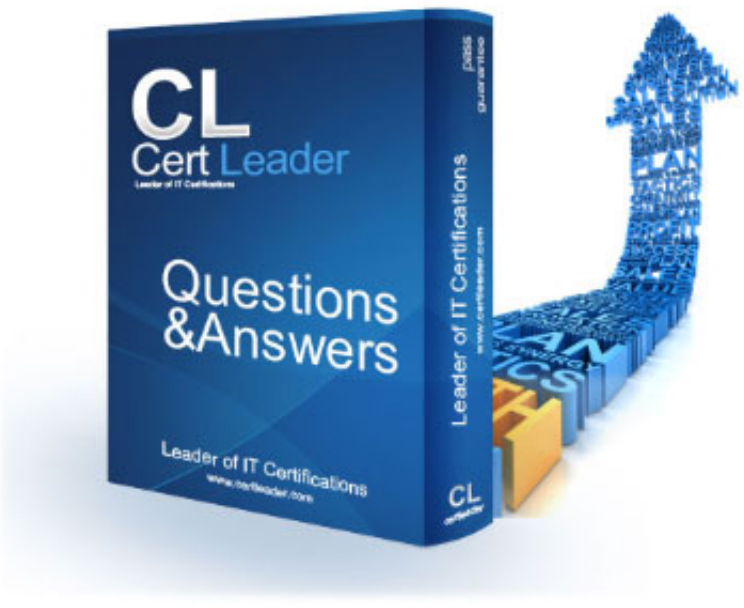
500-651 Dumps

Security Architecture for Systems Engineer

https://www.certleader.com/500-651-dumps.html



NEW QUESTION 1
Which Stealthwatch component is a physical or virtual appliance that aggregates and normalizes NetFlow data?

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

Answer: C

NEW QUESTION 2
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: BEF

Explanation: ASAS Security NGFW and NGIPS SE Module 4

NEW QUESTION 3
Which two Cisco products are part of the mobile threat-centric solution module? (Choose two.)

A. Advanced sandboxing with Threat Grid
B. Automated policy enforcement with ASAv
C. Enhanced control access with ISE and Cloudlock
D. Software-defined segmentation through TrustSec
E. Enforced device security policies with Meraki

Answer: CE

NEW QUESTION 4
What are three benefits that Cisco Umbrella brings to DNS-Layer Security? (Choose three.)

A. Helps provide breach mitigation
B. Blocks Domains/IPs associated with malware, phising, etc
C. Delivers cloud based recursive DNS
D. Provides profiling of devices
E. Logs all internet activity
F. Provides Sandboxing of malware

Answer: BCE

Explanation: ASAS Security Web and Email SE Module 2

NEW QUESTION 5
Which are two main features of Advanced Malware Protection? (Choose two.)

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

Answer: BC

Explanation: ASAS Security Advanced Threats SE Module 6

NEW QUESTION 6
Which feature in the DNS security module provide on and off network DNS protection?

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

Answer: A

NEW QUESTION 7
Which are two key Cisco benefits of the web threat-centric solution? (Choose two.)

A. Data Loss Prevention with NGFW
B. Endpoint device profiling with ISE
C. E-mail encryption with CRES
D. Malware blocking with AMP
E. Rogue web application protection through CTA

Answer: DE

Explanation: ASAS Security Threat Centric Solutions - AM and SE Module 7

NEW QUESTION 8
Which feature discovers and controls malicious cloud apps connected to the corporate environ merit?

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

Answer: C

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.

NEW QUESTION 9
Which three options ate attack vectors protected by DNS-Layer security? (Choose three.)

A. Voicemail
B. Backups
C. Web
D. E-mail
E. Cloud apps
F. Video Surveil lance

Answer: CDE

Explanation: ASAS Security Threat Centric Solutions - AM and SE Module 7

NEW QUESTION 10
Which options Cisco solutions are coveredenable customer's businesses?

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

Answer: D

NEW QUESTION 10
Employee-sponsored network access, guest access, and activity tracking are contributors to which feature of ISE?

A. Device profiting
B. Context-aware access
C. Guest access management
D. Platform exchange grid

Answer: C

Explanation: ASAS Policy and Access SE Module 5

NEW QUESTION 14
Which is a key feature of Cisco Defense Orchestra?

