NSE7_ATP-2.5 Q&As

Fortinet NSE 7 - Advanced Threat Protection 2.5

Pass Fortinet NSE7_ATP-2.5 Exam with 100% Guarantee

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

https://www.geekcert.com/nse7_atp-2-5.html

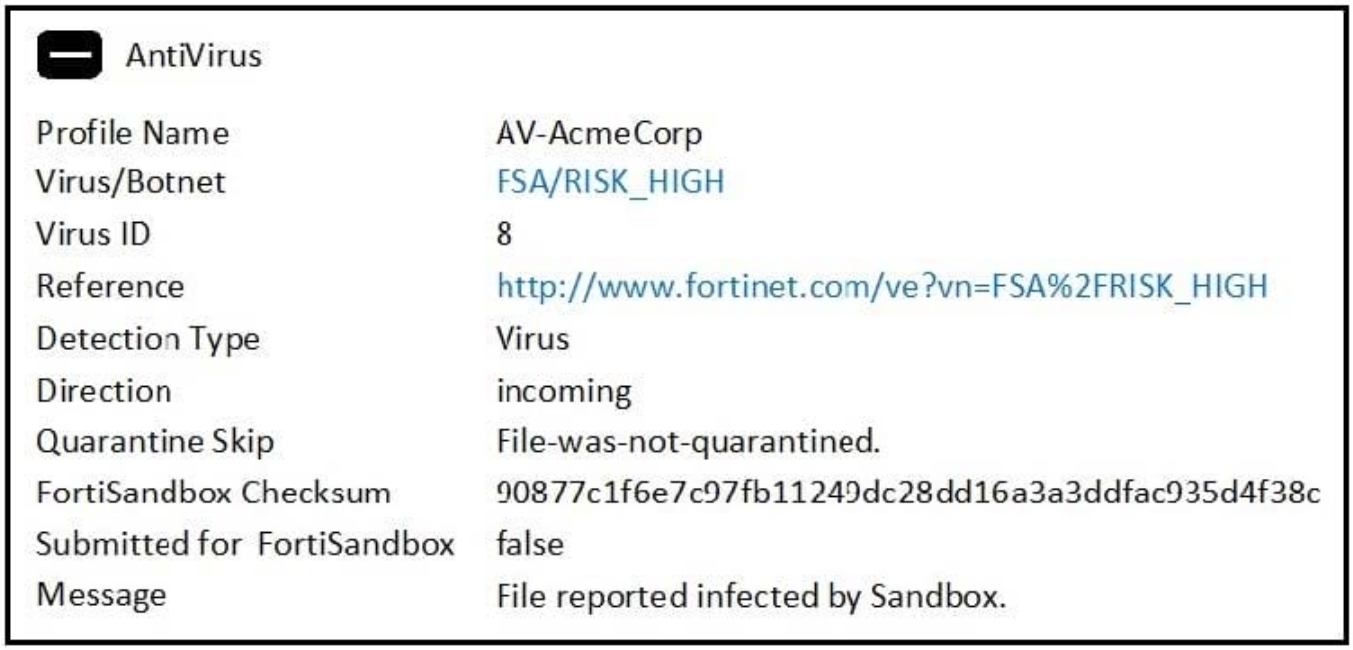
100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

Examine the FortiGate antivirus log detail shown in the exhibit, then answer the following question:


AntiVirus

Profile Name	AV-AcmeCorp
Virus/Botnet	FSA/RISK_HIGH
Virus ID	8
Reference	http://www.fortinet.com/ve?vn=FSA%2FRISK_HIGH
Detection Type	Virus
Direction	incoming
Quarantine Skip	File-was-not-quarantined.
FortiSandbox Checksum	90877c1f6e7c97fb11249dc28dd16a3a3ddfac935d4f38c
Submitted for FortiSandbox	false
Message	File reported infected by Sandbox.

Which of the following statements is true?

A. FortiGate quarantined the file as a malware.

B. The file matched a FortiSandbox-generated malware signature.

C. The file was downloaded from www.fortinet.com.

D. The FSA/RISK_HIGH verdict was generated by FortiSandbox.

Correct Answer: C

QUESTION 2

FortiSandbox generates structured threat information exchange (STIX) packages for which of the following threats? (Choose two.)

A. Botnet connections

B. Malware

C. Intrusion attempts

D. Malicious URLs

Correct Answer: AC

Reference: https://docs.fortinet.com/document/fortisandbox/3.0.3/administration-guide/170699/ioc-package

QUESTION 3

Which FortiSandbox diagnostic command should you use to diagnose Internet connectivity issues on port3?

A. ping

B. tcpdump

C. test-network

D. traceroute

Correct Answer: D

Reference: https://dokumen.tips/documents/fortios-54-cookbook-fortinet-docs-fortinetknowledgebasetechnicaldocumentation-.html

QUESTION 4

Which of the following scan job report sections are generated by static analysis? (Choose two.)

A. Office Behaviors

B. Launched Processes

C. Registry Changes

D. Virtual Simulator

Correct Answer: CD

QUESTION 5

Which of the kill chain stages does Fortinet\\'s advanced threat protection solution block? (Choose three.)

A. Command and control

B. Delivery

C. Reconnaissance

D. Lateral movement

E. Weaponization

Correct Answer: ACD

NSE7_ATP-2.5 VCE Dumps | NSE7_ATP-2.5 Practice Test | NSE7_ATP-2.5 Exam Questions