Opis przedmiotu zamówienia - projekt

1 Wstęp

Niniejszy dokument stanowi projekt dokumentu opis przedmiotu zamówienia pod nazwą: **„Testy bezpieczeństwa klasy APT oraz dostawa i wdrożenie oprogramowania do badania podatności w infrastrukturze Urzędu Zamówień Publicznych”**.

2 Cel zamówienia

Celem zamówienia jest przeprowadzenie kompleksowej oceny bezpieczeństwa systemów Urzędu Zamówień Publicznych (UZP) oraz dostawa i wdrożenie narzędzia do ciągłego monitoringu podatności z wykorzystaniem automatycznego skanera. Projekt ma na celu podniesienie poziomu bezpieczeństwa infrastruktury IT UZP, ograniczenie przestrzeni ataku, poprawę odporności na zagrożenia oraz zwiększenie kompetencji zespołu IT Zamawiającego.

2.1 Zakres zamówienia

Zakres zamówienia obejmuje w szczególności:

- modelowanie zagrożeń (threat modeling) i rekomendacje zmian architektury,
- przeprowadzenie testów bezpieczeństwa klasy APT usług udostępnianych przez Urząd w sieci Internet oraz infrastruktury wewnętrznej Urzędu,
- dostawę, wdrożenie i konfigurację oprogramowania do automatycznego skanowania podatności,
- rekomendacje zmian w konfiguracji sieci i politykach bezpieczeństwa,
- szkolenia dla 5 pracowników UZP,
- wsparcie powdrożeniowe oraz konsultacje przy wdrażaniu rekomendacji.

2.2 Zakres podmiotowy

Zamówienie dotyczy wyłącznie infrastruktury Urzędu Zamówień Publicznych, ul. Postępu 17A, 02-676 Warszawa.

2.3 Ochrona informacji i danych

W ramach realizacji zamówienia przewidziane są szczególne wymagania dotyczące ochrony danych wrażliwych. Wykonawca zobowiązany jest do podpisania umowy o zachowaniu poufności (NDA) oraz umowy powierzenia danych zgodnie z RODO.

2.4 Wizja lokalna

Z uwagi na specyfikę infrastruktury oraz konieczność zapewnienia rzetelnej wyceny i realizacji zamówienia, udział w wizji lokalnej jest obowiązkowy dla wszystkich wykonawców zamierzających złożyć ofertę. Wizja lokalna umożliwia zapoznanie się z rzeczywistym stanem środowiska, architekturą sieci oraz politykami bezpieczeństwa. Szczegółowe informacje techniczne i dokumentacja infrastruktury zostaną udostępnione wyłącznie podczas wizji lokalnej po podpisaniu zobowiązania do zachowania poufności.

2.5 Przewidywane rezultaty projektu

Realizacja zamówienia przyczyni się do:

- poprawy odporności infrastruktury UZP na współczesne zagrożenia cybernetyczne,
- wdrożenia skutecznych mechanizmów automatycznego wykrywania podatności,
- zwiększenia kompetencji zespołu IT Zamawiającego w zakresie zarządzania bezpieczeństwem,
- zapewnienia zgodności z najlepszymi praktykami branżowymi i wymogami audytowymi.

3 Opis środowiska i infrastruktury

3.1 Skala środowiska

Środowisko objęte zamówieniem obejmuje:

Serwery fizyczne: 5 jednostek

Maszyny wirtualne: 64 instancje na platformie VMware

Stacje robocze: 367 urządzeń

Użytkownicy: 230 aktywnych kont w domenie

3.2 Segmentacja i architektura sieci

Segmentacja sieci: 30 VLAN-ów z wydzielonymi strefami DMZ

Architektura sieci: 3-warstwowa (Core-Distribution-Access)

Urządzenia brzegowe: Firewall Barracuda NGFW, przełączniki Aruba

Publiczne adresy IP: zakres 31 adresów

Technologie bezprzewodowe: brak sieci Wi-Fi

VPN: rozwiązanie bez uwierzytelniania wieloskładnikowego

3.3 Usługi dostępne z sieci Internet objęte testami

Serwis	**Liczba usług składających się na serwis**	**Liczba formularzy podlegających testom**	**Zakres testów**
espd.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera
wokanda.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera
formularz.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera
ekomentarzpzp.uzp.gov.pl	1 serwis www	-	Konfiguracja serwera
orzeczenia.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera
ankieta.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera
elearning.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera
bzp.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera
miniportal.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera

aukcje.uzp.gov.pl	1 serwis www	do 3 formularzy	Aplikacja www i konfiguracja serwera

3.4 Obecny stan bezpieczeństwa

Zabezpieczenia sieciowe: WAF Barracuda

Oprogramowanie antywirusowe: ESET

Infrastruktura PKI: wewnętrzna

Natywne zabezpieczenia: Microsoft 365

3.5 Zespół techniczny po stronie Zamawiającego

Dział IT: 4 osoby

Specjalista ds. bezpieczeństwa: 1 osoba

Outsourcing: zarządzanie infrastrukturą sieciową

3.6 Informacje uzupełniające

Wszelkie szczegółowe informacje dotyczące:

- wersji systemów operacyjnych i baz danych,
- środowisk testowych,
- polityk bezpieczeństwa,
- systemów backupu i monitoringu,
- zarządzania kontami uprzywilejowanymi,
- rozwiązań do zarządzania tożsamością,
- procedur reagowania na incydenty,
- rozwiązań szyfrowania danych,
- narzędzi do zarządzania konfiguracją,
- systemów redundancji i wysokiej dostępności

zostały zawarte w **Załączniku nr 2 – Szczegółowa dokumentacja środowiska i infrastruktury**, który jest dostępny do wglądu w procedurze wizji lokalnej.

