [ckis@wroclaw.sa.gov.pl](mailto:ckis@wroclaw.sa.gov.pl)

L.p.	Nazwa wymagania	Opis wymagań minimalnych
1.	Ogólne	<ol style="list-style-type: none"> <li>Rozwiązanie musi być wdrożone jako dedykowana platforma do skanowania plików przesyłanych do systemów Zamawiającego przez ich użytkowników. Platforma musi umożliwiać przyjmowanie do skanowania plików za pomocą interfejsu API oraz protokołu ICAP.</li> <li>Nie dopuszcza się instalacji dodatkowego oprogramowania w systemach Zamawiającego do których docelowo mają trafiać przeskanowane pliki.</li> <li>Rozwiązanie musi umożliwiać jego instalację w systemach Microsoft Windows Server (wersje wspierane przez Microsoft) i Linux (min. Debian 11, 12 oraz Ubuntu 22.04, 24.04).</li> <li>Rozwiązanie musi zapewniać możliwość pełnej konfiguracji strony blokowania dostępu (blocking page).</li> <li>Rozwiązanie musi udostępniać konsolę zarządzającą dostępną z poziomu przeglądarek internetowych: Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Internet Explorer oraz Microsoft Edge.</li> <li>Całość rozwiązania nie może być zbudowana na bazie oprogramowania typu Open Source oraz musi być w całości wyprodukowane i wspierane przez jednego producenta.</li> </ol>

		<p>7. Rozwiązanie musi być zainstalowane w dwóch Ośrodkach Przetwarzania Danych Zamawiającego i działające w trybie active-active jako dwie niezależne od siebie instancje.</p>
2.	Bezpieczeństwo	<p>1. Dostęp do platformy musi być realizowany wyłącznie z wykorzystaniem protokołu HTTPS.</p> <p>2. Rozwiązanie musi obsługiwać mechanizm kontroli dostępu opartej na rolach (RBAC).</p> <p>3. Rozwiązanie musi umożliwiać integrację z systemami klasy SIEM oraz serwerami syslog.</p> <p>4. Rozwiązanie musi umożliwiać pracę w środowiskach z dostępem do sieci Internet jak również odseparowanych od sieci Internet.</p> <p>5. Rozwiązanie musi wykorzystywać jeden, jednoznacznie określony adres URL do pobierania aktualizacji definicji sygnatur.</p> <p>6. Rozwiązanie musi umożliwiać ręczne wgrywanie definicji sygnatur pobranych uprzednio na systemach posiadających dostęp do Internetu.</p> <p>7. Mechanizm aktualizacji silników oraz definicji wirusów musi obsługiwać tryb aktualizacji automatycznej przez Internet, tryb ręczny oraz aktualizację z lokalnego katalogu.</p>
3.	Zarządzanie	<p>1. Rozwiązanie musi zapewniać centralny punkt zarządzania konfiguracją („single pane of glass”).</p> <p>2. Rozwiązanie musi integrować się z systemami syslog oraz SIEM.</p> <p>3. Rozwiązanie musi umożliwiać tworzenie kont użytkowników z różnymi rolami administracyjnymi oraz audytowymi.</p> <p>4. Rozwiązanie musi obsługiwać role administracyjne oparte na grupach Active Directory oraz LDAP.</p> <p>5. Logi systemowe muszą być archiwizowane lokalnie oraz możliwe do pobrania z poziomu interfejsu graficznego.</p> <p>6. Rozwiązanie musi umożliwiać zdalną administrację z wykorzystaniem protokołów RDP oraz HTTPS.</p> <p>7. Rozwiązanie musi posiadać wbudowaną bazę danych.</p> <p>8. Rozwiązanie musi umożliwiać eksport konfiguracji oraz wykonywanie kopii zapasowych.</p>
4.	Wykrywanie zagrożeń	<p>1. Rozwiązanie musi obsługiwać co najmniej 8 różnych silników antywirusowych z możliwością rozszerzenia ich liczby do 30.</p> <p>2. Rozwiązanie musi wykorzystywać mechanizmy detekcji oparte na sygnaturach.</p> <p>3. Rozwiązanie musi wykorzystywać mechanizmy detekcji heurystycznej.</p> <p>4. Rozwiązanie musi wykorzystywać mechanizmy detekcji oparte na uczeniu maszynowym.</p> <p>5. Silniki antywirusowe muszą działać w trybie wielowątkowym.</p>

