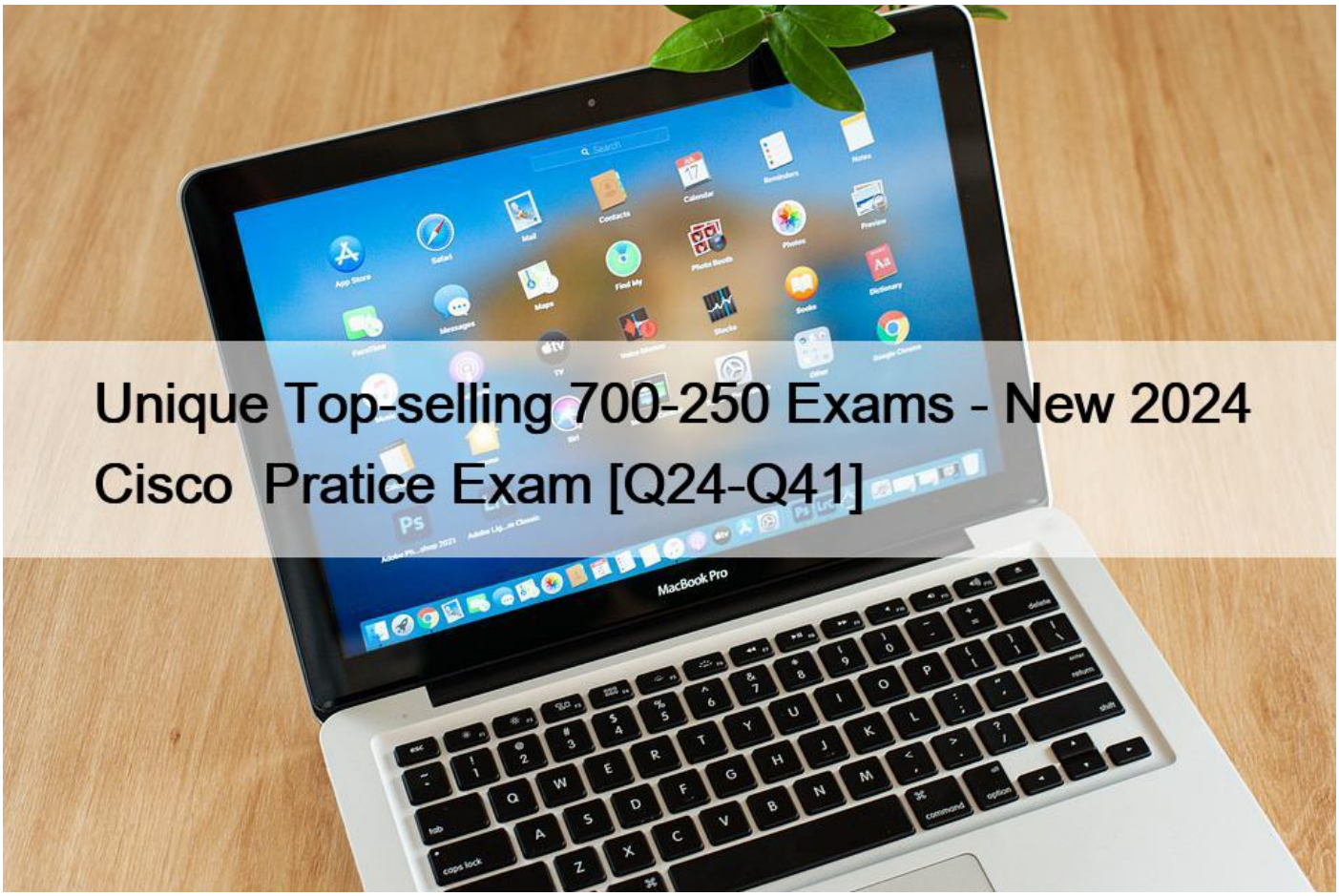
Unique Top-selling 700-250 Exams - New 2024 Cisco Pratice Exam [Q24-Q41



Unique Top-selling 700-250 Exams - New 2024 Cisco Pratice Exam
Cisco Small and Medium Business Sales Specialization Dumps 700-250 Exam for Full Questions - Exam Study Guide

NO.24 What enables Umbrella to offer unprecedented insight into launched and staged attacks?
* data set of multiple geographies and protocols
* understanding the types of sensitive data loss by customers
* DNS redundancy
* Umbrella’s geofenced network

Umbrella offers unprecedented insight into launched and staged attacks through its extensive data set of multiple geographies and protocols. This large and diverse data set allows Umbrella to detect and analyze patterns of malicious activity across different regions and protocols, providing early warning and comprehensive understanding of potential threats.

