CISCO 300-215

Cisco CyberOps Professional Certification Questions & Answers

Exam Summary – Syllabus – Questions

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:

Know Your 300-215 Certification Well:

The 300-215 is best suitable for candidates who want to gain knowledge in the Cisco CyberOps. Before you start your 300-215 preparation you may struggle to get all the crucial CyberOps Professional materials like 300-215 syllabus, sample questions, study guide.

But don't worry the 300-215 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the 300-215 syllabus?
- How many questions are there in the 300-215 exam?
- Which Practice test would help me to pass the 300-215 exam at the first attempt?

Passing the 300-215 exam makes you Cisco Certified CyberOps Specialist - CyberOps Forensic Analysis and Incident Response. Having the CyberOps Professional certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Cisco 300-215 CyberOps Professional Certification Details:

Exam Name	Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps
Exam Code	300-215
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 - 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

Section	Weight	Objectives
		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 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

Section	Weight	Objectives
		files from endpoints and performing ad-hoc scans in a given scenario - Analyze threat intelligence provided in different formats (such as, STIX and TAXII)

Cisco 300-215 Sample Questions:

Question: 1

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: 2

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.)

a) Inspect registry entries
b) Inspect processes.
c) Inspect file hash.
d) Inspect file type.
e) Inspect PE header.

Answer: b, c

Question: 3

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: 4

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: 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

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: 8

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

Question: 9

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: 10

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

Study Guide to Crack Cisco CyberOps Professional 300-215 Exam:

- Getting details of the 300-215 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 300-215 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Cisco provided training for 300-215 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 300-215 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 300-215 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for 300-215 Certification

Make NWExam.com your best friend during your Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps exam preparation. We provide authentic practice tests for the 300-215 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual 300-215 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the 300-215 exam.

Start online practice of 300-215 Exam by visiting URL
https://www.nwexam.com/cisco/300-215-conducting-forensic-analysis-and-incident-response-using-cisco-technologies-cyberops