3.7 Wizja lokalna

Z uwagi na konieczność zapewnienia pełnej transparentności oraz umożliwienia rzetelnej wyceny oferty, Zamawiający wymaga obowiązkowego udziału w wizji lokalnej przed złożeniem oferty. Wizja lokalna umożliwia zapoznanie się z rzeczywistym stanem infrastruktury, architekturą sieci, rozmieszczeniem urządzeń oraz politykami bezpieczeństwa.

Warunki wizji lokalnej: Wizja lokalna jest obowiązkowa dla wszystkich Wykonawców zamierzających złożyć ofertę.

- Udział w wizji lokalnej możliwy jest wyłącznie po podpisaniu zobowiązania do zachowania poufności (NDA) stanowiący załącznik nr 1.
- Szczegółowa dokumentacja środowiska i infrastruktury – zostanie udostępniony wyłącznie podczas wizji lokalnej, po podpisaniu NDA (nie jest udostępniany w trakcie konsultacji rynkowych).
- Brak udziału w wizji lokalnej skutkuje odrzucenia oferty na podst. art. 226 ust. 1 pkt 18.

4 Zakres przedmiotu zamówienia

4.1 Ogólne założenia

Zakres zamówienia obejmuje kompleksową ocenę bezpieczeństwa środowiska teleinformatycznego Zamawiającego, w tym testy bezpieczeństwa klasy APT, dostawę i wdrożenie oprogramowania do automatycznego skanowania podatności oraz wsparcie powdrożeniowe. Testy będą realizowane na kopii środowiska produkcyjnego, przygotowanej i udostępnionej przez Zamawiającego.

4.2 Zakres szczegółowy

4.2.1 Modelowanie zagrożeń (threat modeling) i rekomendacje zmian architektury

W zakresie zadania znajduje się wykonanie modelowania zagrożeń w zakresie możliwości:

- Dostępu do systemów backoffice poprzez przełamanie zabezpieczeń serwisów www wystawionych do Internetu.
- Dostępu do systemów backoffice poprzez przełamanie zabezpieczeń VPN.

Rezultat zadania: raport z modelowania zagrożeń, zawierający priorytetyzację ryzyk i zagrożeń, rekomendacje środków zaradczych. Raportowi towarzyszy sesja podsumowująca (warsztat / konsultacja z zespołem Zamawiającego).

4.2.1.1 Weryfikacja poprawności konfiguracji reguł na usłudze VPN, NGFW oraz WAF

Weryfikacja poprawności konfiguracji:

- Polityki konfiguracji bramki VPN
- Polityki konfiguracji NGFW oraz WAF

Zadanie wykonywane na podstawie informacji pochodzących z załącznika „Szczegółowa dokumentacja środowiska i infrastruktury", informacji uzupełniających uzyskanych od pracowników UZP oraz eksportu polityk skonfigurowanych na urządzeniach.

Rezultat zadania: raport z audytu konfiguracji, zawierający listę wykrytych nieprawidłowości i klasyfikację ryzyka, rekomendacje działań naprawczych i optymalizacyjnych. Raportowi towarzyszy sesja podsumowująca (warsztat / konsultacja z zespołem Zamawiającego).

4.2.2 Przeprowadzenie testów bezpieczeństwa klasy APT dla domen publicznych usług udostępnianych przez Urząd w sieci Internet oraz infrastruktury wewnętrznej Urzędu

W zakresie testów APT znajdują się:

- Testy penetracyjne dla domen publicznych ujętych w wykazie 3.3 Usługi dostępne z sieci Internet objęte testami. Testy realizowane będą na kopii środowiska produkcyjnego (kopie serwisów www udostępnione przez Zamawiającego).
- Testy bezpieczeństwa sieci wewnętrznej, w tym próby lateral movement oraz privilege escalation.
- Testy bezpieczeństwa urządzeń końcowych (stacje robocze). Wykonawca otrzyma laptopa służbowego w celu weryfikacji jego konfiguracji i możliwości uzyskania dostępu do danych na nim zapisanych.
- Testy bezpieczeństwa usługi zdalnego dostępu (VPN).

Rezultat zadania: raport dla każdego elementu osobno zawierający badany zakres, listę wykrytych podatności i klasyfikację ryzyka oraz rekomendacje działań naprawczych.

4.2.2.1 Badanie przestrzeni ataku i rekonesans

Wykonanie rekonesansu usług i portów dostępnych z Internetu będących w domenie *.uzp.gov.pl lub adresacji IP Zamawiającego.

Szkolenie dla 5 pracowników z zakresu ponownego użycia narzędzi rekonesansu.

Rezultat zadania: raport zawierający zidentyfikowane usługi (aplikacje) oraz otwarte porty i ich prawdopodobne przeznaczenie.

4.2.2.2 Symulacja ataku po przejęciu serwera wystawionego do Internetu

Wykonawca otrzymuje dostęp do maszyny w DMZ i przeprowadza symulację ataku na inne maszyny, w tym krytyczne serwery lub urządzenia administratorów.

