CREST
CRIA
CREST Registered Intrusion Analyst (CRIA)

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**



Latest Version: 6.0

Question: 1

Hunting for interesting files on a charity's Windows workstation, the analyst runs dir /r in the user's Documents folder:
14/09/2026 09:12 48,210 budget-2026.xlsx
14/09/2026 09:40 22,016 minutes.docx
184,320 minutes.docx:svc.exe:$DATA
26 minutes.docx:Zone.Identifier:$DATA
What does the listing show?

A. minutes.docx was downloaded, and its Zone.Identifier stream holds the payload
B. svc.exe hidden in an alternate data stream
C. Two versions of minutes.docx, one of them an older saved copy named svc.exe
D. A macro inside minutes.docx, displayed by dir as an extracted object

Answer: B

Question: 2

Two binaries were recovered from different hosts at a utilities company. The triage output reads:
s1.exe SHA-256 4f1c…9a02 imphash 7d3e…b1c4 ssdeep 1536:Ab…
s2.exe SHA-256 c86b…e317 imphash 7d3e…b1c4 ssdeep 1536:Ab…
ssdeep comparison s1/s2: 88
How should the sample-identifier section of the malware report record them?

A. Two samples, each by its SHA-256, with the shared hashes noted as a link
B. As one sample under the shared imphash, the matching imports showing the same file on both hosts
C. As one sample under the ssdeep hash, the score of 88 marking them as identical
D. As two samples identified by MD5 alone, the imphash and fuzzy hashes being left out as unreliable

Answer: A

Question: 3

A web application on a Windows server (10.40.2.15) at a Leeds logistics firm was compromised. You have taken one line from each of three sources:
Reverse proxy access log: 14/Jul/2025:10:41:12 +0100 "POST /upload.php HTTP/1.1" 200
Security.evtx event 4688 (exported with UTC times): 2025-07-14T09:41:50Z New Process Name C:\Windows\System32\cmd.exe, Creator Process Name C:\php\php-cgi.exe

Perimeter firewall: 2025-07-14 05:42:05 ALLOW TCP 10.40.2.15:51322 -> 203.0.113.88:4444
The firewall's configuration sets its clock zone to America/New_York, and it writes local time with no offset.
Normalised to UTC, in what order did these events occur?

A. 05:42:05 outbound connection, 09:41:50 cmd.exe, 10:41:12 upload
B. 09:41:50 cmd.exe, 09:42:05 outbound connection, 10:41:12 upload
C. 09:41:12 upload, 09:41:50 cmd.exe started, 09:42:05 outbound connection
D. 08:41:50 cmd.exe, 09:41:12 upload, 09:42:05 outbound connection

Answer: C

Question: 4

Security log extracts from server DB-SRV02 (times UTC):
09:41:06 4624 Logon Type 3, Account CORP\j.okafor, Logon ID 0x3E1A2F, Source Network Address 10.30.8.21
09:41:07 4698 Subject CORP\j.okafor, Logon ID 0x3E1A2F, Task Name \UpdateCheck, Exec C:\ProgramData\uc\run.cmd, Principal UserId S-1-5-18
10:00:00 4688 Subject NT AUTHORITY\SYSTEM, New Process cmd.exe, Command Line cmd /c C:\ProgramData\uc\run.cmd, Creator Process svchost.exe
Who should the execution of run.cmd be attributed to?

A. j.okafor's network logon from 10.30.8.21, which created the task, with SYSTEM only the run-as principal
B. The SYSTEM account, as a compromised local service launched cmd.exe
C. j.okafor, sitting at the server console when cmd.exe started
D. The Task Scheduler service, as the creator of the cmd.exe process

Answer: A

Question: 5

At a housing developer, the proxy holds two requests from workstation 10.80.3.44 within the same hour:
Request 1, the user browsing the intranet:
GET / HTTP/1.1 • Host: intranet.example.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Accept: text/html,… • Accept-Encoding: gzip, deflate, br • Accept-Language: en-GB,en;q=0.9
Request 2, repeated every fifteen minutes:
GET /api/v2/task HTTP/1.0 • Host: tasks.example.net
User-Agent: identical to request 1
Connection: close • no Accept, Accept-Encoding or Accept-Language header

A colleague concludes that request 2 is the user's Chrome. Which assessment of request 2 is best supported?

