SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

A. Przedmiot zamówienia

W ramach realizacji przedmiotu zamówienia mieści się:

1. Dostawa licencji centralnie zarządzanego oprogramowania do zabezpieczenia serwerów fizycznych, wirtualnych i w chmurze – w terminie nie dłuższym niż 14 dni kalendarzowych od daty podpisania umowy.
2. Świadczenie serwisu i wsparcia technicznego Producenta przez okres minimum 24 miesięcy, licząc od daty podpisania bez uwag protokołu odbioru.

B. Wymagania dotyczące dostawy sprzętu, oprogramowania oraz licencji

1. Koszty dostawy (w tym koszty opakowania, ubezpieczenia, transportu) ponosi Wykonawca
2. Licencja musi być nowa, wcześniej nieużywana.
3. Wykonawca zobowiązuje się dostarczyć wymagane oprogramowanie oraz licencje pochodzące z legalnego źródła, fabrycznie nowe, zakupione w autoryzowanym kanale sprzedaży producenta i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie Polski.
4. Dostarczone do Zamawiającego licencje muszą być w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie wygenerowanych i przesłanych emailem przez Wykonawcę plików na adres email wskazany przez Zamawiającego (sbt@ncbr.gov.pl).

C. Wymagania dotyczące zakresu usług

1. Wymagania dot. świadczenie wsparcia technicznego i serwisu Producenta zostały szczegółowo opisane w minimalnych wymaganiach poszczególnych urządzeń i oprogramowania.
2. Wymagania dot. gwarancji Producenta zostały szczegółowo opisane w minimalnych wymaganiach oprogramowania

D. Opis istniejącego środowiska

1. Zamawiający oparł swoje środowisko wirtualizacyjne o rozwiązanie vSphere7 Essentials Plus dla 6 CPU z jedną licencjonowaną instancją vCenter Server.
2. Zamawiający posiada i wykorzystuje licencje MSSQL Standard 2019
3. Zamawiający posiada i wykorzystuje licencje Microsoft Windows 2022 Data Center oraz Redhat Enterprise Linux 9

E. Wymagania funkcjonalne dla centralnie zarządzanego oprogramowania do zabezpieczenia serwerów fizycznych, wirtualnych i w chmurze

LP	Cecha	Wymagalne minimalne parametry techniczne
	Wymagania ogólne	1. System musi składać się z centralnej konsoli zarządzania instalowanej w infrastrukturze Zamawiającego (onpremise) oraz agentów zainstalowanych na serwerach. Zamawiający nie dopuszcza rozwiązań chmurowych (np. SaaS) 2. Wszystkie funkcjonalności oprogramowania aktywnej ochrony serwerów muszą być zarządzane z tej samej centralnej konsoli, za pomocą wspólnego interfejsu dostępnego z poziomu przeglądarki internetowej 3. Centralna konsola zarządzania musi umożliwiać definiowanie polityk bezpieczeństwa (także ich przypisywanie do konkretnych maszyn oraz grup maszyn) oraz generowanie raportów, a także zarządzanie agentami (ich aktualizacje, dystrybucja, konfiguracja). 4. Wszystkie wymienione funkcje agenta powinny być realizowane w jednej aplikacji. Uruchomienie dodatkowych funkcji (modułów) nie może wymagać instalacji dodatkowych aplikacji i musi odbywać się

		poprzez ich włączenie w konsoli zarządzającej. Nie dopuszcza się rozwiązania które wymaga instalacji więcej niż jednego agenta; 5. Rozwiązanie zabezpieczające musi posiadać wsparcie dla środowisk skonteneryzowanych typu Docker i zapewniać ochronę hostów Docker: o Wykrywać uruchomione na hoście dockerowym kontenery i chronić je, w zakresie wykrywania niebezpiecznego oprogramowania (Anti-Malware) oraz przed znanymi i zero-day exploitami poprzez wirtualne łatanie nowo znalezionych podatności o Rozwiązanie musi posiadać funkcjonalność zarządzania zdarzeniami i raportowania – natychmiastowe alarmowanie o aktywności niebezpiecznego kodu na chronionym serwerze 6. Rozwiązanie musi umożliwiać nanoszenie zmian w profilach bezpieczeństwa w czasie rzeczywistym bez potrzeby restartu systemu i chronionych obiektów 7. Rozwiązanie musi umożliwiać ochronę następujących dystrybucji systemu operacyjnego Linux: RedHat Enterprise Linux 7, 8, 9, CentOS 7, 8, CentOS Stream 8, 9 SUSE Linux 12, 15, Ubuntu 18, 20, 22, Debian 9, 10, 11 8. Rozwiązanie musi umożliwiać ochronę następujących dystrybucji systemu operacyjnego Windows: Windows 2019, Windows 2022; 9. Rozwiązanie musi mieć funkcjonalność generowania i wysyłania e-mailem na zdefiniowany adres raportów w wybranym formacie (co najmniej .pdf). Możliwość dodania opcjonalnej klasyfikacji wrażliwości informacji dla przesyłanego/wygenerowanego raportu. 10. Rozwiązanie musi oferować interfejs API do automatyzacji, monitorowania i zarządzania bezpieczeństwem oraz integracji z zewnętrznymi systemami. Dokumentacja API musi być powszechnie dostępna. 11. Musi być możliwość wyświetlania listy zdarzeń generowanych przez oprogramowanie (np. wykrycie wirusa) oraz automatycznego wyboru trybu przekazywania zdarzeń do centralnego serwera logów lub systemu typu SIEM z wykorzystaniem szyfrowanego