Możliwość wykorzystania socjotechniki w celu uzyskania wyższych uprawnień.

Rezultat zadania: raport z przebiegu ataku i rekomendacje zmian w konfiguracji sieci.

4.2.3 Wdrożenie oprogramowania do automatycznego skanowania podatności sieci i usług, działające w sieci wewnętrznej

Instalacja, konfiguracja i uruchomienie narzędzia do automatycznego skanowania podatności – oprogramowanie Nuclei lub równoważne.

Konfiguracja cotygodniowych skanów usług wewnątrz sieci UZP.

Szkolenie dla 5 pracowników z obsługi narzędzia i metod raportowania.

Dokumentacja powdrożeniowa.

Rezultat zadania: zainstalowane oprogramowanie w sieci wewnętrznej UZP; otrzymanie raportu wygenerowanego automatycznie.

4.2.3.1 Warunki równoważności dla oprogramowania Nuclei

Oprogramowanie równoważne musi posiadać co najmniej:

Możliwość tworzenia własnych testów:

- Oprogramowanie musi umożliwiać definiowanie i uruchamianie testów bezpieczeństwa, które mogą być edytowane i rozszerzane przez użytkownika.

Obsługa wielu protokołów:

- Oprogramowanie musi umożliwiać skanowanie podatności w usługach dostępnych przez co najmniej protokoły HTTP/HTTPS, TCP, DNS.
- Musi istnieć możliwość rozszerzenia obsługi o inne protokoły przez użytkownika.

Skanowanie równoległe (asynchroniczne):

- Oprogramowanie musi umożliwiać jednoczesne skanowanie wielu celów (adresów IP, domen, hostów) z możliwością konfiguracji liczby równoległych wątków.

Możliwość integracji z systemami CI/CD:

- Oprogramowanie musi posiadać możliwość uruchamiania z poziomu linii poleceń oraz integracji z narzędziami automatyzującymi procesy (np. Jenkins, n8n, Power Automate lub równoważne).

Aktualizowana baza szablonów:

- Oprogramowanie musi umożliwiać automatyczną lub ręczną aktualizację bazy testów podatności, w tym pobieranie nowych szablonów z repozytoriów udostępnianych przez producenta.
- Producent powinien zapewniać bezpłatną aktualizacje reguł skanowania.

Raportowanie wyników:

- Oprogramowanie musi generować raporty z przeprowadzonych testów w formacie czytelnym dla człowieka (np. HTML, CSV, JSON lub równoważny).
- Raporty muszą zawierać co najmniej: identyfikator podatności, opis, poziom zagrożenia, adres/zasób, datę i godzinę wykrycia.

Obsługa uwierzytelniania:

- Oprogramowanie musi umożliwiać testowanie zasobów wymagających uwierzytelnienia (np. Basic Auth, Bearer Token, JWT, OAuth2 lub równoważne).

Operowanie w środowisku Zamawiającego:

- Oprogramowanie musi być dostępne w wersji umożliwiającej instalację i uruchomienie na systemach operacyjnych Linux lub Windows.

Wsparcie techniczne i dokumentacja:

- Oprogramowanie musi być udokumentowane w języku polskim lub angielskim, z opisem sposobu instalacji, konfiguracji oraz tworzenia własnych szablonów.
- Musi być zapewnione wsparcie techniczne producenta lub społeczności (np. forum, system zgłoszeń, dokumentacja online).

Licencja:

- Oprogramowanie musi być pozbawione opłat licencyjnych za użytek do działalności instytucji publicznej.

Dostęp do kodu źródłowego:

- Kod źródłowy powinien być publicznie dostępny (np. na portalu github.com), a samo oprogramowanie powinno być publicznie rozpoznawalne i aktywnie rozwijane.

- Za rozpoznawalność uznane zostanie posiadanie co najmniej 20 000 „gwiazdek” (licznik uznań społeczności) na portalu github lub tyle samo na równoważnym repozytorium publicznym;
- Za oprogramowanie aktywnie rozwijanie uznane zostanie takie, dla którego zmiany (ang. commits) w publicznym repozytorium kodu zachodzą średnio nie rzadziej niż raz w tygodniu przez ostatni rok.

4.2.4 Wdrożenie oprogramowania zarządzania podatnościami oraz automatycznego skanowania podatności usług wystawionych do Internetu

Dostarczenie oprogramowania chmurowego, umożliwiającego:

4.2.4.1 pozyskiwanie, agregowanie, powiadamianie administratorów i zarządzanie statusami (aktualne/usunięte) wynikami skanowania podatności zidentyfikowanych w wyniku działania oprogramowania wskazanego w 4.2.2.2 Symulacja ataku po przejęciu serwera wystawionego do Internetu

Wykonawca otrzymuje dostęp do maszyny w DMZ i przeprowadza symulację ataku na inne maszyny, w tym krytyczne serwery lub urządzenia administratorów.

Możliwość wykorzystania socjotechniki w celu uzyskania wyższych uprawnień.

Rezultat zadania: raport z przebiegu ataku i rekomendacje zmian w konfiguracji sieci.

