

Szkolenia

1. Przedmiot zapytania: Przeprowadzenie certyfikowanego szkolenia CCISO (Certified Chief Information Security Officer) dla 1 pracownika. Szkolenie online.

Zakres i cel szkolenia:

Celem szkolenia jest przygotowanie uczestników do egzaminu certyfikacyjnego EC-Council CCISO oraz zdobycie wiedzy z zakresu pięciu domen CCISO:

1. Governance, Risk, Compliance (Nadzór i ład korporacyjny).
2. Information Security Controls and Audit Management (Zarządzanie ryzykiem i audyt).
3. Security Program Management & Operations (Zarządzanie projektami i operacjami).
4. Information Security Core Competencies (Kluczowe kompetencje bezpieczeństwa).
5. Strategic Planning, Finance, Procurement, and Third-Party Management (Planowanie strategiczne i finanse).

Wymagania wobec Wykonawcy:

1. posiadanie akredytacji EC Council
2. ważny wpis/certyfikat RIS oraz ISO 9001:2015
3. aktywne konto w Bazie Usług Rozwojowych
4. 3 referencje po zrealizowanych szkoleniach/usługach

2. Przedmiot zapytania: Zaawansowana konfiguracja usług hybrydowych systemu Windows Server dla 1 pracownika. Szkolenie online.

Zakres i cel szkolenia:

Celem szkolenia jest poszerzenie wiedzy administratorów w obszarze wykorzystania możliwości hybrydowych Azure, jak migrować obciążenia serwerów wirtualnych i fizycznych do Azure IaaS oraz jak zarządzać i zabezpieczać wirtualne maszyny Azure uruchamiane na Windows Server. Szkolenie powinno składać się z modułów:

Moduł 1: Bezpieczeństwo Windows Server

Zabezpieczenia kont użytkowników Windows Server

Wzmacnianie Windows Server

Windows Server Update Management

Secure Windows Server DNS

Laboratorium: Konfigurowanie bezpieczeństwa w Windows Server

Moduł 2: Wdrażanie rozwiązań bezpieczeństwa w scenariuszach hybrydowych

Wdrażanie zabezpieczeń sieciowych maszyn wirtualnych IaaS Windows Server

Audytywanie rozwiązań bezpieczeństwa maszyn wirtualnych IaaS Windows Server

Zarządzanie aktualizacjami Azure

Tworzenie i wdrażanie aplikacji z adaptacyjną kontrolą

Konfigurowanie szyfrowanie dysków BitLocker dla wirtualnych maszyn Windows IaaS

Wdrożenie śledzenia zmian i monitorowania integralności plików dla maszyn wirtualnych

IAAS Windows Server

Laboratorium: Używanie Azure Security Center w scenariuszach hybrydowych

Moduł 3: Wdrażanie wysokiej dostępności

Wprowadzenie do Cluster Shared Volumes.

Wdrożenie klastrów pracy awaryjnej Windows Server

Wdrożenie wysokiej dostępności maszyn wirtualnych z systemem Windows Server

Wdrożenie wysokiej dostępności serwera plików Windows Server

Wdrożenie skalowania i wysokiej dostępności za pomocą maszyn wirtualnych Windows Server

Laboratorium: Wdrożenie klastrów pracy awaryjnej

Moduł 4: Odzyskiwanie po awarii w Windows Server

Wdrażanie Hyper-V Replica

Ochrona infrastruktury lokalnej przed awariami z Azure Site Recovery

Laboratorium: Wdrażanie Hyper-V Replica oraz Windows Server Backup

Moduł 5: Wdrożenie usług odzyskiwania w scenariuszach hybrydowych

Wdrożenie hybrydowego tworzenia kopii zapasowych i odzyskiwania danych przy użyciu

Windows Server IaaS

Ochrona infrastruktury Azure infrastructure z Azure Site Recovery

Ochrona wirtualnych maszyn używając Azure Backup

Laboratorium: Wdrożenie usług odzyskiwania danych opartych na Azure

Moduł 6: Aktualizacja i migracja w systemie Windows Server

Migracja Active Directory Domain Services

Migracja obciążeń serwera plików za pomocą usługi migracji pamięci

Migracja ról Windows Server

Laboratorium: Migracja obciążeń Windows Server do maszyn wirtualnych IaaS

Moduł 7: Wdrażanie migracji w scenariuszach hybrydowych

Migracja lokalnych zasobów Windows Server do wirtualnych maszyn Azure

Aktualizacja i migracja maszyn wirtualnych w Windows Server IaaS

Konteneryzacja i migracja aplikacji ASP.NET do Azure App Service

Laboratorium: Migracja lokalnych zasobów Windows Server do wirtualnych maszyn Azure

