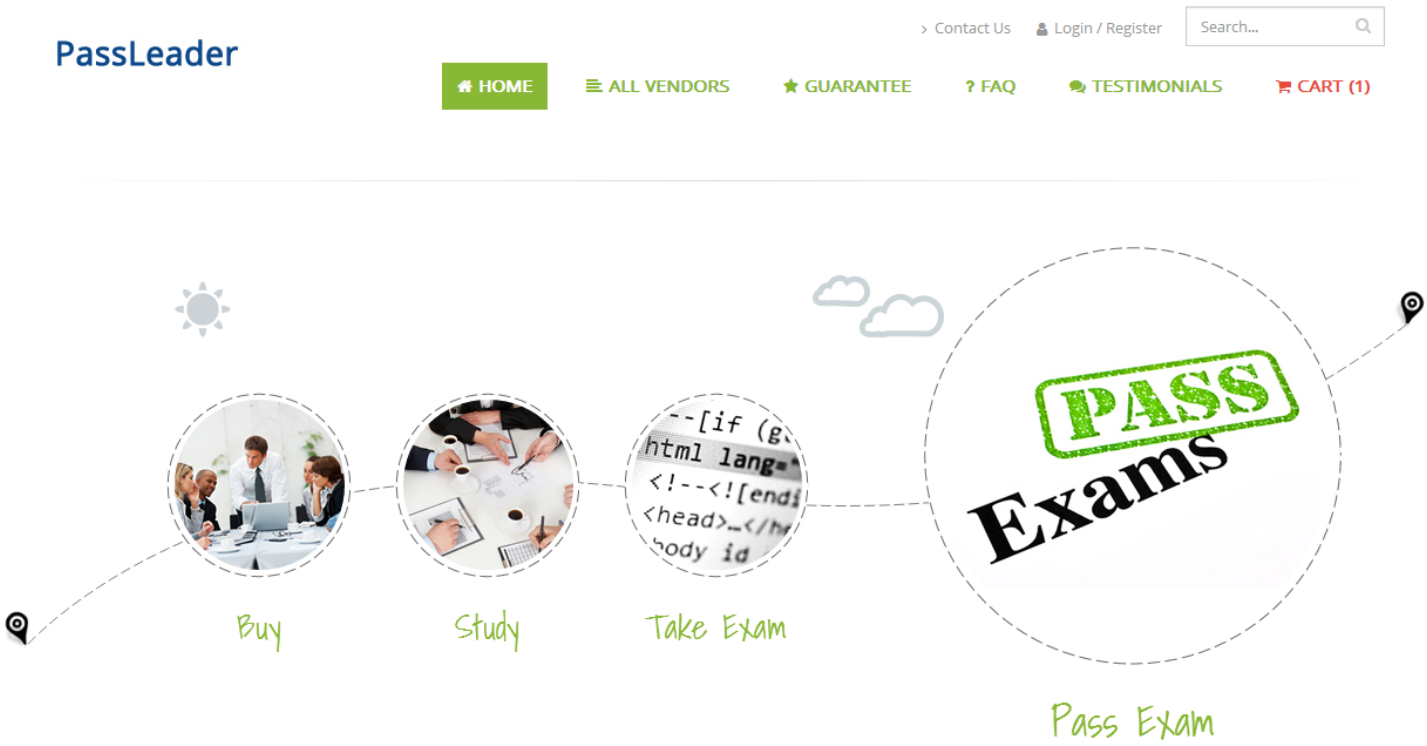
PassLeader



Try **PDF Demo** before you buy

We're not the only ones **happy** about PassLeader Practice Material ...

63159+ customers in 100+ countries use PassLeader Test Engine. Meet our customers.

VOREED GetCustom JET ORANGE iCompany Paradoxx iMessenger

http://www.passleader.top/

Latest Exam Guide & Learning Materials

Exam : **CCFR-201b**

Title : CrowdStrike Certified Falcon Responder

Vendor : CrowdStrike

Version : DEMO

NO.1 While the host timeline is comprehensive, some data is not included in that specific view. Which of the following CANNOT be seen directly from the host timeline?
A. Timestamp
B. Event Name
C. PID (Process ID)
D. CPU Temperature
Answer: D

NO.2 Within the context of CrowdStrike's behavioral detection engine, what does the acronym 'IOA' stand for?
A. Indicator of Activity
B. Indicator of Attack
C. Integrated Operation Alert
D. Internal Objective Analysis
Answer: B

NO.3 To understand how a threat moved on a system, a responder must know the role of common processes. Which of the following statements best describes the standard functionality of explorer.exe?
A. It is a system process responsible for the Local Security Authority subsystem.
B. It is the primary process responsible for the File Explorer UI and the user's desktop environment.
C. It is the Windows Command Processor used for executing batch files.
D. It is the service control manager that handles the starting of background tasks.
Answer: B