		<ol style="list-style-type: none"> <li>6. Rozwiązanie musi obsługiwać zaawansowane przetwarzanie oraz ekstrakcję archiwów.</li> <li>7. Rozwiązanie musi umożliwiać konfigurację zasad obsługi archiwów.</li> <li>8. Rozwiązanie musi umożliwiać przetwarzanie plików i archiwów zabezpieczonych hasłem.</li> <li>9. Proces detekcji musi odbywać się w całości lokalnie (on-premise), bez wykorzystania połączeń chmurowych.</li> <li>10. Rozwiązanie musi posiadać jeden wspólny komponent licencyjny dla wszystkich silników antywirusowych.</li> <li>11. Wszystkie silniki antywirusowe muszą być zdolne do pracy w środowiskach air-gapped.</li> <li>12. Częstotliwość aktualizacji definicji sygnatur musi być konfigurowalna.</li> <li>13. Wszystkie definicje sygnatur muszą pochodzić z jednego, centralnego źródła.</li> <li>14. Rozwiązanie musi umożliwiać integrację w trybie inline z systemami bezpieczeństwa firm trzecich.</li> <li>15. Rozwiązanie musi umożliwiać umieszczanie złośliwych próbek w kwarantannie w celu dalszej analizy.</li> <li>16. Rozwiązanie musi umożliwiać wyłączenie wybranych silników antywirusowych z procesu skanowania.</li> <li>17. Rozwiązanie musi umożliwiać konfigurację progu fałszywych alarmów.</li> </ol>
5.	Moduł ICAP	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi skanować ruch HTTP.</li> <li>2. Rozwiązanie musi integrować się z systemami typu forward proxy obsługującymi protokół ICAP.</li> <li>3. Rozwiązanie musi integrować się z systemami typu reverse proxy obsługującymi protokół ICAP.</li> <li>4. Rozwiązanie musi integrować się z rozwiązaniami pamięci masowej obsługującymi protokół ICAP.</li> <li>5. Rozwiązanie musi integrować się z zaporami sieciowymi nowej generacji (NGFW) obsługującymi protokół ICAP.</li> <li>6. Rozwiązanie musi integrować się z zaporami aplikacyjnymi (WAF) obsługującymi protokół ICAP.</li> <li>7. Rozwiązanie musi umożliwiać definiowanie reguł bezpieczeństwa w oparciu o host, klienta lub dowolny nagłówek HTTP.</li> <li>8. Rozwiązanie powinno umożliwiać wykorzystanie szablonów F5 iApps w celu uproszczenia integracji.</li> <li>9. Rozwiązanie musi zapewniać mechanizmy równoważenia obciążenia (Round Robin) oraz tryb awaryjny (Failover) dla serwera skanującego.</li> <li>10. Rozwiązanie musi obsługiwać ekstrakcję archiwów: Zip, 7z, Jar, RAR, TAR, ISO, CAB, ARJ, LZH, RPM, DEB, LZMA, WIM, SFX, XZ, VDI, VHD, MBR, CPIO, HFS, .apk, .gz, .msi, .tgz, .tbz, .bz2.</li> <li>11. Rozwiązanie musi przetwarzać dokumenty Microsoft Office jako archiwa.</li> </ol>

		<p>12. Rozwiązanie musi obsługiwać archiwa samorozpakowujące: 7zip, WinRAR, PKZIP, IExpress.</p> <p>13. Rozwiązanie musi umożliwiać tworzenie list dozwolonych oraz zabronionych w oparciu o hash pliku, nazwę pliku, typ pliku lub typ MIME.</p>
--	--	---

