



CompTIA Cybersecurity Analyst (CySA+)



Zakres tematyczny

- Reagowanie na luki w zabezpieczeniach, obsługa i zarządzanie.
- Koncepcje; „Threat Intelligence” i „Threat Hunting”.
- Kluczowe koncepcje architektury systemów i sieci
- Usprawnianie procesów w operacjach bezpieczeństwa
- Wdrażanie metod skanowania podatności
- Wykonywanie analizy podatności
- Przekazywanie informacji o podatnościach.
- Wyjaśnienie działań związanych z reagowaniem na incydenty.
- Komunikacja w zakresie reagowania na incydenty.
- Narzędzia do identyfikacji złośliwej aktywności
- Analizowanie potencjalnie złośliwej aktywności.
- Ocena podatności aplikacji na zagrożenia.
- Ocena podatności aplikacji
- Najlepsze praktyki w zakresie bezpieczeństwa aplikacji i ograniczania ataków.
- Przygotowanie do egzaminu CompTIA Cybersecurity Analyst+ (egzamin CS0-003)