OPIS PRZEDMIOTU ZAMÓWIENIA

1) PRZEDMIOT ZAMÓWIENIA

Przedmiot zamówienia jest realizowany w ramach projektu pt. „Jeden Uniwersytet – Wiele Możliwości. Program Zintegrowany”. Projekt, a tym samym przedmiot zamówienia jest współfinansowany ze środków Unii Europejskiej w ramach środków Europejskiego Funduszu Społecznego, Program Operacyjny Wiedza Edukacja Rozwój, Oś Priorytetowa III Szkolnictwo wyższe dla gospodarki i rozwoju, Działanie 3.5. Kompleksowe programy szkół wyższych, o numerze POWR.03.05.00-00-Z301/18

Przedmiotem zamówienia są szkolenia dla kadry administracyjnej i zarządzającej Uczelni podnoszące kompetencje cyfrowe w obszarze cyberbezpieczeństwa.

Zamówienie obejmuje udział pracowników w otwartych szkoleniach stacjonarnych lub online.

Warunki realizacji:

- Zamawiający dopuszcza udział pracowników w szkoleniach stacjonarnych organizowanych wyłącznie na terenie Polski.
- Szkolenia powinny być realizowane w języku polskim.
- Każde szkolenie zakończone jest wydaniem zaświadczenia lub/i certyfikatu dla uczestnika.

Podział na części:

Część A – Szkolenie z zakresu: atakowanie i ochrona aplikacji webowych

Część B – Szkolenie z zakresu: bezpieczeństwa aplikacji mobilnych

Część C – Szkolenie z zakresu: bezpieczeństwa sieci (testy penetracyjne)

Część D – Szkolenie z zakresu: bezpieczeństwa Windows (praktyczne warsztaty z ochrony systemu)

Część E – Szkolenie z zakresu: zaawansowane pozyskiwanie szczegółowych informacji na temat ludzi i firm.

Część A

Zamówienie obejmuje udział maksymalnie 4 pracowników w otwartych szkoleniach z tematu **atakowanie i ochrona aplikacji webowych** realizowanych w wymiarze co najmniej 12 godzin dydaktycznych w okresie 2 dni. Szkolenie realizowane w formule warsztatowej tj. oparte o realizację ćwiczeń praktycznych, które umożliwiają omawianie konkretnego ataku oraz rozwój umiejętności obrony przed nim.

Minimalny zakres tematyczny szkolenia winien obejmować zagadnienia:

1. Współczesne problemy bezpieczeństwa aplikacji webowych:
   a) zagrożenia wynikające z architektury webaplikacji (np. CGI, SSI, etc.)
   b) zagrożenia wynikające z języków programowania (PHP, JS, etc.) i technologi, np. ASP, JSP
   c) problem styku webaplikacji z bazą danych
   d) interfejsy zewnętrzne webaplikacji
   e) zagrożenia po stronie serwera, środowiska, sieci, a zagrożenia po stronie klienta
   f) zagrożenia stron tworzonych pod urządzenia mobilne (telefony, tablety)
2. Ataki na aplikacje webowe:
   a) wyszukiwanie adresów serwerów deweloperskich
   b) bezpieczeństwo hostingu i webserwera
   c) brak obsługi błędów
   d) manipulacje parametrami (metody GET, POST)
   e) techniki podsłuchu i manipulowania transmisją
   f) atak Forcefull browsing
   g) atak Path Traversal
   h) technika Google Hacking
   i) wstrzyknięcie kodu (PHP shell) i komend systemowych do webaplikacji
   j) problem filtrowania danych wejściowych
   k) ataki XSS (persistent, reflected)
   l) omijanie filtrowania danych wejściowych i encodingu wyjściowych
   m) ataki na sesję aplikacji webowej
   n) podsłuchiwanie sesji i kradzież ciasteczek HTTP
   o) jak poprawnie zarządzać sesją w webapikacji?
   p) ataki CSRF/XSRF