		kanału komunikacji. Zamawiający wymaga, aby w przypadku przekazywania zdarzeń do SIEM oprogramowanie dodawało do zdarzeń strefę czasową. Wymaga się aby logi były w formacie CEF lub LEEF2. 12. Oprogramowanie musi mieć funkcjonalność tworzenia ról administratorów i przydzielania im uprawnień, co najmniej w zakresie zarządzania: a. Politykami lub grupami polityk; b. Serwerami lub grupami serwerów; c. Poszczególnymi funkcjami systemu ochrony 13. Oprogramowanie musi mieć funkcjonalność synchronizowania użytkowników z ActiveDirectory, a mechanizm SSO musi być realizowany z wykorzystaniem SAML 14. Oprogramowanie musi współpracować z posiadaną przez Zamawiającego bazą danych. Zamawiający nie dopuszcza oprogramowania, które będzie wymagało instalacji innego oprogramowania bazodanowego do funkcjonowania rozwiazania. 15. Oprogramowanie musi posiadać funkcjonalność skanowania urządzeń i na podstawie tego skanu sugerowania oraz automatycznego przypisywania konfiguracji zabezpieczeń mające na celu ułatwienie konfiguracji urządzeń w oprogramowaniu i przypisanie tylko tych zabezpieczeń, które są wymagane do ochrony danego urządzenia.
	Wykrywanie i przeciwdziałanie włamaniom	1. Rozwiązanie musi kontrolować ruch przychodzący i wychodzący w celu wykrycia i zablokowania podejrzanej aktywności. 2. Oprogramowanie musi zapobiegać wykorzystaniu znanych luk w zabezpieczeniach oraz luk typu zero-day. 3. Rozwiązanie musi obsługiwać mechanizm wirtualnego łatania (virtual patching) tj. wykorzystywane są dostarczone przez producenta reguły zapobiegania włamaniom i ochrony przed znanymi lukami w zabezpieczeniach do czasu ich załatania. 4. Oprogramowanie musi posiadać funkcjonalność zapobiegania włamaniom chroniąc również aplikacje internetowe i przetwarzane przez nie dane przed atakami typu SQL injection, atakami typu cross-site scripting i innymi lukami w zabezpieczeniach aplikacji

		internetowych do czasu np. zakończenia prac nad poprawkami kodu. 5. Musi istnieć mechanizm przełączania z trybu monitorowania zdarzeń w tryb blokowania dla całego zestawu reguł dla danej maszyny lub grupy maszyn 6. Moduł wykrywania oraz przeciwdziałania włamań musi posiadać mechanizm zapewniający blokowanie transmisji na podstawie zdefiniowanej charakterystyki (sygnatury ruchu oraz zdefiniowane ciągi znaków - pattern). 7. Oprogramowanie musi posiadać dostarczony przez producenta zestaw reguł dla najpopularniejszych aplikacji/systemów, który może zostać zaaplikowany na podstawie rekomendacji dla danej maszyny, w zależności od zainstalowanych aplikacji, systemu operacyjnego oraz aktualnie wgranych poprawek. 8. W przypadku, gdy dana poprawka, pochodząca od producenta aplikacji lub/i systemu operacyjnego, zostanie wgrana, system faktycznie zostanie załatany, musi nastąpić automatyczne wyłączenie reguł IPS, które chroniły urządzenie.
	Zapora sieciowa	1. Rozwiązanie musi posiadać funkcjonalność dwukierunkowej stanowej zapory sieciowej (stateful) zapewniające izolację interfejsów bez konieczności restartów chronionych serwerów. 2. Oprogramowanie musi wspierać zarówno protokół IPv4 oraz IPv6 3. Oprogramowanie musi umożliwiać kontrolę połączeń sieciowych, wychodzących i przychodzących, z możliwością kontroli niestandardowych portów TCP (reguły definiowane na podstawie protokołu, adresów ip/mac (src, dest), portów, flag) 4. Musi istnieć możliwość szybkiego przełączenia reguł zapory ogniowej z trybu tylko detekcji na tryb blokowania dla danej maszyny lub grupy maszyn 5. Firewall musi mieć możliwość blokowania ruchu, w którym wystąpiły naruszenia definicji protokołów oraz inne anomalie, w tym w szczególności: zdeformowanych pakietów, brakujących flag, pakietów typu X-mass itp. 6. Zapora musi mieć możliwość definiowania akcji jakie

