

Szczegółowy Opis Przedmiotu Zamówienia, zwany dalej „SOPZ”

1. Kluczowe definicje:

- 1) **Certyfikaty uczestnictwa** – dokumenty potwierdzające uzyskanie kwalifikacji, które osoba uczestnicząca w szkoleniu otrzyma po ukończonym szkoleniu, potwierdzające uzyskanie odpowiedniej wiedzy/umiejętności, należy przez to rozumieć: dyplomy, świadectwa, zaświadczenia, certyfikaty i inne równoważne dokumenty potwierdzające posiadanie kompetencji w zakresie zrealizowanym podczas szkolenia.

Certyfikat GIAC – dokument wystawiany przez GIAC, LLC (zwanym dalej "GIAC")

potwierdzający posiadaną wiedzę i umiejętności z zakresu bezpieczeństwa komputerowego. Uzyskanie certyfikatu poprzedzone jest egzaminem organizowanym przez GIAC.

Szkolenie - szkolenie stacjonarne lub live on-line, w obszarze opisanym poniżej.

Szkolenie live on – line - szkolenie z wykorzystaniem dedykowanej platformy umożliwiającej bezpośrednią komunikację trenera z uczestnikami szkolenia w czasie rzeczywistym.

Szkolenie stacjonarne – szkolenie w lokalizacji wskazanej przez Podmiot szkolący, gdzie trener bezpośrednio i osobiście prowadzi zajęcia z grupą uczestników.

Podmiot szkolący – organizacja realizująca Szkolenie kończące się wystawieniem Certyfikatu Uczestnictwa.

Trener - osoba przeprowadzająca Szkolenie kończące się wystawieniem Certyfikatu Uczestnictwa.

Uczestnik – pracownik Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, zwanego dalej „NASK-PIB” lub „Zamawiającym” skierowany na Szkolenie przez Zamawiającego.

Materiały - nagrania wideo z prezentacjami, podręcznik dla uczestnika szkolenia w formie elektronicznej lub papierowej, materiały techniczne do praktycznych zadań np. maszyna wirtualna z oprogramowaniem narzędziowym niezbędnym do aktywnego uczestnictwa w Szkoleniu.

CPE - Punkty przyznawane za działania w ramach ciągłej edukacji zawodowej (Continuing Professional Education) w obszarze cyberbezpieczeństwa. Kryteria przyznawania punktów CPE są określone przez GIAC i mogą zostać użyte do odnowienia certyfikatów wystawianych przez tę organizację. Zasady przyznawania CPE są opisane na stronie WWW GIAC: <https://www.giac.org/renewal/cpe-information/> oraz <https://www.giac.org/knowledge-base/renewal/>

2. Przedmiot realizacji przedmiotu zamówienia

- 1) Przedmiotem zamówienia jest usługa polegająca na realizacji 6 (słownie: sześciu) specjalistycznych Szkoleń z cyberbezpieczeństwa przygotowujących do certyfikacji GIAC oraz zakup odpowiadających im tematycznie egzaminów certyfikujących GIAC w zakresie zgodnym z poniższym zestawieniem, dla 10 Uczestników (słownie: dziesięciu). Każde Szkolenie powinno kończyć się wystawieniem certyfikatu uczestnictwa, a także każda osoba biorąca udział w Szkoleniu (Uczestnik) otrzyma voucher na egzamin certyfikacji GIAC.

Tabela nr 1:

