

Cisco.500-651.v2019-01-24.q56

Exam Code:	500-651
Exam Name:	Security Architecture for Systems Engineer
Certification Provider:	Cisco
Free Question Number:	56
Version:	v2019-01-24
# of views:	1013
# of Questions views:	21021
https://www.freecram.net/torrent/Cisco.500-651.v2019-01-24.q56.html	

NEW QUESTION: 1

Which feature of Cisco ISE uses Cisco TrustSec Security Group Tags to edit networks dynamically rather than with VLANs?

- A. Device profiling and onboarding
- B. Role and device segmentation
- C. Guest Access
- D. Secure remote access

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Policy and Access SE Module 5

NEW QUESTION: 2

What are two main features of enabling Cloudlock in a customer's environment? (Choose two)

- A. Cloudlock connects via Oauth
- B. Cloud App security works on plug-in
- C. Easily creates network tags for different users
- D. It takes less than five minutes to enable per platform
- E. Protects against cloud-native malware

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Cisco Cloud Security SE - Module 3

NEW QUESTION: 3

How many web requests does Talos process per month?

- A. 1.5 million

- B. 100,000
- C. 130 billion
- D. 130 million

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

ASAS Cisco Security and Threat Landscape Module 1

NEW QUESTION: 4

Which are three main features of the Meraki MX discussed in Cloud App Security module?

(Choose three)

- A. Posture Assessment
- B. Intrusion Prevention
- C. Email Security
- D. Profiling
- E. Next Generation Firewall
- F. Cloud-Brokered VPN

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

Cisco Cloud Security SE - Module 3

NEW QUESTION: 5

What are three major features of Cisco Defense Orchestrator? (Choose three.)

- A. Providing retrospective security to protect against malware
- B. Receive notifications about any unplanned changes to security policies and objects
- C. Plan and model security changes before deploying them across the cloud
- D. Identifying anomalous traffic in customer's network
- E. Ability to deploy changes across virtual environments in real time or offline
- F. Tracking suspicious files through the network

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION: 6

Which two options are attack vectors protected by Identity and Access Control? (Choose two)

- A. Backups
- B. Mobile
- C. Endpoints
- D. Cloud apps

E. Voicemail

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Threat Centric Solutions - AM and SE Module 7

NEW QUESTION: 7

Which two features are part of the ISE Plus license? (Choose two.)

- A. Profiling and feed services
- B. Guest management
- C. Cisco pxGrid
- D. Basic Network Access AAA, 802 1X
- E. Trustsec

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Policy and Access SE Module 5

NEW QUESTION: 8

Which AMP feature is provided by fuzzy fingerprinting?

- A. Identifies specific instances of malware with a signature-based approach
- B. Automatically detects polymorphic variants of known malware
- C. Provides recursive DNS lookup services
- D. Identifies new malware using statistical modeling and analytics engines

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module 6

NEW QUESTION: 9

Which feature of AMP tracks the movement of a file within the environment and monitors its disposition over time?

- A. Fuzzy Fingerprinting
- B. Machine Learning
- C. ThreatGrid
- D. Trajectory

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module 6

NEW QUESTION: 10

Which three Cisco solutions are covered in the Advanced Threat module? (Choose three)

- A. Cognitive Threat Analytics
- B. Intrusion Analytics
- C. AMP
- D. Cisco Defense Orchestrator
- E. NGIPS
- F. Cisco ThreatGrid

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module 6

NEW QUESTION: 11

Which are two main features of Intrusion Prevention?(Choose two.)

- A. Layer-4 traffic monitoring across platforms
- B. Threat analysis through network behavior analysis
- C. Protecting against Zero-Day attacks
- D. Vulnerability-based threat management

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 12

Which three options are attack vectors protected by Email Security? (Choose three)

- A. Endpoints
- B. Offline Devices
- C. Mobile
- D. E-mail
- E. Voicemail
- F. Backups

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Web and Email SE Module 2

NEW QUESTION: 13

How is Cisco Security able to dynamically add IP addresses of known malware domains to its list of ports to detect and block?

- A. Layer-4 Monitoring
- B. Data Loss Prevention
- C. URL Filtering
- D. Sandboxing

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Web and Email SE Module 2

NEW QUESTION: 14

Which is a feature mentioned in the DNS security module?

- A. Layer-4 monitoring
- B. Umbrella
- C. Real-time sandboxing
- D. Data Loss Prevention

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Web and Email SE Module 2

NEW QUESTION: 15

Which three NGFW and NGIPS features support the 'Complex Remote Access' use case?

(Choose three.)