1.Global Data Coverage: Umbrella collects data from a wide range of geographic locations, giving it a broad view of global threat activity.

2.Protocol Analysis: By analyzing traffic across multiple protocols, Umbrella can identify and understand the behavior of different types of attacks.

3.Threat Intelligence: The extensive data set enhances Umbrella’s threat intelligence capabilities, enabling it to detect and respond to emerging threats quickly and accurately.

References:

*Cisco Umbrella Threat Intelligence Overview

*Cisco Umbrella Data Collection and Analysis Documentation

*Cisco Security Solutions for Threat Detection

NO.25 Which security challenge do SMBs face?
* global shortage of security experts
* smaller attack surface
* lack of security products
* lack of knowledge in cloud security

SMBs (Small and Medium Businesses) often face significant challenges regarding cloud security due to a lack of expertise and knowledge in this domain. As many SMBs migrate to cloud services to leverage cost and efficiency benefits, they often do not have the necessary skills or understanding to secure these environments properly. This can lead to misconfigurations, inadequate protection against threats, and potential data breaches.

1.Limited Resources: SMBs typically have fewer resources to dedicate to IT and security, making it challenging to hire or train personnel with cloud security expertise.

2.Complexity of Cloud Security: Cloud environments introduce new security considerations that differ from traditional on-premises infrastructure, requiring specific knowledge and practices.

3.Evolving Threat Landscape: The dynamic nature of cybersecurity threats necessitates ongoing education and adaptation, which can be challenging for SMBs to keep up with.

References:

*Cisco Small Business Security Solutions Overview

*Cisco Cybersecurity Reports

*SMB Cloud Security Challenges Whitepapers

NO.26 Which features are managed in the Cisco Control Hub?
* Cisco IP Phones
* Meraki Cameras
* Meetings and Messagin91
* Catalyst Switches

NO.27 Where do SMB partners find free-to-use customizable campaigns and assets?
* Cisco Solutions Velocity Central
* The Life Cycle Advantage Portal
* Cisco Velocity Advantage Portal
* Cisco Marketing Velocity Central

SMB partners can find free-to-use customizable campaigns and assets on Cisco Marketing Velocity Central.

This platform offers a wide range of marketing resources tailored to help Cisco partners create effective campaigns, promote their services, and drive customer engagement. These resources include templates, guides, and tools that partners can customize to suit their specific needs, making it easier to market Cisco products and solutions effectively.

References:

*Cisco Marketing Velocity Central Overview

*Cisco Partner Marketing Resources

NO.28 How are customers classified who have spent at least $1 in each of the four quarters over the last 12 months?
* Stable Buyer
* Occasional Buyer
* Repeat Buyer
* Frequent Buyer

Customers who have spent at least $1 in each of the four quarters over the last 12 months are classified as Repeat Buyers. This classification indicates a level of consistent purchasing behavior, reflecting customer loyalty and ongoing engagement with the company’s products or services.

1.Consistency in Purchases: Spending in each quarter demonstrates regular interaction and reliance on the products or services offered.

2.Customer Loyalty: Regular purchasing behavior suggests a satisfaction with the products and services, indicating loyalty.

3.Engagement Metrics: Repeat buyers are often seen as a key metric for customer retention and long-term business relationships.

References:

*Customer Classification and Segmentation Guidelines

*Cisco Customer Relationship Management Strategies

*Industry Standards for Customer Purchasing Behavior

NO.29 Which Cisco solution should an SMB IT support company adopt lo help mitigate network vulnerabilities?
* CML
* Catalyst Access Points
* Webex Control Hub
* FirePower Firewalls

Cisco FirePower Firewalls are specifically designed to provide advanced threat protection and mitigation of network vulnerabilities. These firewalls offer next-generation features, such as intrusion prevention systems (IPS), advanced malware protection (AMP), and URL filtering, which are crucial for securing SMB networks against various threats. FirePower Firewalls can detect and block sophisticated threats in real-time, offering comprehensive security solutions that protect network assets from attacks.