Liczba uczestników szkoleń	Zakres tematyczny i opis Szkolenia wraz z ćwiczeniami praktycznymi	Certyfikacja (nazwa certyfikatu)
Kol. 1	Kol.2	Kol. 3
1x	Cloud Security and DevSecOps Automation	+ GIAC certyfikat (GCSA)
	<p>Zakres :</p> <ul style="list-style-type: none"> • DevOps Security Automation – wyzwania bezpieczeństwa, zabezpieczanie CI/CD, kontrole przed zatwierdzeniem kodu • Cloud Infrastructure Security – IaC, zarządzanie konfiguracją, bezpieczeństwo kontenerów i łańcucha dostaw • Cloud Native Security Operations – Kubernetes, ryzyka, monitorowanie • Microservice & Serverless Security – ochrona mikroservisów i funkcji serverless • Continuous Compliance & Protection – ciągła zgodność, automatyzacja działań naprawczych <p>Laboratoria (ćwiczenia praktyczne):</p> <ul style="list-style-type: none"> • Atakowanie i zabezpieczanie łańcucha DevOps • Automatyzacja analizy kodu i ochrona sekretów (Vault) • Utwierdzanie sieci w IaC, tworzenie gold image • Hardening obrazów kontenerów i rejestrów • Kontrola dostępu w Kubernetes, monitorowanie bezpieczeństwa • Automatyczne wdrażanie poprawek, CSPM, blokowanie ataków WAF • Automatyzacja naprawy z użyciem narzędzi typu policy-as-code <p>Efekty szkolenia. Uczestnik będzie potrafił:</p> <ul style="list-style-type: none"> • Zabezpieczać procesy DevOps i środowiska chmurowe • Chronić kontenery, mikroservisów i funkcje serverless • Implementować mechanizmy bezpieczeństwa w Kubernetes • Automatyzować kontrole zgodności i reagować na zagrożenia w chmurze 	
1x	Cybersecurity Engineering: Advanced Threat Detection and Monitoring	+ GIAC certyfikat (GMON)
	<p>Zakres tematyczny:</p> <ul style="list-style-type: none"> • Threat-Informed Defense i Hunting – taktyki przeciwników, frameworki, analiza stanu • Cloud, Edge i Network Security – widoczność, szyfrowanie, ochrona chmury • Threat Hunting z NDR – analiza ruchu sieciowego 	

	<ul style="list-style-type: none"> Hybrid Enterprise Security – EDR, EPP, monitorowanie tożsamości GenAI Defense, Automatyzacja i SOC – obrona aplikacji AI, SOAR/SOC Capstone: Design, Detect, Defend – kompleksowa obrona sieci, endpointów i chmury <p>Laboratoria (ćwiczenia praktyczne):</p> <ul style="list-style-type: none"> Detekcja tradycyjnych i nowoczesnych technik ataku Analiza złożonych włamań (Apache ActiveMQ) WAF (ModSecurity), odszyfrowywanie TLS, honeypoty Analiza Pcap z Zeek, Wireshark, Security Onion Sysmon, AppLocker, analiza kompromitacji CFO Badanie ransomware, DNS over HTTPS, analiza logów Windows Scenariusze Design, Detect, Defend i ćwiczenia NetWars <p>Efekty szkolenia. Uczestnik będzie potrafił:</p> <ul style="list-style-type: none"> Wdrażać strategię Threat-Informed Defense i prowadzić hunting zagrożeń Analizować ruch sieciowy i wykrywać anomalie (NDR, NSM) Zabezpieczać chmurę, sieć i punkty końcowe (EDR, EPP) Chronić aplikacje AI i łańcuch dostaw oprogramowania Automatyzować procesy SOC i reagować na incydenty w czasie rzeczywistym 	
4x	Advanced Incident Response, Threat Hunting, and Digital Forensics	+ 4x GIAC certyfikat (GCFA)
	<p>Zakres tematyczny:</p> <ul style="list-style-type: none"> Zaawansowana reakcja na incydenty i hunting zagrożeń – taktyki IR, identyfikacja trwałości malware Analiza włamań – dowody wykonania, lateral movement, analiza logów Analiza pamięci – pozyskiwanie i badanie pamięci, identyfikacja malware Analiza osi czasu – tworzenie timeline i super-timeline Zaawansowane techniki anty-forensics – Volume Shadow Copy, NTFS <p>Laboratoria (ćwiczenia praktyczne):</p> <ul style="list-style-type: none"> Scenariusz APT: reakcja na incydent Wykrywanie trwałości malware i analiza logów Tworzenie obrazów dowodowych i zdalna triage Analiza ruchu bocznego i nadużyć poświadczeń Badanie pamięci: malware, procesy, ukryte techniki Tworzenie super-timeline i śledzenie działań atakującego 	

