PassQueen
a.k.a dumpsqueen.com

Express Security for Account Managers (ESAM)

Cisco 700-551

Version Demo

Total Demo Questions: 10

Total Premium Questions: 103

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Fundamentals	4
Topic 2, Cisco Security Solutions	53
Topic 3, Selling Cisco Security Solutions	46
Total	103

QUESTION NO: 1

What is the average cost of network attacks?

A. $300B

B. $500K

C. $50K

D. $300K

ANSWER: D

Explanation:

$300K is the expected answer in the ESAM training context. This figure is used to communicate the business impact of network-based security incidents in a concise way for customer conversations: attacks impose direct costs for investigation, remediation, recovery, and interruption to normal business operations. For an account manager, the point of this benchmark is not to produce a forensic loss estimate for every individual incident, but to help establish why investment in an integrated security architecture, threat visibility, and faster response capabilities has measurable business value. Cisco's security research discusses how the operational impact of threats and the complexity of responding to them create material costs for organizations; see Cisco's Security Reports and Research. Cost figures should always be presented with their source, scope, and date because actual loss varies substantially by organization, incident type, industry, and recovery time. Current breach-cost research likewise emphasizes that incident costs are affected by detection and containment performance, as summarized in IBM's Cost of a Data Breach Report. Within the question's intended course material and its fixed benchmark choices, $300K is the applicable average-cost value.

QUESTION NO: 2

What security principle gives users only the access required to perform their assigned job responsibilities?

A. Least privilege

B. Open access

C. Implicit trust

D. Network address translation

E. Load balancing

ANSWER: A

Explanation:

Least privilege is the correct answer because it limits a user's access rights to the applications, systems, and data necessary for that user's role. Restricting unnecessary permissions reduces the potential impact of compromised credentials, insider misuse, and accidental exposure of sensitive information.

Least privilege is a fundamental Zero Trust and access-control practice. It is commonly implemented through identity-based policy, role-based access control, strong authentication, and regular access reviews. Cisco's Zero Trust approach emphasizes verifying access and applying appropriate policy based on user, device, and context. See the Cisco Zero Trust guidance.

QUESTION NO: 3

What NGIPS appliance would you use if your customer is at the enterprise level and requires modular architecture that is scalable?

A. Cisco 4000 series ISR

B. FirePOWER 8000 series

C. ASA 7000 series

D. Cisco 800 series ISR

E. FirePOWER 2100 series

ANSWER: B

Explanation:

FirePOWER 8000 series is the appropriate choice because it was designed as Cisco's high-end, modular FirePOWER/NGIPS platform for large enterprise and service-provider deployments. Its chassis-based architecture supports interchangeable processing and network modules, enabling an organization to select interface density and inspection capacity appropriate to its environment. This modular design also provides a practical growth path: capacity can be expanded through hardware modules rather than requiring a wholesale replacement when traffic volumes or protected segments increase.

For an enterprise customer, scalability must encompass both high throughput and operational flexibility. The FirePOWER 8000 platform was positioned for deployments that need to inspect substantial volumes of traffic while applying advanced threat protection and intrusion-prevention capabilities. Cisco describes the 8000 Series as a modular appliance family built for scalable performance and high port density, which directly matches the stated requirement. See Cisco's FirePOWER 8000 Series data sheet and its FirePOWER 8000 Series product overview.

QUESTION NO: 4

What Cisco security capability helps customers detect and respond to threats by correlating telemetry across multiple security tools?

A. Cisco XDR

B. Cisco Duo

C. Cisco Secure Client

D. Cisco TrustSec

E. Cisco Smart Licensing

ANSWER: A

Explanation:

Cisco XDR is the correct choice because it extends detection and response across endpoint, network, email, cloud, firewall, and other security telemetry sources. It correlates alerts and evidence to help security teams identify incidents that could be missed when each product is reviewed independently.

The value of an extended detection and response approach is improved investigation and response efficiency. By bringing related security events into a common incident view and supporting guided response workflows, Cisco XDR helps analysts prioritize meaningful threats and take action with better context. Cisco describes this capability at Cisco XDR.

