Dipl. ICT Security Engineer SIW

Studieninhalte im Überblick

Die ersten zwei Semester bilden das gemeinsame Basisjahr mit dem Abschluss ICT Assistant KIS. Im dritten Semester vertiefst du dein Wissen gezielt in der gewählten Spezialisierung.

Gemeinsame Basis – Semester 1 und 2

Kompetenzbereich	Themenbereich	Kurz erklärt
IT & Infrastruktur	Hardware, Endgeräte & IT-Grundlagen	Hardware und mobile Endgeräte verstehen, Komponenten austauschen sowie Geräte fachgerecht einrichten und warten.
IT & Infrastruktur	Netzwerke & Konnektivität	Verstehen, wie Netzwerke funktionieren, Router, Switches und WLAN kennenlernen und kleine Netzwerke selbst konfigurieren.
IT & Infrastruktur	Virtualisierung, Cloud & Betriebssysteme	Virtuelle Maschinen und Cloud-Modelle verstehen sowie Windows, macOS und Linux installieren und grundlegend bedienen.
IT & Infrastruktur	Troubleshooting & IT-Support	Hardware-, Netzwerk- und Softwareprobleme systematisch erkennen, analysieren und beheben.
Cyber Security	IT-Sicherheit & Schutzmassnahmen	Geräte, Netzwerke und Daten vor Malware, Angriffen und unbefugtem Zugriff schützen.
Projekt & Prozesse	IT-Betrieb, Standards & Arbeitsprozesse	Mit Dokumentationen, Tickets, Backups, Remote-Support und Change-Prozessen professionell im IT-Betrieb arbeiten.
Projekt & Prozesse	Grundlagen des Projektmanagements	IT-Projekte planen, organisieren und mit klassischen sowie agilen Methoden umsetzen.
Kommunikation & Karriere	Kommunikation, Präsentation & Berufseinstieg	Professionell kommunizieren und präsentieren sowie sich gezielt auf Bewerbungen und den IT-Berufseinstieg vorbereiten.
Lernen & Transfer	Lernmethodik, CompTIA & Studienstart	Effektiv lernen, den Studienaufbau verstehen und sich mit CompTIA CertMaster freiwillig auf A+ Zertifikate vorbereiten.

Semester 3: deine Spezialisierung

Nach dem gemeinsamen Basisjahr vertiefst du dein Wissen gezielt in deiner gewählten Fachrichtung.

Spezialisierung ICT Security Engineer

Schwerpunkt: IT-Systeme schützen, Bedrohungen erkennen, Sicherheitsvorfälle bewältigen und IT-Sicherheit professionell steuern.

Kompetenzbereich	Themenbereich	Kurz erklärt
Cyber Security	**Sicherheitsgrundlagen, Bedrohungen & Schwachstellen**	Zentrale Sicherheitskonzepte verstehen, Bedrohungen und Schwachstellen erkennen und passende Schutzmassnahmen ableiten.
Cyber Security	**Sicherheitskonzepte & Schutz von IT-Systemen**	IT-Infrastrukturen sicher planen und mit Firewalls, VPN, Netzwerksegmentierung, Datenschutz und Recovery-Konzepten schützen.
Cyber Security	**Überwachung & Betrieb der IT-Sicherheit**	Systeme absichern, Sicherheitswarnungen überwachen, Schwachstellen verwalten und professionell auf Sicherheitsvorfälle reagieren.
Management & Steuerung	**Sicherheitsmanagement & Kontrolle**	Sicherheitsrichtlinien, Risiken, Compliance und Audits verstehen und IT-Sicherheit auch organisatorisch steuern.
Praxis & Abschluss	**Diplomprüfung & Transfer**	Den Studiengang mit der Diplomprüfung zum Dipl. ICT Security Engineer SIW abschliessen.