q) bezpieczny upload plików
r) metody ułatwiające przetrwanie ataków DoS/DDoS
s) ataki Clickjacking
t) ataki na bazy danych
u) ataki SQL injection i Blind SQL injection
v) ochrona przed atakami SQL injection
w) szyfrowanie połączenia i ataki na SSL
x) szyfrowanie danych w webaplikacji
y) ochrona przed spamem i enumeracją zasobów oraz haseł
z) podsumowanie zagrożeń i przegląd OWASP TOP10
aa) pozaprogramistyczne środki ochrony (systemy IDS/IPS, WAF)
bb) omijanie detekcji przez systemy WAF/IDS/IPS

3. Problemy przeglądarek:
   a) Same Orgin Policy
   b) Rich Internet Applications
   c) dziury w przeglądarkach
   d) ataki DNS-Rebinding
   e) narzędzia podnoszące bezpieczeństwo i pomagające w testowaniu aplikacji webowych
4. Przegląd narzędzi automatyzujących wykrywanie podatności.

Część B

Zamówienie obejmuje udział maksymalnie 4 pracowników w otwartych szkoleniach z tematu **bezpieczeństwa aplikacji mobilnych** realizowanych w wymiarze co najmniej 12 godzin dydaktycznych w okresie 2 dni. Szkolenie realizowane w formule warsztatowej tj. oparte o realizację ćwiczeń praktycznych, które umożliwiają omawianie konkretnego ataku oraz rozwój umiejętności obrony przed nim.

Minimalny zakres tematyczny szkolenia winien obejmować zagadnienia:

1. Architektury mobilnych systemów operacyjnych:
   a) iOS
   b) Android
2. Bezpieczeństwo z perspektywy użytkownika urządzenia:
   a) domyślnie dostępne sposoby zabezpieczeń urządzeń w danych systemach

   b) wpływ domyślnych zabezpieczeń urządzeń na bezpieczeństwo aplikacji
   c) data wiping
3. Mechanizmy bezpieczeństwa dostarczane developerom przez producentów systemów, m.in.:
   a) system uprawnień (Android)
   b) Data Protection (iOS)
   c) Keychain (iOS)
4. Przełamywanie zabezpieczeń systemów:
   a) eskalacja uprawnień w systemach mobilnych (jailbreak)
   b) wpływ eskalacji uprawnień na bezpieczeństwo aplikacji
   c) dostęp do danych użytkowników (m.in. SMS, e-mail, dane GPS)
   d) analiza systemu plików (ich struktur i typów)
   e) przełamywanie szyfrowania danych
5. Bezpieczeństwo danych:
   a) zagrożenia związane z wykradaniem danych na przykładzie prawdziwych zdarzeń
   b) sposoby bezpiecznego przechowywanie kluczowych danych (login, hasło, klucze, dane osobowe)
   c) implementowanie szyfrowania w aplikacjach mobilnych
   d) zabezpieczanie aplikacji hasłem dostępowym
   e) bezpieczna komunikacja pomiędzy aplikacjami (wymiana danych) oraz komponentami (Android: Activity, Service, Broadcast receiver, Content Resolver)
   f) szyfrowanie baz danych
6. Bezpieczeństwo komunikacji:
   a) zagrożenia płynące z “transportu” danych
   b) poprawna, bezpieczna implementacja aplikacji klient-serwer
   c) mechanizmy szyfrowania (SSL/TLS)
   d) wykorzystanie PKI (Public Key Infrastructure)
7. Bezpieczeństwo aplikacji:
   a) analiza sposobów dystrybucji aplikacji i ryzyka z nią związane
   b) analiza form binarnych aplikacji i ich dystrybucji (m.in. odex, Mach-O, ipa, apk)
   c) Reverse Engineering aplikacji (m.in. Cycript, baksmali, apktool)

d) utrudnianie analizy kodu i modyfikacji działania aplikacji (m.in. blokowanie debugerów, obfuskacja kodu, ASLR)
e) wykrywanie środowisk z podwyższonymi uprawnieniami (jailbreak)
f) narzędzia wspomagające analizę bezpieczeństwa aplikacji

8. Istotne mechanizmy specyficzne dla platform i ataki z nimi związane, m.in.:
   a) multitasking (app state/GUI caching)
   b) wprowadzanie danych (input caching)
   c) zanużanie aplikacji webowych (CSRF, framing, clickjacking)
   d) identyfikacja urządzeń i użytkowników (UDID)
   e) push notifications
   f) tapjacking
   g) zarządzanie logami
9. Ciekawe przypadki przełamywania zabezpieczeń – case studies.

