Szkolenie autoryzowane

CompTIA Security+

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

CompTIA Security+ to globalny certyfikat potwierdzający posiadanie podstawowych umiejętności niezbędnych do wykonywania kluczowych funkcji z zakresu bezpieczeństwa informatycznego. Jest to pierwszy certyfikat z obszaru bezpieczeństwa, jaki powinien uzyskać kandydat na specjalistę IT.

Security+ stanowi fundament wiedzy wymaganej w każdej roli związanej z cyberbezpieczeństwem i otwiera drogę do stanowisk średniego szczebla w tej dziedzinie.

Certyfikat ten uwzględnia najlepsze praktyki w zakresie praktycznego rozwiązywania problemów bezpieczeństwa, gwarantując, że kandydaci nabywają realne umiejętności potrzebne do:

- Oceny poziomu zabezpieczeń środowiska korporacyjnego oraz rekomendacji i wdrażania odpowiednich rozwiązań z zakresu bezpieczeństwa
- Monitorowania i zabezpieczania środowisk hybrydowych, w tym chmurowych, mobilnych oraz urządzeń internetu rzeczy (IoT)
- Działania zgodnie z obowiązującymi przepisami i politykami, w tym z zasadami zarządzania, ryzyka oraz zgodności (governance, risk, compliance)
- Identyfikowania, analizowania i reagowania na zdarzenia oraz incydenty bezpieczeństwa

Zdobycie certyfikatu **CompTIA Security+** oznacza, że kandydat potrafi wspierać kluczowe

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

funkcje bezpieczeństwa IT i jest przygotowany do podjęcia pracy na stanowiskach wymagających praktycznych umiejętności z zakresu cyberbezpieczeństwa. Jest to również solidna podstawa do dalszego rozwoju – zarówno w kierunku bardziej zaawansowanych certyfikatów, jak i specjalistycznych ról w branży cyberbezpieczeństwa.

Certyfikat **CompTIA Security+** jest zgodny ze standardem ISO 17024 oraz zatwierdzony przez Departament Obrony Stanów Zjednoczonych (U.S. DoD) jako spełniający wymagania dyrektywy 8140.03M. Security+ odpowiada również podstawowym celom wymaganym w ramach 20 ról zawodowych NICE.

Certyfikat Security+ jest ważny przez trzy lata od dnia jego uzyskania. Program Continuous Education (CE) umożliwia osobom posiadającym certyfikat Security+ przedłużenie jego ważności w trzyletnich odstępach poprzez udział w działaniach i szkoleniach związanych z tematyką certyfikacji. Cele nauczania w kursie Security+ są zgodne z celami egzaminacyjnymi przypisanymi do poszczególnych domen egzaminu certyfikacyjnego Security+.

Szkolenie jest w języku polskim, materiały są w języku angielskim.

Korzyści

Certyfikat ten uwzględnia najlepsze praktyki w zakresie praktycznego rozwiązywania problemów bezpieczeństwa, gwarantując, że kandydaci nabywają realne umiejętności potrzebne do:

- Oceny poziomu zabezpieczeń środowiska korporacyjnego oraz rekomendacji i wdrażania odpowiednich rozwiązań z zakresu bezpieczeństwa
- Monitorowania i zabezpieczania środowisk hybrydowych, w tym chmurowych, mobilnych oraz urządzeń internetu rzeczy (IoT)
- Działania zgodnie z obowiązującymi przepisami i politykami, w tym z zasadami zarządzania, ryzyka oraz zgodności (governance, risk, compliance)
- Identyfikowania, analizowania i reagowania na zdarzenia oraz incydenty bezpieczeństwa

Zdobycie certyfikatu CompTIA Security+ oznacza, że kandydat potrafi wspierać kluczowe funkcje bezpieczeństwa IT i jest przygotowany do podjęcia pracy na stanowiskach wymagających praktycznych umiejętności z zakresu cyberbezpieczeństwa. Jest to również solidna podstawa do dalszego rozwoju – zarówno w kierunku bardziej zaawansowanych certyfikatów, jak i specjalistycznych ról w branży cyberbezpieczeństwa.

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu
DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Wymagania

Preferowane jest posiadanie certyfikatu CompTIA Network+ oraz doświadczenia w administracji IT, szczególnie w obszarze bezpieczeństwa.

Mile widziane będzie również praktyczne doświadczenie w technicznych aspektach bezpieczeństwa informacji oraz dobra znajomość koncepcji i zasad bezpieczeństwa.

