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.passapply.com/350-201.html

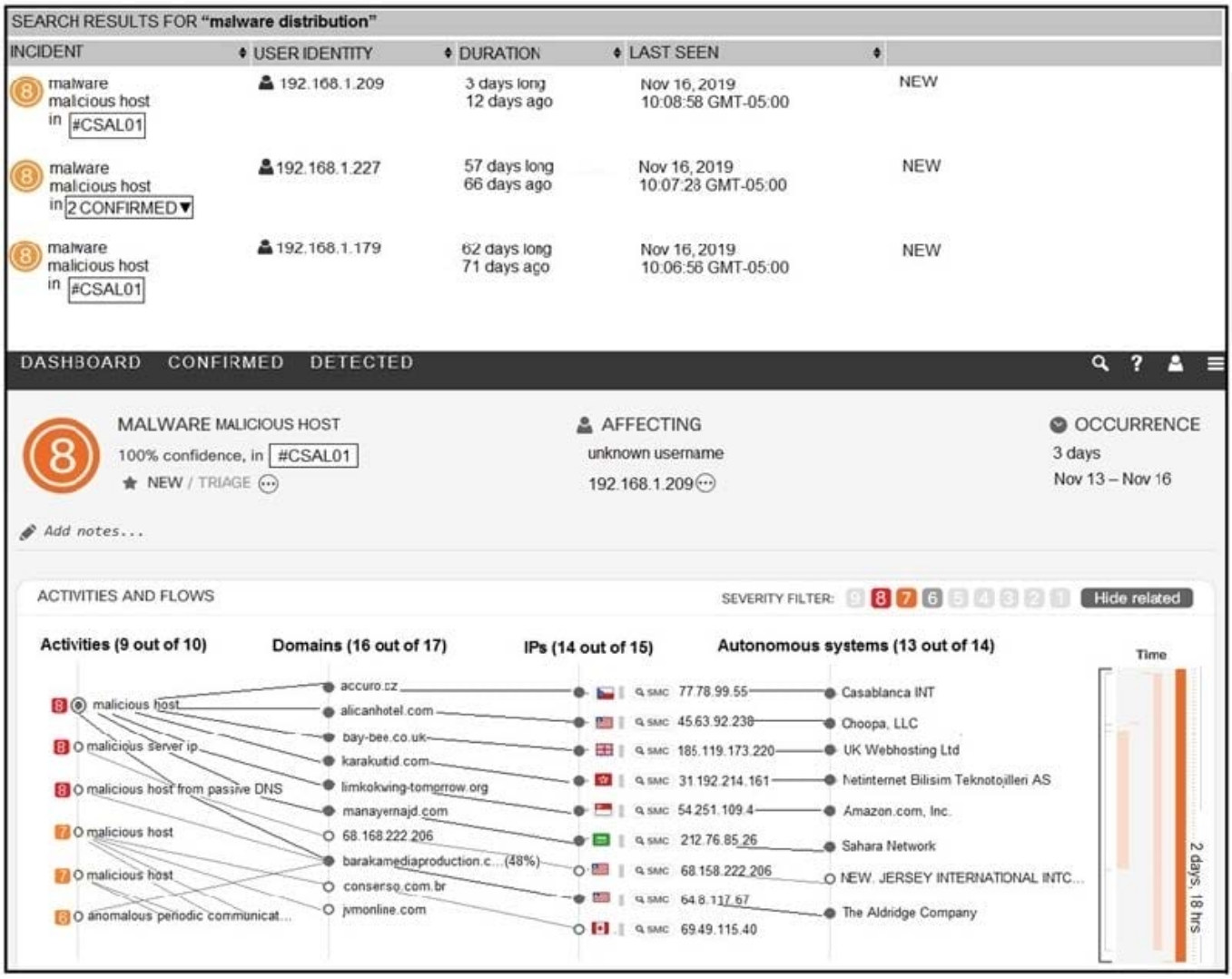
100% Passing Guarantee
100% Money Back Assurance

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

Refer to the exhibit. For IP 192.168.1.209, what are the risk level, activity, and next step?



