Nr sprawy: O-ZP.253.97.2026 Załącznik nr 1

Opis Przedmiotu Zamówienia (OPZ)

Przedłużenie licencji skanera podatności Nessus Expert (Customer ID: 600857) ze wsparciem technicznym producenta na kolejne 12 miesięcy od dnia 23.06.2026 r. lub produkt równoważny.

Licencja w formie elektronicznej.

Równoważność rozumie się poprzez zapewnienie niżej wymienianych funkcjonalności:

1. Skaner podatności infrastruktury IT i aplikacji webowych.
2. Skaner podatności musi być zarządzany przez przeglądarkę.
3. Skaner podatności musi mieć opcję dostarczenia jako oprogramowanie i maszyna wirtualna. W przypadku dostarczenia jako maszyna wirtualna muszą być wspierane środowiska Hyper-V oraz Vmware. W przypadku systemu operacyjnego na którym będzie instalowany produkt jako oprogramowanie, muszą być wpierane co najmniej systemy operacyjne:
   - Windows 11, 10 32/64-bit
   - Windows Server 2012 and 2012 R2 , Windows Server 2016, Windows Server 2019, Windows Server 2022 (x86_64)
   - macOS 12, 13, 14, and 15 (x86_64, Apple Silicon)
   - Amazon Linux 2023
   - CentOS Stream 9 (x86_64)
   - Debian 11 and 12 / Kali Linux 2020 (AMD64)
   - Fedora 38 and 39 (x86_64)
   - Raspberry Pi OS (ARMHF)
   - Red Hat ES 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64, AArch64)
   - Red Hat ES 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) / Rocky Linux 8 (x86_64, AArch64)
   - Red Hat ES 9 / Oracle Linux 9 (including Unbreakable Enterprise Kernel) / Rocky Linux 9 / Alma Linux 9 (x86_64, AArch64)
   - SUSE 12 SP5, SUSE Enterprise 15 SP2 and later (x86_64)
   - Ubuntu 14.04, 6.04, and 17.10 (i386)
   - Ubuntu 14.04, 16.04, 17.10, 18.04, 20.04, 22.04, and 24.04 (AMD64)
   - Ubuntu 18.04 (AArch64, Graviton2)
4. Licencja nie może być ograniczona ilością skanowanych adresów IP.
5. Skaner podatności musi mieć możliwość pracy bez dostępu do Internetu, a dostarczanie nowych reguł skanowania musi odbywać się za pomocą ręcznej aktualizacji z poziomu interfejsu.
6. Aktualizacja reguł wykrywania podatności musi być wykonywana automatycznie w przypadku dostępu systemu do Internetu.
7. Interfejs skanera podatności musi przedstawiać informacje o systemie takie jak: użycie CPU, pamięci, ilość skanowanych systemów, ilość sesji TCP, ruch przesyłany i odbierany do/z skanera.