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

Answer: B

NEW QUESTION 16
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: D

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.

NEW QUESTION 19
Which product was covered in the Cisco Cloud App Security module?

A. Cisco NGFW
B. Cisco Defense Orchestrator
C. Cisco AMP
D. Cloud Cloudlock

Answer: D

NEW QUESTION 23
Which three options does Cisco provides 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. 18-month device release cycle
D. Bandwith Utilization Monitoring
E. Comprehensive policy enforcement
F. Fast device policy updates

Answer: ABF

NEW QUESTION 24
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: B

Explanation: ASAS Policy and Access SE Module 5

NEW QUESTION 25
Which license subscription terms are available for AMP licensing?

A. 1 month 3 months 6 months
B. 1 yea
C. 5 year
D. 10 years
E. 5 years 10 years 30 years
F. 1 yea
G. 3 year
H. 6 years

Answer: D

Explanation: ASA Security Advanced Threats SE Module 6

NEW QUESTION 26
Which are two main features of Intrusion Prevention? (Choose two.)

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

Answer: AD

NEW QUESTION 30
Which two options are attack vectors of the threat-centric defense? (Choose two)

A. Voicemail
B. Backups
C. Mobile
D. Video surveillance
E. Cloud apps

Answer: CE

NEW QUESTION 31
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: A

Explanation: ASAS Policy and Access SE Module 5

NEW QUESTION 35
What are three main challenges addressed by Cisco's cloud delivered security solutions? (Choose three.)

A. Threats are becoming too advanced tor traditional hardware
B. Solutions often require frequent hardware updates
C. Employees are unable to work remotely
D. Businesses are using email too frequently
E. Frequently installing new servers, appliances, and devices adds to the maintenance workload
F. IT staff must continuously grow with additional specializations to address the solutions

Answer: BEF

Explanation: ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION 38
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: C

Explanation: ASAS Security Advanced Threats SE Module 6

NEW QUESTION 39
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: AE

Explanation: ASAS Security Threat Centric Solutions - AM and SE Module

NEW QUESTION 43
Which are two main features of ASAv and NGFWv? (Choose two.)

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

Answer: BD

Explanation: ASAS Security NGFW and NGIPS SE Module 4

NEW QUESTION 45
Which Cisco solution features recursive DNS capabilities?

A. Cisco Defense Orchstrator
B. Identity Services Engine
C. Umbrella
D. Cognitive Threat Analytics

Answer: C

Explanation: ASAS Security Web and Email SE Module 2

NEW QUESTION 50
Which Cisco solution falls under cloud security?

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

Answer: D

Explanation: ASAS Cisco Cloud Security SE – Module 3

NEW QUESTION 53
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: D

Explanation: ASAS Policy and Access SE Module 5

NEW QUESTION 54
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: A

Explanation: ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION 59
Which is a Cisco solution features retrospective security?

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

Answer: A

Explanation: ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION 62
Which is a Cisco recommended driver for network security?

A. Offer a threat-foe used security solution
B. Provide automated impact assessment
C. Focus on point products
D. Assign central, role-based management

Answer: A

NEW QUESTION 67
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: A

Explanation: ASAS Policy and Access SE Module 5

NEW QUESTION 70
Which Cisco solution falls under Advanced Threat?

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

Answer: C

Explanation: ASAS Security Advanced Threats SE Module 6

NEW QUESTION 72
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: B

Explanation: ASAS Security Advanced Threats SE Module 6

NEW QUESTION 73
How is Cisco Security able to dynamically add IP addresses of known malware domains to its list of ports to detect and block?

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

Answer: B

Explanation: ASAS Security Web and Email SE Module 2

NEW QUESTION 76
Which feature of Cisco AnyConnect allows pie-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: A

NEW QUESTION 80
Which feature of AMP tracks the movement of a file within the environment and monitors its disposition over time?

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

Answer: A

Explanation: ASAS Security Advanced Threats SE Module 6

NEW QUESTION 83
Which three values are provided by NGFW and NGIPS in the “Campus NGFW”? (Choose three.)

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

Answer: ABD

NEW QUESTION 84
What is a main benefit of Cisco's Clouldlock Data Loss Prevention feature?

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

Explanation: ASAS Cisco Cloud Security SE - Module 3

NEW QUESTION 85
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: BCE

NEW QUESTION 86
Which TrustSec feature allows customers to simplify firewall administration, avoiding the common rule explosions that happen when new servers are onboarded?