1.Advanced Threat Protection: FirePower Firewalls use a combination of deep packet inspection, real-time threat intelligence, and behavior-based analysis to detect and mitigate threats.

2.Intrusion Prevention System (IPS): This feature identifies and stops malicious traffic and known vulnerabilities before they can enter the network.

3.Advanced Malware Protection (AMP): AMP provides continuous analysis and retrospective security, helping to detect, track, and remediate advanced malware.

4.URL Filtering: This feature blocks access to malicious websites and unwanted content, reducing the risk of phishing and other web-based attacks.

References:

*Cisco Firepower Next-Generation Firewall Data Sheet

*Cisco Small Business Solutions Guide

*Cisco FirePower Threat Defense Configuration Guide

NO.30 Which challenge do customers face with hybrid work?
* hot desking
* collaboration spaces
* exponential increase in cloud data
* non-inclusive experiences

One of the significant challenges customers face with hybrid work is the exponential increase in cloud data. As more employees work remotely and use cloud services, the amount of data stored and processed in the cloud grows dramatically. This increase brings challenges related to data management, security, and compliance.

1.Data Management: Managing the large volumes of data generated by hybrid work environments can be complex and resource-intensive.

2.Security: Ensuring the security of data across various cloud platforms and services becomes more challenging with the increased data volume.

3.Compliance: Meeting regulatory requirements for data protection and privacy can be more difficult as data spreads across multiple cloud environments.

References:

*Cisco Hybrid Work Solutions Overview

*Challenges of Hybrid Work and Cloud Data Management

*Industry Reports on Hybrid Work and Cloud Data Growth

NO.31 Which devices are considered cloud-fiirst technology?
* Catalyst devices
* IP video endpoints
* Meraki devices
* HVAC Sensors

Meraki devices are considered cloud-first technology because they are designed to be managed through the cloud, providing centralized control and visibility over the network. This cloud-based approach simplifies the management of network infrastructure, making it more accessible and efficient for SMBs and enterprises alike.

Meraki’s cloud-first design allows for seamless updates, scalability, and real-time monitoring, which are crucial for modern IT environments. This contrasts with traditional on-premises devices that require more manual management and maintenance.

References:

*Cisco Meraki Product Overview

*Cisco Meraki Cloud Management Documentation

NO.32 Which Cisco product is part of the Secure SMB experience for enabling people?
* Meraki MX
* Cisco Secure Email
* Stealthwatch
* Umbrella

Cisco Umbrella is a key part of the Secure SMB experience for enabling people. Umbrella provides comprehensive security for SMBs by protecting against internet-based threats, offering DNS-layer security, and blocking malicious domains and IP addresses before they can impact the network. This helps ensure that users can work securely from anywhere, providing a safer and more productive environment.

1.DNS-layer Security: Umbrella blocks requests to malicious domains and IP addresses at the DNS layer, preventing threats before they reach the network.

2.Comprehensive Protection: It provides protection against phishing, malware, and command-and-control callbacks, securing users both on and off the network.

3.Ease of Use: Umbrella is easy to deploy and manage, making it an ideal solution for SMBs with limited IT resources.

References:

*Cisco Umbrella Overview

*Cisco SMB Security Solutions

*Umbrella Product Documentation

NO.33 Securing the DNS layer means blocking malicious domains, IP addresses, and cloud applications before establishing a connection. Which Cisco solution helps secure
* Duo
* ThousandEyes
* Umbrella
* Email Threat Defense

Cisco Umbrella secures the DNS layer by blocking malicious domains, IP addresses, and cloud applications before a connection is established. This proactive security measure helps prevent threats from reaching the network and reduces the risk of malware infections and data breaches.

1.DNS-layer Security: Umbrella blocks malicious domains and IP addresses at the DNS layer, preventing users from accessing dangerous websites and applications.

