Cyber Security und die Cisco Security Story

Sales Pitches für Account Manager

Das Thema Security wird zusehends wichtiger, stellt die IT-Infrastruktur in Zeiten der Digitalisierung und Automatisierung ein unternehmenskritisches Gut dar. Zudem steigt die Bedrohungslage täglich, schaffen Trends wie Mobility, IoT, Cloud Computing und Industrie 4.0 immer neue Einfallstore und Herausforderungen. Die Security-Lösungen müssen sich anpassen und neue Technologien sowie Lösungsansätze werden benötigt, um im Wettrüsten mit den Hackern Schritt zu halten. Auch Cisco hat sein Security-Portfolio in den letzten Jahren durch viele Akquisitionen und eigene Weiterentwicklungen angepasst und eine wirkungsvolle Ende-zu-Ende Security-Lösung geschaffen. In diesem Training werden die Veränderungen in der IT und die daraus resultierenden neuen Security-Ansätze vorgestellt. Stakeholder-Analysen für die wichtigsten Bedarfsträger im Security-Umfeld werden erarbeitet und daraus Vertriebsangänge abgeleitet. Es folgt eine Präsentation der wichtigsten Bestandteile der Cisco Security-Lösung sowie deren richtige Positionierung beim Kunden. Das Training schließt mit der Vorstellung der wichtigsten Sales Stories, Bedarfsauslöser, Nutzenargumentationen und Einwandbehandlungen wie auch mit einem Blick auf den Markt.

Kursinhalt

- Wachstumsmarkt Security
- Veränderung durch Cloud Computing, Internet of Things (IoT) und Industrie 4.0
- Security-Rollen beim Kunden
- Stakeholder-Analyse für CDO, CEO, CISO, Security Administrator, Mitarbeiter im Einkauf und den Datenschutzbeauftragten
- Cisco Security Story End to End und Network as a Sensor und Enforcer
- AMP: Talos, Threat Grid, Endpoint AMP und Cisco pxGrid
- Das aktuelle Cisco Security Portfolio im Überblick:
- Firepower Appliances 2100, 4100 und 9300 sowie Cisco ISA 3000
- Cisco Identity Services Engine für LAN und WLAN
- Cisco Email Security Appliance (ESA) und Cisco Web Security Appliance (WSA)
- Cisco VPN und Cisco AnyConnect Secure Mobility Client
- Cisco Stealthwatch: Network Visibility, Security Analytics und Enforcement
- Cisco Umbrella: Cloud Security Platform
- Cyber Defense Orchestrator
- Cisco CloudLock
- Duo Security
- Security in Fabrikumgebungen
- Security für Industrie 4.0: ASA 5506H-X und ISA 3000
- Marktüberblick
- Nutzenargumentation, Use Cases und Sales Stories

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

Der Kurs wendet sich an Account Manager, die Cisco Security-Lösungen erfolgreich verkaufen wollen.

Voraussetzungen

Wer einen Einblick in die Veränderungen des Security-Marktes sucht, seine Kunden in diesem Umfeld öffnen sowie die richtigen Cisco Sales Stories liefern möchte, ist in diesem Kurs genau richtig.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**CYAM**

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 der Schweiz	**2 TageCHF 2.690,-**
Online Training	**2 TageCHF 2.195,-**
Termine auf Anfrage	

Stand 24.02.2024

Cyber Security und die Cisco Security Story

Deutschsprachige Kurse

ExperTeach

Inhaltsverzeichnis

Cyber Security und die Cisco Security Story – Sales Pitches für Account Manager

1 Security Trends
1.1 Marktveränderungen
1.2 Veränderung der Datenströme durch Cloud Computing
1.3 Was passiert gerade?
1.4 Bedrohungslage
1.5 Security Transformation
1.5.1 Security – Herausforderungen
1.5.2 Limitierungen zentraler Security-Lösungen
1.5.3 Komplexität klassischer Security-Lösungen
1.6 Automatisierung – Grundlagen
1.6.1 DevOps
1.6.2 Continuous Delivery
1.6.3 CI/CD: Software Development Lifecycle
1.6.4 Security und Netzwerk verschmelzen
1.6.5 Monitoring und Operations
1.6.6 Observability als 3. Säule
1.7 Megatrend SASE – Marktüberblick
1.8 Was ist SASE?
1.8.1 Ziele von SASE
1.8.2 Definition SASE
1.9 SASE Bestandteile
1.9.1 Zero Trust Network
1.10 Security bei SD-WAN
1.11 SASE Architekturen und Use Cases