		reguła powinna wykonać na pakietach – logowanie, zezwól, odmów. 7. Zapora musi mieć możliwość definiowania priorytetu określającego kolejność, w jakiej stosowane są reguły.
	Ochrona przed złośliwym oprogramowaniem	1. Oprogramowanie musi chronić systemy Windows i Linux przed złośliwym oprogramowaniem, takim jak malware, wirusy, spyware i trojany. 2. Rozwiązanie musi identyfikować i usuwać złośliwe oprogramowanie oraz blokować złośliwe domeny znane jako np. serwery dowodzenia i kontroli (C&C) 3. Ochrona powinna wykorzystywać mechanizmy uczenia maszynowego oraz monitorowanie zachowania kodu w celu detekcji oraz blokowania zagrożeń. 4. Rozwiązanie musi umożliwiać wybór obszarów skanowania, momentu skanowania (otwarcie i/lub modyfikacja pliku) oraz typów skanowanych plików. Musi być możliwe wykluczenie ze skanowania określonych obszarów dla: a. skanowania w czasie rzeczywistym, b. ręcznego skanowania, c. skanowania określonego w harmonogramie; 5. Musi być możliwość wymuszenia skanowania „na żądanie” w każdej chwili 6. Oprogramowanie musi zapewniać określenie harmonogramu skanowania (dla pojedynczych maszyn oraz grup) 7. Oprogramowanie musi stosować mechanizm skanowania nowych bądź zmienionych plików w celu skrócenia czasu skanowania oraz zwiększenia wydajności skanowania; 8. W przypadku wykrycia złośliwego oprogramowania rozwiązanie musi mieć możliwość podjęcia predefiniowanej akcji, takiej jak: czyszczenie, kwarantanna, usunięcie, przepuszczenie, a także raportowania o zdarzeniach w formie co najmniej: e-mail, SNMP TRAP. 9. Oprogramowanie musi posiadać skuteczną ochronę przed zagrożeniami typu „ransomware”; Ochrona powinna także mieć możliwość wykrycia podejrzanego zachowania (polegającego na szyfrowaniu dużej ilości plików), z możliwością jego zablokowania oraz

		odtworzenia pierwszych zaszyfrowanych plików z pamięci. 10. Rozwiązanie nie może wymagać restartu chronionych maszyn wirtualnych po dokonaniu aktualizacji mechanizmów skanujących oraz definicji wirusów; 11. Oprogramowanie musi posiadać funkcję automatycznego blokowania połączeń do adresów URL na podstawie ich reputacji i kategorii określonych przez producenta systemu, również w przypadku, gdy połączenia te są nawiązywane przez procesy działające na chronionych serwerach. 12. Baza danych o adresach URL musi być na bieżąco utrzymywana przez producenta oprogramowania. Musi istnieć możliwość stworzenia lokalnej repliki tej bazy, synchronizującej się z chmurą producenta, tak aby chronione maszyny nie musiały kontaktować się z nią bezpośrednio przez Internet. 13. Musi istnieć możliwość zdefiniowania statycznej listy adresów URL do zablokowania
2	Gwarancja, serwis i wsparcie techniczne producenta	1. Długość gwarancji i wsparcia producenta zgodnie z ofertą, lecz nie krócej niż 24 miesiące miesięcy, 2. Gwarancja i serwis realizowany zdalnie, z czasem reakcji w zależności od poziomu krytyczności awarii/błędy od 1 do 48 godzin od przyjęcia zgłoszenia (szczegóły niżej), możliwość zgłaszania awarii poprzez dedykowany i zabezpieczony kanał komunikacji elektronicznej. 3. Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez system zgłoszeniowy producenta. 4. Gwarancja i serwis realizowany w trybie 8x5 4h-48h Remote Response Time (dla niekrytycznego poziomu błędu/awarii) oraz 24x7x365 1h Remote Response Time (w przypadku krytycznego poziomu błędu/awarii). 5. Zakres wsparcia technicznego a. Dostęp do pomocy technicznej; b. Dostęp do poprawek, nowych wersji oprogramowania; c. Dostęp do dokumentacji technicznej; d. Dostęp do konta wsparcia, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.

		6. Szczegółowe warunki wsparcia technicznego dla Oprogramowania, o którym mowa powyżej regulować powinny umowy licencyjne lub inne stosowne umowy lub warunki wydane lub zaakceptowane przez producenta Oprogramowania, przy czym umowy takie, ani warunki nie mogą ograniczać wskazanych powyżej wymagań, ani stać z nimi w sprzeczności
3	Dokumentacja	1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
4	Licencja	1. Rządowa (jeśli jest to możliwe, w przeciwnym wypadku komercyjna) 2. Na okres 24 miesięcy 3. Licencja musi obejmować ochronę 60 maszyn wirtualnych
6	Wymagania w zakresie instalacji i konfiguracji	1. Brak – instalacja realizowana przez Zamawiającego