Część C

Zamówienie obejmuje udział maksymalnie 4 pracowników w otwartych szkoleniach z tematu **bezpieczeństwa sieci komputerowych (testy penetracyjne)** realizowanych w wymiarze co najmniej 18 godzin dydaktycznych w okresie3 dni. Szkolenie realizowane w formule warsztatowej tj. oparte o realizację ćwiczeń praktycznych, które umożliwiają uczestnikowi zaplanowanie, wykonanie, a następnie udokumentowanie przeprowadzony przez siebie test penetracyjny. Ćwiczenia mają rozwijać umiejętność obsługi narzędzi a także na możliwości ich oskryptowania w celu automatyzacji testów.

Minimalny zakres tematyczny szkolenia winien obejmować zagadnienia:

1. Jak testować bezpieczeństwo sieci, czym są testy penetracyjne?
   a) metodyki i rodzaje pentestów
   b) OSSTMM / OWASP
   c) dokumenty opisujące dobre praktyki (NIST/CIS)
   d) różnice pomiędzy pentestami a audytami
2. Organizacja testów penetracyjnych:
   a) prawne aspekty prowadzenia testów penetracyjnch
   b) opracowanie planu testów penetracyjnych

c) popularne problemy spotykane podczas testów penetracyjnych

3. Poszczególne fazy testu penetracyjnego:

a) rekonesans

— pasywne metody zbierania informacji o celu

- wykorzystanie serwerów proxy
- zbieranie i analiza metadanych
- ataki typu social-engineering i APT
- profilowanie pracowników

— aktywne metody zbierania informacji o celu

— mapowanie sieci ofiary

— omijanie firewalli

b) enumeracja podatności

— rodzaje podatności (buffer overflow, format string, etc.)

- czym jest shellcode?
- mechanizmy DEP/ASLR i ich omijanie
- ROP i heap spray’ing

— dopasowywanie kodu exploita do znalezionych podatności

- rodzaje exploitów
- wyszukiwanie exploitów
- analiza przykładowego exploita
- tworzenie własnego exploita

— wybór drogi wejścia do systemu

c) Atak

— przegląd technik ataków na systemy (Windows/Linux) i sieci komputerowe

- ataki w sieci LAN/WAN/Wi-Fi
- ataki na urządzenia sieciowe (routery, switche, IDS/IPS/WAF, firewalle, load balancery)
- ataki denial of service
- fuzzing
- łamanie haseł

— atak przy pomocy exploita zdalnego

- atak przy pomocy exploita zdalnego

— podniesienie uprawnień do poziomu administratora

- exploity lokalne
- łamanie hashy haseł

d) zacieranie śladów

— backdoorowanie przejętego systemu

— zacieranie śladów włamania, oszukiwanie narzędzi do analizy powłamaniowej

e) sporządzenie raportu z testu penetracyjnego

— budowa szczegółowego raportu technicznego

— raport dla zarządu

4. Metody ochrony przed atakami
   a) idea honeypotów
   b) systemy IDS/IPS
   c) metody hardeningu systemów Windows
   d) metody hardeningu systemów Linux.

