Możliwość dofinansowania

# Security Awareness - cyberbezpieczeństwo w praktyce

Numer usługi 2025/08/07/8386/2928306

1 107,00 PLN brutto
900,00 PLN netto
369,00 PLN brutto/h
300,00 PLN netto/h

TestArmy Group S.A.

4,3 / 5

94 oceny

zdalna w czasie rzeczywistym
Usługa szkoleniowa
3 h
09.01.2026 do 09.01.2026

# Informacje podstawowe

| | |
|---|---|
| **Kategoria** | Informatyka i telekomunikacja / Programowanie |
| **Grupa docelowa usługi** | Szkolenie skierowane jest do osób zarówno technicznych i nietechnicznych, posiadających dostęp do jakichkolwiek danych służbowych. Są to m.in. pracownicy biur, działów obsługi klienta, sprzedawcy, specjaliści i konsultanci posiadający dostep do skrzynek mailowych, urządzeń służbowych typu smartfon/tablet/laptop, wewnętrznych systemów przretwarzania danych (np. CRM), osoby pracujące zdalnie lub w trybie hybrydowym, pracownicy produkcyjni obsługujący systemy oparte o komputery lub sieci, działy helpdesk i kadry/HR. |
| **Minimalna liczba uczestników** | 5 |
| **Maksymalna liczba uczestników** | 40 |
| **Data zakończenia rekrutacji** | 05-01-2026 |
| **Forma prowadzenia usługi** | zdalna w czasie rzeczywistym |
| **Liczba godzin usługi** | 3 |
| **Podstawa uzyskania wpisu do BUR** | Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych |

# Cel

## Cel edukacyjny

Szkolenie ma na celu podniesienie odporności uczestników względem ataków hakerskich, w tym socjotechnicznych. Uczestnicy dowiedzą się o mechanizmach zabezpieczeń systemów IT, jak hakerzy próbują je obejść i o roli czynnika ludzkiego w utrzymaniu bezpieczeństwa danych.

### Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|---|---|---|
| "Uczestnik szkolenia:<br>Rozpoznaje i wyjaśnia kluczowe pojęcia oraz terminologię związaną z cyberbezpieczeństwem, systemami informatycznymi i siecią<br><br>Charakteryzuje różne typy złośliwego oprogramowania i ataków socjotechnicznych<br><br>Opisuje kluczowe wektory i metody wpływu na ofiarę przez hakerów<br><br>Wymienia i rozumie podstawowe spodoby zabezpieczania danych<br><br>Przedstawia przykładowe narzędzia i techniki wykorzystywane zabezpieczaniu danych<br><br>Rozpoznaje rolę polityki bezpieczeństwa w budowaniu cyber-odporności firmy" | "Definiuje kluczowe pojęcia związane z cyberbezpieczeńswem, takie jak: ransomware, keylogger, botnet, trojan, phishing, vishing, smishing, podszywanie się (impersonalization), URL, biblioteki, szyfrowanie.<br><br>Rozróżnia systemy operacyjne: mobilne i stacjonarne oraz podstawy zabezpieczania danych na tych urządzeniach.<br><br>Rozróżnia złośliwe oprogramowanie: ransomware, trojan, keylogger, wabbit, adware, hijacker.<br><br>Wyjaśnia czym jest i na czym polega phishing, smishing, vishing, ataki na URL, atak ctrl-c + crtl-v, atak na pliki Office i na wtyczki w przeglądarce.<br><br>Wyjaśnia czym są ataki socjotechniczne i rozpoznaje ich podłoże psychologiczne.<br><br>Podaje przykłady rozwiązań technologicznych, które można wykorzystać do zwiększenia bezpieczeństwa danych i systemów: np. zapora, szyfrowanie plików, akutalizacje, bezpieczne dzielenie się dostępem, menedżer haseł, weryfikacja wieloskładnikowa.<br><br>Wyjaśnia rolę polityki bezpieczeństwa danych w utrzymaniu cyber-odporności firmy i określa, dlaczego jej obchodzenie jest problematyczne.<br><br>Opisuje jak jego/jej działania wpływają na cyber-odporność firmy." | Test teoretyczny |

# Kwalifikacje

### Kompetencje

Usługa prowadzi do nabycia kompetencji.

**Warunki uznania kompetencji**

**Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?**

TAK

**Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?**

TAK

**Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?**

TAK

# Program

1. Jak zabezpieczamy systemy IT
2. Podstawy sieci i złośliwego oprogramowania
3. Konsekwencje złośliwego oprogramowania dla przedsiębiorstwa
4. Przykłady ataków i wektory
5. Socjotechnika
6. Jak się zabezpieczyć

# Harmonogram

Liczba przedmiotów/zajęć: 6

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 1 z 6 Jak zabezpieczamy systemy IT | Paweł Wałuszko | 09-01-2026 | 09:00 | 09:20 | 00:20 |
| 2 z 6 Podstawy sieci i złośliwego oprogramowania | Paweł Wałuszko | 09-01-2026 | 09:20 | 09:40 | 00:20 |
| 3 z 6 Konsekwencje złośliwego oprogramowania dla przedsiębiorstwa | Paweł Wałuszko | 09-01-2026 | 09:40 | 10:20 | 00:40 |
| 4 z 6 Przykłady ataków i wektory | Paweł Wałuszko | 09-01-2026 | 10:20 | 10:40 | 00:20 |

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 5 z 6 Socjotechnika | Paweł Wałuszko | 09-01-2026 | 10:40 | 11:10 | 00:30 |
| 6 z 6 Jak się zabezpieczyć | Paweł Wałuszko | 09-01-2026 | 11:10 | 11:30 | 00:20 |

# Cennik

## Cennik

| Rodzaj ceny | Cena |
|---|---|
| **Koszt przypadający na 1 uczestnika brutto** | 1 107,00 PLN |
| **Koszt przypadający na 1 uczestnika netto** | 900,00 PLN |
| **Koszt osobogodziny brutto** | 369,00 PLN |
| **Koszt osobogodziny netto** | 300,00 PLN |

# Prowadzący

Liczba prowadzących: 1

1 z 1

### Paweł Wałuszko

Wykładowca akademicki i trener/szkoleniowiec z wieloletnim doświadczeniem.

# Informacje dodatkowe

## Informacje o materiałach dla uczestników usługi

Będąc uczestnikiem szkolenia, otrzymasz komplet materiałów:

- starannie opracowaną prezentację opisującą zagadnienia omawiane podczas szkolenia
- zestaw pytań i ćwiczeń

## Informacje dodatkowe

Warunkiem organizacji szkolenia jest zebranie grupy minimum 5 osób. W przypadku niewystarczającej liczby chętnych wyznaczany jest kolejny termin kursu.

# Warunki techniczne

Szkolenie odbędzie się na platformie Zoom.

Uczestnicy proszeni się o przygotowanie laptopów/PC ze stabilnym łączem internetowym, dowolną przeglądarką internetową oraz edytorem tekstu.

# Kontakt


## Aleksandra Skomorow

**E-mail** aleksandraskomorow@gmail.com
**Telefon** (+48) 662 316 244