	<ul style="list-style-type: none"> Analiza Volume Shadow Copy, NTFS, odzyskiwanie danych <p>Efekty szkolenia. Uczestnik będzie potrafił:</p> <ul style="list-style-type: none"> Prowadzić zaawansowaną reakcję na incydenty w skali enterprise Analizować logi, pamięć i artefakty systemowe w celu identyfikacji ataków Tworzyć i interpretować timeline oraz super-timeline zdarzeń Wykrywać techniki anty-forensics i odzyskiwać ukryte dane 	
2x	Red Team Operations and Adversary Emulation	+ 2x GIAC certyfikat (GRTP)
	<p>Zakres tematyczny:</p> <ul style="list-style-type: none"> Planowanie emulacji przeciwnika i analiza zagrożeń – kill chain, OSINT, socjotechnika Infrastruktura ataku i OPSEC – projektowanie C2, redirectory, hardening Uzyskanie dostępu i utrzymanie obecności – payloady, eskalacja, AMSI bypass Ataki na Active Directory i ruch boczny – pivoting, manipulacja certyfikatami Realizacja celu i raportowanie – eksfiltracja danych, analiza wpływu CTF– pełna emulacja przeciwnika w środowisku enterprise <p>Laboratoria (ćwiczenia praktyczne):</p> <ul style="list-style-type: none"> Konfiguracja środowiska Red Team i implementacja MITRE ATT&CK Deployment frameworków C2 (Cobalt Strike, Empire) Tworzenie payloadów, eskalacja uprawnień, utrzymanie dostępu Ataki na Active Directory, analiza ścieżek BloodHound Eksfiltracja danych, automatyzacja symulacji naruszeń Pełne scenariusze Red Team w trybie CTF <p>Efekty szkolenia. Uczestnik będzie potrafił:</p> <ul style="list-style-type: none"> Planować i realizować kampanie Red Team z wykorzystaniem emulacji przeciwnika Projektować i zabezpieczać infrastrukturę C2 oraz stosować OPSEC Uzyskiwać dostęp, eskalować uprawnienia i utrzymywać obecność w sieci Przeprowadzać zaawansowane ataki na Active Directory i ruch boczny Eksfiltrować dane, analizować wpływ i przygotowywać raporty z działań 	

1x	Security Leadership Essentials for Managers	+ GIAC certyfikat (GSLC)
	<p>Zakres tematyczny:</p> <ul style="list-style-type: none"> • Budowanie programu bezpieczeństwa – ramy, polityki, struktura • Techniczna architektura bezpieczeństwa – sieć, hosty, chmura, IAM • Inżynieria bezpieczeństwa – ochrona danych, prywatność, DevSecOps • Zarządzanie i przywództwo – podatności, świadomość, negocjacje, vendor management • Wykrywanie i reagowanie na ataki – SOC, obsługa incydentów, planowanie awaryjne <p>Laboratoria (ćwiczenia praktyczne):</p> <ul style="list-style-type: none"> • Kalibracja programu bezpieczeństwa i symulacje Cyber42 • Implementacja zabezpieczeń sieciowych i IAM • Ćwiczenia z DevSecOps i zarządzania podatnościami • Symulacje negocjacji, zarządzania oporem i patchowania • Scenariusze reagowania na incydenty, ransomware i planowanie awaryjne <p>Efekty szkolenia. Uczestnik będzie potrafił:</p> <ul style="list-style-type: none"> • Budować i rozwijać program bezpieczeństwa w organizacji • Projektować architekturę bezpieczeństwa obejmującą sieć, chmurę i aplikacje • Zarządzać ryzykiem, podatnościami i dostawcami • Prowadzić zespół bezpieczeństwa i skutecznie negocjować • Organizować procesy monitorowania, reagowania na incydenty i planowania awaryjnego 	
1x	Hacker Tools, Techniques, and Incident Handling	+ GIAC certyfikat (GCIH)
	<p>Zakres tematyczny:</p> <ul style="list-style-type: none"> • Reagowanie na incydenty i cyber-śledztwa – IR, analiza sieci i malware, AI w IR • Ataki skanowania i enumeracji – Nmap, Masscan, SMB, Sigma • Ataki haseł i frameworki exploitów – cracking, Metasploit, Microsoft 365 • Ataki na aplikacje webowe – XSS, SQL Injection, IDOR, API • Post-eksploatacja i ataki AI – pivoting, trwałość, prompt injection • CTF – pełna symulacja incyduentu i eksfiltracji danych 	