- A. Support for device onboarding
- B. Users protected regardless of physical location
- C. Fuzzy Fingerprinting
- D. Detection of anomalous traffic
- E. Controls and protections extended beyond VPN controls
- F. Secure access extended to all users

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security NGFW and NGIPS SE Module 4

NEW QUESTION: 16

What two challenges do customers face in their Campus and Branch deployments? (Choose two)

- A. Securing the entire infrastructure
- B. Stopping data breaches across campuses and branches
- C. Understanding what our users are doing online
- D. Monitoring file behavior across a large set of endpoints
- E. Protect data across multiple cloud applications

Answer: ([SHOW ANSWER](#))

Valid 500-651 Dumps shared by ExamDiscuss.com for Helping Passing 500-651 Exam! ExamDiscuss.com now offer the **newest 500-651 exam dumps**, the ExamDiscuss.com 500-651 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 500-651 dumps with Test Engine here:

<https://www.examdiscuss.com/Cisco/exam/500-651/premium/> (90 Q&As Dumps, **35%OFF**

Special Discount Code: [freecram](#))

NEW QUESTION: 17

Which three are deployment options for E-mail Security? (Choose three.)

- A. ESA
- B. CES
- C. WSAv
- D. AMP
- E. ESAv
- F. WebRoot

Answer: A,B,E ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

ASAS Security Web and Email SE Module 2

NEW QUESTION: 18

Which two features are provided by ISE? (Choose two.)

- A. Device Firewalling
- B. Centralized policy management
- C. DDOS attack prevention
- D. Retrospective Security
- E. Network visibility

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 19

Which Cisco solution falls under Advanced Threat?

- A. Identity Services Engine
- B. Stealthwatch
- C. Threat Grid
- D. Umbrella

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module 6

NEW QUESTION: 20

Which feature of ISE is Terminal Access Control System (TACACS) a part of?

- A. Device Administration
- B. Device Profiling
- C. Centralized Policy Management
- D. Guest Access Management

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Policy and Access SE Module 5

NEW QUESTION: 21

Which is a security product that was covered in the Policy and Access security module?

- A. Cisco NFGW
- B. Cisco Identity Services Engine
- C. Cisco NGIPS
- D. Cisco Defense Orchestrator

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Policy and Access SE Module 5

NEW QUESTION: 22

Which two solutions are part of the data-center threat-centric solution module? (Choose two.)

- A. Rapid threat detection through NGFW and NGFWv
- B. Enforced device security with Meraki
- C. URL filtering
- D. Relationship segmentation
- E. Automated policy enforcement with ASA v

Answer: A,E (LEAVE A REPLY)

Explanation/Reference:

Explanation:

ASAS Security Threat Centric Solutions - AM and SE Module 7

NEW QUESTION: 23

What is key feature of Cognitive Threat Analytics?

- A. It enables safe email usage with event Analytics
- B. It improves threat detection over time with machine learning
- C. It enhances anonymity with URL filtering
- D. It enables greater endpoint device profiling intelligence with entity modeling

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module

NEW QUESTION: 24

Which Cisco product included in the Endpoint threat-centric solution?

- A. Umbrella
- B. ASAv
- C. Meraki MX
- D. Cloudlock

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Threat Centric Solutions - AM and SE Module 7

NEW QUESTION: 25

Which are two key Cisco products that are part of the web threat-centric solution? (Choose two)

- A. Cisco Umbrella
- B. Cisco Identity Services Engine
- C. Cisco Web Security Appliance
- D. Cisco Email Security Appliance
- E. Cisco Defense Orchestrator

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Threat Centric Solutions - AM and SE Module 7

NEW QUESTION: 26

Which are three key features of DNS-layer security? (Choose three.)

- A. Data Loss Prevention
- B. Retrospective Analysis
- C. Real-time sandboxing
- D. Provides visibility into all Internet activity
- E. Acts as first level of protection by providing security at DNS layer
- F. Resolves all DNS request through a single recursive DNS service

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

NEW QUESTION: 27

Which two Cisco solution are part of the Mobile threat centric solution? (Choose two.)

- A. Cisco AnyConnect

- B. Cisco Umbrella
- C. Cisco NGFW
- D. Cisco NGIPS
- E. Cisco Defense Orchestrator

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Threat Centric Solutions - AM and SE Module 7

NEW QUESTION: 28

Which are two main features of DDoS Attack Prevention? (Choose two.)

- A. Leveraging AMP ThreatGrid technology
- B. Block or allow traffic automatically
- C. Redirects DDoS traffic back to attacker
- D. Stop attacks within seconds of detection

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 29

Which three malware categories does real-time Malware Scanning protect you from? (Choose three)

- A. Antivirus Monitoring
- B. Adware
- C. Trojan Downloader
- D. Outbreak Filters
- E. Web Reputation
- F. Phishing URL

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module 6

NEW QUESTION: 30

Which is a key feature of Cisco Defense Orchestrator?

