

Mapa certyfikacji CompTIA

i ścieżki kariery w cyberbezpieczeństwie

1. Gdzie jesteście: Security+ w ścieżce certyfikacji CompTIA

CompTIA buduje swoje certyfikaty jako spójną drabinę kompetencji — od fundamentów IT, przez pierwszy poziom specjalizacji w bezpieczeństwie (na którym dziś jesteście), aż po certyfikaty eksperckie. Poniższa tabela pokazuje tę drabinę wraz z aktualnymi (wrzesień 2026) oznaczeniami egzaminów.

Poziom	Certyfikat (aktualny egzamin)	Czego dotyczy
Fundamenty IT	CompTIA A+ (220-1201 / 220-1202)	Sprzęt komputerowy, systemy operacyjne, podstawy sieci i rozwiązywanie problemów. Zalecany punkt startowy dla osób bez wcześniejszego doświadczenia w IT.
Fundamenty sieci	CompTIA Network+ (N10-009)	Architektura i protokoły sieciowe, adresacja IP, urządzenia sieciowe, rozwiązywanie problemów z siecią.
TU JESTEŚ →	CompTIA Security+ (SY0-701)	Pierwszy poziom specjalizacji w cyberbezpieczeństwie: zagrożenia, kryptografia, architektura bezpieczeństwa, operacje bezpieczeństwa, zarządzanie i zgodność. Uznawany przez amerykański Departament Obrony jako spełniający wymóg bazowy (DoD 8140/8570).
Specjalizacja — obrona	CompTIA CySA+ (CS0-003)	Analiza zagrożeń, monitoring, wykrywanie i reagowanie na incydenty — pogłębienie tego, co ćwiczyliście w Dniu 2 tego szkolenia.
Specjalizacja — ofensywa	CompTIA PenTest+ (PT0-003)	Testy penetracyjne i etyczny hacking — systematyczne, praktyczne wykorzystanie technik ataku poznanych teoretycznie na tym szkoleniu.
Poziom ekspercki	CompTIA SecurityX, dawniej CASP+ (CAS-005)	Architektura bezpieczeństwa przedsiębiorstwa i zarządzanie ryzykiem na poziomie organizacyjnym — certyfikat praktyczny (performance-based), bez ograniczeń co do wymaganego doświadczenia formalnego, ale realnie adresowany do doświadczonych specjalistów.

Wymagania formalne: CompTIA nie stawia twardych, egzekwowanych warunków wstępnych do żadnego z powyższych egzaminów — każdy można podejść bez wcześniejszych certyfikatów. A+ i Network+ są jednak zalecane jako przygotowanie do Security+, a dla Security+ zalecane jest dodatkowo ok. 2 lata doświadczenia w administracji IT z naciskiem na bezpieczeństwo.

2. Ważne: nadchodząca zmiana wersji egzaminu — Security+ V8 (SY0-801)

CompTIA oficjalnie zapowiedziało premierę nowej wersji egzaminu Security+ — V8 (SY0-801) — na listopad 2026.

Nowa wersja rozszerza zakres o zagadnienia związane z ryzykami AI, operacjami bezpieczeństwa i nowoczesnymi środowiskami IT. Obecna wersja SY0-701, którą omawialiśmy na tym szkoleniu, pozostaje w sprzedaży i jest w pełni ważna — CompTIA planuje jej wycofanie dopiero w połowie 2027 r. (11 czerwca 2027 dla wersji angielskiej, 13 sierpnia 2027 dla pozostałych języków).

Praktyczna wskazówka: jeśli planujecie podejść do egzaminu w najbliższych tygodniach lub miesiącach, warto zdawać SY0-701 (materiał z tego szkolenia jest z nim w pełni zgodny). Jeśli egzamin planowany jest później niż na przełomie 2026/2027, warto na bieżąco sprawdzać ostateczną datę udostępnienia SY0-801 na stronie comp-tia.org i zaktualizować plan nauki.

3. Struktura egzaminu SY0-701 — przypomnienie

Maksymalnie 90 pytań (wybór jedno- i wielokrotny oraz zadania performance-based, czyli symulacje praktyczne), 90 minut, próg zdawalności 750 w skali 100–900. Egzamin obejmuje pięć domen wiedzy o różnej wadze — dokładnie tych, na których zbudowany był program obu dni tego szkolenia.