	<p>Laboratoria (ćwiczenia praktyczne):</p> <ul style="list-style-type: none"> • Analiza incydentów: Windows, sieć, malware, IR playbook z AI • Skanowanie hostów i chmury, wykrywanie ataków SMB • Ataki haseł, cracking z Hashcat, Metasploit exploitation • Ataki webowe: XSS, SQL Injection, API exploitation • Post-eksploatacja: pivoting, trwałość, bypass zabezpieczeń • Ataki AI: prompt injection, ofensywne wykorzystanie AI • CTF: pełna symulacja incydentu i eksfiltracji danych <p>Efekty szkolenia. Uczestnik będzie potrafił:</p> <ul style="list-style-type: none"> • Prowadzić skuteczną reakcję na incydenty i analizę malware • Wykrywać i realizować ataki skanowania, enumeracji i haseł • Eksploatować podatności aplikacji webowych i API • Wdrażać techniki post-eksploatacyjne i ruch boczny • Rozpoznawać i przeciwdziałać atakom AI 	
--	---	--

- 2) Zamawiający wymaga od Wykonawcy zapewnienia wyłącznie szkolenia bez transportu, noclegu i wyżywienia.
- 3) Zamawiający wymaga, aby zakres Materiałów, wykładów, warsztatów i zajęć praktycznych tzw. laboratoriów w ramach Szkolenia był tak zaawansowany i szczegółowy, aby zajął Uczestnikowi co najmniej 5 dni w wymiarze co najmniej 5 godzin pracy z Materiałami dziennie. Materiały szkoleniowe, w tym podręcznik, powinny być dostępne on line.
- 4) Terminarz szkoleń wraz z zaznaczeniem, czy dane Szkolenie będzie realizowane live on-line, stacjonarnie lub w obu trybach zostanie określony przy składaniu oferty. Zamawiający wymaga aby dla każdego z 6 (słownie: sześciu) Szkoleń były przypisane minimum 3 terminy realizacji Szkolenia, jednak w terminie najpóźniej do dnia 30 maja 2026 roku. Wymagane jest, aby minimum dwa z tych terminów były terminem szkolenia stacjonarnego.
- 5) **Zamawiający wymaga złożenia wraz z ofertą przedmiotowych środków dowodowych na potwierdzenie, że oferowane usługi spełniają określone przez Zamawiającego wymagania, cechy, tj.:** Zamawiający wymaga, aby Wykonawca złożył wraz z ofertą:
 - a) dowód potwierdzający, że GIAC przyzna za każde Szkolenie co najmniej 30 punktów CPE. Dopuszczalna przez Zamawiającego forma dowodu to: skan/kopia dokumentu/wydruk/zdjęcie strony internetowej, z której wynika ilość przyznanych przez GIAC punktów. Plik sporządza się w postaci elektronicznej i opatruje się kwalifikowalnym podpisem elektronicznym albo podpisem zaufanym albo podpisem osobistym.
 - b) Certyfikat GIAC powiązany z danym szkoleniem zgodnie z kolumną "Certyfikacja (nazwa certyfikatu)" w pkt 2 niniejszej SOPZ tj. w Tabeli 1 w kol. 3 dla każdego trenera prowadzącego Szkolenie podczas realizacji przedmiotu zamówienia w formie wydruku. Plik sporządza się w postaci elektronicznej i opatruje się kwalifikowalnym podpisem elektronicznym albo podpisem zaufanym albo podpisem osobistym.
 - c) Zamawiający przewiduje uzupełnienie powyższych przedmiotowych środków dowodowych.

3. Sposób realizacji przedmiotu zamówienia:

- 1) W przypadku Szkoleń live on-line w celu realizacji poszczególnego Szkolenia Wykonawca przekaże Zamawiającemu najpóźniej na 3 dni robocze przed przewidywanym terminem Szkolenia informacje niezbędne do uzyskania dostępu do Szkolenia.
- 2) W przypadku realizacji Szkoleń stacjonarnych, w celu realizacji poszczególnych Szkoleń Wykonawca przekaże Zamawiającemu w najpóźniej tydzień przed przewidywanym terminem Szkolenia informacje niezbędne do przygotowania się do Szkolenia.

4. Wymagania minimalne wobec trenera/trenerów prowadzących Szkolenia:

Trener/Trenerzy przeprowadzający szkolenia muszą posiadać:

- 1) minimum 5 lat doświadczenia zawodowego, liczonego w terminie przed upływem terminu składania ofert w obszarze cyberbezpieczeństwa,
- 2) doświadczenie w prowadzeniu szkoleń z obszaru cyberbezpieczeństwa – minimum 300 godzin przeprowadzonych szkoleń (w formie stacjonarnej albo online, lub oba jednocześnie) w ciągu ostatnich 3 lat przed upływem terminu składania ofert,
- 3) certyfikaty GIAC z zakresów, o których mowa w Tabeli nr 1, kolumna nr 2 powyżej. Trener przeprowadzający dane szkolenie musi posiadać certyfikat z danego zakresu szkolenia.