Moduł 8: Monitorowanie serwera i wydajności w Windows Server

Monitorowanie wydajności Windows Server

Zarządzanie i monitorowanie event logs w Windows Server

Wdrażanie audytu i diagnostyki Windows Server

Rozwiązywanie problemów z Active Directory

Laboratorium: Monitorowanie i rozwiązywanie problemów z Windows Server

Moduł 9: Wdrożenie monitoringu operacyjnego w scenariuszach hybrydowych

Monitorowanie maszyn wirtualnych IaaS Windows Server IaaS

Monitorowanie stanu maszyn wirtualnych platformy Azure za pomocą Azure Metrics

Explorer and i alertów metryk

Monitorowanie wydajności wirtualnych maszyn używając Azure Monitor VM Insights

Rozwiązywanie problemów z siecią lokalną i hybrydową

Rozwiązywanie problemów z maszynami wirtualnymi Windows Server na platformie Azure

Laboratorium: Monitorowanie i rozwiązywanie problemów z uruchamianiem wirtualnych

maszyn w Windows Server

Wymagania wobec Wykonawcy:

1. posiadanie akredytacji Microsoft
2. ważny wpis/certyfikat RIS oraz ISO 9001:2015
3. aktywne konto w Bazie Usług Rozwojowych
4. 3 referencje po zrealizowanych szkoleniach/usługach

3. Przedmiot zapytania: Przeprowadzenie szkolenia „Cyberbezpieczeństwo pracowników biurowych - kurs o bezpieczeństwie IT” dla 14 pracowników. Szkolenie online.

Zakres i cel szkolenia:

Celem szkolenia jest nabycie przez pracowników biurowych wiedzy na temat najnowszych zagrożeń, technik ataków cyberprzestępczych oraz metod socjotechnicznych, które stanowią zagrożenie podczas codziennej pracy przy komputerze. Kurs powinien być zgodny z dyrektywą NIS2 i pomaga spełnić najnowsze wymogi dotyczące bezpieczeństwa sieci i informacji. Harmonogram szkolenia powinien poruszać poniższe kwestie:

1. Wprowadzenie do cyberprzestępczości: Poznaj podstawy cyberbezpieczeństwa.
2. Krajobraz zagrożeń 2024–2025 w Polsce i na świecie.
3. Czy jestem atrakcyjnym klientem dla cyberprzestępcy?
4. Rodzaje ataków na pracowników biurowych.
5. Straty dla firmy: Skutki udanego cyberataku.
6. Spam jako niegroźny sposób na groźne ataki.
7. Phishing jako metoda okradania naszych kont bankowych.
8. Opłacona faktura jako sposób przemycenia wirusa do naszego systemu.
9. KSeF – czym jest i dlaczego może stać się atrakcyjnym celem ataków.
10. Dlaczego KSeF nie musi zostać „zhakowany” aby doszło do nadużyć.
11. Użytkownik jako najsłabsze ogniwo systemów informatycznych.
12. Skuteczne metody ochrony przed cyberatakami.
13. AI w rękach cyberprzestępców: Nowe zagrożenia z wykorzystaniem sztucznej inteligencji.
14. AI – deepfake co to jest i jakie są rodzaje (generowanie głosu, spreparowanych dokumentów, komunikatów czy obrazów)
15. Procedura weryfikacji danych i użytkowników na dwa kanały.
16. Czy cyberprzestępca jest zawsze anonimowy?
17. Ataki DoS/DDoS: Zagrożenia dla instytucji.
18. Aktualizacja oprogramowania jak ważną rolę spełnia?
19. Sieci Botnet: Jak cyberprzestępcy przejmują urządzenia.
20. Bezpieczeństwo haseł: Jak cyberprzestępcy zdobywają Twoje hasła?
21. Menadżer haseł program, który zwiększa bezpieczeństwo.
22. Metody logowania 2FA oraz MFA.
23. Ataki socjotechniczne, czyli niewinne wyłudzenie danych z użyciem sztucznej inteligencji.
24. Socjotechnika stara metoda w nowoczesnych atakach.
25. Kradzież tożsamości w sieci, jakie to łatwe.
26. Skimming kart płatniczych: Gdzie i kiedy ktoś może zeskanować Twoją kartę?
27. Fizyczne bezpieczeństwo: Jak zabezpieczyć swoje miejsce pracy.

28. Ataki za pomocą przenośnych nośników danych, co zrobić z takimi nośnikami.
29. Sprzęt prywatny vs. firmowy: Jak zarządzać bezpieczeństwem urządzeń.

Wymagania wobec Wykonawcy:

1. posiadanie akredytacji Microsoft, EC Council
2. ważny wpis/certyfikat RIS oraz ISO 9001:2015
3. aktywne konto w Bazie Usług Rozwojowych
4. 3 referencje po zrealizowanych szkoleniach/usługach