QUESTION NO: 5

Which are three Cisco Advanced Threat solutions? (Choose three.)

A. AMP

B. Identity and Access Control

C. Remote Access VPN

D. Stealthwatch

E. Next Generation Intrusion Prevention System

F. Cognitive Threat Analytics

ANSWER: A D F

Explanation:

AMP, **Stealthwatch**, and **Cognitive Threat Analytics** are Cisco Advanced Threat solutions in the terminology used by this exam's security-portfolio material. AMP (Advanced Malware Protection), now represented in Cisco's portfolio by Secure Endpoint, provides continuous malware protection: it can identify malicious files, use threat intelligence and file analysis, and continue monitoring file behavior after initial inspection. Cisco describes Secure Endpoint at Cisco Secure Endpoint.

Stealthwatch, subsequently renamed Cisco Secure Network Analytics, delivers network-based visibility and behavioral analytics. It uses network telemetry to identify suspicious activity, including anomalous communications, lateral movement patterns, and potentially compromised devices. This network context is important to advanced-threat detection and investigation; see Cisco Secure Network Analytics.

Cognitive Threat Analytics is the cloud-based analytics component in the historical Cisco advanced-threat portfolio. It applies behavioral modeling and machine learning to web-proxy and network telemetry to surface attacks that may evade signature-based detection. Together, endpoint malware protection, network behavioral visibility, and cognitive analytics provide complementary detection and response capabilities for advanced threats.

QUESTION NO: 6

Which are three ways that Cisco enables partners to build a security practice? (Choose three.)

A. Operational platforms and enablement

B. ROI models describing the opportunity

C. Practice growth statistics

D. Sales and delivery enablement

E. Increased customer throughput

F. Tools that support practice design

ANSWER: A D F

Explanation:

Cisco enables partners to establish and scale a security practice by combining the operational foundation, practice-planning resources, and skills development required to take security solutions to market. **Operational platforms and enablement** is correct because partners need access to Cisco's partner ecosystem, programs, digital resources, and operational support to engage customers, manage opportunities, and build a repeatable business motion. **Sales and delivery enablement** is correct because a sustainable practice requires both customer-facing sales capability and the technical knowledge needed to deploy, support, and deliver security solutions successfully. Cisco provides partner training and role-based learning resources intended to develop these capabilities. **Tools that support practice design** is also correct because practice-building tools help partners define their business model, assess readiness, organize capabilities, and develop an actionable route to market. Together, these areas support the full lifecycle of a partner security practice: designing the practice, enabling sales and technical teams, and operating the practice through Cisco's partner resources. Cisco describes its partner ecosystem and business support at Partner with Cisco and provides learning and enablement resources through Cisco Partner Training and Events.

QUESTION NO: 7

Which are three key products and benefits of the Datacenter threat-centric solution? (Choose three.)

A. Predictive intelligence through Umbrella and Talos

B. Proactive packet inspection through Stealthwatch

C. Automated policy enforcement with ASAv

D. Software-defines segmentation through TrustSec

E. Deep visibility and data analytics through Stealthwatch

F. Identity-based policy management through Meraki

ANSWER: C D E

Explanation:

The Datacenter threat-centric solution combines enforcement, segmentation, and visibility capabilities to reduce the time required to detect and contain threats in data-center environments. Automated policy enforcement with ASAv is a core capability because Cisco Adaptive Security Virtual Appliance provides virtualized firewall controls that can be deployed alongside workloads and applied consistently as application environments change. Cisco documents ASAv as a virtual security solution designed for cloud and data-center deployments: Cisco ASAv Data Sheet.

Software-defines segmentation through TrustSec is also central to a threat-centric design. TrustSec uses identity and Security Group Tags to express access policy independently of network location, enabling scalable segmentation across infrastructure. This allows security controls to follow users and workloads rather than depending solely on IP addressing or physical topology. Cisco describes this identity-based segmentation architecture in its Cisco TrustSec overview.