5. Proponowane kryteria oceny ofert

- 1) Zamawiający oceni oferty z zastosowaniem następujących kryteriów oceny ofert:

Kryterium	Waga (pkt)
Cena oferty brutto (C)	70,00
Jakość (J)	30,00

- a) W kryterium pt.: „**Cena oferty brutto (C)**”, najwyższą liczbę punktów tj. 70,00 otrzyma oferta zawierająca najniższą cenę brutto spośród ofert niepodlegających odrzuceniu, a każda następna zostanie dokonana w następujący sposób:

$$\begin{array}{l} \text{Cena oferty} \\ \text{brutto} = \frac{\text{najniższa cena oferty brutto spośród wszystkich ofert} \\ \text{podlegających ocenie}}{\text{cena brutto oferty ocenianej}} \times 70,00 \text{ pkt} \end{array}$$

UWAGA:

Oferta w odniesieniu do tego kryterium może uzyskać maksymalnie **70,00 punktów**.
Cena oferty brutto to cena podana w Formularzu „Oferta”.

- b) W kryterium pt.: „**Jakość (J)**”, najwyższa maksymalna liczba punktów jaką może uzyskać oferta Wykonawcy to 30,00 punktów - za dostęp dla każdego uczestnika podczas każdego z 6 (słownie: sześciu) Szkoleń do dodatkowej platformy treningowej typu cyber range (tj.: środowisko symulacyjne służące do bezpiecznego testowania, szkolenia i doskonalenia umiejętności z zakresu cyberbezpieczeństwa. Umożliwia odtwarzanie realistycznych scenariuszy oraz ćwiczenie reakcji obronnych bez ryzyka dla rzeczywistych systemów.), zaprojektowanej tak żeby wzmocnić naukę przez praktycznie realizowane zadania w szerszym aspekcie, niż tematyka danego Szkolenia. **Uwaga! Powyższa platforma jest odrębnym narzędziem, innym od tego które będzie używane podczas Szkolenia w trakcie ćwiczeń praktycznych (Laboratoria).**

30,00 (słownie: trzydzieści) punktów uzyska oferta Wykonawcy, który zaoferuje dostęp do ww. platformy dla każdego z uczestników wszystkich 6 (słownie: sześciu) Szkoleń.

0,00 punktów uzyska oferta Wykonawcy, który nie zaoferuje dostępu do ww. platformy dla każdego z uczestników wszystkich 6 (słownie: sześciu) Szkoleń.

Zamawiający wymaga, żeby Wykonawca w złożonej ofercie w tabeli z wyceną w kolumnie nr 2 złożył opis platformy wraz z opisem możliwości treningowych, żeby Zamawiający mógł obiektywnie ocenić, czy jest to platforma typu cyber range.

Funkcjonalności, które Zamawiający będzie oceniał w celu weryfikacji zaoferowanej przez Wykonawcę platformy:

- tematyka zadań związana z praktycznymi aspektami cyberbezpieczeństwa;
- ocena umiejętności i ranking uczestników;
- obsługa przez przeglądarkę internetową.

- 2) Ocena końcowa będzie dokonywana według ww. skali punktowej, a wynik oceny zostanie obliczony w następujący sposób:

$$S = C \cdot J$$

gdzie:

S – wynik oceny (suma punktów),

C – liczba punktów uzyskanych w kryterium pt.: „Cena oferty brutto” (C),

J – liczba punktów uzyskanych w kryterium pt.: „Jakość (J)”

- 3) Obliczenia punktacji, zgodnie z wyżej wskazanymi kryteriami, zostaną dokonane z dokładnością do dwóch miejsc po przecinku.
- 4) Zamawiający udzieli zamówienia Wykonawcy, którego Oferta uzyska najwyższą liczbę punktów.

6. Termin realizacji przedmiotu zamówienia

Do 6 miesięcy liczonych od dnia zawarcia umowy, jednak nie później niż do dnia 30 czerwca 2026 r. a termin realizacji ostatniego szkolenia do dnia 30 maja 2026 r.