- Wdrożenie oprogramowania do automatycznego skanowania podatności sieci i usług, działające w sieci wewnętrznej,
- wykonywania skanowania podatności usług dostępnych z sieci Internet zapewniając funkcjonalności badania podatności minimum takie same jak oprogramowania dostarczonego w pkt. wyżej oraz: rekonesansu (identyfikacji usług dostępnych w zakresie wskazanych domen i subdomen oraz adresów IP).

Wymagania dotyczące oprogramowania

1. Oprogramowanie musi umożliwiać automatyczne skanowanie podatności usług sieciowych wystawionych do Internetu, w tym protokołów HTTP/HTTPS, TCP, DNS oraz innych powszechnie wykorzystywanych w infrastrukturze IT.
2. System musi umożliwiać zarządzanie wykrytymi podatnościami, w tym:
    a. klasyfikację i priorytetyzację podatności,
    b. przypisywanie zadań naprawczych,
    c. śledzenie statusu usunięcia podatności,
    d. generowanie raportów i statystyk.

4.2.4.2 Oprogramowanie musi umożliwiać integrację z narzędziem dostarczonym w ramach zadania w 4.2.2.2 Symulacja ataku po przejęciu serwera wystawionego do Internetu

Wykonawca otrzymuje dostęp do maszyny w DMZ i przeprowadza symulację ataku na inne maszyny, w tym krytyczne serwery lub urządzenia administratorów.

Możliwość wykorzystania socjotechniki w celu uzyskania wyższych uprawnień.

Rezultat zadania: raport z przebiegu ataku i rekomendacje zmian w konfiguracji sieci.

3. Wdrożenie oprogramowania do automatycznego skanowania podatności sieci i usług, działające w sieci wewnętrznej, w szczególności:
    a. zdalne uruchamianie skanowania na lokalnych instancjach,
    b. pobieranie i agregowanie wyników skanowania,
    c. centralne zarządzanie szablonami i harmonogramami skanowania.
4. System musi umożliwiać harmonogramowanie skanowania oraz uruchamianie skanowania na żądanie.
5. Oprogramowanie musi umożliwiać zarządzanie szablonami testów podatności, w tym:
    a. pobieranie i aktualizację szablonów z repozytoriów publicznych (publikowanych przez różne podmioty w Internecie) i tworzonych przez zamawiającego,
    b. tworzenie i edycję własnych szablonów testów.
6. Oprogramowanie musi być dostępne w modelu chmurowym (SaaS) lub jako rozwiązanie instalowane na infrastrukturze Zamawiającego (on-premise).
7. System musi umożliwiać integrację z lokalnymi narzędziami skanującymi – w szczególności z oprogramowaniem wskazanym w 4.2.2.2.
8. Komunikacja pomiędzy systemem centralnym a lokalnymi instancjami skanującymi musi być szyfrowana (np. TLS 1.2 lub wyższy).
9. Oprogramowanie musi umożliwiać zarządzanie użytkownikami i nadawanie uprawnień zgodnie z rolami (administrator, operator, audytor).
10. System musi umożliwiać eksport wyników skanowania oraz raportów w formatach: CSV, JSON, PDF lub równoważnych.
11. System musi posiadać dokumentację techniczną i użytkową w języku polskim lub angielskim.
12. Dostawca musi zapewnić wsparcie techniczne w zakresie instalacji, konfiguracji oraz bieżącej eksploatacji systemu.
13. Oprogramowanie musi być regularnie aktualizowane, w szczególności w zakresie nowych szablonów podatności i poprawek bezpieczeństwa.
14. System musi umożliwiać rejestrowanie i audytowanie działań użytkowników.

15. Oprogramowanie musi umożliwiać integrację z systemami zarządzania incydentami bezpieczeństwa (SIEM) oraz systemami ticketowymi (GLPI).
16. Oprogramowanie musi umożliwić połączenie z Azure Active Directory celem ujednolicenia sposobu logowania do usług.
17. Wykonawca zapewni licencje dla co najmniej 5 pracowników UZP (administratorów).

Zakres usług wdrożeniowych

Wykonawca zapewni konfiguracje do automatycznego wykonania:

1. Skanowanie raz w tygodniu usług wskazanych w 3.3 Usługi dostępne z sieci Internet objęte testami
2. Rekonesans innych usług z domeny *.uzp.gov.pl
3. Generowanie raportów z każdego testu w postaci panelu dostępnego przez przeglądarkę umożliwiającego zapoznanie się ze zidentyfikowanymi podatnościami i ich poziomem wrażliwości według CVE lub równoważnego standardu;
4. Powiadomienia na adres email wskazanych pracowników UZP o wykrytych podatnościach.

Wykonawca zapewni szkolenie dla 5 osób z wykonanej konfiguracji.

Rezultat zadania: dostęp do oprogramowania którego administratorem będą pracownicy Urzędu w okresach:

- do 30.06.2026 – w ramach zamówienia;
- na okres roczny od 01.07.2026 do 30.06.2027 – w ramach prawa opcji.

4.2.5 Asysta przy wdrażaniu rekomendacji

Wsparcie zespołu technicznego Zamawiającego przy wdrażaniu rekomendacji wynikających z testów.

Zakres: 20 godzin konsultacji powdrożeniowych online.

Rezultat zadania: wykaz zawierający datę, godzinę i czas trwania konsultacji razem z krótkim określeniem celu konsultacji.