- A. Orchestrates security policy management from one place
- B. Consolidates configuration management
- C. Protects customers network against zero-day attacks
- D. Profiles devices connected to customer's network

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION: 31

Which Cisco solution features recursive DNS capabilities?

- A. Anyconnect
- B. Identity Services Engine
- C. Umbrella
- D. Cognitive Threat Analytics

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security Web and Email SE Module 2

Valid 500-651 Dumps shared by ExamDiscuss.com for Helping Passing 500-651 Exam! ExamDiscuss.com now offer the **newest 500-651 exam dumps**, the ExamDiscuss.com 500-651 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 500-651 dumps with Test Engine here:

<https://www.examd Discuss.com/Cisco/exam/500-651/premium/> (90 Q&As Dumps, **35%OFF**

Special Discount Code: [freecram](#))

NEW QUESTION: 32

Which are two features of Cisco FirePOWER NGFW? (Choose two.)

- A. Increased IT management needs
- B. URL filtering to restrict access to specific sites and sub-sites
- C. Data Loss Prevention
- D. Next generation IPS to detect intrusions and prevent threats

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 33

How does the Cisco AnyConnect AMP Module help to protect customer's networks?

- A. AMP is a unified agent that combines posture check and authentication across wired wireless, and VPN networks.
- B. AMP Module can profile devices before allowing them to connect
- C. AMP provides highly secure access for select enterprise mobile applications
- D. AnyConnect can deploy AMP for Endpoints for Windows or OSX

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Policy and Access SE Module 5

NEW QUESTION: 34

Which is a key feature of Cisco Defense Orchestrator?

- A. Simplifies security policy management
- B. Identifies sensitive data in cloud environments
- C. Detects anomalous traffic on customer's network
- D. Provides retrospective security

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION: 35

Which Stealthwatch component is a physical or virtual appliance that aggregates and normalizes NetFlow data?

- A. Flow Collector
- B. Stealthwatch Management Center
- C. UDP Director
- D. Flow Sensor

Answer: (SHOW ANSWER)

NEW QUESTION: 36

Which Cisco solution falls under cloud security?

- A. Identity Services Engine
- B. Firepower Threat Defense
- C. Cisco Defense Orchestrator
- D. Umbrella

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION: 37

Which two Cisco products are a part of the "endpoints" threat-centric solution module? (Choose two)

- A. Cisco Umbrella
- B. Cisco Defense Orchestrator
- C. Cisco VPN 3000
- D. Cisco Stealthwatch
- E. Cisco AMP for Endpoints

Answer: A,E (LEAVE A REPLY)

Explanation/Reference:

Explanation:

ASAS Security Threat Centric Solutions - AM and SE Module

NEW QUESTION: 38

Which is a component of Cisco's Web and E-mail Security Solution?

- A. Device Profiling
- B. Next Generation Intrusion Prevention System
- C. Next Generation Firewall
- D. DNS-Layer security

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Security Web and Email SE Module 2

NEW QUESTION: 39

Which feature of CTA can separate statistically normal traffic from anomalous traffic?

- A. URL filtering
- B. Trust modeling
- C. Anomaly detection
- D. Event classification

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module 6

NEW QUESTION: 40

How does AMP's device trajectory capabilities help address customer's issues?

- A. It determines the scope and cause of an outbreak and tracks suspicious files
- B. It searches for potential threats based on identified activities and behaviors
- C. It isolates suspicious files and runs them in a sandbox environment to determine their authenticity
- D. It analyses the data from suspicious files to provide a new level of threat intelligence

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module 6

NEW QUESTION: 41

What is a key feature of Cisco Cloudlock Data Loss Prevention?

- A. Reduces cost with easy implementation and installation
- B. Provides in depth cloud app analytics and tracking

- C. Allow organizations to retroactively identify malware within their environment
- D. Includes 70+ out of the box policies for enforcement, such as PCI, HIPAA, etc

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION: 42

Which feature of Cisco AnyConnect allows pre-login authentication using windows machines, or single sign-on user authentication using Windows logon credentials?

- A. Secure Layer-2 Network Access
- B. Flexible AAA Options
- C. Differentiated Mobile Access
- D. Trusted Network Detection

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Policy and Access SE Module 5

NEW QUESTION: 43

Which are two main features of ASA v and NGFW v? (Choose two)

- A. File trajectory
- B. API-based management
- C. File reputation
- D. Agile provisioning

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Security NGFW and NGIPS SE Module 4

NEW QUESTION: 44

Which three options are attack vectors protected by Web Security? (Choose three)

- A. Endpoints
- B. Mobile
- C. Offline Devices
- D. Backups
- E. Voicemail
- F. Web

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

NEW QUESTION: 45

Which three values are provided by NGFW and NGIPS in the "Campus NGFW" use case?
(Choose three.)

