CISCO 300-215

Cisco CyberOps Professional Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

300-215

Cisco Certified CyberOps Specialist - CyberOps Forensic Analysis and Incident Response

55-65 Questions Exam – Variable (750-850 / 1000 Approx.) Cut Score – Duration of 90 minutes

Table of Contents:

Discover More about the 300-215 Certification

Are you interested in passing the Cisco 300-215 exam? First discover, who benefits from the 300-215 certification. The 300-215 is suitable for a candidate if he wants to learn about CyberOps. Passing the 300-215 exam earns you the Cisco Certified CyberOps Specialist - CyberOps Forensic Analysis and Incident Response title.

While preparing for the 300-215 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The 300-215 PDF contains some of the most valuable preparation tips and the details and instant access to useful **300-215 study materials just at one click.**

Cisco 300-215 CyberOps Professional Certification Details:

Exam Name	Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps
Exam Number	300-215 CBRFIR
Exam Price	$300 USD
Duration	90 minutes
Number of Questions	55-65
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	**Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)**
Exam Registration	**PEARSON VUE**
Sample Questions	**Cisco 300-215 Sample Questions**
Practice Exam	**Cisco Certified CyberOps Specialist - CyberOps Forensic Analysis and Incident Response Practice Test**

300-215 Syllabus:

Section	Weight	Objectives
Fundamentals	20%	- Analyze the components needed for a root cause analysis report - Describe the process of performing forensics analysis of infrastructure network devices - Describe antiforensic tactics, techniques, and procedures

Section	Weight	Objectives
		- Recognize encoding and obfuscation techniques (such as, base 64 and hex encoding) - Describe the use and characteristics of YARA rules (basics) for malware identification, classification, and documentation - Describe the role of: • hex editors (HxD, Hiew, and Hexfiend) in DFIR investigations • disassemblers and debuggers (such as, Ghidra, Radare, and Evans Debugger) to perform basic malware analysis • deobfuscation tools (such as, XORBruteForces, xortool, and unpacker) - Describe the issues related to gathering evidence from virtualized environments (major cloud vendors)
Forensics Techniques	20%	- Recognize the methods identified in the MITRE attack framework to perform fileless malware analysis - Determine the files needed and their location on the host - Evaluate output(s) to identify IOC on a host • process analysis • log analysis - Determine the type of code based on a provided snippet - Construct Python, PowerShell, and Bash scripts to parse and search logs or multiple data sources (such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, AMP for Network, and PX Grid) - Recognize purpose, use, and functionality of libraries and tools (such as, Volatility, Systernals, SIFT tools, and TCPdump)
Incident Response Techniques	30%	- Interpret alert logs (such as, IDS/IPS and syslogs) - Determine data to correlate based on incident type (host-based and network-based activities) - Determine attack vectors or attack surface and recommend mitigation in a given scenario - Recommend actions based on post-incident analysis - Recommend mitigation techniques for evaluated alerts from firewalls, intrusion prevention systems (IPS), data

Section	Weight	Objectives
		analysis tools (such as, Cisco Umbrella Investigate, Cisco Stealthwatch, and Cisco SecureX), and other systems to responds to cyber incidents - Recommend a response to 0 day exploitations (vulnerability management) - Recommend a response based on intelligence artifacts - Recommend the Cisco security solution for detection and prevention, given a scenario - Interpret threat intelligence data to determine IOC and IOA (internal and external sources) - Evaluate artifacts from threat intelligence to determine the threat actor profile - Describe capabilities of Cisco security solutions related to threat intelligence (such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, and AMP for Network)
Forensics Processes	15%	- Describe antiforensic techniques (such as, debugging, Geo location, and obfuscation) - Analyze logs from modern web applications and servers (Apache and NGINX) - Analyze network traffic associated with malicious activities using network monitoring tools (such as, NetFlow and display filtering in Wireshark) - Recommend next step(s) in the process of evaluating files based on distinguished characteristics of files in a given scenario - Interpret binaries using objdump and other CLI tools (such as, Linux, Python, and Bash)
Incident Response Processes	15%	- Describe the goals of incident response - Evaluate elements required in an incident response playbook - Evaluate the relevant components from the ThreatGrid report - Recommend next step(s) in the process of evaluating files from endpoints and performing ad-hoc scans in a given scenario - Analyze threat intelligence provided in different formats (such as, STIX and TAXII)