4.3 Zakres wyłączony z zamówienia

Elementy świadomie wyłączone z zakresu zamówienia:

- Testy odporności na ataki DDoS.
- Testy bezpieczeństwa aplikacji mobilnych.

- Testy bezpieczeństwa usług chmurowych poza Microsoft 365.
- Analiza polityk bezpieczeństwa, analiza logów bezpieczeństwa, monitoring incydentów w trakcie testów.
- Analiza zgodności z normami (np. ISO 27001, KRI).

4.4 Zakres opcjonalny (opcja)

4.4.1 Retesty (powtórne testy bezpieczeństwa) po wdrożeniu poprawek w zakresie konfiguracji VPN, NGFW oraz WAF

Zamawiający zastrzega sobie prawo do skorzystania z opcji polegającej na zleceniu Wykonawcy przeprowadzenia powtórnych testów bezpieczeństwa (retestów) po wdrożeniu poprawek usuwających wykryte podatności w zakresie 4.2.1.1 Weryfikacja poprawności konfiguracji reguł na usłudze VPN, NGFW oraz WAF.

Skorzystanie z prawa opcji następuje poprzez złożenie przez Zamawiającego pisemnego zlecenia w terminie maksymalnym do 2 miesięcy przed końcem obowiązywania umowy.

Wykonawca zobowiązany jest do realizacji retestów w terminie nie dłuższym niż 40 dni roboczych od dnia otrzymania zlecenia.

4.4.2 Wykonanie hardeningu wybranych systemów operacyjnych

Przedmiotem opcji jest wykonanie usługi hardeningu wybranych maszyn wirtualnych Zamawiającego, obejmującej serwery Windows Server 2016 i wyższe oraz serwery Linux (Debian, Ubuntu).

Wycenie podlega hardening pojedynczej maszyny. Zamawiający może zlecić w prawie opcji hardening do 20 maszyn poszczególnych typów.

4.4.2.1 Wymagania ogólne

4.4.2.1.1 Standardy i zgodność

- Dla Windows: Microsoft Security Baselines (SCT) oraz CIS Benchmarks; minimalny poziom zgodności CIS ≥ 90% (po odliczeniu wyjątków merytorycznie uzasadnionych i zatwierdzonych przez Zamawiającego).
- Dla Linux: zgodność z CIS, OpenSCAP lub USG (Ubuntu Security Guide – profile CIS/STIG; RHEL/Alma/Rocky – OpenSCAP + SCAP Security Guide – profile cis|stig).

4.4.2.1.2 Metodyka realizacji

Realizacja przebiegać powinna w etapach:

1. Discover & Assess: inwentaryzacja ról/usług, backup konfiguracji, identyfikacja zależności, wstępny skan podatności. Wynikiem etapu jest raport podsumowujący aktualny stan maszyny.

2. Plan & Risk: plan zmian z analizą ryzyka i rollbackiem. Wynikiem etapu jest propozycja wyjątków do akceptacji Zamawiającego.
3. Pilot (środowisko testowe): wdrożenie w trybie audytu, testy funkcjonalne. Wynikiem etapu jest możliwość realizacji testów funkcjonalnych przez Zamawiającego.
4. Rollout (środowisko produkcyjne): wdrożenie zgodnie z oknami serwisowymi, zmiany atomowe, komunikacja, punkt przywrócenia. Wynikiem etapu jest wdrożenie ustalonej konfiguracji na maszynie produkcyjnej.
5. Walidacja: kontrole techniczne, skany podatności, pomiary zgodności, przegląd logów. Wynikiem etapu jest potwierdzenie wykonania usługi przez Zamawiającego.
6. Handover: dokumentacja „as-built", runbooki, przekazanie artefaktów, sesja Q&A. Wynikiem etapu jest dokumentacja powdrożeniowa.

4.4.2.2 Zakres techniczny

4.4.2.2.1 Windows Server 2016/2019

- Zastosowanie aktualnych Microsoft Security Baselines (SCT) przez GPO/Intune.
- Policy Analyzer do oceny konfliktów i dokumentowania odchyleń.
- Zdalny dostęp (RDP/NLA): wymuszenie NLA, TLS, „Always prompt for password", ograniczenie grup RDP do kont JIT/JEA.
- TLS/Schannel: wyłączenie TLS 1.0/1.1, wymuszenie TLS 1.2/1.3, wyłączenie słabych szyfrów (RC4/3DES).
- Ochrona endpointa: ESET Protect aktywny, reguły ASR, Tamper Protection, LSA Protection, Credential Guard.
- Kontrola aplikacji: AppLocker/WDAC (tryb Audit → Enforce).
- Szyfrowanie dysków: BitLocker XTS-AES 256, escrow kluczy do AD/Azure AD/MBAM, TPM+PIN dla krytycznych.
- Firewall: domyślnie deny inbound, precyzyjne reguły, logowanie allowed/blocked.
- SMB/Legacy: SMBv1 wyłączony, podpisywanie/szyfrowanie SMB wymuszone, brak ekspozycji SMB do Internetu.
- Audyt/logowanie: Advanced Audit Policy, Sysmon, Windows Event Forwarding do SIEM.

- Konta/hasła: silne polityki, blokady kont, ograniczenie praw logowania, JIT/JEA, Protected Users.
- Aktualizacje: WSUS/WUfB, priorytet dla poprawek security, uwierzytelnione skany podatności po każdej fali zmian.