- A. Identity Services Engine
- B. Differentiated Mobile Access
- C. Additional firewalls across all platforms
- D. Flexible AAA Options
- E. Dynamic routing port to meet all network needs.
- F. High throughput maintained while still protecting domain against threats

Answer: B,E,F (LEAVE A REPLY)

NEW QUESTION: 46

Which of AMP's File capabilities deals with the problem of files passing through perimeter defenses that are later discovered to be a threat?

- A. Dynamic Analytics
- B. Trajectory
- C. Malware Security
- D. File Retrospection

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Tracks the spread of any file within your network and continuously monitors file reputation over time. If a file reputation changes to malicious or is found by file sandboxing to be malicious, AMP provides retrospective alerting in the after phase. AMP identifies every instance of the file within your network to address the problem of malicious files passing through perimeter defenses that are later deemed a threat.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_011101.pdf

Valid 500-651 Dumps shared by ExamDiscuss.com for Helping Passing 500-651 Exam!
ExamDiscuss.com now offer the **newest 500-651 exam dumps**, the ExamDiscuss.com 500-651 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 500-651 dumps with Test Engine here:

<https://www.examdiscuss.com/Cisco/exam/500-651/premium/> (90 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 47

Which feature of AnyConnect provides you the ability to identify data breaches as they happen?

- A. Flexible AAA Options
- B. Network Visibility Module
- C. Differentiated Mobile Access
- D. Trusted Network Detection

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Policy and Access SE Module 5

NEW QUESTION: 48

Which are three main elements of the Cloud App Security? (Choose three.)

- A. Cloud Data Loss Prevention
- B. DNS 2-Layer Protection
- C. User and Entity Behavior Analytics
- D. Rapid Breach Remediation
- E. Apps Firewall

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 49

Which feature discovers and controls malicious cloud apps connected to the corporate environment?

- A. Cognitive Threat Analytics
- B. Cloudlock
- C. Investigate
- D. Umbrella

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation:

Cisco Cloudlock Apps Firewall discovers and controls malicious cloud apps connected to your corporate environment, and provides the world's largest crowd-sourced security solution to identify individual app risk, using our Community Trust Rating.

Reference: <https://www.cloudlock.com/platform/app-discovery/>

NEW QUESTION: 50

Which is a Cisco solution that features retrospective security?

- A. AMP for Endpoint
- B. Cisco Defense Orchestrator
- C. Umbrella
- D. Investigate

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION: 51

Which three options does Cisco provide customers in terms of "Visibility and Control" against today's threats? (Choose three)

- A. Granular device visibility and management
- B. Unparalleled network and endpoint visibility
- C. Bandwidth Utilization Monitoring
- D. 18-month device release cycle
- E. Fast device policy updates
- F. Comprehensive policy enforcement

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 52

Which option helps customers gain insight into security threats?

- A. Share sensitive data across different platforms
- B. Providing visibility into everything to allow granular security policies to be created and, enforced
- C. Providing remote access VPN to allow mobile users to connect securely to customers network
- D. Limit volume of users to applications

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 53

Which is a feature of E-mail Security?

- A. Umbrella
- B. Layer-4 Monitoring
- C. Outbreak Filters
- D. Investigate

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 54

Which options describes how Cisco solutions enable customer's businesses?

- A. Automating the security intelligence updates
- B. Their ability to keep customers networks more secure and make IT more productive
- C. Enhancing remediation operations
- D. Having the fastest threat identification

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 55

Which are two main features of Advanced Malware Protection? (Choose two)

- A. Leverages Global Threat Intelligence to provide zero-day protection
- B. Threat protection across the entire attack continuum
- C. User and Entity Behavior Analytics
- D. Rapid App Containment

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

ASAS Security Advanced Threats SE Module 6

NEW QUESTION: 56

How does AMP's file reputation feature help customers?

- A. It automatically detects polymorphic variants of known malware
- B. It increases time to detection with exact data analytics
- C. It increases the protection to systems with exact fingerprinting
- D. It enables secure web browsing with cognitive threat analytics

Answer: (SHOW ANSWER)

Explanation/Reference:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_011101.pdf

Valid 500-651 Dumps shared by ExamDiscuss.com for Helping Passing 500-651 Exam! ExamDiscuss.com now offer the **newest 500-651 exam dumps**, the ExamDiscuss.com 500-651 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 500-651 dumps with Test Engine here:

<https://www.examdiscuss.com/Cisco/exam/500-651/premium/> (90 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)