Co potrafi osoba posiadająca kwalifikację „Zarządzanie cyberbezpieczeństwem w organizacji” (efekty uczenia się)?

Posiadacz certyfikatu z zakresu zarządzania cyberbezpieczeństwem w organizacji:

- jest świadomy obecnego krajobrazu zagrożeń oraz wektorów ataków na organizacje. Potrafi scharakteryzować najbardziej popularne typy zagrożeń dla organizacji oraz użytkowników i omówić zagrożenia wynikające z nowych oraz wschodzących technologii,

- potrafi przedstawić podstawowe koncepcje architektury bezpieczeństwa, budowę sieci teleinformatycznych wraz omówieniem podstawowych usług sieciowych oraz systemów operacyjnych wykorzystywanych w organizacjach,

- umie przedstawić różnice pomiędzy ryzykami wynikającymi z podatności systemów teleinformatycznych oraz przedstawić metody mierzenia zagrożeń oraz podatności w systemach organizacji. Potrafi omówić źródła informacji o podatnościach oraz metody i zasady pozyskiwania informacji o podatnościach dla systemów i aplikacji. Przedstawia metodykę powiązań podatności oraz wykorzystania ich w atakach sieciowych,

- umie przedstawić podstawowe procesy dotyczące zarządzania ryzykiem, oceną i strategiami postępowania z ryzykiem w obrębie obowiązujących ram, standardów oraz narzędzi zarządzania ryzykiem w organizacji,

- przedstawia zasady zarządzania ryzykiem w łańcuchu dostaw w zakresie monitorowania, klasyfikacji oraz wytycznych zarządzania umowami i stosowania zasad bezpieczeństwa oraz prywatności do zarządzania ryzykiem związanym z wykorzystywaniem, przetwarzaniem, przechowywaniem i przekazywaniem informacji lub danych,

- posiada wiedzę pozwalającą na wykorzystanie zapisów standardów bezpieczeństwa danych dotyczących informacji umożliwiających identyfikację osoby w obrębie ustaw o ochronie danych osobowych, ISO27001 i omawia narzędzia ograniczające ryzyko wystąpienia wycieku informacji,

- zna standardy dotyczące ciągłości biznesu, procedur utrzymania oraz odtwarzania danych – na poziomie norm i standardów, planów ciągłości działania i funkcjonowania po wystąpieniu incydentu,

- przedstawia koncepcję kopii bezpieczeństwa i odtwarzania danych w organizacji oraz metodologie działania i reagowania na incydenty i zdarzenia,

- przedstawia elementy metodologii i technik wykrywania włamań do hostów i sieci oraz metody analizy ruchu sieciowego na poziomie celów, metod pozyskiwania oraz składowania metadanych ruchu sieciowego,

- prezentuje rolę metod oceny, wdrażania, monitorowania, wykrywania i naprawiania bezpieczeństwa poprzez sposoby mierzenia i oceny bezpieczeństwa, wykorzystanie dostępnych narzędzi służących poprawie stanu bezpieczeństwa organizacji oraz inicjacji programu zarządzania podatnościami i aktualizacjami zasobów teleinformatycznych wykorzystywanych w organizacji,

- omawia zagrożenia i benefity wynikające z wykorzystania nowych i wschodzących technologii IT w oparciu o źródła oraz trendy technologiczne,

- omawia zasady utrzymania bezpieczeństwa aplikacji i ich wytwarzania poprzez wykorzystanie metodyki modelowania zagrożeń i roli SDLC i DevSecOps,

- potrafi przedstawić zasady i techniki zarządzania programem bezpieczeństwa informacji oraz zarządzania projektem w organizacji na poziomie obowiązujących polityk i standardów określających zasady zarządzania programem bezpieczeństwa informacji i prowadzenia projektów.

Do kogo adresowana jest kwalifikacja?

Kwalifikacja adresowana jest przede wszystkim do osób:

- stanowiących średnią i wyższą kadrę zarządzającą zespołami IT w obszarze bezpieczeństwa,
- pragnących usystematyzować wiedzę na temat procesów cyberbezpieczeństwa w organizacji,
- pragnących posiąść przekrojową wiedzę dotyczącą technologii wykorzystywanych w celu podniesienia poziomu bezpieczeństwa w organizacji,
- zajmujących się na co dzień zarządzaniem bezpieczeństwem w przedsiębiorstwach lub instytucjach publicznych składających się z dedykowanych zespołów odpowiedzialnych i zarządzających poszczególnymi elementami infrastruktury.

Gdzie można znaleźć zatrudnienie?

Posiadacz kwalifikacji może znaleźć zatrudnienie:

- w przedsiębiorstwach lub instytucjach publicznych posiadających zespoły zajmujące się bezpieczeństwem IT,
- w organizacjach, które planują rozszerzyć swoje procesy bezpieczeństwa celem wsparcia biznesu.

