CrowdStrike
CCFH-202b
CrowdStrike Falcon Hunter

Latest Version: 6.0

Question: 1

What behaviors commonly indicate suspicious command prompt (cmd.exe) usage?
(Choose two)

A. Chained commands using logical operators (e.g., &&, |)
B. Execution from system32 folder under admin user
C. CMD launched with a direct connection to PowerShell
D. CMD invoked by explorer.exe during login

Answer: A,C

Question: 2

Which methods are valid to convert Unix timestamps to human-readable time in Falcon?
(Choose two)

A. Apply custom visualization template
B. Enable auto-conversion in dashboard
C. Manually divide Unix time by 1000
D. Use FORMAT_TIMESTAMP()

Answer: B,D

Question: 3

A key step in minimizing false positives is understanding the _____ in which a process executes, including user, host role, and time of execution.

A. privilege
B. signature
C. context
D. syntax

Answer: A,D

Question: 4

Which actions can be initiated directly from the detection page in Falcon to pivot into deeper investigation?
(Choose two)

A. View process details
B. Disable user account
C. Run full antivirus scan
D. Initiate Host Timeline view

Answer: A,B

Question: 5

Which scenarios justify initiating a hypothesis-driven hunt?
(Choose two)

A. Following an alert for abnormal outbound traffic to a rare domain
B. After a vendor releases a critical vulnerability with known exploits
C. To investigate hosts flagged with expired endpoint licenses
D. To verify administrative user compliance with login policy

Answer: B

Question: 6

What is the purpose of constructing complex EAM queries in the hunting process?

A. To suppress known benign alerts
B. To extract actionable insights from large volumes of endpoint telemetry/
C. To create automated remediation workflows
D. To update sensor drivers on legacy systems

Answer: C

Question: 7

Pivoting from a detection into the _____ Timeline is helpful to identify artifacts created before and after the alert was triggered.

A. Sensor
B. Audit

C. Host
D. Forensic

Answer: B

Question: 8

Why is the Events Full Reference documentation essential when reviewing unusual activity logs?

A. It allows direct editing of detection rules
B. It defines event types, fields, and expected values
C. It lists CrowdStrike partner threat feeds
D. It contains historical IOC archives

Answer: B,C

Question: 9

What actions can be taken after filtering event data in the Falcon platform?
(Choose two)

A. Build detection rules
B. Export results to CSV
C. Visualize with dashboards
D. Apply memory patching

Answer: B,C

Question: 10

When multiple domains are under investigation, analysts can utilize the _____ feature in Falcon to streamline analysis.

A. Threat Intelligence Panel
B. Domain Lookup Wizard
C. Domain Behavior Tracker
D. Bulk Domain Search

Answer: D

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer