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. Szczegóły w 3.7 Wizja lokalna – dostęp do architektury i segmentacji sieci.

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: Barracuda (NGFW i VPN), 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, Active Directory

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 – dostęp do architektury i segmentacji sieci

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, liczbą i rodzajem maszyn wirtualnych i uruchomionych na nich systemach.

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 pod katem wskazanych poniżej scenariuszy. Modelowanie powinno uwzględniać wektory ataku na systemy oraz socjotechniczne, gdzie użytkownik nakłaniany jest do wykonania akcji umożliwiającym atakującym przejęcie chronionej informacji. Wykonawca uwzględni co najmniej 1 warsztat w siedzibie Zamawiającego dla każdego ze wskazanych scenariuszy, trwający co najmniej 3 godziny. Zamawiający będzie również uczestniczył w warsztatach online po uzgodnieniu harmonogramu.

4.2.1.1 Dostępu do systemów backoffice poprzez przełamanie zabezpieczeń serwisów www wystawionych do Internetu

Zakres modelowania:

- Analiza możliwych scenariuszy ataku na publicznie dostępne aplikacje webowe (np. SQLi, XSS, RCE, CSRF, brute-force, ataki na logikę biznesową).
- Identyfikacja ścieżek dostępu z serwisów www do systemów backoffice (np. przez API, integracje, połączenia bazodanowe, mechanizmy SSO).
- Ocena potencjalnych skutków przełamania zabezpieczeń (eskalacja uprawnień, dostęp do danych, lateral movement).

Informacje jakie zostaną udostępnione przez UZP na potrzeby wykonania modelowania:

- Lista wszystkich publicznie dostępnych serwisów www, ich adresów, domen, subdomen.
- Opis architektury logicznej i fizycznej (topologia sieci, segmentacja, strefy DMZ, połączenia z backoffice).
- Wersje i technologie aplikacji (frameworki, serwery www, bazy danych, komponenty zewnętrzne).
- Mapowanie powiązań serwisów www z systemami backoffice (np. jakie API, jakie bazy danych, jakie mechanizmy uwierzytelniania).
- Konfiguracja zabezpieczeń (WAF, reverse proxy, ACL, reguły firewall, mechanizmy uwierzytelniania i autoryzacji).
- Polityki zarządzania kontami i uprawnieniami (szczególnie kont serwisowych i integracyjnych).
- Informacje o backupach, redundancji i procedurach odtwarzania.

4.2.1.2 Dostęp do systemów backoffice poprzez przełamanie zabezpieczeń VPN

Zakres modelowania:

- Analiza możliwych scenariuszy ataku na infrastrukturę VPN (np. brute-force, credential stuffing, exploity na oprogramowanie VPN, ataki na MFA, przejęcie sesji).
- Identyfikacja ścieżek dostępu z VPN do systemów backoffice (jakie zasoby są dostępne po zestawieniu tunelu).

- Ocena skutków przełamania zabezpieczeń VPN (eskalacja uprawnień, lateral movement, dostęp do krytycznych systemów).

Informacje jakie zostaną udostępnione przez UZP na potrzeby wykonania modelowania:

- Opis architektury VPN (rodzaj rozwiązania, producent, wersja).
- Konfiguracja polityk dostępu (jakie sieci/zasoby są dostępne przez VPN, segmentacja, VLAN-y).
- Mechanizmy uwierzytelniania (hasła, certyfikaty, MFA, integracja z AD/AAD).
- Polityki zarządzania kontami VPN (kto ma dostęp, jak są nadawane i odbierane uprawnienia, polityki haseł).
- Logi dostępu i mechanizmy monitorowania sesji VPN.
- Lista reguł VPN.

4.2.1.3 Dostęp do systemów backoffice poprzez przejęcie komputera pracownika

Zakres modelowania:

- Analiza scenariuszy ataku po uzyskaniu dostępu do stacji roboczej użytkownika (np. malware, credential harvesting, privilege escalation, lateral movement, ataki na AD).
- Identyfikacja ścieżek dostępu z komputera użytkownika do systemów backoffice (np. przez mapowane dyski, aplikacje klienckie, RDP, SSH, przeglądarki).
- Ocena skutków przejęcia stacji roboczej (dostęp do danych, eskalacja uprawnień, rozprzestrzenianie się w sieci).

Informacje jakie zostaną udostępnione przez UZP na potrzeby wykonania modelowania:

- Opis typowych stacji roboczych (systemy operacyjne, wersje, zainstalowane oprogramowanie, polityki bezpieczeństwa).
- Polityki zarządzania uprawnieniami użytkowników (standardowe vs. uprzywilejowane konta, dostęp do zasobów sieciowych).
- Mechanizmy ochrony endpointów (AV, EDR, DLP, szyfrowanie dysków, polityki aktualizacji).

- Konfiguracja sieci (segmentacja, dostępność usług z poziomu stacji roboczej, VLAN-y, reguły firewall).
- Mechanizmy uwierzytelniania i autoryzacji (AD, SSO, MFA).
- Informacje o backupach i procedurach odtwarzania danych użytkownika.
- Sposób zarządzania urządzeniami przenośnymi (pendrive, CD, BYOD).
- Informacje o typowych scenariuszach użycia (czy użytkownicy korzystają z RDP, SSH, VPN, aplikacji webowych, poczty, itp.).

4.2.1.4 Rezultat zadania

Raport z modelowania zagrożeń, zawierający mapowanie reguł firewall na urządzenia, porty i usługi funkcjonujące w sieci, priorytetyzację ryzyk i zagrożeń, rekomendacje środków zaradczych. 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

4.2.2.1 Testy penetracyjne dla domen publicznych (kopie serwisów www)

Zakres:

- Wykonanie testów penetracyjnych aplikacji webowych oraz infrastruktury serwerowej dla wszystkich domen wskazanych w wykazie 3.3.
- Testy obejmują: identyfikację podatności OWASP Top 10, testy autoryzacji i uwierzytelniania, testy podatności na ataki XSS, SQLi, CSRF, RCE, LFI/RFI, brute-force, ataki na logikę biznesową, podatności konfiguracyjne serwera www i systemu operacyjnego.
- Testy prowadzone w trybie white-box (z dostępem do dokumentacji technicznej) oraz black-box (bez znajomości kodu źródłowego).

Wymagania szczegółowe:

- Wykonawca zobowiązany jest do przeprowadzenia rekonesansu (mappingu) usług i portów dostępnych z Internetu dla domen *.uzp.gov.pl oraz adresacji IP Zamawiającego.
- Weryfikacja poprawności wdrożenia mechanizmów bezpieczeństwa (WAF, nagłówki bezpieczeństwa, polityki CORS, rate-limiting, mechanizmy blokowania kont).

- Testy podatności na ataki automatyczne (np. brute-force) muszą być prowadzone z zachowaniem limitów ustalonych z Zamawiającym, by nie zakłócić działania środowiska.
- Weryfikacja odporności na ataki na mechanizmy resetowania haseł, rejestracji kont, API publiczne.
- Weryfikacja podatności na ujawnienie danych wrażliwych (np. przez błędną konfigurację, debug, logi).

Rezultat:

- Raport z testów penetracyjnych dla każdej domeny osobno, zawierający: opis zakresu, listę wykrytych podatności (z klasyfikacją wg CVSS), opis ryzyka, rekomendacje naprawcze, przykłady exploitacji, dowody wykonania testów.

Premia:

Wykonanie zadania kwalifikuje się do uzyskania premii wynagrodzenia w sytuacji:

- Wykrycia podatności krytycznych (CVSS ≥ 9.0): za podatność o poziomie krytycznym, potwierdzoną przez Zamawiającego.
- Wykrycie podatności typu 0-day lub nieznanej w publicznych bazach: za wykrycie podatności, która nie była dotąd zgłoszona w publicznych bazach (np. CVE).

4.2.2.2 Testy bezpieczeństwa sieci wewnętrznej – serwer w DMZ

Zakres:

- Wykonawca otrzyma dostęp do serwera w DMZ (dane dostępowe, adres IP, zakres uprawnień).
- Celem jest przeprowadzenie symulacji ataku na inne maszyny w sieci wewnętrznej, w tym krytyczne serwery i urządzenia administratorów.
- Testy obejmują: próby eskalacji uprawnień (lokalnych i domenowych), lateral movement, credential harvesting, ataki na usługi sieciowe, próby obejścia segmentacji sieci.

Wymagania szczegółowe:

- Weryfikacja możliwości uzyskania dostępu do maszyn spoza DMZ, w tym do systemów backoffice.

- Próby wykorzystania znanych podatności systemowych i aplikacyjnych, błędów konfiguracyjnych, słabych haseł, podatności na ataki relay, pass-the-hash, Kerberoasting.
- Możliwość wykorzystania socjotechniki (np. phishing, spear phishing, pretexting) w celu uzyskania wyższych uprawnień, pod warunkiem uzgodnienia zakresu i formy z Zamawiającym. Zakresem socjotechnik mogą być objęci wyłącznie administratorzy (4 osoby). Nie są dopuszczone działania socjotechniczne na innych pracownikach UZP.
- Weryfikacja logowania i detekcji incydentów przez systemy SIEM/SOC Zamawiającego.

Rezultat:

- Raport z przebiegu ataku, zawierający: opis uzyskanych dostępów, ścieżki eskalacji, wykryte podatności, rekomendacje zmian w konfiguracji sieci i systemów, dowody wykonania testów.

Premia:

Wykonanie zadania kwalifikuje się do uzyskania premii wynagrodzenia w sytuacji:

- Uzyskania dostępu do systemów spoza DMZ (np. kontroler domeny, systemy backoffice): za potwierdzone przełamanie segmentacji i uzyskanie uprawnień wyższych niż przewidziane w punkcie startowym.
- Wykrycia podatności umożliwiającej lateral movement lub eskalację uprawnień domenowych: za wykrycie i udokumentowanie ścieżki eskalacji do uprawnień administratora domeny lub innego krytycznego systemu.

4.2.2.3 Testy bezpieczeństwa urządzeń końcowych (fizyczny dostęp do stacji roboczej)

Zakres:

- Wykonawca otrzyma fizyczny dostęp do wybranej stacji roboczej (laptopa służbowego).
- Testy obejmują: weryfikację wdrożenia szyfrowania dysku, próbę obejścia mechanizmów uwierzytelniania lokalnego, testy odporności na ataki offline (bootowanie z zewnętrznych nośników, ataki na TPM, cold boot), weryfikację zabezpieczeń BIOS/UEFI.

Wymagania szczegółowe:

- Próba uzyskania dostępu do danych bez znajomości poświadczeń użytkownika.
- Weryfikacja zabezpieczeń przed resetem haseł, dostępem do BIOS/UEFI, bootowaniem z USB/CD.
- Sprawdzenie, czy dane są chronione po utracie/kradzieży sprzętu.

Rezultat:

- Raport z testów fizycznego dostępu, zawierający: opis przeprowadzonych prób, wykryte podatności, rekomendacje zmian.

Premia:

Wykonanie zadania kwalifikuje się do uzyskania premii wynagrodzenia w sytuacji:

- Uzyskania dostępu do danych użytkownika bez znajomości poświadczeń: za skuteczne obejście mechanizmów szyfrowania lub uwierzytelniania i uzyskanie dostępu do danych na dysku.
- Wykrycia podatności w zabezpieczeniach sprzętowych (BIOS/UEFI, TPM): za wykrycie podatności umożliwiającej atak offline lub obejście zabezpieczeń sprzętowych.

4.2.2.4 Testy bezpieczeństwa sieci wewnętrznej – konto użytkownika

Zakres:

- Wykonawca otrzyma dane dostępowe do konta standardowego użytkownika oraz dostęp do stacji roboczej w środowisku testowym.
- Testy obejmują: próbę eskalacji uprawnień lokalnych i domenowych, lateral movement, dostęp do zasobów sieciowych, credential dumping, pass-the-hash, ataki na AD.

Wymagania szczegółowe:

- Weryfikacja możliwości uzyskania dostępu do systemów backoffice z poziomu zwykłego użytkownika.
- Próby pozyskania poświadczeń innych użytkowników, w tym administratorów.
- Weryfikacja odporności segmentacji sieci i polityk bezpieczeństwa.

Rezultat:

- Raport z testów eskalacji uprawnień i lateral movement, zawierający: opis prób, wykryte podatności, rekomendacje zmian.