4.4.2.2.2 Linux (Debian/Ubuntu)

- Zgodność z CIS/OpenSCAP/USG.
- Minimalna instalacja pakietów, usunięcie zbędnych usług.
- Automatyczne aktualizacje bezpieczeństwa (unattended-upgrades/dnf-automatic/kpatch).
- Podłączenie do domeny, dostęp tylko dla grupy w domenie.
- SSH: PermitRootLogin no, tylko klucze, silne szyfry/MAC/KEX, ograniczenia użytkowników.
- Usługi/porty: wyłączenie zbędnych demonów.
- Kernel/sysctl: wyłączenie IP forwarding, włączenie rp_filter, tcp_syncookies, brak redirectów/source routing, logowanie martians.
- Firewall: domyślnie deny inbound, reguły tylko dla wymaganych portów/źródeł.
- Logowanie/audyt: rsyslog/journald do SIEM, auditd, AIDE.
- TLS: wymuszenie TLS 1.2+, automatyzacja certyfikatów, HSTS, OCSP stapling.
- NTP/chrony: konfiguracja z zaufanymi źródłami.

4.4.2.3 Kryteria akceptacyjne

4.4.2.3.1 Windows

- CIS zgodność ≥ 90% (po wyłączeniu uzasadnionych wyjątków).
- 0 krytycznych i 0 wysokich podatności w skanie końcowym.
- RDP niedostępne bezpośrednio z Internetu, dostęp tylko przez RDG/VPN z MFA i allowlistą IP.
- TLS 1.0/1.1 wyłączone, testy sslscan/nmap-ssl potwierdzają TLS ≥ 1.2, brak RC4/3DES.
- ASR w trybie Enforce, brak negatywnego wpływu na aplikacje produkcyjne.
- AppLocker/WDAC w trybie Enforce z udokumentowanymi wyjątkami.

- BitLocker: 100% woluminów zaszyfrowane, klucze w escrow, raport manage-bde OK.
- Firewall: inbound default deny, otwarte tylko porty/usługi z listy i zakresy źródeł.
- WEF/Sysmon: logi do SIEM, brak błędów subskrypcji, rozmiary logów zgodne z wytycznymi.

4.4.2.3.2 Linux

- Profil CIS zastosowany, remediacje po przeglądzie.
- Minimalny zestaw pakietów, zbędne usługi wyłączone/usunięte.
- PAM: pwquality, pwhistory, faillock włączone.
- SSH: root off, klucze only, silne szyfry/MAC/KEX, ograniczenia użytkowników.
- Firewall: default deny inbound, reguły tylko dla wymaganych portów/źródeł.
- sysctl: rp_filter, syncookies, brak redirectów/source routing, log_martians.
- SELinux/AppArmor enforcing.
- rsyslog/journald→SIEM, auditd reguły, AIDE cykliczne.
- TLS 1.2+, mocne ciphers, certy automatyczne.
- NTP/chrony poprawnie skonfigurowane.
- Skany podatności i walidacja CIS/STIG wykonane.

4.4.2.4 Rezultaty zadania

- Plan zmian + rejestr ryzyk i wyjątków (z uzasadnieniem i akceptacją).
- Backup i eksport: GPO, Policy Analyzer, reguły FW, konfiguracje ASR, AppLocker/WDAC, Sysmon, WEF, BitLocker, auditpol, listy usług/portów.
- Raporty zgodności: CIS-CAT/Policy Analyzer/MDE baseline compliance, wyniki skanów podatności przed i po.
- Dokumentacja „as-built”: opis zmian, wyjątki, instrukcje rollback, runbook operacyjny, checklisty.

4.4.2.5 Wymagania organizacyjne

- Wykonawca zobowiązany jest do realizacji usługi zgodnie z harmonogramem uzgodnionym z Zamawiającym, z uwzględnieniem okien serwisowych.

- Wszelkie wyjątki od standardów muszą być uzasadnione i zatwierdzone przez Zamawiającego.
- Wykonawca zapewni wsparcie powdrożeniowe, w tym sesję Q&A oraz przekazanie pełnej dokumentacji.

4.4.3 Dodatkowy pakiet godzin konsultacji powdrożeniowych w wysokości 100 godzin.

Wykonawca zapewni pakiet godzin konsultacji w wymiarze 100 godzin konsultacyjnych w okresie obowiązywania umowy.

4.4.4 Dostęp na rok do oprogramowania dostarczonego w ramach 4.2.4 Wdrożenie oprogramowania zarządzania podatnościami oraz automatycznego skanowania podatności usług wystawionych do Internetu

Wykonawca zapewni dostęp do oprogramowania przez okres roku na warunkach na jakich zostało ono dostarczone w ramach umowy.

4.5 Wymagania ogólne

Metodologia testów: Testy bezpieczeństwa muszą być realizowane w trybie “white box” oraz “green box”, z pełnym dostępem do dokumentacji technicznej udostępnionej przez Zamawiającego.

Okna czasowe: Testy mogą być prowadzone wyłącznie w dni robocze (poniedziałek-czwartek), w godzinach 6:30-8:00 oraz 16:00-20:00.

