



Załącznik nr 1 do SWZ po zmianach

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1) Opis przedmiotu zamówienia

Przeprowadzenie szkolenia CompTIA wraz z wydaniem vouchera na egzamin certyfikacyjny dla 9 osób w ramach projektu pt. „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej” współfinansowanego z Funduszu Bezpieczeństwa Wewnętrznego (nr 80/PL/2020/FBW).

Szkolenie obejmuje następujące moduły:

- 1* Przeprowadzenie szkolenia przygotowującego do egzaminu CompTIA Network+ N10 wraz z voucherem na egzamin certyfikacyjny CompTIA Network+ N10 ważnym min. 3 miesiące dni po zakończeniu szkolenia;
- 2* Przeprowadzenie szkolenia przygotowującego do egzaminu CompTIA Security+ SY0 wraz z voucherem na egzamin certyfikacyjny CompTIA Security+ SY0 ważnym min. 3 miesiące dni po zakończeniu szkolenia;
- 3* Przeprowadzenie szkolenia przygotowującego do egzaminu CompTIA Cybersecurity Analyst (CySA+) CS0 wraz z voucherem na egzamin certyfikacyjny CompTIA Cybersecurity Analyst (CySA+) CS0 ważnym min. 3 miesiące po zakończeniu szkolenia.

*w wersji kodowej (examcode) najbardziej aktualnej na dzień podpisania umowy

2) Odbiorcy szkolenia

Szkolenie przeznaczone jest dla specjalistów i praktyków z zakresu informatyki śledczej oraz cyberbezpieczeństwa z Komend Wojewódzkich Policji. Uczestnikami szkolenia będzie łącznie 9 osób w ramach jednej grupy szkoleniowej w każdym z wyżej wymienionych modułów.

3) Wymagania ogólne dotyczące realizacji szkolenia

- a) Wykonawca musi posiadać status autoryzowanego partnera CompTIA.
- b) Wykonawca szkolenia zapewni dla każdego uczestnika dostęp do platformy szkoleniowej do komunikacji audio/video dającej możliwość przeprowadzenia na żywo, przy użyciu sieci Internet, zajęć teoretycznych i praktycznych z możliwością udostępniania obrazu z pulpitu zarówno przez prowadzących, jak i uczestników. Indywidualne stanowiska robocze (komputery kursantów) zostaną zapewnione przez Zamawiającego.
- c) Wykonawca przeprowadzi szkolenie w języku polskim
- d) Każdy moduł realizowany będzie w ramach jednej grupy szkoleniowej składającej się z 9 osób. Nie dopuszcza się uczestnictwa w zajęciach innych odbiorców szkolenia niż wskazane przez zamawiającego.
- e) Wykonawca zrealizuje szkolenie w terminie 3 miesięcy od daty podpisania Umowy.
- f) Wykonawca w ramach uzgodnień w trybie kontaktów roboczych z zamawiającym, wyznaczy termin szkolenia dla każdego z modułów.
- g) Każdy moduł musi obejmować 5 kolejnych dni roboczych od poniedziałku do piątku.
- h) Każdy dzień szkoleniowy to 7 godzin zegarowych. Dokładny harmonogram dzienny dla poszczególnych modułów zostanie uzgodniony z Wykonawcą w ramach kontaktów roboczych.
- i) Zamawiający wymaga, aby termin kolejnego modułu był wyznaczony nie wcześniej niż po upływie 21 dni kalendarzowych od zakończenia poprzedniego modułu.
- j) Wykonawca zapewni akredytowane materiały szkoleniowe CompTIA dla poszczególnych modułów, dla każdego z uczestników szkolenia. Materiały szkoleniowe muszą być przygotowane w języku polskim lub angielskim. Materiały szkoleniowe mogą być w formie papierowej lub w formie elektronicznej. Koszty opracowania, powielenia i transportu materiałów szkoleniowych ponosi Wykonawca. Wykonawca ponosi pełną odpowiedzialność za zgodność merytoryczną oraz aktualność przekazywanych danych/informacji w materiałach szkoleniowych.
- k) Wykonawca zapewni konsultacje on-line w zakresie tematyki określonej w szkoleniu do 20 dni kalendarzowych po zakończeniu każdego z modułów dla każdego z uczestników szkolenia.





- l) Uczestnicy otrzymają imienne certyfikaty ukończenia każdego z modułów, sygnowane przez firmę CompTIA.
- m) Po zakończeniu każdego z modułów Wykonawca zobowiązuje się do przekazania uczestnikom szkolenia imiennych voucherów na egzaminy certyfikacyjne CompTIA – odpowiednie dla danego modułu, najpóźniej w dniu zakończenia każdego z modułów.

