

Najpopularniejsze certyfikacje

poniedziałek, 10 listopad 2008

CISSP - Certified Information Systems Security Professional - jest jednym z najbardziej rozpoznawanych certyfikatów w dziedzinie bezpieczeństwa informacji, który spełnia wymogi standardu ISO/IEC 17024:2003. O jego wartości świadczy także fakt, iż został on zatwierdzony przez amerykański Departament Obrony (DoD).

CISSP obejmuje dziesięć domen bezpieczeństwa:

1. Kontrola dostępu
2. Bezpieczeństwo telekomunikacji i sieci
3. Bezpieczeństwo aplikacji
4. Planowanie ciągłości funkcjonowania organizacji oraz odtwarzania systemów
5. Zarządzanie ryzykiem i bezpieczeństwo informacji
6. Prawo, regulacje, normy, dochodzenia
7. Kryptografia
8. Modelowanie i architektura bezpieczeństwa
9. Bezpieczeństwo operacyjne
10. Bezpieczeństwo fizyczne

Aby móc starać się o uzyskanie tytułu CISSP należy:

- wykazać się udokumentowanym, minimum pięcioletnim doświadczeniem pracy w co najmniej dwóch domenach dziedziny bezpieczeństwa informacji; okres ten może zostać skrócony do czterech lat, pod warunkiem ukończenia szkoły wyższej lub posiadania innych certyfikatów z bezpieczeństwa określonych przez (ISC)²,
- zaakceptować i stosować kodeks etyki CISSP,
- odpowiedzieć na pytania dotyczące niekaralności i braku historii kryminalnej,
- zdać egzamin składający się z 250 pytań, po 4 odpowiedzi każde, w czasie 6 godzin,
- przedstawić opinię polecającą od osoby posiadającej certyfikat (ISC)².

CISSP ważny jest przez trzy lata i aby go odnowić należy zdać egzamin ponownie. Przedłużenia uzyskuje się także poprzez zdobywanie punktów CPE (Continuing Professional Education), minimum 120 CPE w ciągu trzech lat, z czego w ciągu roku minimum 20 CPE. Punkty otrzymuje się uczestnicząc w konferencjach (1 CPE/h), poprzez przygotowania do szkoleń innych osób - nie samych szkoleniach - (4 CPE/h), publikując artykuły (10 CPE/art) i książki (40 CPE/książkę).

CISM - Certified Information Security Manager dedykowany dla osób projektujących, oceniających i zarządzających systemami bezpieczeństwa w organizacjach. Osoby chcące otrzymać certyfikat, muszą zdać egzamin i wykazać się pięcioletnim doświadczeniem w branży security, w tym co najmniej trzema latami pracy przy zarządzaniu bezpieczeństwem informacji. Od kandydatów wymagane jest przestrzeganie zasad etyki wyznaczonych przez ISACA oraz ciągłe podnoszenie swoich kwalifikacji, dokumentowane punktami CPE - minimum 20 CPE rocznie i 120 CPE w ciągu trzech lat.

Egzamin CISM weryfikuje następujące obszary wiedzy:

- audyty systemów informacyjnych pod kątem spełnienia standardów i najlepszych praktyk,
- sposoby spełnienia wymagań stawianym IT przez organizacje,
- zarządzanie ryzykiem,
- zarządzanie bezpieczeństwem.

W czasie egzaminu można uzyskać maksymalnie 800 punktów, z czego do zdania wymagane jest 450.

GIAC - Global Information Assurance Certification jest programem szkoleń i certyfikatów. Jego celem jest potwierdzenie wiedzy i umiejętności z obszarów bezpieczeństwa komputerowego, bezpieczeństwa oprogramowania i informacji. Na program składa się wiele niezależnych certyfikatów z wąskich dziedzin bezpieczeństwa.

W odróżnieniu od innych certyfikatów związanych z bezpieczeństwem, wiedza potrzebna do uzyskania danego tytułu GIAC nie skupia się na wiedzy ogólnej z dziedziny security lecz na konkretnych aspektach technicznych i sposobach realizacji danych zagadnień. Certyfikaty GIAC można uzyskać w następujących obszarach wiedzy: audytu, detekcji intruzów, zarządzania incydentami, analizy śledczej, bezpieczeństwa systemów operacyjnych, bezpiecznego programowania.

Egzaminy GIAC trwają zazwyczaj około 3-5 godzin i zawierają 150-200 pytań w zależności od dziedziny. Aby je zdać należy zdobyć co najmniej 70% punktów. Certyfikaty ważne są przez cztery lata i w celu ich przedłużenia należy ponownie zdać egzamin. Po zdaniu egzaminu otrzymuje się srebrny certyfikat - GIAC Silver. Tytuł złoty można uzyskać przygotowując część praktyczną i opisując ją w publikacji. GIAC Gold otrzymuje się po pozytywnej recenzji przygotowanego dokumentu.

Jedne z najważniejszych certyfikatów GIAC to:

GCIA - GIAC Certified Intrusion Analyst - potwierdza umiejętności posiadacza w dziedzinie monitorowania bezpieczeństwa sieci. Osoba legitymująca się tym certyfikatem posiada dogłębną wiedzę z rozpoznawania niepożądanych działań w sieciach komputerowych, systemów detekcji intruzów, znajomości narzędzi służących do analizy ruchu sieciowego a także systemów IPS.

GCIH - GIAC Certified Incident Handler - obejmuje wiedzę i umiejętności niezbędne w reagowaniu na incydenty. Aby zdać egzamin GCIH należy poznać oraz zrozumieć techniki i narzędzia wykorzystywane do ataków na systemy informatyczne, sposoby zabezpieczania i reagowania na niepożądane zdarzenia, podejmowania działań i przeprowadzania dochodzeń pozdarzeniowych.

GCFA - GIAC Certified Forensics Analyst - jest certyfikatem obejmującym obszary wiedzy związanej z prowadzeniem analizy śledczej systemów informatycznych, zaawansowanych zagadnień z dziedziny reagowania na incydenty sieci i systemów komputerowych.

GSEC - GIAC Security Essentials Certification ukierunkowany jest na ogólną wiedzę bezpieczeństwa komputerowego, niezbędną przy wdrażaniu różnego rodzaju rozwiązań technicznych z dziedziny security.

Cały program GIAC zawiera o wiele więcej możliwości certyfikacyjnych. Oprócz zdania egzaminów, należy zaakceptować kodeks etyki określony przez GIAC. Posiadanie kilku - zazwyczaj dwóch lub trzech certyfikatów - świadczy o wysokiej klasy specjalistcie z wieloletnim doświadczeniem.

ISSA Polska

www.issa.org.pl