

IT-Sicherheit Microsoft



Zeitnahe, bundesweite Starttermine

GFN-Erfolgsgarantie²> 95 % Integrationsquote³

Unser modulares Kurssystem bietet dir unzählige Möglichkeiten, dich weiterzubilden – und zwar ganz nach deinem Bedarf. Gerne helfen dir unsere Berater:innen bei der Auswahl und Kombination geeigneter Kurse. Wir nehmen uns Zeit für dich und schauen, welche Weiterbildung zu dir und deinen Zielen passt. Den Bedarf des Arbeitsmarkts haben wir dabei immer mit im Blick. Gemeinsam stellen wir deinen persönlichen Lehrplan mit zeitnahem Einstiegstermin zusammen – und du startest schnell und unkompliziert in deine Wunsch-Weiterbildung.

Dauer

mehr als 1 Monat bis 3 Monate

Kursinhalt

Inhalte auf einen Blick: IT-Sicherheit, Microsoft-Technologien, Datenschutz, Cloud-Computing, Netzwerksicherheit

Die Weiterbildung IT-Sicherheit Microsoft vermittelt umfassende Kenntnisse in der Absicherung von Microsoft-Systemen und -Netzwerken. Teilnehmer lernen, wie sie Microsoft-Technologien effektiv schützen und Sicherheitslücken identifizieren, um Bedrohungen zu minimieren. Der Kurs bietet praxisnahe Übungen zur Implementierung von Sicherheitsmaßnahmen in Microsoft-Umgebungen und fördert das Verständnis für die Integration von Microsoft-Sicherheitslösungen. Absolventen können in Berufsfeldern wie IT-Administration, Netzwerkmanagement und IT-Sicherheit tätig werden, wo sie ihre Microsoft-Kompetenzen anwenden. Durch den Fokus auf Microsoft-Produkte werden die Teilnehmer befähigt, in verschiedenen Branchen die IT-Sicherheit zu optimieren und Microsoft-Systeme zu verwalten.

IT – Sicherheit und Datenschutz

Informationssicherheit

- › Unterscheidung von Datensicherheit und Datenschutz
- › Schutzziele der Sicherheit in der IT
- › Risikolage für Unternehmen und Sicherheit
- › Rechtliche Aspekte, Urheberrechte



Wir bilden Menschen in ganz Deutschland weiter.
Alle Standorte findest Du auf gfn.de/standorte



Datenschutzgrundverordnung (DSGVO)

- › Betroffenenrechte
- › Rechtmäßigkeit der Verarbeitung
- › Auftragsverarbeitung

BSI und Datengrundschutz

- › Risikomanagement
- › Gefährdungskatalog
- › Schutzbedarfsfeststellung
- › IT-Risikoanalyse zur Sicherheit

Angriffsvorbereitung

- › Hacker und Cracker, staatliche Hacker, elektronische Kriegsführung
- › Angriffe auf Dienste und Protokolle als Bedrohung von Sicherheit
- › Mitarbeiter als Problem für die Sicherheit
- › Viren und ihre Verbreitung

Technisch-organisatorische Maßnahmen: Kryptographie

- › Grundlagen, Verschlüsselungsziele für Sicherheit
- › Symmetrische und asymmetrische Verschlüsselung
- › Kryptographische Protokolle und ihre Anwendungen
- › Sicherheit von Kennwörtern
- › Sichere E-Mail-Verfahren

Technisch-organisatorische Maßnahmen: Datensicherung

- › Datensicherungskonzept
- › Datenträgerauswahl
- › Löschkonzept

Technisch-organisatorische Maßnahmen der Sicherheit: Firewalls

- › Paketfilter, Stateful Packet Inspection, Proxies, Next Generation Firewall
- › Firewall-Konzepte für Sicherheit
- › Intrusion Detection, Intrusion Prevention

Technisch-organisatorische Maßnahmen: VPN

Wir bilden Menschen in ganz Deutschland weiter.
Alle Standorte findest Du auf gfn.de/standorte



- › Topologien von VPNs
- › VPN-Verfahren
- › Schlüsselaustauschmethoden/Protokolle
- › AAA-Dienste

Sicherheit WLAN

- › Komponenten und Standards
- › Sicherheitsrisiken
- › Sicherheitsmechanismen

IT-Sicherheit in der Industrie 4.0

- › IoT, IIoT
- › Risikoanalyse, Netzsegmentierung, Nutzung sicherer Protokolle für mehr Sicherheit

Schwachstellenanalyse, Monitoring

- › Maßnahmen zur Störungsvermeidung
- › Rechtliche Grundlagen zur Sicherheit
- › Pentesting
- › Netzwerk- und Vulnerabilityscanner

Sicherheit in der Cloud

- › Cloudcomputing
- › Sicherheitsmaßnahmen
- › Bereitstellungsmodelle

Einführung in Cloud-Computing und das Microsoft-Produktportfolio**Einführung in die Cybersicherheit und die Kursinhalte**

- › Einführung in die Cybersicherheit
- › Bedrohungen und Angriffsarten
- › Compliancevorgaben und Sicherheitsstandards

Cloudservices und Sicherheitskonzepte

Wir bilden Menschen in ganz Deutschland weiter.
Alle Standorte findest Du auf gfn.de/standorte



- › Verantwortlichkeiten in der Cloud
- › Moderne Sicherheits- und Compliance-Ansätze
- › Verschlüsselung

Authentifizierung, Autorisierung und Identitätsdienste

- › Grundlagen des logischen Zugriffsschutzes und moderne Identitätskonzepte
- › Zugriffe für Organisationen verwalten

