

kod szkolenia: CySA+ (+ exam) / PL DL 5d NIS2

CompTIA Cybersecurity Analyst (CySA+) - szkolenie autoryzowane wraz z egzaminem CS0-004

Jeśli chcesz zostać profesjonalnym analitykiem cyberbezpieczeństwa, zdobyć umiejętności wykrywania, zapobiegania i reagowania na incydenty związane z cyberzagrożeniami, a także nauczyć się monitorować bezpieczeństwo systemów w sposób ciągły, to certyfikat CompTIA Cybersecurity Analyst (CySA+) jest dla Ciebie idealny.

Certyfikat CompTIA Cybersecurity Analyst (CySA+) potwierdza, że kandydaci posiadają wiedzę i umiejętności niezbędne do wykrywania i analizowania oznak działalności złośliwej, rozumienia wywiadu i zarządzania zagrożeniami, odpowiadania na ataki i podatności, wykonywania działań odpowiedzi na incydenty, oraz raportowania i komunikowania się na tematy związane z cyberbezpieczeństwem.

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Sprawdź swoją wiedzę z zakresu:

- [CompTIA CySA+](#)

- [CompTIA Security+](#)
- [CompTIA Network+](#)
- [OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji](#)
- [CEH - Certified Ethical Hacker](#)
- [ECIH - Certified Incident Handler](#)
- [Testy penetracyjne](#)
- [CompTIA SecurityX \(Formerly CASP+\)](#)
- [CompTIA SecAI+](#)
- [CompTIA Linux+](#)



Odbiorcy szkolenia

Szkolenie skierowane jest dla osób pracujących na stanowiskach:

- Analityk bezpieczeństwa IT
- Analityk bezpieczeństwa cybernetycznego
- Analityk Security Operations Center (SOC)
- Inżynier bezpieczeństwa IT
- Specjalista ds. bezpieczeństwa cybernetycznego



Korzyści

Na tym szkoleniu poznasz narzędzia i metody zarządzania ryzykiem cybernetycznym, rozpoznawania różnych rodzajów powszechnych zagrożeń, oceny poziomu bezpieczeństwa organizacji, zbierania i analizowania informacji o cyberprzestępczości, oraz radzenia sobie z sytuacjami kryzysowymi.

Uczestnicy szkolenia zdobędą wiedzę i umiejętności w zakresie:

- wyszukiwania i automatyzacji,
- monitorowania bezpieczeństwa ruchu sieciowego,
- bezpieczeństwa oprogramowania i aplikacji.



Program szkolenia

1. Understanding ACCybersecurity Leadership Concepts
 - Exploring Control Types and Methods
 - Explaining Patch Management Concepts

2. Exploring Threat Intelligence and Threat Hunting Concepts
 - Exploring Threat Actor Concepts
 - Identifying Active Threats
 - Exploring Threat-Hunting Concepts
3. Explaining Important System and Network Architecture Concepts
 - Reviewing System and Network Architecture Concepts
 - Exploring Identity and Access Management (IAM)
 - Maintaining Operational Visibility
4. Understanding Process Improvement in Security Operations
 - Exploring Leadership in Security Operations
 - Understanding Technology for Security Operations
5. Implementing Vulnerability Scanning Methods
 - Explaining Compliance Requirements
 - Understanding Vulnerability Scanning Methods
 - Exploring Special Considerations in Vulnerability Scanning
6. Performing Vulnerability Analysis
 - Understanding Vulnerability Scoring Concepts
 - Exploring Vulnerability Context Considerations
7. Communicating Vulnerability Information
 - Explaining Effective Communication Concepts
 - Understanding Vulnerability Reporting Outcomes and Action Plans
8. Explaining Incident Response Activities
 - Exploring Incident Response Planning
 - Performing Incident Response Activities
9. Demonstrating Incident Response Communication
 - Understanding Incident Response Communication
 - Analyzing Incident Response Activities
10. Applying Tools to Identify Malicious Activity
 - Identifying Malicious Activity
 - Explaining Attack Methodology Frameworks
 - Explaining Techniques for Identifying Malicious Activity
11. Analyzing Potentially Malicious Activity
 - Exploring Network Attack Indicators
 - Exploring Host Attack Indicators
 - Exploring Vulnerability Assessment Tools
12. Understanding Application Vulnerability Assessment
 - Analyzing Web Vulnerabilities
 - Analyzing Cloud Vulnerabilities
13. Exploring Scripting Tools and Analysis Concepts
 - Understanding Scripting Languages
 - Identifying Malicious Activity Through Analysis

14. Understanding Application Security and Attack Mitigation Best Practices

- Exploring Secure Software Development Practices
- Recommending Controls to Mitigate Successful Application Attacks
- Implementing Controls to Prevent Attacks



Oczekiwane przygotowanie uczestnika

1. Wymagana wiedza z zakresu szkoleń:
 - SPLUS+ - Warsztaty z CompTIA Security + (przygotowanie do egzaminu SY0-701)
2. Minimum 3-4 letnie doświadczenie pracy na stanowisku administratora bezpieczeństwa.



Szkolenie obejmuje

- 5 dni pracy z trenerem
- Nadzór trenera
- Autoryzowany podręcznik: The Official CompTIA CySA+
- Środowisko laboratoryjne - ważne 12 miesięcy
- voucher na egzamin CS0-004
- Metoda szkolenia
- wykład
- warsztaty



Język

- Szkolenie: polski
- Materiały: angielski

Czas trwania

5 dni / 35 godzin

Opis egzaminu

Do egzaminu można przystąpić w autoryzowanych ośrodkach egzaminacyjnych PearsonVue.

Informacje o egzaminie: CS0-004

Tytuł – The CompTIA Cybersecurity Analyst (CySA+)

Format testu: Multiple choice and performance-based

Ilość pytań – max 85

Czas trwania – 165 min

Passing Score - 750 (on a scale of 100-900)

Szczegółowe informacje dotyczące egzaminu znajdują się na stronie Comptia: [The CompTIA Cybersecurity Analyst \(CySA+\)](#).

*** Istnieje możliwość wykupienia vouchera z opcją retake za dodatkową dopłatą 450 zł, opcja ta dostępna jest do wyboru wyłącznie w momencie zgłoszenia na szkolenie.**