

Durch die anhaltende Digitalisierung der Geschäftsprozesse werden die IT-Infrastrukturen zunehmend Business-kritischer und die Anforderungen bezüglich Verfügbarkeit, Performanz, Skalierbarkeit, Agilität und Sicherheit steigen deutlich an. Die Anbieter haben darauf reagiert und viele neue Innovationen auf den Markt gebracht, wobei den Software-defined Networks (SDN) die größten Zukunftschancen vorhergesagt werden. Der Marktführer Cisco treibt diese Entwicklung maßgeblich voran und hat mit Software-defined Access (SDA) eine Lösung entwickelt, die neue Maßstäbe setzt und eine Abkehr von klassischen Infrastrukturen bedeutet. Dieses Training beleuchtet diese Veränderungen aus Sicht eines Account Managers und zeigt Wege auf, wie man die neuen Lösungen beim Kunden platzieren kann. Die Teilnehmer erarbeiten sich Argumente, Tools, Strategien und Techniken, die sie später im Vertriebsalltag gewinnbringend einsetzen können, ganz nach der Erkenntnis des Neurobiologen Gerhard Roth: „Wissen kann nicht übertragen werden; es muss im Gehirn eines jeden Lernenden neu geschaffen werden.“

Kursinhalt

- IT-Vertrieb 4.0
- Verständnis für Enterprise Networks: LAN, WAN, WLAN und Security
- Aufbau von Cisco Enterprise-Infrastrukturen
- Marktveränderungen, Marktüberblick und Herstellerlösungen
- Bedeutung von Enterprise Networks für Unternehmen – Business Needs
- Stand der Technik bei Software-defined Networks (SDN)
- Cisco Digital Network Architecture (Cisco DNA)
- Cisco Software-defined Access (SDA)
- Klassisches Cisco LAN-, WAN-, WLAN- und Security-Produktportfolio sowie dessen Positionierung
- Cisco Meraki-Produktpalette sowie deren Positionierung
- Erarbeiten einer Kundennutzenargumentation - Gruppenarbeit
- Wie positioniere ich das Thema beim Kunden und welche Möglichkeiten des Up and Cross Sellings bestehen?
- Welche Lösungen passen auf welchen Kunden und warum - USPs?
- Argumentation im Wettbewerb

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket von ExperTeach – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

Zielgruppe

Das Training richtet sich an Account Manager, welche Cisco IT-Infrastrukturen erfolgreich verkaufen möchten und neben dem vertrieblichen auch ein technisches Interesse mitbringen. Wer darüber hinaus seine Kunden beraten möchte wie Enterprise Networks optimiert werden können und wie sich die Cisco IT-Infrastrukturen von den Lösungen der Marktbegleiter unterscheiden, wird optimalen Nutzen ziehen. Auch als Refresher ist dieses Seminar bestens geeignet.

Voraussetzungen

Besondere Vorkenntnisse werden für einen erfolgreichen Kursbesuch nicht benötigt. Wichtig sind Interesse an der Thematik und die Bereitschaft zur vertrieblichen und technischen Auseinandersetzung mit den Inhalten.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/360B

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in Österreich	3 Tage € 1.995,-
Online Training	3 Tage € 1.995,-
Termine auf Anfrage	