Premia:

Wykonanie zadania kwalifikuje się do uzyskania premii wynagrodzenia w sytuacji:

- Eskalacji uprawnień do poziomu administratora domeny lub innego krytycznego systemu: za potwierdzone przejęcie konta uprzywilejowanego.
- Wykrycia ścieżki lateral movement do systemów o podwyższonym poziomie ochrony: za udokumentowaną ścieżkę ataku do systemów krytycznych.
- Pozyskania poświadczeń innych użytkowników (np. credential dumping): za skuteczne przeprowadzenie ataku i pozyskanie poświadczeń.

4.2.2.5 Testy bezpieczeństwa usługi zdalnego dostępu (VPN)

Zakres:

- Testy odporności na ataki brute-force, credential stuffing, próby obejścia MFA, testy podatności na exploity znane dla używanego rozwiązania VPN.
- Weryfikacja polityk blokowania kont, logowania incydentów, skuteczności mechanizmów ochrony.

Wymagania szczegółowe:

- Testy prowadzone w uzgodnionych oknach czasowych, z limitem prób ustalonym z Zamawiającym.
- Weryfikacja skuteczności mechanizmów detekcji i blokowania ataków.

Rezultat:

- Raport z testów VPN, zawierający: opis prób, wykryte podatności, rekomendacje zmian.

Premia:

Wykonanie zadania kwalifikuje się do uzyskania premii wynagrodzenia w sytuacji:

- Przełamania zabezpieczeń VPN (np. brute-force, obejście MFA): za skuteczne przełamanie zabezpieczeń i uzyskanie dostępu do sieci wewnętrznej.
- Wykrycia podatności umożliwiającej atak na infrastrukturę VPN: za wykrycie podatności umożliwiającej eskalację uprawnień lub dostęp do krytycznych zasobów przez VPN.

4.2.2.6 Wymagania ogólne dla wszystkich testów

- Wszystkie testy muszą być prowadzone zgodnie z uzgodnionym harmonogramem i w oknach czasowych zaakceptowanych przez Zamawiającego.
- Wykonawca zobowiązany jest do niezwłocznego zgłaszania wykrycia podatności krytycznych.
- Każdy raport musi zawierać: zakres testów, szczegółowy opis podatności, ocenę ryzyka (CVSS), rekomendacje naprawcze, dowody wykonania testów (zrzuty ekranu, logi), status podatności (usunięta/pozostająca/nowa – w przypadku retestów).
- Raporty muszą być przekazane w wersji elektronicznej, podpisane elektronicznie przez wykonawcę.

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:

Brak opłat licencyjnych

- **Wymaganie:** Oprogramowanie musi być dostępne na licencji, umożliwiającej nieograniczone użytkowanie przez instytucję publiczną bez opłat licencyjnych, subskrypcyjnych ani za aktualizacje np. open source (MIT, Apache 2.0, GPL, AGPL lub równoważna).
- **Metoda weryfikacji:** Przedłożenie przez Wykonawcę kopii licencji oraz oświadczenia o braku opłat licencyjnych/subskrypcyjnych, wraz z linkiem do oficjalnego repozytorium projektu.

Samodzielność działania

- **Wymaganie:** Oprogramowanie musi umożliwiać pełną instalację i uruchomienie w środowisku Zamawiającego (on-premise), bez konieczności stałego połączenia z Internetem lub zewnętrznymi serwerami producenta.
- **Metoda weryfikacji:** Przeprowadzenie testowej instalacji w środowisku Zamawiającego lub prezentacja nagrania wideo z procesu instalacji i uruchomienia bez połączenia z Internetem; przedłożenie dokumentacji instalacyjnej.

Aktualna i szeroka baza reguł skanowania

- **Wymaganie:** Oprogramowanie musi umożliwiać korzystanie z aktualnej biblioteki reguł/testów podatności, aktualizowanej automatycznie lub ręcznie przez administratora. Biblioteka musi być publicznie dostępna i obejmować testy dla najnowszych podatności (CVE/CWE) oraz typowych usług sieciowych.
- **Metoda weryfikacji:** Przedłożenie dokumentacji opisującej mechanizm aktualizacji reguł oraz linku do repozytorium reguł.

Funkcjonalność skanowania

- **Wymaganie:** Oprogramowanie musi umożliwiać skanowanie podatności w usługach dostępnych przez co najmniej protokoły: HTTP/HTTPS, TCP, UDP, DNS, SMB, SSH, RDP; równoległe skanowanie wielu celów; testowanie zasobów wymagających uwierzytelnienia; generowanie raportów w formatach HTML, CSV.
- **Metoda weryfikacji:** Przedłożenie dokumentacji funkcjonalnej.

Wsparcie techniczne i dokumentacja

- **Wymaganie:** Oprogramowanie musi być udokumentowane w języku polskim lub angielskim, z opisem instalacji, konfiguracji oraz tworzenia własnych reguł; wsparcie społeczności (forum, system zgłoszeń).
- **Metoda weryfikacji:** Przedłożenie dokumentacji użytkownika/administratora oraz linków do oficjalnych forów wsparcia lub systemu zgłoszeń.

Dostęp do kodu źródłowego

- **Wymaganie:** Kod źródłowy musi być publicznie dostępny (np. na github.com); oprogramowanie musi być aktywnie rozwijane (zmiany w repozytorium nie rzadziej niż raz na miesiąc w ostatnim roku); minimum 5 000 „gwiazdek” na GitHub lub równoważny poziom uznania.

- **Metoda weryfikacji:** Przedłożenie linku do repozytorium kodu źródłowego; Zamawiający zweryfikuje historię commitów oraz liczbę „gwiazdek” na portalu GitHub lub równoważnym.

Bezpieczeństwo i prywatność

- **Wymaganie:** Oprogramowanie nie może przesyłać wyników skanowania, danych konfiguracyjnych ani żadnych informacji o środowisku Zamawiającego poza infrastrukturę Zamawiającego bez wyraźnej zgody; musi umożliwiać eksport wyników do pliku i archiwizację lokalną.
- **Metoda weryfikacji:** Przedłożenie dokumentacji dotyczącej polityki prywatności i bezpieczeństwa uwzględniającej to zagadnienie.

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

Dostarczenie licencji na oprogramowanie projectdiscovery.io lub równoważne, umożliwiające:

- pozyskiwanie, agregowanie, powiadamianie administratorów i zarządzanie statusami (aktualne/usunięte) wynikami skanowania podatności zidentyfikowanych w wyniku działania oprogramowania wskazanego w 4.2.3 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).

4.2.4.1 Warunki równoważności dla projectdiscovery.io

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.
3. Oprogramowanie musi umożliwiać integrację z narzędziem dostarczonym w ramach zadania w 4.2.3 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 4.2.3.
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).

4.2.4.2 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.

4.2.4.3 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 Wynagrodzenie za realizację zadania 4.2.2

1) Wykonawca za należyte wykonanie zadania 4.2.2 otrzyma wynagrodzenie w wysokości 85% wartości zaoferowanego wynagrodzenia.
2) Pozostałe 15% wartości wynagrodzenia stanowi pula premii, która może zostać przyznana Wykonawcy za wykrycie i udokumentowanie istotnych luk w zabezpieczeniach, zgodnie z zasadami premii ujętymi w opisie zadań wskazanych w 4.2.2.
3) Za spełnienie dowolnego z warunków Wykonawcy przysługuje premia w wysokości 3% wartości zaoferowanego wynagrodzenia. Każdy warunek może zostać rozliczony tylko raz, niezależnie od liczby wystąpień luk zabezpieczeń w danym obszarze testów.

4) Łączna suma premii nie może przekroczyć 15% wartości zaoferowanego wynagrodzenia.
5) Premia jest przyznawana po potwierdzeniu przez Zamawiającego spełnienia warunku i zaakceptowaniu raportu z testów.
6) Poziom wynagrodzenia Wykonawcy może zostać zwiększony do maksymalnie 100% wartości zaoferowanego wynagrodzenia, w przypadku spełnienia pięciu różnych warunków premiowych. Spełnienie szóstego i więcej warunków nie zwiększa poziomu wynagrodzenia.

4.4 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).

4.5 Zakres opcjonalny (opcja)

4.5.1 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 **Błąd! Nie można odnaleźć źródła odwołania. Błąd! Nie można odnaleźć źródła odwołania.**.

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.

4.5.2 Dodatkowy pakiet godzin konsultacji powdrożeniowych w wysokości 100 godzin.

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

4.5.3 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.

4.6 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 na środowiskach testowych, testy w sieci Zamawiającego mogą być prowadzone w godzinach 8:15-16:15.
- Testy na środowiskach produkcyjnych usług www 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: styczniu 2026 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: 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: marzec – maj 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: czerwiec 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.