# CompTIA Security+

**Cursusduur: 5 Dagen  Cursuscode: G013  Version: SY0-701  Trainingsmethode: Virtual Learning**

## Beschrijving:

De CompTIA Security+ cursus is ontworpen om u te helpen zich voor te bereiden op het SY0-701 examen. Het CompTIA Security+-examen certificeert dat de succesvolle kandidaat over de kennis en vaardigheden beschikt die nodig zijn om systemen te installeren en te configureren om applicaties, netwerken en apparaten te beveiligen; dreigingsanalyse uit te voeren en te reageren met passende mitigatietechnieken; deel te nemen aan risicobeperkende activiteiten; en werken met een bewustzijn van het toepasselijke beleid, wetten en voorschriften.

Virtueel en Klassikaal™

Virtueel en Klassikaal™ is een eenvoudig leerconcept en biedt een flexibele oplossing voor het volgen van een klassikale training. Met Virtueel en Klassikaal™ kunt u zelf beslissen of u een klassikale training virtueel (vanuit huis of kantoor )of fysiek op locatie wilt volgen. De keuze is aan u! Cursisten die virtueel deelnemen aan de training ontvangen voor aanvang van de training alle benodigde informatie om de training te kunnen volgen.

## Doelgroep:

**CompTIA Security+ is gericht op IT-professionals met functies zoals:**BeveiligingsbeheerderBeveiliging

## Doelstelling:

- **Aan het einde van de cursus zou u in staat moeten zijn om de volgende doelstellingen te bereiken:**
- Beoordeel de beveiligingsstatus van een bedrijfsomgeving en beveel passende beveiligingsoplossingen aan en implementeer deze.
- Bewaak en beveilig hybride omgevingen, waaronder cloud, mobiel, Internet of Things (IoT) en operationele technologie.
- Werk met een bewustzijn van de toepasselijke regelgeving en beleidsregels, waaronder principes van governance, risico en naleving.
- Identificeer, analyseer en reageer op beveiligingsgebeurtenissen en -incidenten.

## Vereiste kennis en vaardigheden:

- G005 - CompTIA Network+

## Examens en certificering

CompTIA Security+ is de eerste cyberbeveiligingscertificering die een kandidaat aan het begin van zijn carrière moet behalen. Het voorziet cyberbeveiligingsprofessionals van de fundamentele beveiligingsvaardigheden die nodig zijn om netwerken te beveiligen, bedreigingen te detecteren en gegevens te beveiligen door middel van prestatiegerichte vragen, waardoor ze de deur kunnen openen naar een carrière op het gebied van cyberbeveiliging en een betrouwbare verdediger van digitale omgevingen kunnen worden.

- **Vereist examen:** SY0-701
- **Aantal vragen**: Maximaal 90
- **Soorten vragen:** Meerkeuzevragen en op basis van prestaties
- **Duur van de test:** 90 minuten
- **Aanbevolen ervaring:** Minimaal 2 jaar ervaring in IT-beheer met een focus op security, hands-on ervaring met technische

## Vervolgcursussen:

- GK5867 - CompTIA CySA+ Cybersecurity Analyst
- G015 - CompTIA PenTest+ Certification Prep Course
- GK2951 - CompTIA SecurityX Certification Prep Course

## Cursusinhoud:

Algemene beveiligingsconcepten 12%

- Vergelijk en contrasteer verschillende soorten beveiligingscontroles.
- Vat fundamentele beveiligingsconcepten samen.
- Leg het belang van veranderingsbeheerprocessen en de impact op de beveiliging uit.
- Leg uit hoe belangrijk het is om de juiste cryptografische oplossingen te gebruiken.

Bedreigingen, kwetsbaarheden en mitigaties 22%

- Vergelijk en contrasteer veelvoorkomende bedreigingsactoren en motivaties.
- Leg veelvoorkomende bedreigingsvectoren en aanvalsoppervlakken uit.
- Leg verschillende soorten kwetsbaarheden uit.
- Analyseer, op basis van een scenario, indicatoren van kwaadaardige activiteiten.
- Leg uit wat het doel is van de mitigatietechnieken die worden gebruikt om de onderneming te beveiligen.

Beveiligingsarchitectuur 18%

- Vergelijk en contrasteer de beveiligingsimplicaties van verschillende architectuurmodellen.
- Op basis van een scenario past u beveiligingsprincipes toe om de bedrijfsinfrastructuur te beveiligen.
- Vergelijk en contrasteer concepten en strategieën om gegevens te beschermen.
- Leg het belang uit van veerkracht en herstel in de beveiligingsarchitectuur.

Beveiligingsactiviteiten 28%

- Op basis van een scenario past u algemene beveiligingstechnieken toe op computerbronnen.
- Leg uit wat de beveiligingsimplicaties zijn van het juiste beheer van hardware, software en gegevensactiva.
- Leg verschillende activiteiten uit die verband houden met kwetsbaarheidsbeheer.
- Leg concepten en tools voor beveiligingswaarschuwingen en -bewaking uit.
- Wijzig op basis van een scenario de Enterprise-mogelijkheden om de beveiliging te verbeteren.
- Op basis van een scenario implementeert en onderhoudt u identiteits- en toegangsbeheer.
- Leg het belang uit van automatisering en orkestratie met betrekking tot veilige operaties.
- Leg de juiste activiteiten voor incidentrespons uit.
- Gebruik op basis van een scenario gegevensbronnen om een onderzoek te ondersteunen.

Beheer en toezicht op beveiligingsprogramma's 20%

- Vat elementen van effectief beveiligingsbeheer samen.
- Leg elementen van het risicobeheerproces uit.
- Leg de processen uit die verband houden met risicobeoordeling en -beheer door derden.
- Vat elementen van effectieve beveiligingsnaleving samen.
- Leg de soorten en doelen van audits en beoordelingen uit.
- Op basis van een scenario implementeert u beveiligingsbewustzijnspraktijken.

## Extra informatie:

Geaccrediteerd door ANSI om aan te tonen dat wordt voldaan aan de ISO 17024-norm.

## Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk  030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein