Latest Cisco 300-215 Exam Simulator & Exam 300-215 Tips

DOWNLOAD the newest ActualVCE 300-215 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1BwtFUxLG1sAjyyjhW2IgT_yL6B7o-PlS

ActualVCE can promise that our 300-215 training material have a higher quality when compared with other study materials. With over a decade's business experience, our 300-215 study tool has attached great importance to customers' purchasing rights all along. The 300-215 study materials of our website do not affect the user's normal working and learning, and greatly improves the utilization rate of time, killing two birds with one stone. It is no doubt that our study materials will help you pass your 300-215 Exam in a shortest time.

Cisco 300-215 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Forensics Processes	15%	- Data acquisition: memory, disk, network - Legal and compliance considerations - Evidence handling and chain of custody - Antiforensic techniques: debugging, geolocation, obfuscation
Topic 2: Malware Analysis	15%	- Static and dynamic malware analysis - Malware classification and behavior analysis - Malware family and campaign identification - Reverse engineering principles
Topic 3: Fundamentals	20%	- Root cause analysis reporting components - Evidence collection in virtualized environments - Encoding and obfuscation techniques - Network infrastructure device forensics - Antiforensic tactics, techniques, and procedures - YARA rules for malware identification and classification
Topic 4: Incident Response Techniques	30%	- Response to zero-day exploits and vulnerabilities - Post-incident analysis and improvement actions - Cisco security solutions for detection and prevention - Interpreting alerts from SIEM, IDS/IPS, syslog - Attack vector analysis and mitigation recommendations - Correlating host and network activity data - Threat intelligence interpretation: IOCs, IOAs, actor profiling

Topic 5: Forensics Techniques	20%	- Identifying Indicators of Compromise (IOC) from tools output - Forensic tools: Volatility, Sysinternals, SIFT, TCPdump - MITRE ATT&CK framework for fileless malware analysis - Script analysis (Python, PowerShell, Bash) for log processing - Host-based evidence location and collection

Exam 300-215 Tips, 300-215 Reliable Test Syllabus

Passing the 300-215 exam certification will be easy and fast, if you have the right resources at your fingertips. As the advanced and reliable website, ActualVCE will offer you the best study material and help you 100% pass. 300-215 online test engine can simulate the actual test, which will help you familiar with the environment of the 300-215 real test. The 300-215 self-assessment features can bring you some convenience. The 24/7 customer service will be waiting for you, if you have any questions.

Cisco Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps Sample Questions (Q113-Q118):

NEW QUESTION # 113
A security team needs to prevent a remote code execution vulnerability. The vulnerability can be exploited only by sending '${ string in the HTTP request. WAF rule is blocking '${', but system engineers detect that attackers are executing commands on the host anyway. Which action should the security team recommend?

- A. Enable URL decoding on WAF.
- B. Block incoming web traffic.
- C. Add two WAF rules to block 'S' and '{' characters separately.
- D. Deploy antimalware solution.

Answer: A

Explanation:
When Web Application Firewalls (WAFs) are configured to block specific patterns (like${), attackers may bypass this using URL encoding (e.g.,%24%7B). In such cases, the WAF must decode these patterns before applying matching rules. EnablingURL decodingensures the WAF recognizes encoded payloads and applies protections appropriately. This is a recommended hardening strategy against bypass techniques for command injection and remote code execution.
Reference: Cisco CyberOps v1.2 Guide, Chapter on WAFs and Input Validation Techniques.
-

NEW QUESTION # 114
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. Take an image of the workstation.
- B. Restore to a system recovery point.
- C. Replace the faulty CPU.
- D. Format the workstation drives.
- E. Disconnect from the network.

Answer: A,B

NEW QUESTION # 115
An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action

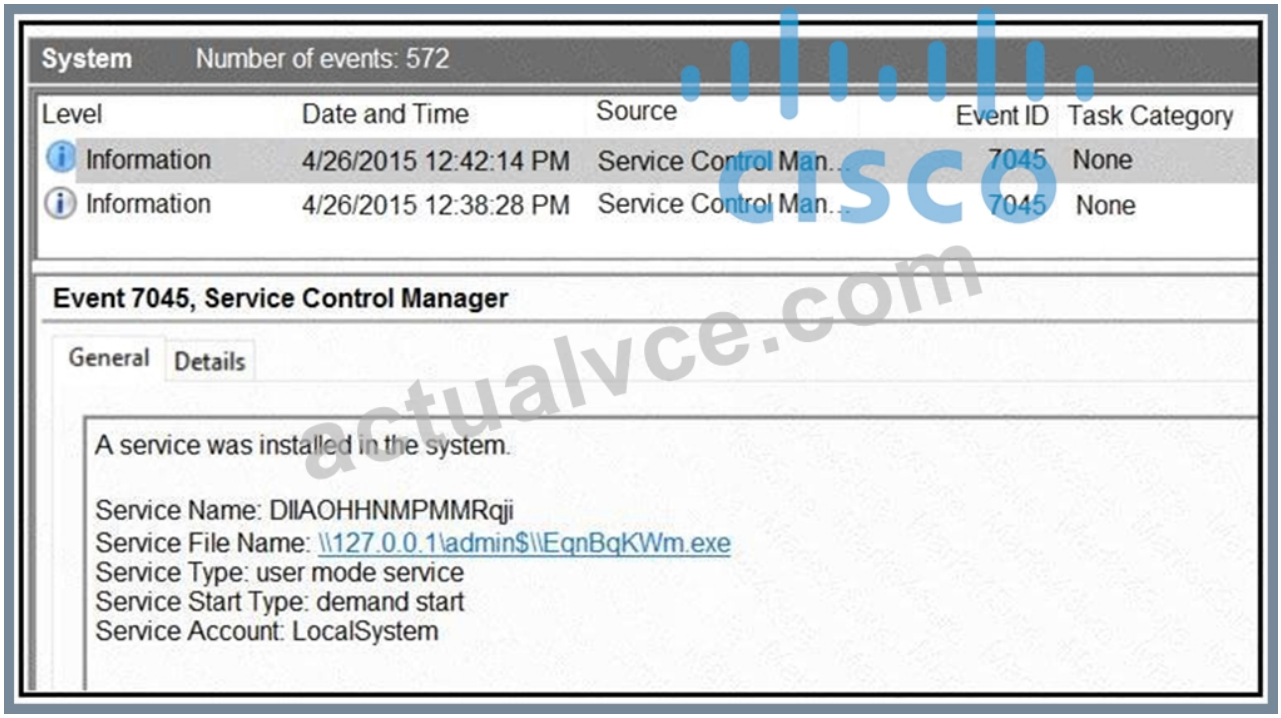
the engineer should take?

- A. Upload the file signature to threat intelligence tools to determine if the file is malicious.
- B. Investigate the sender of the email and communicate with the employee to determine the motives.
- C. Contain the threat for further analysis as this is an indication of suspicious activity.
- D. Monitor processes as this is standard behavior of Word macro embedded documents.

Answer: C

Explanation:
This behavior is consistent withmalicious macro activity. A PowerShell process being spawned fromwinword.exeviacmd.exestrongly indicates execution of an embedded script. Cisco recommends containment as a critical next step:
"Contain the threat as soon as malicious behavior is observed to prevent lateral movement or additional compromise".

NEW QUESTION # 116
Refer to the exhibit.



An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hours prior. Which two indicators of compromise should be determined from this information? (Choose two.)

- A. privilege escalation
- B. malware outbreak
- C. unauthorized system modification
- D. denial of service attack
- E. compromised root access

Answer: B,C

Explanation:
According to the event log, a suspicious service was installed (DIAOHHNMPMMRgji) with a service file pointing to a remote share (\\127.0.0.1\admin$\EqnBqKWm.exe). This type of activity strongly suggests:
* A. Unauthorized system modification: Installation of a service without proper authorization, especially with a random or obfuscated name, directly fits the description of system modification. The use of admin$ (administrative share) further implies this wasn't part of standard operations.
* E. Malware outbreak: The use of a service that points to an executable with a seemingly random name and the demand start configuration indicate a potential backdoor or remote-controlled malware. As stated in the Cisco CyberOps Associate guide, event ID 7045 with unusual service names or file paths is a strong Indicator of Compromise (IoC) for malware or persistence mechanisms.

Options like privilege escalation or DoS are not directly evidenced in the event log shown. There's no indication that the LocalSystem account was elevated beyond its default, nor that system resources were overwhelmed (as would be typical in DoS).

NEW QUESTION # 117
During a recent incident response investigation, several suspicious network connections originating from a specific host were identified. The host was quickly isolated and the machine was rebuilt During the post mortem, it became clear that there was unpreparedness regarding network artifacts necessitating adjustments to the playbooks to address this data from multiple sources must be correlated. Which two sources should be prioritized for data gathering? (Choose two.)

- A. antivirus alerts and system event togs
- B. Netflow data and host firewall logs
- C. user authentication logs and packet capture data
- D. DNS logs and web server togs
- E. application and system error logs

Answer: B,C

NEW QUESTION # 118
.....