ul. Bartosza Głowackiego 14; 10-448 Olsztyn +48 89 6131340 sekretariat@wmcnt.pl

8. Skaner podatności musi mieć możliwość określenia ilości jednocześnie skanowanych systemów jak również, maksymalną ilość równoczesnych sesji TCP do pojedynczego skanowanego systemu, maksymalną ilość równoczesnych sesji TCP w przypadku wykonania skanu sieci.
9. Musi być możliwość wymuszenia polityki haseł dla administratorów logujących się do systemu.
10. Skaner podatności musi być dostarczony z predefiniowanymi politykami skanowania. Minimum polityka dotycząca wykrycia hostów w sieci, skanowanie pod kontem artefaktów związanych ze złośliwym oprogramowaniem (malware) .
11. Skaner podatności musi dawać możliwość skanowania systemów pod kontem zgodności z regulacjami takimi jak CIS (Center for Internet Security), DISA (Defence Industry Security Association). W przypadku zgodności z regulacjami, producent musi dostarczać gotowe wzorce polityk zgodności z CIS, DISA jak również musi być możliwość zbudowania własnej polityki sprawdzania pod kontem zgodności z przyjętymi regulacjami w firmie w oparciu o dokumentację dostarczoną przez producenta. Wzorce zgodności z regulacjami dostarczone przez producenta muszą być możliwe do edycji. Sprawdzanie systemu pod kontem zgodności z regulacjami oraz dostęp do wzorców regulacji na stronie producenta nie może wymagać żadnej dodatkowej licencji.
12. Skaner podatności musi mieć możliwość skanowania zewnętrznej powierzchni ataku.
13. Skaner podatności musi mieć możliwość dodawania w pełni kwalifikowanych nazw domen (FQDN).
14. Skaner podatności musi mieć możliwość skanowanie aplikacji internetowych.
15. Skaner podatności musi mieć możliwość skanowanie infrastruktury chmurowej.
16. Skaner podatności musi mieć możliwość przeprowadzania skanów zgodności infrastruktury chmurowej, w tym gotowe polityki skanowania.
17. Skaner podatności musi mieć możliwość tworzenia własnej polityki skanowania, w której administrator wybiera jakie podatności będą sprawdzane.
18. System musi umożliwiać skanowanie z uwierzytelnieniem i bez uwierzytelnienia. W przypadku skanowania z uwierzytelnieniem muszą być wspierane następujące metody:
    - Windows – Kerberos, LM Hash, NTLM Hash, hasło;
    - SSH – kluczy publiczny, Kerberos, hasło, certyfikat;
    - SNMP3;
19. Skaner podatności musi pozwalać na tworzenie jak również używanie dostarczonych przez producenta wzorców skanowania pod kontem konfiguracji systemów bezpieczeństwa i sieciowych. Muszą być wspierane przynajmniej wymienione systemy:
    - FireEye;
    - SonicWall;
    - Fortinet FortiGate;
    - BlueCoat ProxySG;
    - Amazon AWS;
    - Microsoft Azure;
20. System musi pozwalać na tworzenie harmonogramu skanowania podatności jak również uruchomienia skanowania na żądanie.
21. Skaner podatności musi umożliwiać sprawdzenie konfiguracji systemu bez dostępu do niego. Sprawdzenie ma być dokonane na podstawie pliku konfiguracyjnego. Muszą być wspierane przynajmniej systemy jak:
    - FireEye;
    - SonicWall;

ul. Bartosza Głowackiego 14; 10-448 Olsztyn +48 89 6131340 sekretariat@wmcnt.pl

- Fortinet FortiGate;
- BlueCoat ProxySG;

22. System musi umożliwiać skanowanie oraz prezentację wyników skanowania przynajmniej po takich parametrach jak:
    - CVE;
    - CVSS v3;
    - czy jest dostępny exploit;
    - hostname;
    - kiedy była upubliczniona aktualizacja na daną podatność;
    - port;
    - protokół;
    - wrażliwość w oparciu o punktację CVSS;
    - zwartość opisu podatności;
    - Bugtraq ID;
    - CPE;
    - IAVB ID;
23. Skaner podatności musi mieć możliwość przetrzymywania historii wykonanych skanów.
24. Skaner podatności musi mieć możliwość wyeksportowania wyników skanowania przynajmniej do formatów:
    - HTML;
    - CSV;
    - PDF;
25. System musi prezentować wynik skanowania wraz z rekomendacją od jakich aktualizacji zacząć aby wyeliminować największe ryzyko/podatność.
26. System musi umożliwiać zmianę wagi wykrytej podatności w wykonanym skanie jak również uwzględnić zmianę w skanach, które będą wykonane w przyszłości.
27. Skaner podatności musi posiadać API.
28. Skaner podatności musi umożliwiać konfigurację mailowych notyfikacji z wynikami skanu, rekomendacjami i zaleceniami poprawiającymi bezpieczeństwo.
29. Wsparcie techniczne producenta dla skanera podatności:
    - prawo do bezpłatnego korzystania z wydawanych przez producenta najnowszych wersji, aktualizacji, poprawek;
    - dostęp elektroniczny do bazy wiedzy, dokumentacji skanera podatności.

W przypadku produktu równoważnego Dostawca zapewni szkolenie personelu (2 osób) u Zamawiającego z administracji oraz użytkowania skanera podatności.

Szkolenie w wymiarze 16 godzin (2 dni po 8 godzin) na miejscu u Zamawiającego.

Wykonawca przeniesie dotychczasową konfigurację (harmonogramy, wzory raportów, spersonalizowane skany).

ul. Bartosza Głowackiego 14; 10-448 Olsztyn +48 89 6131340 sekretariat@wmcnt.pl