Stand 07.05.2024



Inhaltsverzeichnis

Cisco Enterprise Networks – 360° Selling Experts

1 Motivation und SD-LAN Grundlagen	4 Typische SD-WAN Use Cases und Limitierungen	6.6 Cisco Umbrella SIG – Vertriebsargumente
1.1 LAN-Topologie	4.1 SD-WAN für spezielle Anwendungsfälle	7 Cisco Netzwerk Security Portfolio
1.2 Typische LAN-Designs	4.1.1 SD-WAN für Office 365	7.1 Cisco Netzwerk Security Portfolio
1.3 Herausforderungen bei klassischen LANs	4.1.2 SD-WAN für Voice und Video	7.1.1 Cisco Firepower Appliances
1.4 SDN im LAN	4.2 SD-WAN in Multi-Cloud-Lösungen	7.1.2 Cisco Identity Services Engine für LAN und WLAN
1.5 SD-LAN-Arbeitsweise	4.2.1 Anbindung von Lokationen	7.1.3 Cisco Email Security Appliance (ESA)
1.6 Rolle des Controllers	4.2.2 Anbindung Azure	7.1.4 Cisco Web Security Appliance – WSA
1.7 Underlay und Overlay	4.2.3 Anbindung AWS	7.1.5 Cisco VPN und Cisco AnyConnect Secure Mobility Client
1.8 Security-Konzepte	4.2.4 Anbindung Google Cloud	7.1.6 Cisco pxGrid
1.9 Kundennutzen	4.3 Automatisierungsmöglichkeiten und Self Service	7.1.7 Talos
1.10 Moderne Sales Pitches für das LAN	4.4 WAN-Optimierung	7.2 Secure Network Analytics
2 Cisco SD-LAN	4.5 Grenzen des SD-WANs	7.2.1 Cisco Secure Network Analytics
2.1 Enterprise LAN- und WAN-Markt im Überblick	4.6 Wann spart SD-WAN Geld?	7.2.2 Stealthwatch Endpoint Visibility
2.2 Marktüberblick: WLAN	4.7 Gegenüberstellung klassisches WAN versus SD-WAN	7.2.3 Cisco Endpoint Security Analytics (CESA)
2.3 Marktüberblick: SD-WAN	4.8 Cisco Meraki SD-WAN	7.3 Cisco Advanced Malware Protection – AMP
2.4 Cisco Classic-Architekturen	4.9 Cisco SD-WAN (Viptela)	7.3.1 Funktionsweise AMP
2.4.1 Cisco Digital Network Architecture (DNA)	4.9.1 Cisco SD-WAN: Bestandteile	7.3.2 Cisco Secure Malware Analytics
2.4.2 Cisco Enterprise LAN im Überblick	4.9.2 Cisco SD-WAN: Fabric	7.3.3 Cisco Secure Endpoint ehemals AMP for Endpoints
2.4.3 Herausforderungen bei klassischen LANs	5 Markt und SASE-Grundlagen	7.4 Cisco SecureX
2.4.4 Cisco SD Access	5.1 Marktüberblick	7.5 Vertriebsgangang Cisco Security
2.4.5 Cisco ISE OnPrem versus Cloud-based	5.2 Triebfedern für SASE	7.5.1 Warum Cisco?
2.4.6 TrustSec im Überblick	5.3 Was ist SASE?	8 Cisco Manufacturing & IoT
2.4.7 Makro- und Mikrosegmentierung	5.3.1 Ziele von SASE	8.1 Einstieg in das Thema IoT
2.4.8 Zero Trust Network	5.3.2 Definition SASE	8.2 Cisco Lösungsbausteine
2.4.9 Cisco DNA Center	5.4 SASE Bestandteile	8.2.1 Sensoren und Endpoints
2.4.10 Typische Use Cases	5.4.1 Zero Trust Network	8.2.2 IoT System Network Connectivity
2.4.11 Stärken Cisco Classic und Zielgruppen	5.4.2 Secure Web Gateway (SWG)	8.2.3 Fog Computing
2.4.12 Typische LAN-Architekturen	5.4.3 Aufgaben von Next Generation Firewalls	8.2.4 Applications
2.5 Use Cases für den Einsatz von SD Access	5.4.4 Cloud Access Security Broker (CASB)	8.3 Nutzenargumentation Cisco IoT
2.6 Cisco Meraki	5.4.5 Weitergehende Leistungsmerkmale	8.4 Typische Einsatzszenarien im Überblick