Einstieg in Microsoft Entra

- › Grundlagen von Microsoft Entra ID
- › Identitätstypen in Microsoft Entra ID

Authentifizierungsmethoden und Zugriffsschutz in Microsoft Entra

- › Authentifizierungsmethoden
- › Einstieg in Berechtigungskonzepte
- › Zugriffsverwaltungsoptionen mit Microsoft Entra ID
- › Rollenbasierte Zugriffsverwaltung in Microsoft Entra ID

Microsoft Entra Governancefunktionen und Identitätsschutz

- › Der Lebenszyklus von Berechtigungen und deren Verwaltung
- › Privilegierte Rechte
- › Identitätsrisiken erkennen, beseitigen und untersuchen

KI und Microsoft Security Copilot

- › IT-Sicherheit mittels KI-Unterstützung
- › Microsoft Copilot Integration

Azure-Sicherheitsinfrastruktur

- › Sicherheitsdienste und -funktionen für die Kerninfrastruktur in Azure

Azure-Sicherheitsverwaltungsfunktionen

- › Microsoft Defender for Cloud
- › Microsoft Sentinel

Bedrohungsschutz durch Microsoft Defender XDR

Wir bilden Menschen in ganz Deutschland weiter.
Alle Standorte findest Du auf gfn.de/standorte



- › Einstieg in Microsoft Defender XDR
- › Sicherheitsrisikomanagement mit Microsoft Defender XDR

Informationsschutz und Data-Compliance

- › Datenschutzlösung Microsoft Priva
- › Einführung in Microsoft Purview und dessen Datensicherheitslösungen
- › Data Compliance und Microsoft Purview-Datenkonformitätslösungen
- › Compliance nachweisen
- › Prüfungsvorbereitung und Zertifizierung

Microsoft Zertifikat – Experte für Microsoft 365 inkl. Microsoft Zertifikat Teams Administrator**Überblick zu Microsoft Teams und zum Microsoft Zertifikat**

- › Sicherheit und Compliance in Microsoft Teams
- › Verwaltung von Microsoft Teams

Implementierung von Governance, Sicherheit und Compliance für Microsoft Teams als Kernbestandteil des Microsoft Zertifikats

- › Planung und Konfiguration von Governance für Office-365-Gruppen einschließlich Ablauf- und Namensgebungsrichtlinien
- › Implementierung von Sicherheit: Konfiguration von bedingtem Zugriff, MFA oder Bedrohungsverwaltung
- › Implementierung von Compliance mithilfe von DLP-Richtlinien, eDiscovery-Fällen oder Supervisionsrichtlinien

Vorbereitung der Umgebung für eine Microsoft-Teams-Bereitstellung – Bestandteil Microsoft Zertifikat

- › Upgrade von Skype for Business auf Microsoft Teams
- › Planung und Konfiguration von Netzwerkeinstellungen für Microsoft Teams
- › Bereitstellung und Verwaltung von Microsoft-Teams-Endpunkten

Bereitstellung und Verwaltung von Microsoft Teams

- › Erstellen und Verwalten von Teams
- › Verwalten der Mitgliedschaft
- › Verwalten des Zugriffs für externe Benutzer



Wir bilden Menschen in ganz Deutschland weiter.
Alle Standorte findest Du auf gfn.de/standorte



Verwaltung der Zusammenarbeit in Microsoft Teams

- › Verwaltung der Kommunikation in Microsoft Teams
- › Verwalten von Live-Events und Besprechungen
- › Verwalten von Telefonnummern
- › Verwalten des Telefonsystems für Microsoft Teams
- › Troubleshooting von Audio-, Video- und Clientproblemen
- › Prüfungsvorbereitung und Prüfung Microsoft Zertifikat MS-700 – Abschluss als Experte für Microsoft 365 inkl. Microsoft Zertifikat Teams Administrator

Die Weiterbildung bietet eine fundierte Grundlage für den Einstieg in die IT-Sicherheit. Teilnehmer erlangen wertvolle Kenntnisse zur Absicherung von Microsoft-Systemen.

Voraussetzungen

- › Fortgeschrittenes Sprachniveau Deutsch
- › Gute PC-Kenntnisse
- › Erfahrung mit Microsoft-365-Diensten und -Konzepten
- › Erste IT-Kenntnisse im Hardware-, Netzwerk- und Serverbereich sowie Grundlagen der Virtualisierung
- › Teilnahme an einem unverbindlichen Beratungsgespräch

Zielgruppe

- › IT-interessierte Arbeitssuchende mit Vorwissen, die in der IT-Administration arbeiten möchten
- › Arbeitssuchende, die Know-how in IT-Sicherheit, Compliance und Cloud-Technologien aufbauen möchten
- › IT-Administrator:innen und -Fachkräfte, die ihre Kenntnisse aktualisieren und zertifizieren möchten
- › Quer- und Wiedereinsteigende, sich rehabilitierende Personen sowie Hochschulabgänger:innen mit oder ohne Abschluss, die eine Zusatzqualifikation für ihren beruflichen (Wieder-)Einstieg erwerben möchten

Abschluss

Trägerinternes GFN-Zertifikat, international anerkanntes Microsoft-Zertifikat: Microsoft Certified: Security,



Wir bilden Menschen in ganz Deutschland weiter.
Alle Standorte findest Du auf gfn.de/standorte



Compliance and Identity Fundamentals (SC-900), Microsoft 365 Certified: Teams Administrator Associate (MS-700)



Wir bilden Menschen in ganz Deutschland weiter.
Alle Standorte findest Du auf gfn.de/standorte