Domena	Waga	Zakres (jak na szkoleniu)
1. General Security Concepts	12%	Triada CIA, rodzaje kontroli, zarządzanie zmianą, podstawy kryptografii — Dzień 1, Bloki 1–2.
2. Threats, Vulnerabilities & Mitigations	22%	Aktorzy zagrożeń, malware, ataki sieciowe i aplikacyjne, zarządzanie podatnościami — Dzień 1, Bloki 1, 3, 4, 6.
3. Security Architecture	18%	Architektura sieci, Zero Trust, segmentacja, bezpieczeństwo chmury — Dzień 1 Blok 5 i Dzień 2 (IAM).
4. Security Operations	28% (największa domena)	Monitoring, SIEM, reagowanie na incydenty, hardening, IAM — główny temat Dnia 2.
5. Security Program Management & Oversight	20%	Zarządzanie ryzykiem, zgodność regulacyjna (NIS2/UoKSC/CRA), audyt, BCP/DR — Dzień 2, Bloki 12–13.

Orientacyjny koszt egzaminu (voucher CompTIA, cena producenta, stan na 2026 r.): ok. 439 USD — cena może się różnić w zależności od regionu, promocji i pakietu (np. z materiałami CertMaster). Aktualną cenę i dostępność w PLN warto zawsze zweryfikować bezpośrednio na comptia.org lub u autoryzowanego dostawcy voucherów.

4. Ścieżki kariery w cyberbezpieczeństwie

Security+ to wspólny fundament dla kilku dobrze zdefiniowanych kierunków rozwoju zawodowego. Poniżej pięć ścieżek, do których nawiązywaliśmy w trakcie obu dni szkolenia.

Ścieżka kariery	Na czym polega (nawiązanie do szkolenia)	Naturalny kolejny krok
Analitik SOC (Tier 1 → Tier 2 → Tier 3)	Ścieżka operacyjna — dokładnie ta, którą ćwiczyliście w Dniu 2: monitoring, detekcja, coraz bardziej samodzielna analiza i reagowanie na kolejnych poziomach doświadczenia.	Naturalny kolejny certyfikat: CompTIA CySA+ (CS0-003).
Specjalista ds. bezpieczeństwa aplikacji (AppSec)	Pogłębienie Bloku 4 z Dnia 1: OWASP Top 10, testowanie bezpieczeństwa aplikacji (SAST/DAST/SCA), współpraca z zespołami deweloperskimi nad DevSecOps.	Typowa dalsza specjalizacja: certyfikaty branżowe AppSec/DevSecOps (poza portfolio CompTIA) lub CySA+ jako baza analityczna.
Inżynier / Architekt bezpieczeństwa sieci	Pogłębienie Bloków 3 i 5 z Dnia 1: projektowanie segmentacji sieci, zapory nowej generacji, architektura Zero Trust.	Naturalny kolejny certyfikat: CompTIA SecurityX (CAS-005) po zdobyciu doświadczenia.
Specjalista GRC (Governance, Risk, Compliance)	Pomost między techniką a Blokiem 13 z Dnia 2: zarządzanie zgodnością z NIS2/UoKSC/CRA, audyty, polityki bezpieczeństwa.	Uzupełniające certyfikaty branżowe: ISO/IEC 27001 (Audyt Wewnętrzny), CompTIA SecurityX na poziomie zarządczym.
Pentester / Red Teamer	Ścieżka ofensywna, naturalnie prowadząca do PenTest+ — systematyczne testowanie bezpieczeństwa z perspektywy atakującego, budowane na technikach ataku z Dnia 1.	Naturalny kolejny certyfikat: CompTIA PenTest+ (PT0-003).

5. Co dalej: jak przygotować się do egzaminu

- To szkolenie to solidny fundament teoretyczny i praktyczny (12 laboratoriów CertMaster Labs) — droga do zdania egzaminu wymaga jeszcze systematycznego powtórzenia materiału.
- Materiały otrzymane w ramach szkolenia: prezentacje slajdów z obu dni, arkusz ćwiczeń (Gap Analysis, rejestr ryzyk, wzór procedury IR), niniejsza mapa certyfikacji oraz lista zasobów do dalszej nauki.
- Część pytań na egzaminie to zadania performance-based — nie tylko wybór odpowiedzi, ale symulacje praktyczne. Dlatego 12 laboratoriów w tym szkoleniu miało znaczenie wykraczające poza samą teorię — warto wracać do platformy CertMaster Labs w ramach powtórek.
- Realistyczny harmonogram: większość zdających poświęca dodatkowo 4–8 tygodni samodzielnej nauki po szkoleniu tego typu, zanim podejdzie do egzaminu.
- Dalsza nauka — zasoby zewnętrzne: CERT Polska, publikacje NIST (seria SP 800), ENISA, polskie portale branżowe (np. sekurak.pl) — pełna, opisana lista znajduje się w osobnym dokumencie „Lista zasobów do dalszej nauki”.

Fakty dotyczące certyfikatów CompTIA (kody egzaminów, ceny, daty premier) zweryfikowano na podstawie comptia.org, stan na wrzesień 2026. Przed zapisem na egzamin zalecamy sprawdzenie aktualnych informacji bezpośrednio na comptia.org.