Broaden Your Knowledge with Cisco 300-215 Sample Questions:

Question: 1

Over the last year, an organization's HR department has accessed data from its legal department on the last day of each month to create a monthly activity report.

An engineer is analyzing suspicious activity alerted by a threat intelligence platform that an authorized user in the HR department has accessed legal data daily for the last week.

The engineer pulled the network data from the legal department's shared folders and discovered above average-size data dumps. Which threat actor is implied from these artifacts?

a) privilege escalation
b) internal user errors
c) malicious insider
d) external exfiltration

Answer: c

Question: 2

Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

a) process injection
b) privilege escalation
c) GPO modification
d) token manipulation

Answer: a

Question: 3

What is a concern for gathering forensics evidence in public cloud environments?

a) High Cost: Cloud service providers typically charge high fees for allowing cloud forensics.
b) Configuration: Implementing security zones and proper network segmentation.
c) Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.
d) Multitenancy: Evidence gathering must avoid exposure of data from other tenants.

Answer: d

Question: 4

A security team received an alert of suspicious activity on a user's Internet browser. The user's anti-virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address.

Which two actions should be taken by the security analyst with the executable file for further analysis?

(Choose two.)

a) Evaluate the process activity in Cisco Umbrella.
b) Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).
c) Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).
d) Analyze the Magic File type in Cisco Umbrella.
e) Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Answer: b, c

Question: 5

An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

a) An engineer should check the list of usernames currently logged in by running the command $ who | cut – d' ' -f1| sort | uniq
b) An engineer should check the last hundred entries of a web server with the command sudo tail -100 /var/ log/apache2/access.log.
c) An engineer should check the services on the machine by running the command service -status-all.
d) An engineer should check the server's processes by running commands ps -aux and sudo ps -a.

Answer: b

Question: 6

Which information is provided bout the object file by the "-h" option in the objdump line command objdump –b oasys –m vax –h fu.o?

a) bfdname
b) debugging
c) headers
d) help

Answer: c

Question: 7

A security team detected an above-average amount of inbound tcp/135 connection attempts from unidentified senders. The security team is responding based on their incident response playbook.

Which two elements are part of the eradication phase for this incident?

(Choose two.)

a) anti-malware software
b) data and workload isolation
c) centralized user management
d) intrusion prevention system
e) enterprise block listing solution

Answer: c, d

Question: 8

What is the function of a disassembler?

a) aids performing static malware analysis
b) aids viewing and changing the running state
c) aids transforming symbolic language into machine code
d) aids defining breakpoints in program execution

Answer: a

Question: 9

A security team receives reports of multiple files causing suspicious activity on users' workstations. The file attempted to access highly confidential information in a centralized file server.

Which two actions should be taken by a security analyst to evaluate the file in a sandbox?

(Choose two.)

- Inspect registry entries
- Inspect processes.
- Inspect file hash.
- Inspect file type.
- Inspect PE header.

Answer: b, c

Question: 10

What is the steganography anti-forensics technique?

a) hiding a section of a malicious file in unused areas of a file
b) changing the file header of a malicious file to another file type
c) sending malicious files over a public network by encapsulation
d) concealing malicious files in ordinary or unsuspecting places

Answer: d

Avail the Study Guide to Pass Cisco 300-215 CyberOps Professional Exam:

- Find out about the 300-215 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **300-215 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the 300-215 training. Joining the Cisco provided training for 300-215 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **300-215 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. 300-215 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

Passing the 300-215 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.