24: APPLIED LAB: Incident Response: Detection

Security+ (Exam SY0-701)

8/8

Congratulations, you passed!

Duration: 18 minutes, 46 seconds

✓ What is the MITRE ATT&CK technique associated with the event with Rule ID 92652? (Enter exactly as presented under the *Name* heading on the *Details* page) *Score: 1*

Pass the Hash

Congratulations, you have answered the question correctly.

✓ What are the Technique(s) reference codes for a logon failure event? (Select two) *Score: 1*

- ☑ T1078
- ☐ T5309
- ☑ T1531
- ☐ T1507

Congratulations, you have answered the question correctly.

✓ What is the description for the security alert for the clearing of the Application and System logs? *Score: 1*

- ● The audit log was cleared
- ○ A Windows log file was cleared
- ○ Event viewer logs were cleared
- ○ A log file was cleared

Congratulations, you have answered the question correctly.

✓ What sources can be used by wazuh to detect suspicious activity? (Select all that apply) *Score: 1*

- ☑ OS logs
- ☑ application logs
- ☑ network equipment logs
- ☑ cloud logs

Congratulations, you have answered the question correctly.

☑ What was the MITRE ATT&CK tactic identified by wazuh related to the deletion of an audit log? *Score: 1*

○ Persistence
○ Privilege Escalation
○ Lateral Movement
● Defense Evasion

Congratulations, you have answered the question correctly.

☑ The phase of an Incident Response Plan that creates a record of events or notifies the security personnel about violations is? *Score: 1*

○ Analysis
● Detection
○ Eradication
○ Containment

Congratulations, you have answered the question correctly.

☑ Once the security team is made aware of a potentially violating incident, what is the next phase in Incident Response? *Score: 1*

○ Preperation
● Analysis
○ Eradication
○ Recovery
○ Lessons learned

Congratulations, you have answered the question correctly.

☑ Potential signs of security breaches or malicious activities within an IT infrastructure are known as? *Score: 1*

● IoCs (Indicators of Compromise)
○ Event records
○ False positives
○ Registry values

Congratulations, you have answered the question correctly.