Możliwość dofinansowania

Szkolenie: Jak zostać hakerem? Pierwsze kroki w etycznym hakowaniu z Kali Linux” Rozdział 3 – Symulacje phishingowe i proces testowania socjotechniki.

Numer usługi 2025/08/11/47095/2933601

5 000,00 PLN brutto
5 000,00 PLN netto
312,50 PLN brutto/h
312,50 PLN netto/h

ADN AKADEMIA spółka z ograniczoną odpowiedzialnością spółka komandytowa

4,6 / 5

316 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
12.02.2026 do 20.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Grupa docelowa szkolenia:** • **Administratorzy IT, specjaliści ds. bezpieczeństwa i SOC** – osoby odpowiedzialne za ochronę systemów i reagowanie na incydenty. • **Pentesterzy i audytorzy** – prowadzący testy bezpieczeństwa, w tym symulacje ataków socjotechnicznych. • **Kadra menedżerska (CISO, ISO, kierownicy IT)** – decydenci wdrażający polityki bezpieczeństwa i strategie obrony. • **Pracownicy helpdesku i wsparcia IT** – pierwsza linia kontaktu z użytkownikami narażonymi na phishing. • **Specjaliści ds. compliance i audytu wewnętrznego** – odpowiedzialni za zgodność z regulacjami i procedurami bezpieczeństwa. • **Zaawansowani użytkownicy biznesowi / liderzy działów** – wspierający budowanie świadomości i szkolenia w swoich zespołach. T • **renerzy i osoby odpowiedzialne za edukację pracowników** – którzy wdrażają programy podnoszenia świadomości w organizacjach.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	11-02-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16

Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Usługa przygotowuje uczestników do rozpoznawania i przeciwdziałania zagrożeniom socjotechnicznym. Szkolenie obejmuje mechanizmy ataków phishingowych, praktyczne symulacje, obsługę narzędzi testowych oraz analizę reakcji użytkowników. Uczestnicy nauczą się wdrażać zabezpieczenia techniczne i budować świadomość bezpieczeństwa w organizacji, zwiększając odporność na ataki.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wyjaśnia pojęcie inżynierii społecznej oraz klasyfikuje główne rodzaje ataków socjotechnicznych (phishing, vishing, smishing).	Definiuje inżynierię społeczną i opisuje charakterystykę wybranych ataków.	Test teoretyczny
Wyjaśnia etapy ataku phishingowego oraz metody zbierania informacji (OSINT).	Wymienia i opisuje wszystkie etapy ataku phishingowego oraz techniki OSINT stosowane do zbierania informacji o celu.	Test teoretyczny
Charakteryzuje techniki podszywania się (spoofing, typosquatting) i mechanizmy ochronne (SPF, DKIM, DMARC).	Wymienia i opisuje techniki spoofingu i typosquattingu oraz wyjaśnia zasady działania mechanizmów ochrony przed phishingiem	Test teoretyczny
Przeprowadza analizę celu ataku phishingowego wykorzystując techniki OSINT.	Opisuje, jak identyfikuje i zbiera informacje o celu ataku przy użyciu narzędzi OSINT.	Wywiad swobodny
Opracowuje plan budowania świadomości oraz procedury reagowania na incydenty phishingowe.	Opisuje, jak tworzy i wdraża działania edukacyjne oraz procedury postępowania w przypadku wykrycia ataku.	Wywiad swobodny
Przestrzega zasad etycznych i prawnych podczas wykonywania testów socjotechnicznych.	Wyjaśnia, jakie zasady etyczne i prawne stosuje podczas testów oraz dlaczego są one ważne.	Wywiad swobodny
Promuje kulturę bezpieczeństwa i świadomość zagrożeń w organizacji.	Przedstawia argumenty i przykłady działań, które podejmuje, aby zwiększyć świadomość bezpieczeństwa w miejscu pracy.	Wywiad swobodny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/ sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa Podmiotu prowadzącego walidację	Design Center
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa Podmiotu certyfikującego	Design Center
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

Program

Usługa prowadzona jest w godzinach dydaktycznych. Przerwy nie są wliczone w ogólny czas usługi rozwojowej. Harmonogram usługi może ulec nieznacznemu przesunięciu, ponieważ ilość przerw oraz długość ich trwania zostanie dostosowana indywidualnie do potrzeb uczestników szkolenia. Łączna długość przerw podczas szkolenia nie będzie dłuższa aniżeli zawarta w harmonogramie.

Szczegółowy harmonogram realizacji usługi zostanie dostosowany do potrzeb i możliwości uczestników a jego finalna wersja zostanie podana zgodnie z wymaganiami systemu BUR, przed rozpoczęciem realizacji usługi.

Zajęcia zostaną przeprowadzone przez ekspertów z wieloletnim doświadczeniem, którzy przekazuje nie tylko wiedzę teoretyczną, ale także praktyczne wskazówki i najlepsze praktyki. Uczestnicy mają możliwość czerpania z jego wiedzy i doświadczeń.

