350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is a benefit of key risk indicators?

A. clear perspective into the risk position of an organization

B. improved visibility on quantifiable information

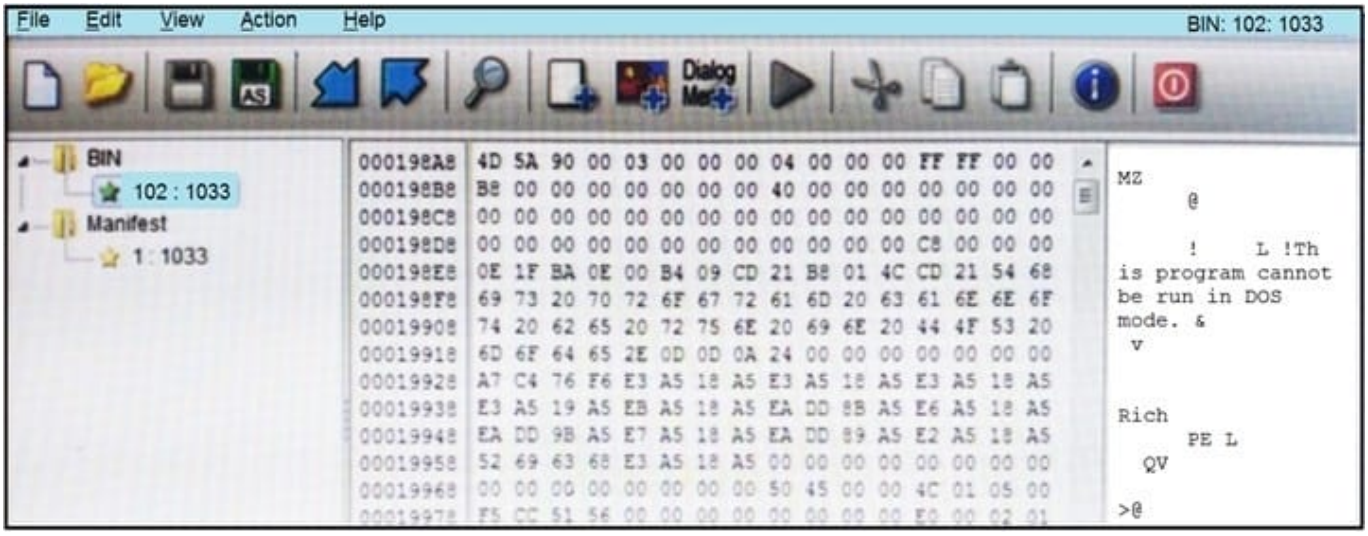
C. improved mitigation techniques for unknown threats

D. clear procedures and processes for organizational risk

Correct Answer: C

Reference: https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20(ERM)-,Overview,and%20mitigate%20them%20in%20time.

QUESTION 2



Refer to the exhibit. An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

A. a DOS MZ executable format

B. a MS-DOS executable archive

C. an archived malware

D. a Windows executable file

Correct Answer: D

Reference: https://stackoverflow.com/questions/2577545/why-is-this-program-cannot-be-run-in-dos-mode-text-present-in-dll-files#:~:text=The%20linker%20places%20a%20default,using%20the%20%2FSTUB%20linker%20option.andtext=This

%20information%20enables%20Windows%20to,has%20an%20MS-DOS%20stub.

QUESTION 3

An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

A. Modify the alert rule to "output alert_syslog: output log"

B. Modify the output module rule to "output alert_quick: output filename"

C. Modify the alert rule to "output alert_syslog: output header"

D. Modify the output module rule to "output alert_fast: output filename"

Correct Answer: A

Reference: https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256andX-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20201231%2Fuseast-1%2Fs3%2Faws4_requestandX-Amz-Date=20201231T141156ZandX-Amz-Expires=172800andX-Amz-SignedHeaders=hostandX-Amz-Signature=e122ab6eb1659e13b3bc6bb2451ce693c0298b76c1962c3743924bc5fd83d382

QUESTION 4

An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal data. Which type of attack is occurring?

A. Address Resolution Protocol poisoning

B. session hijacking attack

C. teardrop attack

D. Domain Name System poisoning

Correct Answer: D

QUESTION 5

Refer to the exhibit. An engineer is analyzing this Vlan0386-int12-117.pcap file in Wireshark after detecting a suspicious network activity. The origin header for the direct IP connections in the packets was initiated by a google chrome extension on a WebSocket protocol. The engineer checked message payloads to determine what information was being sent off-site but the payloads are obfuscated and unreadable.

What does this STIX indicate?

A. The extension is not performing as intended because of restrictions since ports 80 and 443 should be accessible

B. The traffic is legitimate as the google chrome extension is reaching out to check for updates and fetches this information

C. There is a possible data leak because payloads should be encoded as UTF-8 text

D. There is a malware that is communicating via encrypted channels to the command and control server

Correct Answer: C