4) Zakres merytoryczny szkolenia (trzy moduły)

Zakres merytoryczny szkolenia musi obejmować wszystkie tematy wyszczególnione w dokumentach „CompTIA Certification Exam Objectives” dla danego typu modułu, dostępnych na oficjalnej stronie CompTIA, to jest:

Moduł 1.:

a) CompTIA Network+

- Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
- Explain the characteristics of network topologies and network types.
- Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
- Given a scenario, configure a subnet and use appropriate IP addressing schemes.
- Explain common ports and protocols, their application, and encrypted alternatives.
- Explain the use and purpose of network services.
- Explain basic corporate and datacenter network architecture.
- Summarize cloud concepts and connectivity options.
- Compare and contrast various devices, their features, and their appropriate placement on the network.
- Compare and contrast routing technologies and bandwidth management concepts.
- Given a scenario, configure and deploy common Ethernet switching features.
- Given a scenario, install and configure the appropriate wireless standards and technologies.
- Given a scenario, use the appropriate statistics and sensors to ensure network availability.
- Explain the purpose of organizational documents and policies.
- Explain high availability and disaster recovery concepts and summarize which is the best solution.
- Explain common security concepts.
- Compare and contrast common types of attacks.
- Given a scenario, apply network hardening techniques.
- Compare and contrast remote access methods and security implications.
- Explain the importance of physical security.
- Explain the network troubleshooting methodology.
- Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.
- Given a scenario, use the appropriate network software tools and commands.
- Given a scenario, troubleshoot common wireless connectivity issues.
- Given a scenario, troubleshoot general networking issues.

Moduł 2.:

b) CompTIA Security+

- Compare and contrast different types of social engineering techniques.
- Given a scenario, analyze potential indicators to determine the type of attack.
- Given a scenario, analyze potential indicators associated with application attacks.
- Given a scenario, analyze potential indicators associated with network attacks.
- Explain different threat actors, vectors, and intelligence sources.
- Explain the security concerns associated with various types of vulnerabilities.
- Summarize the techniques used in security assessments.
- Explain the techniques used in penetration testing.
- Explain the importance of security concepts in an enterprise environment.
- Summarize virtualization and cloud computing concepts.
- Summarize secure application development, deployment, and automation concepts.
- Summarize authentication and authorization design concepts.





- Given a scenario, implement cybersecurity resilience.
- Explain the security implications of embedded and specialized systems.
- Explain the importance of physical security controls.
- Summarize the basics of cryptographic concepts.
- Given a scenario, implement secure protocols.
- Given a scenario, implement host or application security solutions.
- Given a scenario, implement secure network designs.
- Given a scenario, install and configure wireless security settings.
- Given a scenario, implement secure mobile solutions.
- Given a scenario, apply cybersecurity solutions to the cloud.
- Given a scenario, implement identity and account management controls.
- Given a scenario, implement authentication and authorization solutions.
- Given a scenario, implement public key infrastructure.
- Given a scenario, use the appropriate tool to assess organizational security.
- Summarize the importance of policies, processes, and procedures for incident response.
- Given an incident, utilize appropriate data sources to support an investigation.
- Given an incident, apply mitigation techniques or controls to secure an environment.
- Explain the key aspects of digital forensics.
- Compare and contrast various types of controls.
- Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
- Explain the importance of policies to organizational security.
- Summarize risk management processes and concepts.
- Explain privacy and sensitive data concepts in relation to security.

Moduł 3.:

c) **CompTIA Cybersecurity Analyst (CySA+)**

- Explain the importance of threat data and intelligence.
- Given a scenario, utilize threat intelligence to support organizational security.
- Given a scenario, perform vulnerability management activities.
- Given a scenario, analyze the output from common vulnerability assessment tools.
- Explain the threats and vulnerabilities associated with specialized technology.
- Explain the threats and vulnerabilities associated with operating in the cloud.
- Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
- Given a scenario, apply security solutions for infrastructure management.
- Explain software assurance best practices.
- Explain hardware assurance best practices.
- Given a scenario, analyze data as part of security monitoring activities.
- Given a scenario, implement configuration changes to existing controls to improve security.
- Explain the importance of proactive threat hunting.
- Compare and contrast automation concepts and technologies.
- Explain the importance of the incident response process.
- Given a scenario, apply the appropriate incident response procedure.
- Given an incident, analyze potential indicators of compromise.
- Given a scenario, utilize basic digital forensics techniques.
- Understand the importance of data privacy and protection.
- Given a scenario, apply security concepts in support of organizational risk mitigation.
- Explain the importance of frameworks, policies, procedures, and controls.