Moduł 1: Wprowadzenie do socjotechniki i phishingu(2h)

- Czym jest inżynieria społeczna?
- Rodzaje ataków socjotechnicznych: phishing, vishing, smishing
- Elementy psychologii wpływu i manipulacji w cyberatakach

Moduł 2: Etapy ataku phishingowego – od planowania do wykonania(3h)

- Wybór celu i zbieranie informacji (OSINT)
- Opracowanie wektora ataku: e-mail, formularz, domena
- Techniki podszywania się (spoofing, typosquatting)

Moduł 3: Narzędzia do testowania phishingu w Kali Linux(4h)

- SET – Social Engineering Toolkit
- Gophish – platforma do kampanii phishingowych
- Spoofing e-maili i rejestrowanie reakcji ofiar

- Analiza skuteczności ataku

Moduł 4: Projektowanie kampanii phishingowych – symulacje(3h)

- Projektowanie realnych scenariuszy (np. faktury, alerty logowania)
- Testy na wewnętrznych użytkownikach (bezpieczne środowisko labowe)
- Analiza błędów użytkownika i rekomendacje zabezpieczeń

Moduł 5: Ochrona przed phishingiem i edukacja użytkowników(3h)

- Mechanizmy ochrony: SPF, DKIM, DMARC
- Systemy wykrywania ataków socjotechnicznych
- Budowanie świadomości w organizacji
- Jak raportować i reagować na incydenty

Walidacja końcowa(1h)

Harmonogram

Liczba przedmiotów/zajęć: 8

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Moduł 1: Wprowadzenie do socjotechniki i phishingu	Paweł Pudo	12-02-2026	17:00	18:30	01:30
2 z 8 Przerwa	Paweł Pudo	12-02-2026	18:30	18:45	00:15
3 z 8 Moduł 2: Etapy ataku phishingowego – od planowania do wykonania	Paweł Pudo	12-02-2026	18:45	21:00	02:15
4 z 8 Moduł 3: Narzędzia do testowania phishingu w Kali Linux	Paweł Pudo	16-02-2026	17:00	20:00	03:00
5 z 8 Moduł 4: Projektowanie kampanii phishingowych – symulacje	Paweł Pudo	18-02-2026	17:00	19:15	02:15
6 z 8 Moduł 5: Ochrona przed phishingiem i edukacja użytkowników	Paweł Pudo	20-02-2026	17:00	19:15	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 8 Przerwa	Paweł Pudo	20-02-2026	19:15	19:30	00:15
8 z 8 Walidacja	-	20-02-2026	19:30	20:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	312,50 PLN
Koszt osobogodziny netto	312,50 PLN
W tym koszt walidacji brutto	0,00 PLN
W tym koszt walidacji netto	0,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Pudo

Od ponad pięciu lat Paweł Pudo intensywnie rozwija kompetencje w obszarach cyberbezpieczeństwa, administracji IT oraz edukacji cyfrowej, z powodzeniem łącząc umiejętności techniczne z talentem do klarownego przekazywania wiedzy nietechnicznym odbiorcom.

Obecnie odpowiada za całość infrastruktury IT w jednostce edukacyjnej, gdzie zarządza m.in. środowiskiem sieciowym, Azure Active Directory, pakietem Office 365, drukiem 3D i administracją stron internetowych. Równocześnie prowadzi audyty zgodne z normami ISO/IEC 27001:2017-06, ISO 22301:2020-04 oraz RODO, wspierając instytucje w budowaniu bezpiecznych i zgodnych z przepisami systemów informatycznych. Ukończył kurs audytora wiodącego SZBI (ISO 27001).

Paweł od lat prowadzi szkolenia z zakresu cyberbezpieczeństwa dla szkół, samorządów i przedsiębiorstw, dzieląc się praktyczną wiedzą i doświadczeniem. Znany z wyjątkowej umiejętności tłumaczenia skomplikowanych zagadnień technicznych w prosty i przystępny sposób, co czyni go niezwykle skutecznym edukatorem i konsultantem.

W 2021 roku ukończył studia podyplomowe "Bezpieczeństwo i ochrona cyberprzestrzeni" na Uniwersytecie Ekonomicznym w Katowicach.

W ostatnim czasie intensywnie szkoli się również w zakresie zastosowań sztucznej inteligencji w edukacji i biznesie, wykorzystując AI m.in. do budowania narzędzi szkoleniowych. Regularnie występuje jako prelegent na wydarzeniach branżowych, dzieląc się wiedzą jako członek społeczności cybersec.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma skrypt, materiały dydaktyczne w formie prezentacji oraz zestaw ćwiczeń w formie cyfrowej- pdf.

Warunki uczestnictwa

Warunki uczestnictwa:

- Podstawowa znajomość obsługi komputera, przeglądarek internetowych i systemu operacyjnego (Windows lub Linux).
- Podstawowa wiedza z zakresu działania sieci komputerowych i protokołu HTTP.
- Umiejętność pracy z edytorem tekstu i terminalem systemowym (cmd/bash).
- Własny komputer z dostępem do Internetu, możliwością instalacji oprogramowania oraz uprawnieniami administratora.
- Zainstalowana przeglądarka internetowa (np. Firefox, Chrome)
- Chęć pracy w środowiskach testowych i respektowania zasad etycznego testowania bezpieczeństwa.

Informacje dodatkowe

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień - w przypadku dofinansowania w co najmniej 70%

3) W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT

Warunki techniczne

Szkolenie realizowane jest w czasie rzeczywistym za pośrednictwem platformy wideokonferencyjnej (Click Meeting).

Uczestnik powinien dysponować:

- komputerem/laptopem z min. 4 GB RAM, procesorem x64 (zalecane: 8 GB RAM i SSD),
- systemem operacyjnym umożliwiającym uruchomienie **maszyny wirtualnej (np. VirtualBox)** lub środowiska **Kali Linux (VM/Live USB)**,
- stabilnym łączem internetowym (min. 10 Mb/s),

- przeglądarką internetową (zalecany: Chrome/Firefox),
- aktywnym mikrofonem i kamerą (wymagane),

Kontakt

Ariel Banaszewski

E-mail ariel.banaszewski@adn.pl

Telefon (+48) 22 1627 981