Harmonogram szkolenia

1. **Podsumowanie fundamentalnych koncepcji bezpieczeństwa**
    1. Koncepcje bezpieczeństwa
    2. Środki kontroli bezpieczeństwa (Security Controls)
2. **Porównanie typów zagrożeń**
    1. Typy podmiotów zagrożenia (Threat Actors)
    2. Powierzchnia ataku (Attack Surfaces)
    3. Inżynieria społeczna (Social Engineering)
3. **Wyjaśnianie rozwiązań kryptograficznych**
    1. Algorytmy kryptograficzne
    2. Publiczna infrastruktura klucza (PKI)
    3. Rozwiązania kryptograficzne
4. **Wdrażanie zarządzania tożsamością i kontrolą dostępu**
    1. Uwierzytelnianie (Authentication)
    2. Autoryzacja (Authorization)
    3. Zarządzanie tożsamością (Identity Management)
5. **Bezpieczna architektura sieci przedsiębiorstwa**
    1. Architektura sieci przedsiębiorstwa
    2. Urządzenia zabezpieczające sieć (Network Security Appliances)
    3. Bezpieczna komunikacja (Secure Communications)
6. **Bezpieczna architektura sieci w chmurze**
    1. Infrastruktura chmurowa (Cloud Infrastructure)
    2. Systemy wbudowane i architektura Zero Trust (Embedded Systems and Zero Trust Architecture)
7. **Wyjaśnianie koncepcji odporności i bezpieczeństwa lokalizacji**
    1. Zarządzanie zasobami (Asset Management)

2. Strategie redundancji (Redundancy Strategies)
3. Bezpieczeństwo fizyczne (Physical Security)

8. **Wyjaśnianie zarządzania lukami w zabezpieczeniach**
    1. Luki w zabezpieczeniach urządzeń i systemów operacyjnych (Device and OS Vulnerabilities)
    2. Luki w aplikacjach i środowiskach chmurowych (Application and Cloud Vulnerabilities)
    3. Metody identyfikacji luk (Vulnerability Identification Methods)
    4. Analiza i usuwanie luk (Vulnerability Analysis and Remediation)
9. **Ocena możliwości zabezpieczeń sieci**
    1. Benchmarki zabezpieczeń sieci (Network Security Baselines)
    2. Wzmacnianie możliwości zabezpieczeń sieci (Network Security Capability Enhancement)
10. **Ocena zabezpieczeń urządzeń końcowych**
    1. Wdrażanie zabezpieczeń urządzeń końcowych (Implement Endpoint Security)
    2. Utwardzanie urządzeń mobilnych (Mobile Device Hardening)
11. **Wzmacnianie zabezpieczeń aplikacji**
    1. Benchmarki protokołów i aplikacji (Application Protocol Security Baselines)
    2. Koncepcje zabezpieczeń aplikacji chmurowych i webowych (Cloud and Web Application Security Concepts)
12. **Wyjaśnianie zagadnień odpowiedzi na incydenty i monitorowania**
    1. Reagowanie na incydenty (Incident Response)
    2. Cyfrowe śledztwo (Digital Forensics)
    3. Źródła danych (Data Sources)
    4. Narzędzia monitorowania i alarmowania (Alerting and Monitoring Tools)
13. **Analiza wskaźników złośliwej aktywności**
    1. Wskaźniki ataków złośliwego oprogramowania (Malware Attack Indicators)
    2. Wskaźniki ataków fizycznych i sieciowych (Physical and Network Attack Indicators)
    3. Wskaźniki ataków aplikacyjnych (Application Attack Indicators)
14. **Podsumowanie zagadnień zarządzania bezpieczeństwem**
    1. Polityki, standardy i procedury (Policies, Standards, and Procedures)
    2. Zarządzanie zmianą (Change Management)
    3. Automatyzacja i orchestracja (Automation and Orchestration)
15. **Wyjaśnianie procesów zarządzania ryzykiem**
    1. Procesy i koncepcje zarządzania ryzykiem
    2. Zarządzanie dostawcami (Vendor Management)
    3. Audyty i oceny (Audits and Assessments)
16. **Podsumowanie zagadnień ochrony danych i zgodności z przepisami**
    1. Klasyfikacja danych i zgodność z przepisami (Data Classification and Compliance)
    2. Polityki dotyczące personelu (Personnel Policies)

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.