NO.4 By default, when a file is quarantined by the Falcon sensor to prevent execution, how many days does that file remain on the host's local disk?
A. 7 days
B. 14 days
C. 30 days
D. 90 days
Answer: C

NO.5 An analyst needs to quickly view the activity surrounding a suspicious process. Which of the following sequences of steps will pivot to an auto-filled process timeline in the Falcon UI?
A. Host Search > Processes and Services > Filename > Start Time > Process ID
B. Activity Dashboard > Click Detection > Export to PDF
C. Investigate > Bulk Search > Enter SHA256 > View Results
D. Configuration > Host Groups > Select Host > Network History
Answer: A

NO.6 An analyst notices a detection that has been automatically flagged with the 'New Activity' status. Which of the following statements best describes what this status indicates?

A. A brand new detection has been triggered on a host that was recently added to the network.
B. A detection that was previously moved to a resolved status has generated new telemetry and activity.
C. A user has logged into a machine for the first time since the sensor was installed.
D. The Falcon Overwatch team has manually verified that the detection is an active threat.
Answer: B

NO.7 What information does the MITREATT AND CKFramework provide?
A. It provides best practices for different cybersecurity domains, such as Identify and Access Management
B. It provides a step-by-step cyber incident response strategy
C. It provides the phases of an adversary's lifecycle, the platforms they are known to attack, and the specific methods they use
D. It is a system that attributes an attack techniques to a specific threat actor
Answer: C

NO.8 Which of the following subtitles/sub-views cannot be seen in the results of a 'Hash Search'?
A. File Metadata
B. Process Timeline
C. Intel Indicators
D. Execution History
Answer: B

NO.9 While most searches are accessible from a detection, some require a manual jump. Which search is not available as a direct pivot from a detection?
A. Host Search
B. Hash Search
C. User Search
D. IP Search
Answer: C

NO.10 When reviewing the data within a process timeline, what specific type of information is being displayed to the responder?
A. A capture of all raw network packets sent by the process.
B. All cloudable process-related events (files written, network connections, etc.) for that process in a given timeframe.
C. A list of every user who has ever logged into that specific endpoint.
D. A summary of the hardware performance metrics during the time of the detection.
Answer: B

NO.11 You notice that taskeng.exe is one of the processes involved in a detection. What activity should you investigate next?
A. User logons after the detection

B. Executions of schtasks.exe after the detection
C. Scheduled tasks registered prior to the detection
D. Pivot to a Hash search for taskeng.exe
Answer: C

NO.12 In the 'Graph View' of a detection, processes are connected by arrows. Which of the following does a yellow arrow connecting two processes indicate?
A. A standard Parent-Child relationship.
B. A Network connection was established between the two processes.
C. A Thread Injector-Injectee relationship (Process Injection).
D. A file was written by the first process and read by the second.
Answer: C

NO.13 According to the Falcon Overwatch Best Practice workflow, what is the required next step after a responder completes the 'Understand the process(es) involved' step?
A. Isolate the host to prevent lateral movement.
B. Examine what is normal for the system to identify deviations.
C. Delete the malicious file from the endpoint.
D. Pivot to the Intelligence dashboard for actor attribution.
Answer: B

NO.14 What happens when a quarantined file is released?
A. It is moved into theC:\CrowdStrike\Quarantine\Releasedfolder on the host
B. It is allowed to execute on the host
C. It is deleted
D. It is allowed to execute on all hosts
Answer: D

NO.15 During the configuration of a new IOA rule, the administrator must decide what action the sensor should take.
Which of the following is NOT a valid IOA rule action?
A. Monitor
B. Block
C. No Action
D. Kill Process
Answer: C

NO.16 Which of the following sentences best describes the technical visibility provided by the 'Host Timeline' view?
A. A list of every time a user has logged in or out of the machine.
B. Every host-relevant event (Process, File, Registry, Network) recorded in a given timeframe.
C. A history of every hardware change or driver update on the endpoint.
D. A log of every time the Falcon sensor was updated or restarted.

Answer: B

NO.17 Which statement is TRUE regarding the "Bulk Domains" search?
A. It will show a list of computers and process that performed a lookup of any of the domains in your search
B. The "Bulk Domains" search will allow you to blocklist your queried domains
C. The "Bulk Domains" search will show IP address and port information for any associated connections
D. You should only pivot to the "Bulk Domains" search tool after completing an investigation
Answer: A

NO.18 A responder is unsure about the difference between 'Detection' and 'Prevention' settings. Where can they find information about Detection and Prevention Policies?
A. On the public CrowdStrike blog.
B. In the Support page under the Docs section.
C. By clicking the 'About' button in the user profile.
D. In the training videos on the main Dashboard.
Answer: B