

Warsztaty z CompTIA Cybersecurity Analyst (CySA+) (przygotowanie do egzaminu CS0-003)

Warsztaty z CompTIA Cybersecurity Analyst (CySA+) (przygotowanie do egzaminu CS0-003)



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](#)

PRZEZNACZENIE 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 WYNIKAJĄCE Z UKOŃCZENIA SZKOLENIA

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.

METODA EGZAMINOWANIA

Do egzaminu można przystąpić w autoryzowanych ośrodkach egzaminacyjnych PearsonVue.

Egzamin nie jest zawarty w cenie szkolenia.

Informacje o egzaminie: CS0-003

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 \(CySA+\)](#).

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

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.

AGENDA SPOTKANIA

Sala szkoleniowa

1. Understanding Vulnerability Response, Handling, and Management

- Understanding Cybersecurity 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

Kod szkolenia	CySA+ / PL AA 5d
Czas trwania	5 dni
Poziom	Średnio zaawansowany
Autoryzacja	Altkom