2.Threat Intelligence: Umbrella leverages real-time threat intelligence to identify and block new and emerging threats.

3.Cloud-based Protection: As a cloud-delivered solution, Umbrella is easy to deploy and manage, providing scalable protection for users both on and off the network.

References:

*Cisco Umbrella Overview

*Cisco DNS-layer Security Whitepaper

*Cisco Umbrella Product Documentation

NO.34 Which Cisco product features Integrated Mobile Device Mana,gement?
* Duo
* Umbrella
* Meraki
* Webex

Cisco Meraki offers integrated mobile device management (MDM) as part of its cloud-managed networking solutions. The Meraki Dashboard provides centralized management of network devices, including mobile devices, which allows IT administrators to enforce security policies, monitor device compliance, and manage app deployment.

1.Centralized Management: The Meraki Dashboard enables centralized control over all network devices, including mobile endpoints, through a single interface.

2.Device Enrollment: Administrators can enroll mobile devices in the Meraki system for management and monitoring.

3.Security Policies: Meraki allows the application of security policies to mobile devices, ensuring they meet organizational security standards.

4.App Management: IT administrators can deploy, manage, and update applications on enrolled mobile devices remotely.

References:

*Cisco Meraki Mobile Device Management Data Sheet

*Cisco Meraki Dashboard Overview

*Cisco Small Business Solutions Guide

NO.35 Which security feature provides insights into Internet activity and facilitates real-time activity search?
* Control Hub
* Duo
* Cloud-Delivered Al
* Secure Web Gateway

A Secure Web Gateway (SWG) provides insights into internet activity and facilitates real-time activity search.

It monitors and controls web traffic, enforcing security policies to protect against threats and ensuring compliance with corporate policies. SWG solutions offer visibility into user activity on the internet and allow for the analysis and searching of real-time activity data.

1.Internet Activity Monitoring: SWGs provide detailed visibility into web traffic, enabling organizations to monitor user behavior

and internet activity.

2.Real-Time Activity Search: They allow IT administrators to search and analyze real-time activity data to identify potential threats and enforce security policies.

3.Threat Protection: SWGs protect users from web-based threats such as malware, phishing, and malicious websites by filtering and blocking harmful content.

References:

*Cisco Secure Web Gateway Overview

*Internet Activity Monitoring Solutions

*Cisco Web Security Documentation

NO.36 Which Cisco product protects against the loss of sensitive data?
* Meraki Systems Manager
* Meraki MX
* DUO
* Umbrella

The Cisco Meraki MX series is a comprehensive security and SD-WAN appliance that includes features specifically designed to protect against the loss of sensitive data. It provides robust security measures such as advanced threat protection, content filtering, and intrusion prevention, which help safeguard sensitive data from breaches and unauthorized access.

1.Advanced Threat Protection: The Meraki MX includes features like malware protection and advanced security analytics to detect and prevent data breaches.

2.Content Filtering: It helps in preventing sensitive data from being sent out or accessed by filtering web content and applications.

3.Intrusion Prevention System (IPS): The built-in IPS provides deep packet inspection to detect and block potential threats, ensuring sensitive data remains secure.

References:

*Cisco Meraki MX Security and SD-WAN Overview

*Cisco Meraki MX Data Sheet

*Meraki Security and Threat Protection Documentation

NO.37 Which Meraki product is used in Remote SMB work from home?
* Z4 teleworker gateway
* Meraki Insight
* Meraki MV
* Meraki MT

The Meraki Z4 teleworker gateway is designed to support remote work environments for SMBs. It provides secure and reliable connectivity for employees working from home, ensuring they can access corporate resources efficiently and securely.

1.Secure VPN Connectivity: The Z4 teleworker gateway offers secure VPN connections, allowing remote workers to securely access

the corporate network.

2.Comprehensive Features: It includes advanced networking features such as traffic shaping, content filtering, and integrated Wi-Fi, which are essential for home office setups.

3.Remote Management: The Z4 can be easily managed via the Meraki Dashboard, providing IT administrators with the tools to deploy, monitor, and troubleshoot remotely.

