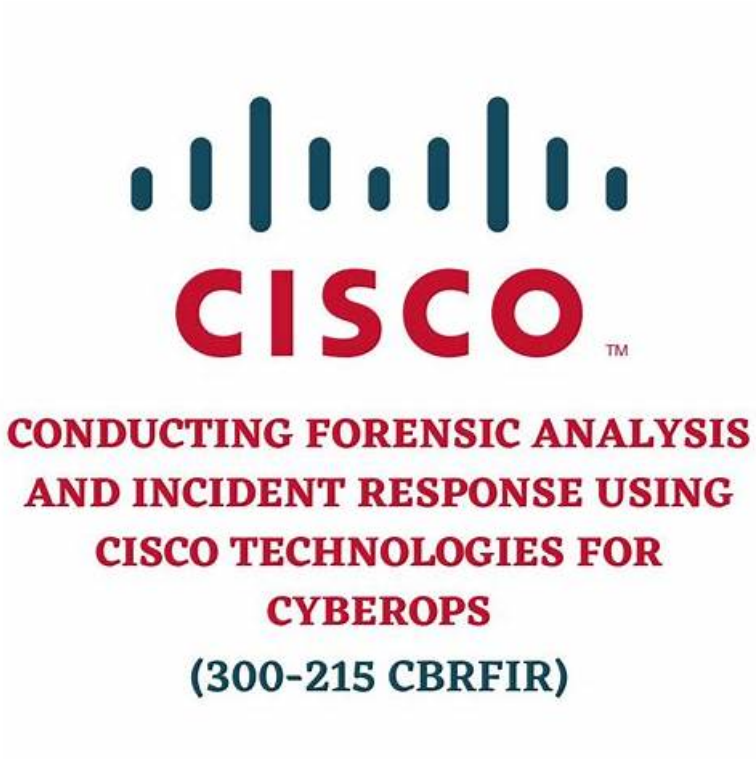
# 2025 Cisco Unparalleled 300-215: Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps Authorized Certification




DOWNLOAD the newest ValidDumps 300-215 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1iAxGh_RmjjfC94TNdm3ZZ0yHBzES_ka4

We stick to the principle "Credit management first and first class service". While purchasing our 300-215 exma questions, not only you have no need to worry about the quality of our 300-215 exam materials quality but also our service is satisfying on the 300-215 study guide. We promise buyers “Pass Guaranteed” and we only offer the latest 300-215 Training Materials. If you would like to choose safely high passing rate of 300-215 exam torrent materials, our 300-215 learning guide will be the first choice for you.

Cisco 300-215 Exam is a certification exam conducted by Cisco. It is a professional-level exam designed for candidates who want to gain expertise in conducting forensic analysis on Cisco technology-based infrastructures as well as to investigate security incidents. 300-215 exam serves as an essential tool for IT professionals to develop their knowledge and skills in conducting comprehensive network forensic analysis.

## Certification Path for Conducting Forensic Analysis and Incident Response Using Cisco CyberOps Technologies (CBRFIR)

This exam is designed for individuals seeking a role as an associate-level cybersecurity analyst and IT professionals desiring knowledge in Cybersecurity operations or those in pursuit of the Cisco Certified CyberOps Associate certification including:

- Current IT professionals
- Students pursuing a technical degree
- Recent college graduates with a technical degree

It has no pre-requisite.

**>> 300-215 Authorized Certification <<**

# Newest 300-215 Authorized Certification - Best Accurate Source of 300-215 Exam

Our 300-215 exam prep boosts many merits and useful functions to make you to learn efficiently and easily. Our 300-215 guide questions are compiled and approved elaborately by experienced professionals and experts. The download and tryout of our 300-215 torrent question before the purchase are free and we provide free update and the discounts to the old client. Our customer service personnel are working on the whole day and can solve your doubts and questions at any time. so you can download, install and use our 300-215 Guide Torrent quickly with ease.

## Cisco Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps Sample Questions (Q81-Q86):

**NEW QUESTION # 81**
Refer to the exhibit.

What is the indicator of compromise?

- A. MD5 file hash
- B. indicator ID: malware--a932fcc6-e032-476c-826f-cb970a569bce
- C. SHA256 file hash
- D. indicator type: malicious-activity

**Answer: C**

Explanation:
The STIX data structure shows apatternfield with this entry:
file:hashes.'SHA-256' = '3299f07bc0711b3587fe8a1c6bf3ee6cbcc14cb775f64b28a61d72ebcb8968d3' This value is aSHA-256 file hash, a well-knownindicator of compromise (IoC)for identifying malicious files.
Therefore, the correct answer is:
A). SHA256 file hash.

**NEW QUESTION # 82**
An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)

- A. Format the workstation drives.
- B. Restore to a system recovery point.
- C. Take an image of the workstation.
- D. Disconnect from the network.
- E. Replace the faulty CPU.

**Answer: C,D**

Explanation:
When suspicious activity is detected on a workstation, immediate steps need to be taken to preserve evidence and prevent further compromise:
* Disconnecting the system from the network (C)is crucial to stop potential exfiltration of data or ongoing communications with a command-and-control server. This isolation prevents further spread or damage while preserving the state of the compromised system for further investigation.
* Taking an image of the workstation (E)is part of the forensics acquisition process. It involves creating a bit-by-bit copy of the system's disk, which preserves all evidence in its current state. This allows for thorough forensic analysis without affecting the original evidence.
These steps align with the best practices outlined in the incident response and forensics processes (as described in theCyberOps Technologies (CBRFIR) 300-215 study guide). Specifically, in theIdentification and Containmentphases of the incident response cycle, it's emphasized that isolating the system and preserving evidence through imaging are critical to ensuring both containment of the threat and successful forensic investigation.
Reference:CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter: Understanding the Security Incident Response Process, Identification and Containment Phases, page 102-104.

**NEW QUESTION # 83**
What is an antiforensic technique to cover a digital footprint?

- A. authentication
- B. privilege escalation
- C. authorization
- D. obfuscation

**Answer: D**

Explanation:
Antiforensic techniques are methods attackers use to cover their tracks. According to the Cisco CyberOps curriculum, "obfuscation" refers to techniques such as encoding, encrypting, or otherwise disguising commands, payloads, or scripts to avoid detection and analysis. This is a standard antiforensic tactic used to prevent attribution and hinder forensic investigation.
Options like privilege escalation and authentication are part of attack vectors or access control and not antiforensic methods.

**NEW QUESTION # 84**
An incident response analyst is preparing to scan memory using a YARA rule. How is this task completed?

- A. XML injection
- B. deobfuscation
- C. data diddling
- D. string matching

**Answer: D**

Explanation:
YARA rules are pattern-matching rules used to identify malware based on specific strings, conditions, and binary patterns. They are most effective in memory or file scans where analysts search for known indicators or unique signatures via string matching.
Correct answer: C. string matching.

**NEW QUESTION # 85**
Which tool is used for reverse engineering malware?

- A. Wireshark
- B. SNORT
- C. NMAP
- D. Ghidra

**Answer: D**

Explanation:
Ghidrais a free and open-source software reverse engineering (SRE) suite developed by the NSA. It includes disassembly, decompilation, and debugging tools specifically designed for analyzing malware and other compiled programs.
The Cisco CyberOps guide referencesGhidraas a top tool for reverse engineering binary files during malware analysis tasks, making it ideal for understanding malicious code behavior at a deeper level.

**NEW QUESTION # 86**
.....