A. Chrome on the host, its user-agent matching the user's browser exactly
B. Chrome running an extension that polls a task service every fifteen minutes
C. Undetermined, the user-agent being identical and headers varying by page type
D. A non-browser program copying the browser's user-agent

Answer: D

Question: 6

Dynamic analysis of a loader recovered from a manufacturer's workstation produced:
DNS query: telemetry.example.org A -> 203.0.113.77
POST http://telemetry.example.org:8080/api/v2/sync HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1)
Repeated every 300 s
Which entry should the malware report record under network indicators?

A. telemetry.example.org, 203.0.113.77, TCP 8080, POST /api/v2/sync and the exact User-Agent string
B. 203.0.113.77 on TCP 8080 alone, leaving out the domain, URI and User-Agent to keep the list short
C. example.org and the sample's SHA-256
D. Periodic HTTP POSTs every five minutes to an external web service, using an outdated Internet Explorer User-Agent

Answer: A

Question: 7

You are triaging a laptop image (evidence item EV-07, SHA-256 verified on receipt) from a law firm that suspects data exfiltration. A Prefetch parser run against the image reports:
RCLONE.EXE-6F1D3A2B.pf Run count: 4 Last run: 2025-05-06 02:13:40 UTC
Which contemporaneous note entry records this finding to the required standard?

A. Prefetch evidence of rclone execution on the laptop, several runs, last in the early hours; details to follow
B. 09:52 UTC, EV-07: Prefetch file RCLONE.EXE-6F1D3A2B.pf shows 4 runs, last 2025-05-06 02:13:40 UTC (Prefetch parser on the verified image)
C. 09:52, EV-07: RCLONE.EXE ran 4 times, last 02:13:40
D. 09:52 UTC, EV-07: the attacker used rclone overnight to exfiltrate the client files share, running it 4 times up to 2025-05-06 02:13:40 UTC per Prefetch

Answer: B

Question: 8

On 2026-05-28 the analyst reviews a direct outbound connection from the previous week:
Firewall 2026-05-21T14:03:19Z allow TCP 10.15.6.22:60311 -> 192.0.2.77:443
The internal DNS log for that host shows:
2026-05-21T14:03:17Z client=10.15.6.22 query=fonts.example.org type=A response=198.51.100.9
2026-05-21T14:03:18Z client=10.15.6.22 query=k7-relay.example.net type=A response=192.0.2.77 ttl=60
Today, a reverse lookup of 192.0.2.77 returns cdn-edge.example.net, the address serves www.example.com, and k7-relay.example.net now resolves to 203.0.113.140.
Which domain should the connection be attributed to?

A. k7-relay.example.net, the name the host resolved to 192.0.2.77 one second earlier
B. www.example.com, the site 192.0.2.77 serves today
C. cdn-edge.example.net, from the reverse lookup
D. None, as k7-relay.example.net now resolves elsewhere

Answer: A

Question: 9

The resolver log at an insurance broker shows workstation 10.15.2.90 making 40 queries in 38 seconds:
14:20:02 A qk3vzj7tmwa.example.com NXDOMAIN
14:20:03 A p0x9rrb2lyu.example.net NXDOMAIN
… 37 further queries of the same form, all NXDOMAIN …
14:20:40 A h7fa2nq0wce.example.org NOERROR 203.0.113.145
The firewall then logs 10.15.2.90:51811 → 203.0.113.145:443 allowed at 14:20:41, repeating every 60 seconds.
What does the evidence establish, and which indicator matters most for containment?

A. A mistyped search suffix producing failed internal lookups that can be ignored
B. Domain generation, with the 39 NXDOMAIN names as the C2 domains to block and sinkhole
C. Ordinary HTTPS browsing following a brief resolver outage
D. Domain generation, with 203.0.113.145 as the live C2 contact

Answer: D

Question: 10

Correlated evidence for one host at an architecture practice (UTC):
09:58:12 mail gateway delivered to knd@example.com attachment remittance.docm

10:01:40 4688 WINWORD.EXE C:\Users\knd\Downloads\remittance.docm
10:01:52 4688 powershell.exe parent WINWORD.EXE
10:02:05 proxy GET http://files.example.org/u/a.bin 200
10:02:30 AV detection C:\Users\knd\AppData\Local\Temp\a.exe
What should the malware report record as the infection vector?

A. The download of a.bin from files.example.org at 10:02:05 UTC
B. The executable a.exe, written to the user's Temp folder and detected by the AV product at 10:02:30 UTC
C. Macro-enabled attachment remittance.docm, delivered 09:58:12 UTC and opened in Word at 10:01:40
D. A PowerShell process launched by Word at 10:01:52 UTC

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/