

FORMULARZ REKRUTACYJNY NA SZKOLENIE
DLA KADRY DYDAKTYCZNEJ

DANE OSOBOWE:

Nazwisko i imię	
Komórka organizacyjna	
Stanowisko pracy	
Forma i okres zatrudnienia	

ZAKRES WSPARCIA

W ramach zgłoszenia kandydat deklaruje chęć uczestnictwa w szkoleniach (proszę zaznaczyć wybrane szkolenia):

Nazwa szkolenia	Wybór preferowanej formy wsparcia
SEC503 Intrusion Detection In-Depth	
SEC511 Continuous Monitoring and Security Operations	
SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling	
SEC560 Network Penetration Testing and Ethical Hacking	
SEC542 Web App Penetration Testing and Ethical Hacking	
FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics	
FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	
SEC501 Advanced Security Essentials - Enterprise Defender	
SEC505 Securing Windows and PowerShell Automation	
SEC575 Mobile Device Security and Ethical Hacking	
SEC617 Wireless Penetration Testing and Ethical Hacking	
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	
AUD507 Auditing & Monitoring Networks, Perimeters & Systems	
SEC401 Security Essentials: Network, Endpoint, and Cloud	
FOR308 Digital Forensics Essentials	
FOR498 Battlefield Forensics & Data Acquisition	
SEC301 Introduction to Cyber Security	
FOR518 Mac and iOS Forensic Analysis and Incident Response	



FOR585 Smartphone Forensic Analysis In-Depth	
FOR500 Windows Forensic Analysis	
SEC487 Open-Source Intelligence (OSINT) Gathering and Analysis	
SEC573 Automating Information Security with Python	
ICS410 ICS/SCADA Security Essentials	
ICS515 ICS Visibility, Detection, and Response	
SEC760 Advanced Exploit Development for Penetration Testers	
SEC460 Enterprise and Cloud Threat and Vulnerability Assessment	
SEC488 Cloud Security Essentials	
SEC510 Public Cloud Security: AWS, Azure, and GCP	
SEC540 Cloud Security and DevSecOps Automation	
SEC541 Cloud Security Monitoring and Threat Detection	
SEC588 Cloud Penetration Testing	
FOR509 Enterprise Cloud Forensics and Incident Response	
MGT516 Managing Security Vulnerabilities: Enterprise and Cloud	
MGT520 Leading Cloud Security Design and Implementation	
SEC522 Application Security: Securing Web Apps, APIs, and Microservices	
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques	

KRYTERIA OCENY KANDYDATA:

KRYTERIUM	DEKLARACJA
Pracownik dydaktyczny Uczelni (wymóg konieczny) ¹	TAK/NIE
Zatrudnienie na podstawie umowy o pracę/ umowy zlecenie obejmującej okres realizacji projektu (wymóg konieczny) ¹	TAK/NIE
Nieukończone 30 lat ¹	TAK/NIE
Ukończone 45 lat ¹	TAK/NIE
Orzeczona niepełnosprawność ¹	TAK/NIE

.....
Data i podpis Kandydata

Załączniki:

- Wypełniony formularz zgłoszeniowy

¹ Niepotrzebne skreślić





- Oświadczenie o zgodzie na przetwarzanie danych osobowych
- Ankieta motywacyjna
- Orzeczenie o niepełnosprawności (jeżeli dotyczy)

Suma punktów:

Decyzja Wydziałowej Komisji Rekrutacyjnej:

- zakwalifikowana/y do udziału
- niezakwalifikowana/y do udziału z powodu:
 - uzyskania niewystarczającej liczby punktów
 - zgłoszenie nie spełnia kryteriów formalnych
 - inne.....