A. Firewall administration
B. Push policies
C. Traffic tagging
D. Regulate access

Answer: C

Explanation: ASAS policy and Access SE Module 5

NEW QUESTION 87
What feature of Anti-Spam Defense determines the reputation of an e-mail?

A. IP addresses
B. Threat analysis
C. Context analysis
D. Encryption score

Answer: C

NEW QUESTION 90
Which are two main features of DDoS Attack Prevention? (Choose two)

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

Answer: AD

NEW QUESTION 91
What is a key difference between Basic Data Loss Prevention and Advanced Data Loss Prevention?

A. Providing content analysis
B. Instant visibility
C. Dynamic outbreak considerations
D. Ability to filter in real-time

Answer: C

NEW QUESTION 95
What are two key points of the Cisco Security and Threat Landscape module? (Choose two.)

A. The Cisco Security Solutions Portfolio drives customer business outcomes by providing threat-centric defense, visibility and control, and flexible solutions
B. The threat landscape is expanding, becoming more complex, and threats are increasingly costing more to customers
C. The Cisco Security Solutions Portfolio stops all threat from entering a customers network.
D. Customers need several solutions to protect their environment.

Answer: AB

Explanation: ASAS Security NGFW and NGIPS SE Module 4

NEW QUESTION 98
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: ACF

Explanation: ASAS Security Advanced Threats SE Module 6

NEW QUESTION 103
Which Cisco product is a part of the Data Center threat centric solution?

A. Cloudlock
B. Cisco Defense Orchestrator
C. NGFWv
D. Meraki MX

Answer: C

Explanation: ASAS Security Threat Centric Solutions - AM and SE Module 7

NEW QUESTION 108
Which are three main features of the Meraki MX discussed in Cloud App Security module? (Choose three)

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

Answer: CEF

NEW QUESTION 110
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: BC

NEW QUESTION 113
Which three are deployment options for E-mail Security? (Choose three.)

A. ESA
B. CES

C. WSAv
D. AMP
E. ESAv
F. WebRoot

Answer: ABE

NEW QUESTION 118
Which options describes how Cisco solutions enable customer's businesses?

A. Enhancing remediation operations
B. Having the fastest threat identification
C. Automating the security intelligence updates
D. Cisco platforms are open, agile and expandable

Answer: D

NEW QUESTION 123
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: D

Explanation: ASAS Security Web and Email SE Module 2

NEW QUESTION 124
How many web requests does Talos process per month?

A. 1.5 million
B. 100,000
C. 130 billion
D. 130 million

Answer: C

Explanation: ASAS Cisco Security and Threat Landscape Module 1

NEW QUESTION 127
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: B

Explanation: ASAS Security Web and Email SE Module 2

NEW QUESTION 132
Which Cisco Product is integrated with the AnyConnect Web Security Module?

A. Cisco Stealthwatch
B. Cisco Defense Orchestrator
C. Cisco Cloud Web Security
D. Cisco Email Security Appliance

Answer: C

Explanation: ASAS Policy and Access SE Module 5

NEW QUESTION 136
Which three features provided by NGFW and NGIPS support the Internet Edge' use case? (Choose three.)

A. Supports High Availability
B. Support for profiling devices
C. Supports dynamic routing protocols such as OSPF or BGP
D. Support for Platform exchange grid

E. Support for High Bandwith environments
F. Support for integrated posture assessment

Answer: ACE

NEW QUESTION 141
Which two features are provided by ISE? (Choose two.)

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

Answer: AD

NEW QUESTION 143
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: B

Explanation: ASAS Security Advanced Threats SE Module

NEW QUESTION 146
Which are three key features or benefits of DNS-layer security? (Choose three.)

A. Real-time sandboxing
B. Identify the internet infrastructure used for attacks
C. Uncover current & emergent threats
D. Protect any device on or off the network
E. Data Loss Prevention
F. Retrospective Analysis

Answer: BCD

NEW QUESTION 151
Which option helps customers gain insight into security threats?

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

Answer: D

NEW QUESTION 152
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: DEF

NEW QUESTION 154
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 500-651 Exam with Our Prep Materials Via below:

https://www.certleader.com/500-651-dumps.html