Deep visibility and data analytics through Stealthwatch completes the solution by collecting and analyzing network telemetry to identify suspicious behavior, support threat investigation, and provide context for response decisions. Together, these capabilities provide policy control, segmentation, and actionable network visibility.

QUESTION NO: 8

What application works with customers to eliminate security gaps and ensure safe data access and storage in the cloud across devices?

A. AMP Threat Grid

B. Next Generation Firewall

C. TrustSec

D. Stealthwatch

E. Cloudlock

F. AnyConnect

ANSWER: E

Explanation:

Cloudlock is the correct choice because it is Cisco's cloud access security broker solution, designed to help organizations protect information as users access cloud applications and store data outside the traditional network perimeter. It provides visibility into cloud usage, identifies sensitive data and risky user activity, and applies policy-based controls to reduce gaps in cloud security. These capabilities support secure access and storage across common software-as-a-service environments and across the devices from which users connect.

A key Cloudlock use case is enforcing data-loss-prevention policies in cloud applications. For example, an organization can detect sensitive records, classify them, and take an automated remediation action when data is shared inappropriately or exposed to an unacceptable audience. Cloudlock also uses analytics to help identify anomalous behavior and potential account compromise, giving customers a way to address cloud risk without relying solely on controls within the customer's physical network.

This cloud-focused visibility, data protection, and policy enforcement model directly matches the requirement to eliminate security gaps while enabling safe cloud data access and storage. Cisco describes the solution's cloud-security capabilities in its Cloudlock product information and explains cloud access security broker functions in its CASB overview.

QUESTION NO: 9

What three types of solutions are provided in the Cisco security portfolio? (Choose three)

A. Cloud Security

B. Policy & Access

C. E-mail Analytics

D. Advanced Threat

E. SaaS and Cloud Platform

F. Firewall Security

ANSWER: A B D

Explanation:

Cisco's security portfolio is organized around solution areas that help customers securely connect users, devices, applications, and data while preventing, detecting, and responding to threats. **Cloud Security** is a core solution area because Cisco provides cloud-delivered security controls for protecting internet access, cloud applications, and users regardless of location. **Policy & Access** is also a portfolio solution area: identity, authentication, authorization, and access-policy enforcement are foundational to ensuring that only appropriate users and devices can reach business resources. **Advanced Threat** represents Cisco capabilities for identifying sophisticated attacks, analyzing malicious activity, and improving detection and response across the environment. Together, these solution types address cloud-delivered protection, trusted access, and advanced-threat defense—the principal security outcomes customers need as their users and workloads become more distributed. Cisco describes its current security approach as a unified security platform that protects users, applications, devices, and data across hybrid environments. See the Cisco Security portfolio and Cisco's overview of secure access.

QUESTION NO: 10

Which three are profit incentives for partners? (Choose three.)

A. Opportunity Incentive Program

B. Profit Incentive Program

C. Value Incentive Program

D. Solution Incentive Program

E. Training Incentive Program

F. Cross-sell Incentive Program

ANSWER: A C D

Explanation:

Cisco's partner profitability model has historically included the Opportunity Incentive Program, the Value Incentive Program, and the Solution Incentive Program as distinct incentive mechanisms. The Opportunity Incentive Program rewards eligible partners for identifying, developing, and closing qualified customer opportunities, helping protect the value of partner-led demand generation. The Value Incentive Program provides performance-based rebates for selling targeted Cisco architectures, products, and services, aligning partner rewards with strategic technology adoption and customer outcomes.

The Solution Incentive Program is intended to reward partners for building and delivering qualifying Cisco-based solutions, recognizing the added value created through solution expertise and integrated offers. Together, these programs support profitability across the sales lifecycle: creating opportunities, selling strategic Cisco offerings, and delivering differentiated solutions. Cisco's partner incentives are designed to complement partner margins and encourage investment in the capabilities that improve customer success and accelerate adoption of Cisco solutions. Cisco provides program and incentive information through its partner resources at Cisco Partner Incentives and describes its broader partner engagement framework at Cisco Partners.