References:

*Cisco Meraki Z4 Teleworker Gateway Data Sheet

*Meraki Remote Work Solutions Overview

*Cisco SMB Remote Work Product Documentation

NO.38 What is a crucial concern for Hybrid SMB?
* process automation
* complexity of applications
* more data with too little contextualization
* protect employees, devices, and company data

A crucial concern for hybrid SMBs is protecting employees, devices, and company data. The hybrid work model introduces new security challenges as employees access company resources from various locations and devices. Ensuring the security of these elements is paramount to maintaining business continuity and protecting sensitive information.

1.Employee Protection: Implementing security measures to safeguard employees’ digital identities and ensuring their safe access to company resources.

2.Device Security: Managing and securing a diverse range of devices used by employees, including laptops, mobile phones, and tablets.

3.Data Security: Protecting sensitive company data from unauthorized access and breaches, especially as data is accessed and shared across different environments.

References:

*Cisco Hybrid Work Security Solutions

*Security Challenges for SMBs in Hybrid Work Environments

*Cisco Best Practices for Securing Remote and Hybrid Workforces

NO.39 Which Cisco solution provides end-to-end visibility from every user to any application?
* Cisco Overwatch
* ThousandEyes
* Meraki Dashboard
* Cisco Control Hub

ThousandEyes provides end-to-end visibility from every user to any application, which is crucial for maintaining optimal network performance and user experience. It offers detailed insights into network paths and application delivery, enabling IT teams to monitor and troubleshoot performance issues across the entire network, including the internet, cloud, and enterprise networks.

1.End-to-End Visibility: ThousandEyes provides comprehensive visibility into the entire network path, from the user to the application, regardless of the location or network segments involved.

2.Network and Application Performance Monitoring: It continuously monitors the performance of applications and the underlying network, identifying bottlenecks and issues affecting user experience.

3.Troubleshooting and Analysis: ThousandEyes offers powerful tools for diagnosing and resolving performance issues, providing detailed metrics and analysis to pinpoint the source of problems.

References:

*Cisco ThousandEyes Overview

*ThousandEyes Data Sheet

*Cisco Network Performance Monitoring Solutions

NO.40 Which groundbreaking feature leverages Meraki Cameras?
* Smart Health Notifications
* Smart Cleaning Notifications
* Smart loT Notifications
* Smart Secure Notifications

Meraki Cameras leverage Smart IoT Notifications as part of their innovative features. These notifications are part of the broader Meraki IoT (Internet of Things) ecosystem, enabling advanced capabilities such as detecting unusual activity, monitoring environmental conditions, and integrating with other IoT devices for comprehensive smart management. The cameras provide intelligent alerts and notifications based on various triggers and conditions, enhancing security and operational efficiency.

1.Integration with IoT Ecosystem: Meraki Cameras can integrate with other IoT devices and systems, allowing for comprehensive monitoring and management.

2.Advanced Analytics: The cameras use advanced video analytics to detect unusual patterns and activities, sending smart notifications to administrators.

3.Enhanced Security: By leveraging IoT notifications, Meraki Cameras provide real-time alerts on potential security breaches or anomalies.

References:

*Cisco Meraki MV Cameras Data Sheet

*Cisco Meraki IoT Solutions Overview

*Meraki Smart Notifications and Analytics Documentation

NO.41 How does Cisco help SMBs to be truly smart?
* secure connectivity
* operational inefficiencies
* employee automation
* utilities cost control

Cisco helps SMBs to be truly smart through secure connectivity. Secure connectivity is fundamental for SMBs to operate efficiently, protect their data, and ensure that their network infrastructure supports their business needs. Cisco provides comprehensive solutions that include secure networking, advanced security features, and robust infrastructure management, all designed to help SMBs achieve secure and reliable connectivity.

1.Secure Networking Solutions: Cisco offers a range of networking solutions that provide secure and reliable connectivity for SMBs.

2.Advanced Security Features: These include firewalls, VPNs, and intrusion prevention systems to protect SMB networks from threats.

3.Comprehensive Management: Tools like the Meraki Dashboard allow SMBs to manage their network infrastructure securely and efficiently.

References:

*Cisco Secure Connectivity Solutions Overview

*Cisco SMB Networking Solutions Guide

*Cisco Security Products and Services Documentation