Część D

Zamówienie obejmuje udział maksymalnie 4 pracowników w otwartych szkoleniach z tematu **bezpieczeństwa Windows (praktyczne warsztaty z ochrony systemu)** realizowanych w wymiarze co najmniej 12 godzin dydaktycznych w okresie 2 dni. Szkolenie realizowane w formule treningu umiejętności tj. Ćwiczenia praktyczne wykonywane przez uczestników, stanowią 90% czasu szkolenia. Omawiane zagadnienia są poprzedzone zwięzłym wstępem teoretycznym oraz demonstracją ewentualnego ataku lub techniki zabezpieczeń w wykonaniu trenera.

Uczestnicy szkolenia powinni mieć zapewnione dostęp do środowisko pracy, zawierające aktualne oprogramowanie Microsoft, które zostało skonfigurowane tak, aby najwierniej oddać typowe sytuacje pracy (kontoler domeny i stacje klienckie).

Minimalny zakres tematyczny szkolenia winien obejmować zagadnienia:

1. Narzędzia:
   a) Active Directory Domain Services
   b) Group Policy Object
   c) Microsoft Security Compliance Toolkit
   d) Local Admin Password Solution

e) Sysinternals Sute

2. Rekomendacje:
   a) NIST – National Institute of Standards and Technology
   b) STIG – Security Technical Implementation Guides
   c) CIS Security Benchmark
3. Bezpieczne środowisko pracy oraz centralne zarządzanie konfiguracją:
   a) Access Control List – ograniczenie dla zwykłego użytkownika do tworzenia plików tylko w profilu
   b) Advanced Auditing – ustawienia audytu zdarzeń w systemie
   c) Event Viewer – ustawienia, archiwizacja logów
   d) Event Forwarding – centralna archiwizacja logów,
   e) User Rights – uprawnienia użytkownika w systemie
   f) Restricted Groups – zarządzanie przynależnością do grup lokalnych
   g) Security Options – opcje bezpieczeństwa systemu
   h) Local Admin Password Solution – zarządzanie wbudowanymi kontami administracyjnymi
   i) Services – usługi systemowe
   j) AppLocker/SRP – ograniczenie uruchamianych aplikacji tylko do autoryzowanych
   k) Integrity Levels – zarządzanie uprawnieniami na obiektach systemowych
   l) Firewall & IPSec – systemowa zapora sieciowa
   m) Preferences – specyficzne zmiany w rejestrach, np. konfiguracja Adobe Reader, Java
   n) Folder Redirection –
   o) Internet Explorer 11/Edge
   p) Office 2013/2016/2019/2021
   q) Enhanced Mitigation Experience Toolkit 5.52/ Windows Defender Exploit Guard
   r) Windows Defender Security Center
   s) BitLocker – szyfrowanie dysków
   t) Microsoft Security Compliance Toolkit – zbiór rekomendowanych ustawień dla produktów Microsoft
   u) Sysinternal Suite – pakiet przydatnych narzędzi np. AccessChk, Procmon
   v) System Microsoft Windows – konfiguracja środowiska,
   w) Sysmon

x) File Screening – zarzadzanie zawartością na serwerze plików

y) Dynamic Access Control – nowe podejście do nadawania uprawnień

Część E

Zamówienie obejmuje udział maksymalnie 6 pracowników w otwartych szkoleniach z tematu **OSINT - zaawansowanego pozyskiwania szczegółowych informacji na temat ludzi i firm** realizowanych w wymiarze co najmniej 6 godzin dydaktycznych. Szkolenie realizowane w formule warsztatowej tj. oparte o realizację ćwiczeń praktycznych i prezentację narzędzi i technik służących do zdobywania informacji na temat osoby lub firmy.

Minimalny zakres tematyczny szkolenia winien obejmować zagadnienia:

1. Jak stworzyć bezpieczne i gwarantujące anonimowość i bezpieczeństwo analityka środowisko pracy?
   a) przydatne oprogramowanie
   b) na co zwrócić uwagę podczas tworzenia kont do czynności operacyjnych w serwisach internetowych przy zachowaniu OPSEC-u
2. Pozyskiwanie danych z rejestrów państwowych (tych w internecie i tych poza nim).
3. Wyszukiwanie informacji za pomocą zaawansowanych operatorów wyszukiwania popularnych i niszowych wyszukiwarek internetowych.
4. Sposoby ustalania informacji dotyczących celu, m.in. adresów, numeru telefonu i danych abonenta, wizerunku, ustalanie sieci znajomych, ustalanie lokalizacji, ustalanie zasobów internetowych (kont w serwisach, adresów e-mail, adresów IP. etc.) itp.
5. Techniki szczegółowej analizy śladów internetowych figuranta lub firmy
   a) analiza infrastruktury (domen, adresów IP, adresów e-mail, etc.)
   b) analiza powiązań z innymi podmiotami
   c) sposoby na deanonimizację (jeśli cel kryje się za VPN-em, Torem, Proxy lub bullet-proof hostingiem).
6. Analiza metadanych pozyskanych dokumentów, fotografii, plików dźwiękowych, nagrań video:
   a) ustalanie lokalizacji (współrzędnych GPS)
   b) ustalanie czasu stworzenia pliku
7. Zaawansowane techniki analizy obrazu:
   a) Techniki wykrywania retuszu zdjęcia (fałszowania danych)
   b) Techniki odzyskiwania utraconych (meta)danych

c) Techniki pozatechnicznej analizy materiałów audio-video ustalające czas i miejsce wykonania nagrania/fotografii.

8. Pozyskiwanie danych z mediów społecznościowych:
   a) techniki manualne
   b) narzędzia automatyczne
   c) podejście bazujące na prowokacjach
9. Poszerzanie danych o celu na podstawie analizy wykradzionych baz danych (wycieków danych):
   a) jak pozyskać dostęp do wykradzionych baz i jak wygodnie je przeszukiwać?
   b) do czego wykorzystać pozyskane informacje?
   c) kiedy to legalne?
10. Przeszukiwanie Deep Webu:
   a) Darknet
   b) Sieć Tor
   c) użyteczne serwisy i narzędzia
11. Budowanie prowokacji pozwalających na poszerzenie wiedzy na temat celu
   a) Spoofing tożsamości
   b) socjotechniki i preteksty
   c) pozyskiwanie aktualnego adresu IP figuranta
12. Korelacja danych i rekurencyjne poszerzanie zbioru informacji na temat celu na podstawie danych szczątkowych
   a) co zrobić mając tylko numer telefonu?
   b) co zrobić mając tylko zdjęcie celu?
   c) co zrobić mając tylko adres e-mail celu?
   d) jak na podstawie e-maila ustalić nazwisko?
   e) jak na podstawie adresu IP ustalić konta celu w serwisach internetowych?
   f) jak na podstawie nazwy użytkownika w serwisie X ustalić lokalizację celu?
13. Czy wszystkim pozyskanym danym można wierzyć?
14. Jak chronić się przed OSINT-em i pozostać prywatnym w Internecie?

2) TERMIN REALIZACJI ZAMÓWIENIA

1. Wymagany termin realizacji zamówienia: od dnia zawarcia umowy do 9 miesięcy od daty zawarcia umowy nie później niż **30.11.2023** r.
2. Realizacja winna odbywać się zgodnie z aktualnym harmonogramem szkoleń oferowanych przez Wykonawcę, który będzie aktualizowany na bieżąco w okresie realizacji umowy.
3. Zamawiający ustali wraz z Wykonawcą dogodne dla obu stron terminy szkoleń.

3) MIEJSCE REALIZACJI ZAMÓWIENIA

1. Wykonawca zapewnia miejsce realizacji każdego szkolenia realizowanego w formule stacjonarnej.
2. Wykonawca zapewnia catering (przerwa kawowa i lunch) każdego szkolenia realizowanego w formule stacjonarnej.
3. Dopuszcza się prowadzenie szkolenia stacjonarnego w formule” Bring Your Own Laptop” pod warunkiem udostępnienia przez Wykonawcę obrazu maszyny wirtualnej na której będą odbywały się ćwiczenia oraz zapewnia dostęp do sieci umożliwiający połączenie z wirtualną maszyną. Wykonawca jest zobowiązany do zapewnienia uczestnikom szkolenia oprogramowania umożliwiającego połączenie z wirtualną maszyną.
4. Zamawiający zapewni rozwiązania techniczne wymagane przez Wykonawcę.