A. high risk level, anomalous periodic communication, quarantine with antivirus

B. critical risk level, malicious server IP, run in a sandboxed environment

C. critical risk level, data exfiltration, isolate the device

D. high risk level, malicious host, investigate further

Correct Answer: A

QUESTION 2

A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

A. Assess the network for unexpected behavior

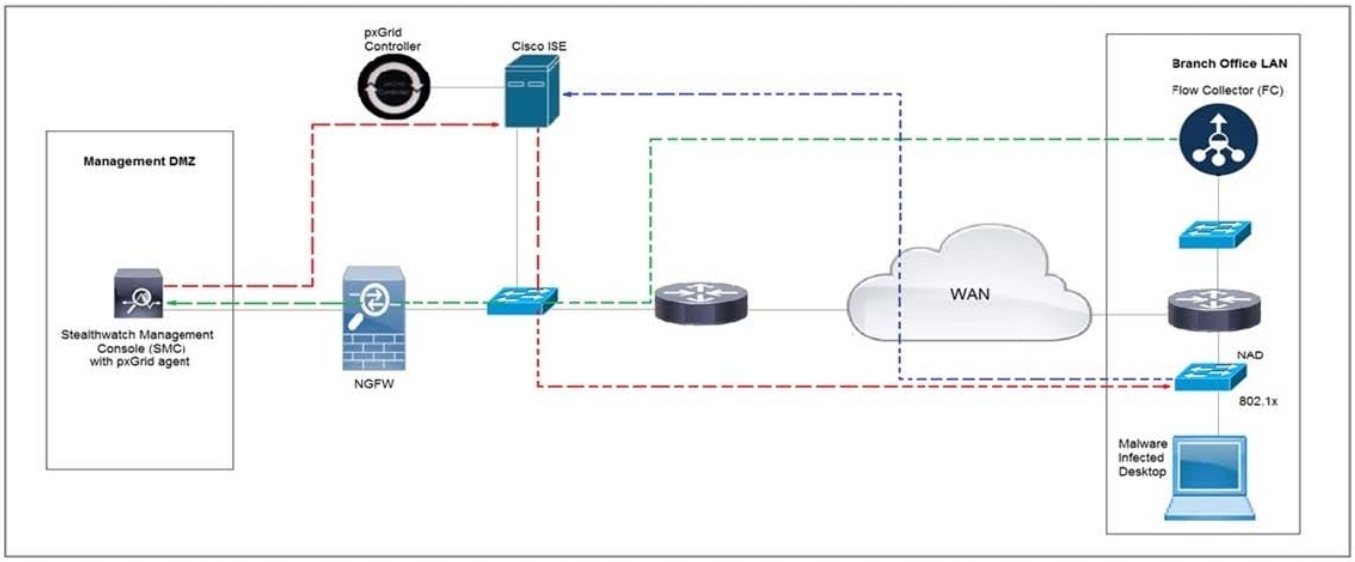
B. Isolate critical hosts from the network

C. Patch detected vulnerabilities from critical hosts

D. Perform analysis based on the established risk factors

Correct Answer: B

QUESTION 3



Refer to the exhibit. Cisco Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a Quarantine VLAN using Adaptive Network Control policy.

Which telemetry feeds were correlated with SMC to identify the malware?

A. NetFlow and event data

B. event data and syslog data

C. SNMP and syslog data

D. NetFlow and SNMP

Correct Answer: B

QUESTION 4

Refer to the exhibit. Which command was executed in PowerShell to generate this log?

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

A. Get-EventLog -LogName*

B. Get-EventLog -List

C. Get-WinEvent -ListLog* -ComputerName localhost

D. Get-WinEvent -ListLog*

Correct Answer: A

Reference: https://lists.xymon.com/archive/2019-March/046125.html

QUESTION 5

An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

A. aligning access control policies

B. exfiltration during data transfer

C. attack using default accounts

D. data exposure from backups

Correct Answer: B