kod szkolenia: SecurityX / PL DL 5d NIS2

CompTIA SecurityX (Formerly CASP+)- szkolenie autoryzowane

Zobacz film: https://youtu.be/AMMd7j0ZMSg

Szkolenie CompTIA SecurityX zostało stworzone z myślą o doświadczonych inżynierach bezpieczeństwa oraz architektach bezpieczeństwa, którzy są odpowiedzialni za prowadzenie i ulepszanie gotowości cyberbezpieczeństwa w przedsiębiorstwie.

Jest skierowana do profesjonalistów z kilkuletnim doświadczeniem. Uczestnik pozna umiejętności niezbędne do zrozumienia architektury i operacji bezpieczeństwa jak również inżynierii bezpieczeństwa i kryptografii. Zapozna metody zarządzanie ryzykiem oraz zgodnością z obowiazującymi regulacjami prawnymi.

Szkolenie umożliwi przygotowanie kandydata do przystąpienia do egzaminu certyfikacyjnego CompTIA SecurityX.

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 (PenTest+/CPENT)**

Odbiorcy szkolenia

- Security Architect
- Senior Security Architect
- Information Security Officer

Korzyści

- **Zaawansowane umiejętności w zakresie bezpieczeństwa IT** – Zdobycie wiedzy na poziomie mistrzowskim, umożliwiającej projektowanie i wdrażanie skutecznych rozwiązań z zakresu cyberbezpieczeństwa na złożonych sieciach przedsiębiorstw, zarówno lokalnych, jak i w chmurze.
- **Międzynarodowo uznawany certyfikat** – SecurityX to certyfikat o globalnym uznaniu, który poświadcza kompetencje w zakresie architektury bezpieczeństwa, senior engineering oraz integracji celów biznesowych przedsiębiorstwa z systemami zabezpieczeń.
- **Umiejętność zarządzania cyberbezpieczeństwem na poziomie przedsiębiorstwa** – Certyfikowani specjaliści potrafią oceniać, zarządzać i chronić potrzeby w zakresie cyberbezpieczeństwa w organizacjach, wykorzystując najnowsze techniki i najlepsze praktyki w branży.
- **Zwiększenie szans na awans zawodowy** – Certyfikat potwierdza zdolność do pełnienia ról związanych z zarządzaniem bezpieczeństwem, takich jak architekt bezpieczeństwa czy starszy inżynier bezpieczeństwa, co może prowadzić do lepszych możliwości kariery.
- **Gotowość na rosnące zagrożenia związane z bezpieczeństwem informacji** – Certyfikowani profesjonaliści są przygotowani do radzenia sobie z rosnącą liczbą zagrożeń w cyberprzestrzeni, a także do rozwiązywania problemów związanych z brakiem odpowiednio wykwalifikowanego personelu IT zajmującego się bezpieczeństwem.
- **Zwiększenie wartości organizacji** – Specjaliści z certyfikatem SecurityX mogą skutecznie

projektować i utrzymywać bezpieczne środowiska IT, co przyczynia się do poprawy bezpieczeństwa organizacji i ochrony jej danych w obliczu rosnących zagrożeń.

Program szkolenia

1. Governance, Risk & Compliance (GRC)
   - Wprowadzenie do governance w bezpieczeństwie
   - Polityki, standardy, procedury, odpowiedzialność, COBIT, ITIL, CMDB, GRC
   - Zarządzanie ryzykiem
   - Compliance i wymagania regulacyjne (GDPR, CCPA, PCI DSS, ISO 27001, NIST CSF)
   - Threat Modeling (STRIDE, MITRE ATT&CK, Diamond, OWASP)
   - AI i bezpieczeństwo (deepfakes, prompt injection, overreliance)
2. Security Architecture
   - Projektowanie odpornych systemów (WAF, VPN, NAC, CDN)
   - Skalowalność, nadmiarowość, recoverability
   - Bezpieczeństwo w SDLC (CI/CD, SAST/DAST/RASP, SBoM)
   - Redukcja powierzchni ataku, klasyfikacja danych, DLP
   - Dostęp, uwierzytelnienie, autoryzacja (modele RBAC, ABAC, DAC, MAC)
   - PKI, OCSP stapling, federacja, SSO, logowanie
3. Cloud Security & Zero Trust
   - Bezpieczeństwo w chmurze
   - CASB, Shadow IT, CI/CD w chmurze, konteneryzacja, serverless
   - Zarządzanie kluczami, remanencja danych, strategia kontroli
   - Zero Trust Architecture
   - Autoryzacja kontekstowa, mikrosegmentacja, SD-WAN
   - API security, granice bezpieczeństwa, deperymetryzacja
4. Security Engineering
   - IAM Troubleshooting (MFA, SAML, OAuth, PAM, provisioning, secrets management)
   - Endpoint i Server Hardening (EDR, HIPS, SELinux, MDM, browser isolation)
   - Sieć i infrastruktura (IDS/IPS, DNSSEC, błędy konfiguracji, tunelowanie)
   - Systemy legacy
5. Security Operations, Automation & Incident Response
   - Monitoring i analiza danych, korelacja logów, zbieranie artefaktów, SIEM
   - Ataki i podatności
   - Threat hunting i threat intelligence (IOC, MITRE ATT&CK, narzędzia analityczne)
   - Incident Response (Fazy IR, testowanie planów, analiza post-mortem)
   - Automatyzacja bezpieczeństwa (SOAR, scripting, harmonogramy, generative AI)
6. SecurityX CAS-005 Practice Exams
   - Przygotowanie do egzaminu CompTIA SecurityX

Oczekiwane przygotowanie uczestnika

- Kilkuletnie doświadczenie w bezpieczeństwie IT
- Wiedza z zakresu: CompTIA Security+,

Szkolenie obejmuje

- 5 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty

Język

Szkolenie: polski
Materiały: angieski

Czas trwania

5 dni / 35 godzin

Opis egzaminu

CompTIA SecurityX (Formerly CASP+) (CAS-005)
Liczba pytań – Max 90 pytań
Rodzaj pytań – pytania wielokrotnego wyboru i oparte na wydajności
Czas trwania – 165 min
Wynik zaliczenia – tylko zdany/niezdany; brak skali ocen.

Egzamin certyfikacyjny CompTIA SecurityX potwierdza, że kandydat posiada wiedzę i umiejętności niezbędne do:

- Projektowania, inżynierii, integracji i wdrażania bezpiecznych rozwiązań w złożonych środowiskach wspierających odporną organizację.
- Wykorzystania automatyzacji, monitorowania, wykrywania oraz reagowania na incydenty, aby proaktywnie wspierać ciągłe operacje bezpieczeństwa w środowisku przedsiębiorstwa.
- Stosowania praktyk bezpieczeństwa w środowiskach chmurowych, lokalnych oraz hybrydowych.
- Uwzględniania technologii kryptograficznych i technik, a także wpływu pojawiających się trendów (np. sztucznej inteligencji) na bezpieczeństwo informacji.
- Stosowania odpowiednich strategii zarządzania, zgodności, zarządzania ryzykiem i modelowania zagrożeń w całym przedsiębiorstwie.

SecurityX jest zgodny z normami ISO/ANSI 17024 i zatwierdzony przez Departament Obrony USA (DoD) w celu spełnienia wymagań Dyrektywy 8140.03M. Certyfikat CompTIA SecurityX (dawniej CASP+) odpowiada 19 rolom zawodowym NICE oraz 19 rolom w ramach Cyber Work Force (DCWF) Departamentu Obrony, zawartym w podręczniku DoD 8140.03.