4) LICZBA UCZESTNIKÓW

Szkolenia w każdej części obejmuje jedną edycję. Zamawiający zapewnia udział co najmniej 2 pracowników dla każdej części.

Część A:

Minimalna liczba osób: 3

Maksymalna liczba osób: 4

Część B:

Minimalna liczba osób: 3

Maksymalna liczba osób: 4

Część C:

Minimalna liczba osób: 3

Maksymalna liczba osób: 4

Część D:

Minimalna liczba osób: 3

Maksymalna liczba osób: 4

Część E:

Minimalna liczba osób: 2

Maksymalna liczba osób: 6

Przez godzinę dydaktyczną Zamawiający rozumie 45 minut.

5) REKRUTACJA, INFORMACJA ORAZ ORGANIZACJA KURSU

1. Za rekrutację na szkolenia odpowiedzialny jest Zamawiający. Zamawiający zobowiązuje się dostarczyć **listę uczestników/uczestniczek szkolenia** oraz najpóźniej **10 dni roboczych** przed planowanym terminem rozpoczęcia każdego szkolenia.
2. Wykonawca zobowiązany jest do niezwłocznego poinformowania Zamawiającego o niezgłoszeniu się uczestników na szkolenie, przerwaniu szkolenia lub rezygnacji z uczestnictwa oraz każdorazowej nieobecności skierowanych osób na szkolenie oraz o innych sytuacjach, które mają wpływ na ewentualne niezrealizowanie programu zajęć i umowy. Wykonawca zobowiązany jest do niezwłocznego poinformowania Zamawiającego o niezgłoszeniu się uczestników na szkolenie, przerwaniu szkolenia lub rezygnacji z uczestnictwa oraz każdorazowej nieobecności skierowanych osób na szkolenie oraz o innych sytuacjach, które mają wpływ na ewentualne niezrealizowanie programu zajęć i umowy.
3. Wykonawca po uzgodnieniu szczegółów z Zamawiającym zobowiązany jest do umożliwienia osobom wskazanym przez Zamawiającego przeprowadzenia kontroli realizacji zajęć w tym w szczególności ich przebiegu, treści, wykorzystywanych materiałów, frekwencji uczestników.

6) MATERIAŁY INFORMACYJNE: PRZYGOTOWANIE, OPRAWA, DRUK I DYSTRYBUCJA

Wykonawca jest zobowiązany do:

1. Przygotowania aktualnego harmonogramu szkoleń i wysłania do Zamawiającego w terminie do 5 dni od dnia zawarcia umowy oraz niezwłocznego aktualizowania harmonogramu w okresie obowiązywania umowy.

2. Udostępnienia materiałów szkoleniowych i pomocy dydaktycznych każdemu uczestnikowi szkolenia. Materiały szkoleniowe powinny zostać udostępnione w wersji papierowej.
3. Wydania uczestnikom zaświadczeń o uczestnictwie w szkoleniu. Przez zaświadczenie Zamawiający rozumie standardowe zaświadczenie / certyfikatu o ukończeniu szkolenia. Zamawiający nie wymaga logotypów – zaświadczenia powinien wystawić Wykonawca zgodnie ze swoimi wzorami.

7) DOKUMENTACJA ZWIĄZANA Z REALIZACJĄ SZKOLEŃ:

Wykonawca zobowiązany będzie do przekazania Zamawiającemu dokumentów w terminie do 10 dni roboczych od dnia zakończenia każdego szkolenia dokumentów, a w szczególności: kopii potwierdzonej za zgodność z oryginałem zaświadczeń /certyfikatu wydanych uczestnikom skierowanym przez Zamawiającego. Niedotrzymanie ww. terminu Zamawiający uzna jako nienależyte wykonywanie przedmiotu umowy. Prawa autorskie odnoszą się tylko do utworów wykonanych podczas szkolenia przez naszych uczestników, nie mają nic wspólnego z materiałami szkoleniowymi.

8) ROZLICZENIE

Rozliczenie odbywać się będzie po zakończeniu realizacji szkolenia dla danej osoby i po podpisaniu przez Zamawiającego protokołu odbioru, który stanowi podstawę do wystawienia rachunku/faktury. Warunkiem podpisania protokołu odbioru usługi będzie dostarczenie do Zamawiającego w określonym terminie (do 10 dni roboczych) dokumentów wymienionych w punkcie 7. Wynagrodzenie wypłacone będzie w oparciu o cenę jednostkową za 1 osobę. Zamawiający zobowiązuje się dokonać zapłaty należności na rachunek Wykonawcy podany na fakturze/rachunku w terminie 14 dni od daty jej otrzymania. Wykonawca wystawi protokół odbioru i fakturę osobno po każdej osobie.

9) PRAWA AUTORSKIE

Z dniem odbioru przedmiotu umowy Wykonawca przenosi (jeśli wytworzy) na Zamawiającego, w ramach wynagrodzenia określonego w umowie, autorskie prawa majątkowe z materiałów powstałych/stworzonych przez Uczestników w trakcie szkolenia niniejszego zamówienia materiałów noszących cechy utworu w rozumieniu przepisów ustawy z dnia 04 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

Zamawiający będzie miał prawo do rozporządzania i korzystania z tych materiałów, w całości lub we fragmentach, bez ograniczeń czasowych i terytorialnych, zgodnie z ich przeznaczeniem, we wszystkich wymienionych poniżej polach eksploatacji, w tym prawo do:

1) utrwalenia i zwielokrotniania w całości lub we fragmentach dowolną techniką, w tym m.in. drukarską, reprograficzną, cyfrową, audiowizualną, na jakichkolwiek nośnikach, bez ograniczeń co do ilości i wielkości nakładu,
2) wprowadzania do pamięci komputera,
3) wprowadzania do obrotu,
4) w zakresie rozpowszechniania utworu – publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie w całości lub we fragmentach za pomocą wizji i fonii przewodowej albo bezprzewodowej ze stacji naziemnej lub za pośrednictwem satelity, wprowadzanie w całości lub we fragmentach do pamięci komputera, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym:
   - sieć – zwłaszcza strony internetowe Zamawiającego,
   - prasa – zwłaszcza „Gazeta Uniwersytecka UŚ”,
   - czasopisma i publicystyka dotycząca Zamawiającego,

5) udzielania licencji na wykorzystanie,

6) wprowadzania poprawek, zmian, modyfikacji, uzupełnień kontynuacji lub wykorzystania dokumentacji przez osoby trzecie.

Wykonawca zobowiązuje się, że wykonując umowę będzie przestrzegał przepisów ustawy z dnia 4 lutego 1994 r. – o prawie autorskim i prawach pokrewnych (Dz. U. 2019 poz. 1231, z późn. zm.) i nie naruszy praw majątkowych osób trzecich (w tym autorskich praw majątkowych), a przekazane Zamawiającemu materiały będą wolne od obciążeń prawami tych osób”.

10. KRYTERIA OCENY WYKONAWCY:

Kryterium	**Waga**
Cena (C)	100%

Opis stosowanych kryteriów oraz sposób oceny ofert:

a) zasady przyznawania punktów w kryterium **„cena”**

Cena (C)- oznacza cenę brutto za wykonanie całości przedmiotu zamówienia zgodnie z treścią ogłoszenia oraz umową. Cena wskazana w formularzu oferty oceniana będzie w następujący sposób:

$$Xc\ punktów = \frac{Najniższa\ cena\ występująca\ w\ ofertach\ x\ 100}{Cena\ wskazana\ w\ rozpatrywanej\ ofercie}$$

Xc punktów – liczba punktów za kryterium „cena”