Informacje o szkoleniu

Szkolenie zostało zaprojektowane, aby pomóc liderom organizacji lepiej zrozumieć, zarządzać i redukować zagrożenia cybernetyczne. Zapewnia wiedzę na temat wdrożenia, utrzymywania i audytu standardów oraz najlepszych praktyk cyberbezpieczeństwa. Umożliwi zrozumienie, wykrywanie, korygowanie i monitorowanie jego skuteczności.
Uczestnictwo w szkoleniu pozwoli na zapoznanie się i zrozumienie metod i technik dostępnych dla zarządzania bezpieczeństwem teleinformatycznym w oparciu o procesy organizacyjne oraz technologie.

Podczas szkolenia zostaniesz przeprowadzony przez:

- przegląd głównych środków cyberbezpieczeństwa i architektury ich wdrażania,
- wyjaśnienie dostępnych działań utrzymaniowych i audytowych,
- opis zasad i technik badania skuteczności wdrożonych rozwiązań z zakresu cyberbezpieczeństwa,
- wytyczne w zakresie obsługi problemów i niezgodności.

Wyposażenie sali szkoleniowej

1. Projektor multimedialny.
2. Tablica/flipchart.
3. Nieograniczony dostęp do sieci Internet poprzez WIFI lub LAN.
4. Opcjonalnie: Komputery/terminale z dostępem do Internetu oraz oprogramowaniem (dla każdego uczestnika i trenera/egzaminatora).

Wymogi dla trenera

Posiada udokumentowaną wiedzę oraz doświadczenie zawodowe w obszarze kwalifikacji.

Egzamin

Wymagania poprzedzające dla kandydatów:

brak

Stanowisko egzaminacyjne

Egzamin przeprowadza się w pomieszczeniu wyposażonym w stoliki, krzesła z dostępem do sieci internetowej spełniającej następujące warunki:

- swobodny, w żaden sposób nieograniczony dostęp do wyszukiwarek oraz ich wyników,
- podłączone urządzenia do sieci LAN poprzez WiFi lub połączenie kablowe,
- skonfigurowane serwery nazw oraz inne niezbędne elementy służące do poprawnego korzystania z sieci Internet.

Wymogi dla egzaminatora

- posiada przynajmniej 5 letnie doświadczenie w zarządzaniu cyberbezpieczeństwem w przedsiębiorstwie lub instytucjach publicznych we wdrażaniu rozwiązań cyberbezpieczeństwa i opracowywaniu architektury teleinformatycznej i procesów w zakresie cyberbezpieczeństwa,
- stosuje kryteria weryfikacji przypisane do efektów uczenia się dla opisywanej kwalifikacji oraz kryteria oceny formalnej i merytorycznej dowodów na posiadanie efektów uczenia się właściwych dla opisywanej kwalifikacji.

Zasady przeprowadzania egzaminu (walidacja)

Walidacja dla kwalifikacji „Zarządzanie cyberbezpieczeństwem w organizacji" przeprowadzana jest przez Stowarzyszenie Ekspertów Bezpieczeństwa RP oraz GMP Defence Sp. z o.o.

1. Metody stosowane w walidacji

Egzamin praktyczny przeprowadzany jest z wykorzystaniem notatek i komputera, trwa 60 minut, polega na rozwiązaniu problemu z zakresu cyberbezpieczeństwa, tj. zaproponowaniu odpowiedniej metody zabezpieczenia środowiska w zależności od wylosowanego typu zagrożenia.

2. Certyfikaty i odznaki cyfrowe potwierdzające kwalifikacje

Certyfikaty i odznaki cyfrowe potwierdzające kwalifikację wydawane są na podstawie dostarczonych potwierdzeń wyników egzaminu. Certyfikat i odznaka cyfrowa są wystawiane dla uczestników, którzy uzyskali pozytywny wynik egzaminu. Certyfikaty i cyfrowe odznaki są wystawiane w terminie maksymalnie 30 dni roboczych od daty egzaminu.

3. **Uczestnicy mają prawo do złożenia odwołania od wyniku egzaminu** (patrz procedura odwoławcza).

4. **Kryteria oceny**

Ocena merytoryczna posiadanej wiedzy jest zgodna z efektami uczenia dla kwalifikacji „Zarządzanie cyberbezpieczeństwem w organizacji".

5. Proces zgłoszenia i obsługi egzaminu:

- Stowarzyszenie Ekspertów Bezpieczeństwa RP przygotowuje listę uczestników egzaminu na podstawie prawidłowo wypełnionych Formularzy Kandydata/ki,
- przed egzaminem uczestnikom przekazywane są zasady jego oceniania,
- potwierdzenie odbycia egzaminu jest podpisywane przez uczestników oraz egzaminatorów,
- wyniki egzaminu są protokołowane - egzaminatorzy przygotowują arkusze dla egzaminu wraz z dokumentacją,
- kompletną dokumentację egzaminu egzaminatorzy przesyłają w oryginałach do Stowarzyszenia,
- dokumentacja egzaminu jest przechowywana w Stowarzyszeniu Ekspertów Bezpieczeństwa RP.