5 Raportowanie i dokumentacja z badań podatności będących rezultatem zadania 4.2.2 i podzadań

5.1 Wymagania ogólne

Wykonawca zobowiązany jest do sporządzenia osobnych raportów z badania podatności dla każdego systemu objętego testami, osobnego raportu z badania sieci oraz osobnego raportu z modelowania zagrożeń.

Raporty z testów penetracyjnych muszą być przekazywane osobno dla każdego systemu, a także podpisywane elektronicznie przez wykonawcę.

Raporty z testów automatycznych generowane przez narzędzie do zarządzania podatnościami muszą być dostępne w formacie elektronicznym (CSV, XML, PDF) oraz w wersji angielskiej (polska opcjonalnie).

5.1.1 Zakres i szczegółowość raportów

Każdy raport musi zawierać:

- szczegółowy opis techniczny zidentyfikowanych podatności,

- ocenę poziomu ryzyka zgodnie ze skalą CVSS,
- potencjalne konsekwencje wykorzystania podatności,
- klasyfikację podatności (CVE/CVSS lub równoważną),
- opis zagrożenia i systemu, którego dotyczy,
- rekomendacje naprawcze,
- status podatności (usunięta/pozostająca/nowa – w przypadku retestów).

Raport końcowy musi podsumowywać wszystkie działania, wyniki testów, rekomendacje oraz wnioski ogólne.

5.1.2 Częstotliwość i forma raportowania

Raporty z automatycznych skanów podatności mają być generowane i przekazywane Zamawiającemu w formie elektronicznej co tydzień (zbiorcze wyniki skanów z danego dnia).

Raporty z testów penetracyjnych przekazywane są po zakończeniu każdego etapu testów oraz po zakończeniu całości prac.

Raporty z retestów (opcja) powinny odnosić się do pierwszego raportu, wskazując na podatności usunięte, pozostające oraz wykryte nowe.

5.1.3 Raportowanie incydentów i podatności krytycznych

W przypadku wykrycia podatności wysokiego ryzyka (High/Critical) wykonawca zobowiązany jest do niezwłocznego poinformowania Zamawiającego (bez zbędnej zwłoki po ich wykryciu), niezależnie od harmonogramu raportowania.

5.1.4 Dokumentacja powdrożeniowa

Wykonawca zobowiązany jest do przekazania dokumentacji powdrożeniowej obejmującej:

- opis wdrożonego rozwiązania,
- instrukcję instalacji i konfiguracji narzędzi,
- opis integracji z innymi systemami (jeśli dotyczy),
- instrukcję użytkownika (dla administratora i użytkownika),
- dokumentację harmonogramów skanowania,
- przykładowe raporty,
- treść licencji,
- procedurę backupu i odtwarzania konfiguracji narzędzi.

5.1.5 Materiały szkoleniowe

Po przeprowadzonych szkoleniach wykonawca zobowiązany jest przekazać Zamawiającemu materiały szkoleniowe (prezentacje, instrukcje dla uczestników).

5.1.6 Przekazywanie raportów i dokumentacji

Wszystkie raporty i dokumentacja przekazywane są wyłącznie Zamawiającemu w formie elektronicznej.

Raporty z testów penetracyjnych muszą być podpisane elektronicznie przez wykonawcę.

Raporty z automatycznych skanów nie wymagają podpisu elektronicznego.

5.1.7 Archiwizacja i dostępność raportów

Zamawiający nie wymaga archiwizowania raportów przez wykonawcę po zakończeniu projektu.

5.2 Wymagania dodatkowe i opcje

5.2.1 Retesty i raporty z retestów (opcja)

W przypadku zlecenia retestów po wdrożeniu poprawek, wykonawca sporządza raport z retestu, który odnosi się do pierwotnego raportu i wskazuje podatności usunięte, pozostające oraz nowe.

5.2.2 Raportowanie skuteczności wdrożonych rekomendacji

W ramach opcji przewidziana jest możliwość raportowania skuteczności wdrożonych rekomendacji po retestach.

5.2.3 Raportowanie incydentów bezpieczeństwa

W przypadku wykrycia incydentu bezpieczeństwa podczas testów, wykonawca zobowiązany jest do niezwłocznego zgłoszenia tego faktu Zamawiającemu.

6 Harmonogram realizacji

6.1 Ogólne założenia

Okres realizacji umowy: Umowa obowiązuje przez 3 lata od daty podpisania, przy czym wszystkie działania podstawowe (modelowanie zagrożeń, wdrożenie narzędzi, testy bezpieczeństwa, raport końcowy) muszą zostać zakończone do dnia 1 czerwca 2026 r.

Start prac: Przewidywany start realizacji zamówienia: październik 2025 r.

Szczegółowy harmonogram: Szczegółowy harmonogram realizacji poszczególnych zadań zostanie uzgodniony z Zamawiającym przed rozpoczęciem każdego etapu. W OPZ określono wyłącznie ogólne wytyczne.

6.1.1 Etapy realizacji i kamienie milowe

6.1.1.1 Etap 1: Modelowanie zagrożeń oraz wdrożenie narzędzia do automatycznego skanowania podatności

Zawiera zadania:

- 4.2.1 Modelowanie zagrożeń (threat modeling) i rekomendacje zmian architektury
- 4.2.3 Wdrożenie oprogramowania do automatycznego skanowania podatności sieci i usług, działające w sieci wewnętrznej
- 4.2.4 Wdrożenie oprogramowania zarządzania podatnościami oraz automatycznego skanowania podatności usług wystawionych do Internetu

Termin realizacji: do końca stycznia 2026 r.