Otrzymana liczba punktów zostanie pomnożona przez wagę kryterium, tj. 60%

Cena usługi ma zawierać Wynagrodzenie Wykonawcy i obejmować wszelkie koszty poniesione w celu należytego i pełnego wykonania zamówienia, zgodnie z wymaganiami opisanymi w **opz**, a w szczególności koszt wynagrodzenia osób zaangażowanych do realizacji zamówienia, koszt materiałów szkoleniowych, koszt wydania zaświadczeń, koszty związane z zapewnieniem niezbędnego sprzętu i oprogramowania (w tym oprogramowania do zajęć zdalnych), a także koszty ogólne, w tym: wszelkie podatki, opłaty i elementy ryzyka związane z realizacją zamówienia, zysk Wykonawcy oraz podatek VAT w wysokości zgodnej z obowiązującymi przepisami.

Otrzymana liczba punktów zostanie pomnożona przez wagę kryterium, tj. **60%**.

12. WARUNKI PŁATNOŚCI.

Rozliczenie odbywać się będzie po zakończeniu realizacji szkolenia i po podpisaniu przez Zamawiającego protokołu odbioru, który stanowi podstawę do wystawienia rachunku/faktury. Warunkiem podpisania protokołu odbioru usługi będzie dostarczenie do Zamawiającego w określonym terminie (do 10 dni roboczych) dokumentów wymienionych w punkcie 7. Wynagrodzenie wypłacone będzie w oparciu o cenę jednostkową za 1 h zajęć oraz faktyczną liczbę godzin zrealizowanych zajęć. Zamawiający zobowiązuje się dokonać zapłaty należności na rachunek Wykonawcy podany na fakturze/rachunku w terminie 14 dni od daty jej otrzymania.

13. WARUNEK UDZIAŁU

W odniesieniu do warunku dotyczącego zdolności zawodowej, Zamawiający wymaga, aby wykonawca wykazał, iż dysponuje lub będzie dysponował co najmniej jedną osobą, która zostanie skierowana do realizacji niniejszego zamówienia, która to osoba:

a) posiada co najmniej wykształcenie wyższe magisterskie (dotyczy każdej części)

oraz

CZĘŚĆ A:

b) w ciągu ostatnich trzech lat przed upływem terminu składania ofert przeprowadziła co najmniej dwa szkolenia z zakresu atakowanie i ochrona aplikacji webowych

CZĘŚĆ B:

b) w ciągu ostatnich trzech lat przed upływem terminu składania ofert przeprowadziła co najmniej dwa szkolenia z zakresu bezpieczeństwa aplikacji mobilnych

CZĘŚĆ C:

b) w ciągu ostatnich trzech lat przed upływem terminu składania ofert przeprowadziła co najmniej dwa szkolenia z zakresu bezpieczeństwa sieci (testy penetracyjne)

CZĘŚĆ D:

b) w ciągu ostatnich trzech lat przed upływem terminu składania ofert przeprowadziła co najmniej dwa szkolenia z zakresu bezpieczeństwa Windows (praktyczne warsztaty z ochrony systemu)

CZĘŚĆ E:

b) w ciągu ostatnich trzech lat przed upływem terminu składania ofert przeprowadziła co najmniej dwa szkolenia z zakresu zaawansowane pozyskiwanie szczegółowych informacji na temat ludzi i firm.

Zamawiający zastrzega, że od Wykonawcy na każdym etapie postępowania może żądać dokumentów potwierdzających posiadane wykształcenie i doświadczenie (tj. kserokopię dyplomu oraz dowody potwierdzające należyte wykonanie wykazanych szkoleń, takich jak np. protokół odbioru, referencje lub inne dokumenty z których wynika, że wskazana osoba przeprowadziła dane szkolenie). Odmowa okazania wymaganych dokumentów, lub ich brak będzie skutkować odrzuceniem oferty, lub odstąpieniem od umowy i naliczeniem kar umownych, określonych we wzorze umowy.