2 Cisco IT Security-Lösungen
2.1 Das klassische Cisco Security Portfolio
2.1.1 Cisco Firepower Appliances
2.1.2 Cisco Identity Services Engine für LAN und WLAN
2.1.3 Cisco Email Security Appliance (ESA)
2.1.4 Cisco Secure Email Cloud Mailbox
2.1.5 Cisco Web Security Appliance – WSA
2.1.6 Cisco VPN und Cisco AnyConnect Secure Mobility Client
2.2 Die Cisco Security Story: End to End
2.2.1 Eine Lösung für alle Phasen eines Angriffs
2.2.2 Cisco pxGrid
2.2.3 Talos
2.3 Secure Network Analytics
2.3.1 Cisco Secure Network Analytics
2.3.2 Stealthwatch Endpoint Visibility
2.3.3 Cisco Endpoint Security Analytics (CESA)
2.4 Cisco Advanced Malware Protection – AMP
2.4.1 Funktionsweise AMP
2.4.2 Cisco Secure Malware Analytics
2.4.3 Cisco Secure Endpoint ehemals AMP for Endpoints
2.5 Cisco Umbrella
2.5.1 Cisco Umbrella – DNS Security
2.5.2 Cisco Umbrella SIG – SASE-Lösung

3 Cisco OT Security
3.1 Sicherheit in Fabrikationsumgebungen
3.1.1 Neue Risiken und Herausforderungen
3.1.2 Design und Architektur von industriellen Sicherheitslösungen
3.2 Verschmelzung von IT und OT Security
3.3 Cisco IoT Security
3.3.1 Cisco Cyber Vision
3.3.2 ISA3000 Industrial Security Appliance
3.3.3 SecureX Threat Response
3.3.4 Security-Architektur für Produktionsumgebungen
3.3.5 Security-Architektur für Kraftwerke
3.3.6 Integration in Cisco und Third-Party-Lösungen
3.3.7 Stakeholder für die Sicherheit in Fabrikumgebungen

4 Security in Cisco Meraki-Umgebungen
4.1 Cisco Meraki MX Portfolio
4.2 Ergänzende Security-Lösungen
4.3 Firewall
4.3.1 Layer 7 Firewall
4.3.2 Network Address Translation
4.4 SD-WAN, Priorisierung und Traffic Shaping
4.4.1 Priorisierung
4.4.2 SD-WAN & Traffic Shaping
4.5 Standortkopplungen via VPN
4.6 Auto VPN in Richtung Public Cloud
4.7 Client VPN
4.8 Access Control
4.9 Threat Protection: AMP und IDS/IPS
4.9.1 Threat Protection: Konfiguration
4.10 Content Filtering
4.11 Redundanz
4.11.1 VPN-Gateway-Redundanz
4.12 Meraki MX und Cisco Umbrella Integration
4.13 Meraki MX und Cisco SASE
4.13.1 Aktuelle Meraki Umbrella-Integration
4.13.2 SASE Roadmap
4.13.3 Meraki MX und Cisco Umbrella SIG – Phase 1
4.13.4 Meraki MX und Cisco Umbrella SIG – Phase 2
4.14 Meraki MX und Cisco Umbrella SIG – Phase 1 versus 2
4.15 Vorteile im Wettbewerb

5 Sales Pitches, Bedarfsauslöser, Nutzenargumentation, Einwandbehandlung
5.1 Sales Pitch
5.1.1 Warum Cisco?
5.1.2 Wie reagiert der Markt?
5.2 Use Cases
5.3 Nutzenargumentation
5.4 Cisco Security: Einwandbehandlung
5.5 Argumentation im Wettbewerb, Marktüberblick
5.5.1 Warum kauft der Kunde bei unserem Unternehmen?

6 Zusammenfassung
6.1 Zusammenfassung, Diskussion und Feedback

ExperTeach AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch