

I. Opis Przedmiotu Zamówienia

1. Przedmiot zamówienia jest:

Zakup systemu do wykrywania podatności sieci i serwerów.

2. Opis systemu posiadanego przez Zamawiającego.

System monitorowania podatności, w skład którego wchodzi jeden serwer z zainstalowanym systemem Nessus Professional w wersji 10.

System nie posiada aktywnej subskrypcji, Zamawiający ma przydzielony tzw. Tenable Customer ID: 20129 dla oprogramowania Nessus Professional.

3. Szczegółowy wykaz przedmiotu zamówienia.

1) Dostawa oprogramowania Tenable Nessus Professional

Nazwa	Oprogramowanie typu Nessus Professional lub równoważne
Licencja	<ol style="list-style-type: none">1. Subskrypcja na oprogramowanie2. Uprawnia do sprawdzania podatności nieograniczonej liczby IP3. Subskrypcja typu On-Premise4. 1 subskrypcja na 24 miesiące / 2 lata
Cechy oprogramowania	<ol style="list-style-type: none">1. Skanowanie podatności (IP4, IP6, sieci hybrydowe)2. Skanowanie systemu docelowego w trybie bez poświadczeń oraz z poświadczeniami3. Obsługiwanie różnych form uwierzytelniania (poświadczenia) dla hostów, systemów operacyjnych, baz danych w tym:<ul style="list-style-type: none">- bazy danych Oracle, DB2, SQL Server, MongoDB, MySQL, PostgreSQL,- hosty, które obejmuje loginy Windows, SSH i SNMPv3- różne usługi, w tym VMware, Palo Alto Networks PAN-OS i usługi katalogowe (ADSI i X.509),- protokoły uwierzytelniania w postaci zwykłego tekstu.4. Zasoby objęte skanowaniem, min.:<ol style="list-style-type: none">1) urządzenia sieciowe (firewall, router, switch),2) storage,3) wirtualizatory (ESX, ESXi, vSphere, vCenter, Hyper-V),4) systemy operacyjne (Windows, Linux, IBM iSeries, Cisco iOS),5) bazy danych (Oracle, DB2, SQL Server, MongoDB, MySQL, PostgreSQL),6) serwery aplikacyjne,7) aplikacje web,8) aplikacje użytkowników końcowych.5. Rodzaje wykrywanych zagrożeń:<ol style="list-style-type: none">1) wirusy,2) malware,3) backdoor,

	<ul style="list-style-type: none"> 4) nieznane procesy, 5) webserwisy ze szkodliwą zawartością, 6) komunikacja z zainfekowanymi botnetami. <ul style="list-style-type: none"> 6. Audyt konfiguracji: COBIT, ITIL, CERT, ISO, NSA 7. Audyt zawartości wrażliwych: dane osobowe (np. numery kart płatniczych, PESEL itd.) 8. Szablony konfiguracji i zestawy polityk dostępne w domyślnej instalacji produktu 9. Szacowanie ryzyka 10. Priorytet zagrożeń 11. Aktualizacje podatności w czasie rzeczywistym 12. Konfigurowalny dashboard wykrytych zagrożeń z uwzględnieniem krytyczności 13. Powiadamianie mailowe z wynikami skanu, rekomendacjami i zaleceniami poprawiającymi bezpieczeństwo 14. Skanowanie w trybie harmonogramu (godzinowe, dzienne, tygodniowe, miesięczne i roczne) 15. Możliwość eksportowania wyników skanowania 16. Możliwość tworzenia raportów na podstawie wyników skanowania: <ul style="list-style-type: none"> 1) PDF, 2) HTML, 3) CSV.
--	--

4. Zasady świadczenia wsparcia technicznego dla Oprogramowania

W ramach wsparcia technicznego dla Oprogramowania, o którym mowa powyżej, Zamawiający ma:

- 1) prawo do bezpłatnego korzystania z wydawanych przez producenta najnowszych wersji, aktualizacji Oprogramowania, poprawek do Oprogramowania;
- 2) dostęp elektroniczny do pomocy technicznej;
- 3) dostęp elektroniczny do bazy wiedzy, dokumentacji, biuletynów i informacji na temat oprogramowania, posiadanych produktów.

Szczegółowe warunki wsparcia technicznego dla Oprogramowania, regulują umowy licencyjne wydane przez producenta Oprogramowania, o ile nie są sprzeczne z niniejszym Opiszem przedmiotu zamówienia.

II. Wymagania ogólne.

1. Dostarczona licencja musi pozwalać na swobodne przenoszenie pomiędzy serwerami (np. w przypadku wymiany serwera).
2. Wykonawca do zaoferowanej licencji, subskrypcji oraz wsparcia technicznego zobowiązuje się dostarczyć Zamawiającemu nośnik z wersją instalacyjną Oprogramowania (dla Oprogramowania w wersji pudełkowej) lub dane dostępne do pobrania Oprogramowania oraz kanału subskrypcji, licencję (umowę licencyjną w wersji papierowej lub elektronicznej) oraz wszystkie wymagane klucze licencyjne i aktywacyjne w formie elektronicznej na adres email: **licensing@stat.gov.pl**.
3. Termin dostarczenia danych dostępowych o których mowa w pkt.2. nastąpi w terminie wskazanym w Ofercie, nie dłuższym niż 30 dni od dnia zawarcia Umowy.
4. Wszystkie licencje pochodzić będą z legalnego, tj. akceptowanego przez producenta Oprogramowania kanału dystrybucji. Wszystkie licencje pochodzić będą z kanału dystrybucji na teren Unii Europejskiej.