### III. Wymagania dla usługi wsparcia technicznego.

1. Przedmiot zamówienia objęty będzie usługą wsparcia technicznego producenta rozwiązania świadczoną w miejscu użytkowania Systemu przez okres 12 miesięcy.
2. Bieg terminu wsparcia technicznego rozpoczyna się z chwilą podpisania bez zastrzeżeń Protokołu Odbioru przez obie Strony.
3. W trakcie trwania usługi wsparcia technicznego, Zamawiający będzie uprawniony do pobierania nowych wersji oprogramowania.
4. Usługa wsparcia technicznego zapewni minimum:
  - a) udzielanie odpowiedzi na pytania dotyczące instalacji, używania i konfiguracji oferowanego Systemu,
  - b) bezpośrednie konsultacje w dni robocze w godzinach 7:00 – 19:00 za pośrednictwem portalu zgłoszeniowego lub chat z inżynierem producenta lub jego autoryzowanego polskiego przedstawiciela dotyczące bieżących problemów związanych z instalacją, używaniem i konfiguracją oferowanego Systemu,
  - c) analizę informacji diagnostycznych mającą na celu określenie przyczyny problemu, np. pomoc w interpretacji dokumentacji problemów związanych z instalacją, używaniem i konfiguracją oferowanego Systemu,
  - d) w przypadku znanych defektów oprogramowania, przekazywanie informacji o sposobie ich usunięcia lub obejścia, a także udzielanie pomocy w uzyskaniu poprawek, do otrzymania których Zamawiający jest uprawniony w ramach posiadanej gwarancji i wsparcia technicznego producenta,
  - e) nieprzerwany i nieograniczony dostęp do zasobów elektronicznych, baz samopomocy, FAQ, baz wiedzy producenta oferowanych urządzeń.
  - f) możliwość elektronicznego zgłaszania awarii dotyczących Systemu bezpośrednio do jego producenta w dni robocze, w godzinach 7:00-19:00 w okresie trwania usługi wsparcia technicznego.
  - g) gwarantowany czas odpowiedzi na zgłoszenie o poziomie Krytyczne i Wysokie – 2 godziny; dla zgłoszeń o poziomie Średnie i Niskie – 8 godzin roboczych zgodnie z poniższą tabelą poziomów istotności problemów,

Poziom istotności	Nazwa poziomu	Opis
1	Krytyczny	Występuje całkowita niedostępność systemu albo zdarzenie powoduje krytyczny wpływ na ciągłość funkcjonowania działalności Zamawiającego. Producent zobowiązany jest do niezwłocznego zaangażowania zasobów w godzinach świadczenia wsparcia oraz do podjęcia działań z należytą

		starannością w celu dostarczenia rozwiązania tymczasowego (workaround) i/lub trwałego usunięcia problemu.
2	Wysoki	Funkcjonowanie systemu jest istotnie ograniczone, a znaczące obszary działalności Zamawiającego są negatywnie dotknięte na skutek niedopuszczalnej wydajności, stabilności lub dostępności. Producent zobowiązany jest do zaangażowania odpowiednich zasobów w godzinach świadczenia wsparcia oraz do podjęcia działań zmierzających do obejścia problemu i/lub jego usunięcia.
3	Średni	Większość procesów biznesowych pozostaje operacyjna, jednak występują nieprawidłowości wpływające na komfort lub efektywność pracy użytkowników, w tym m.in. nieprawidłowe wykrywanie, klasyfikowanie lub obsługa zdarzeń bezpieczeństwa. Producent podejmuje działania w godzinach świadczenia wsparcia w celu przywrócenia prawidłowego i satysfakcjonującego poziomu działania systemu.
4	Niski	Zgłoszenie dotyczy zapotrzebowania na informacje, wyjaśnienia lub pomoc w zakresie funkcjonalności, instalacji, konfiguracji lub eksploatacji systemu, w tym również zagadnień związanych z obsługą mechanizmów bezpieczeństwa. Producent udziela wsparcia informacyjnego lub konsultacyjnego w godzinach świadczenia wsparcia, zgodnie z zakresem zgłoszenia.