6.1.1.2 Etap 2: Rekonfiguracja sieci przez Zamawiającego

Termin realizacji: styczeń – luty 2026 r.

Zamawiający wdraża rekomendacje dotyczące segmentacji i konfiguracji sieci na podstawie raportu z modelowania zagrożeń i skanowania.

Rezultat: potwierdzenie wdrożenia zmian przez Zamawiającego.

6.1.1.3 Etap 3: Testy bezpieczeństwa klasy APT oraz testy penetracyjne

Termin realizacji: luty – marzec 2026 r.

Zawiera zadanie:

- 4.2.2 Przeprowadzenie testów bezpieczeństwa klasy APT dla domen publicznych usług udostępnianych przez Urząd w sieci Internet oraz infrastruktury wewnętrznej Urzędu

6.1.1.4 Etap 4: Konsultacje powdrożeniowe i asysta przy wdrażaniu rekomendacji

Termin realizacji: kwiecień – maj 2026 r.

Zadanie:

- 4.2.5 Asysta przy wdrażaniu rekomendacji

6.1.1.5 Etap 5: Raport końcowy

Termin realizacji: maj do 20.06.2026 r.

Przekazanie raportu końcowego podsumowującego wszystkie działania.

Rezultat: akceptacja raportu końcowego.

6.1.2 Harmonogram działań automatycznych

Pierwsze skanowanie usług dostępnych z Internetu i sieci wewnętrznej powinno zostać uruchomione w ciągu 30 dni od podpisania umowy.

Kolejne skanowania powinny być realizowane automatycznie, zgodnie z harmonogramem tygodniowym.

6.1.3 Retesty i działania opcjonalne

Retesty (powtórne testy bezpieczeństwa po wdrożeniu poprawek) oraz integracja narzędzi z SIEM realizowane są w ramach prawa opcji, na odrębne zlecenie Zamawiającego.

Harmonogram działań opcjonalnych zostanie każdorazowo uzgodniony z Zamawiającym przed ich realizacją. W przypadku retestów raport powinien być przekazany w terminie nie dłuższym niż 30 dni od zlecenia.

6.1.4 Przerwy i ograniczenia w realizacji

Harmonogram powinien uwzględniać okresy świąteczne, urlopowe oraz inne przerwy wskazane przez Zamawiającego.

Wszelkie zmiany terminów wymagają uzgodnienia z Zamawiającym.

6.1.5 Akceptacja i raportowanie postępu

Każdy etap kończy się przekazaniem raportu cząstkowego lub końcowego do akceptacji Zamawiającego.

Zamawiający ma prawo zgłosić uwagi do raportów w terminie 10 dni roboczych od ich przekazania. Wykonawca zobowiązany jest do uwzględnienia uwag i przekazania poprawionych raportów w terminie 7 dni roboczych.

Postęp realizacji będzie raportowany Zamawiającemu po zakończeniu każdego etapu.

Uwaga: Szczegółowy harmonogram realizacji poszczególnych zadań oraz terminy przekazania raportów zostaną uzgodnione z Zamawiającym przed rozpoczęciem każdego zadania i mogą być dostosowane do bieżących potrzeb oraz dostępności środowiska testowego.

7 Wymagania dotyczące Zespołu Wykonawcy

7.1 Zespół wykonawcy

Minimalny skład zespołu: 4 osoby, w tym:

- co najmniej 2 osoby posiadające certyfikaty z zakresu penetration testing (np. OSCP, CEH, GPEN lub równoważne),

- co najmniej 1 osoba posiadająca certyfikat web application security (np. GWAPT, eWPT, lub równoważny),
- co najmniej 1 osoba z doświadczeniem w administracji systemami Windows i Linux,
- co najmniej 1 osoba z doświadczeniem w prowadzeniu szkoleń z zakresu bezpieczeństwa IT.

Kluczowi członkowie zespołu muszą posługiwać się językiem polskim w stopniu umożliwiającym prowadzenie szkoleń i konsultacji.

7.2 Certyfikaty i normy

Wykonawca musi wykazać się wdrożonym systemem zarządzania bezpieczeństwem informacji zgodnym z normą ISO 27001 (potwierdzenie certyfikatem lub oświadczeniem).

Wymagane są kopie certyfikatów potwierdzających kwalifikacje członków zespołu.

8 Wymagania techniczne i operacyjne

Wdrożenie narzędzi: Wykonawca musi zapewnić wdrożenie i konfigurację narzędzia do automatycznego skanowania podatności oraz narzędzia do zarządzania podatnościami, zgodnie z wymaganiami funkcjonalnymi i technicznymi OPZ.

Praca w środowisku izolowanym: Narzędzie do badania podatności musi umożliwiać pracę w środowisku izolowanym (bez dostępu do Internetu) oraz eksport wyników do pliku.

Wsparcie powdrożeniowe: Wykonawca zobowiązany jest do zapewnienia wsparcia powdrożeniowego w wymiarze minimum 20 godzin konsultacji w okresie 3 miesięcy od zakończenia testów bezpieczeństwa.

Wsparcie dla systemów operacyjnych: Narzędzia wdrażane przez wykonawcę muszą działać na systemach Windows oraz Linux.