2.6.1 Portfolio	5.4.6 Advanced Persistent Threats (APT)	8.5 Sicherheit in Fabrikationsumgebungen
2.6.2 Typische Use Cases	5.5 SASE Möglichkeiten und Grenzen	8.5.1 Neue Risiken und Herausforderungen
2.6.3 Typische LAN-Architekturen	5.6 Anbieterlandschaft	8.5.2 Design und Architektur von industriellen Sicherheitslösungen
2.6.4 Stärken Cisco Meraki sowie Zielgruppen	5.6.1 Netzerkanbieter	8.6 Verschmelzung von IT und OT Security
2.7 Einsatzgebiete Cisco Classic versus Cisco Meraki	5.6.2 Security-Anbieter	8.7 Cisco IoT Security
2.8 Gegenüberstellung OnPrem-Controller vs. Cloud-controlled	5.6.3 Cloud-native Security-Anbieter	8.7.1 Cisco Cyber Vision
2.9 Edge Computing in Industrieumgebungen	5.7 SASE Architekturen und Use Cases	8.7.2 ISA3000 Industrial Security Appliance
2.9.1 Auswirkungen auf das LAN	5.8 SASE-Kriterien für die Anbieterswahl	8.7.3 SecureX Threat Response
2.9.2 Local Survivability – Ausfallsicherheit	5.9 Einfluss der SASE-Lösung auf das WAN-Design	8.7.4 Security-Architektur für Produktionsumgebungen
2.9.3 Architekturen für Edge Computing	6 Cisco Security: Einstieg über Cisco Umbrella SIG	8.7.5 Security-Architektur für Kraftwerke
2.10 Moderne LAN-Architekturen: Status und Zukunft	6.1 Cisco Umbrella SIG: SASE-Lösung von Cisco	8.7.6 Integration in Cisco und Third-Party-Lösungen
2.11 LAN als Trigger für das Thema Data Center	6.2 Zero Trust Networks (ZTN)	8.7.7 Stakeholder für die Sicherheit in Fabrikumgebungen
3 Moderne WAN-Architekturen: SD-WAN	6.3 Cisco Umbrella Secure Internet Gateway (SIG)	8.8 Vertriebsgangang Manufacturing & IoT
3.1 Mögliche neue Kundenanforderungen	6.4 Bestandteile von Cisco Umbrella SIG	9 Das Big Picture: Die Cisco Architektur im Überblick
3.1.1 Steigender Backhaul-Verkehr durch Cloud-Architekturen	6.4.1 DNS-Layer Security	9.1 Die Bestandteile
3.1.2 Bedarf an dezentralen Security-Lösungen	6.4.2 Umbrella Cloud-Delivered Firewall	9.1.1 IT Architekturen mit Cisco Meraki
3.2 SD-WAN: Arbeitsweise	6.4.3 Secure Web Gateway	9.1.2 IT Architekturen mit Cisco Classic
3.3 SD-WAN: Kundennutzen	6.4.4 Cisco Umbrella Remote Browser Isolation	9.2 Die Vorteile der Homogenität
3.4 SD-WAN-Konzept: Underlay und Overlay	6.4.5 Cisco Secure Malware Analytics (Threat Grid) Sandboxing	9.3 Wie zahlen moderne Entwicklungen auf den homogenen Ansatz ein?
3.5 Direct Internet Access (DIA)	6.4.6 Cisco CASB – CloudLock und Umbrella	9.3.1 SDN
3.6 Aufbau von SD-WAN-Lösungen	6.4.7 Cisco Duo	9.3.2 Automation und ML/KI
3.7 Zusatzfunktionen von SD-WAN-Lösungen	6.5 Weitere Veredelungen von Cisco Umbrella SIG	9.3.3 Einfachheit
3.8 Rolle klassischer WANs: Underlay-Funktion	6.5.1 Cisco Meraki Systems Manager	9.4 Cross Selling-Potenzial
3.9 Security-Konzepte bei SD-WAN	6.5.2 Cisco AnyConnect Secure Mobility Client	9.5 Zusammenfassung und Feedback
3.9.1 Lokale SD-WAN-Security	6.5.3 Cisco Secure Endpoint	
3.9.2 Secure Access Service Edge (SASE)	6.5.4 SecureX	
3.10 Security-Architekturen für Hybride-Lösungen	6.5.5 ThousandEyes	
3.11 Kommerzielle Betrachtung		

