SOC LAB REPORT

Cloud Security Alert Report

Task 7 – Document the Alert

Lab Name	Implement Cloud Monitoring and Alerting Using SIEM Tools
Alert ID	CLOUD-SIEM-001
Cloud Platform	AWS training environment
SIEM	Wazuh
Wazuh Server	192.168.1.69
Test User	soclab
Report Status	Resolved

Purpose

To document the cloud security alert generated when an IAM permission was changed on the authorized test account, summarize the investigation, record the defensive response, and confirm final resolution.

Authorized Training Use Only

1. Task 7 Alert Record

The following record captures the fields required by Task 7 of the lab.

Alert ID	CLOUD-SIEM-001
Alert	IAM Permission Change
User	soclab
Resource	IAM user: soclab
Source IP	49.207.12.34
Severity	High (Wazuh rule level 10)
Action	AttachUserPolicy
Response	Temporary lab permission removed using DetachUserPolicy
Status	Resolved

2. Alert Detection

Detection rule: Custom Wazuh rule 100201

Detection condition: AWS CloudTrail event AttachUserPolicy affecting the test IAM user soclab.

Cloud log source: AWS CloudTrail logs collected by Wazuh from the configured cloud logging pipeline.

Observed alert: Wazuh generated a high-severity alert indicating that an IAM policy was attached to the test user soclab.

3. Investigation

The generated alert was opened in Wazuh and reviewed using the available CloudTrail event metadata. The investigation focused on the identity involved, source address, affected IAM resource, API action, event time, and alert severity.

Item	Observed Value	Analyst Interpretation
User identity	soclab	Authorized lab test identity
Source IP	49.207.12.34	Source recorded by CloudTrail
Affected resource	IAM user soclab	Target of the permission change
Cloud action	AttachUserPolicy	Permission was attached to the test user
Policy	SoclabLabDescribeEC2	Temporary lab policy used for testing
Region	ap-south-1	AWS Asia Pacific (Mumbai) training region
Wazuh severity	Level 10 / High	Alert requires analyst review

Classification: Suspicious Test Activity. In a production environment, an unexpected IAM permission attachment could indicate privilege manipulation or unauthorized access. In this lab, the event was intentionally generated in the authorized training environment to validate SIEM detection and investigation.

4. Defensive Response

The temporary IAM permission added for the test was removed after the alert was investigated. The response was verified through the corresponding AWS CloudTrail/Wazuh event.

Step	Response Action	Result
1	Reviewed the IAM permission attached to soclab.	Test policy identified.
2	Removed the temporary SoclabLabDescribeEC2 policy.	Permission reverted.
3	Verified the DetachUserPolicy activity in centralized cloud logs.	Response recorded in Wazuh.
4	Continued SIEM monitoring for additional IAM permission changes.	No further suspicious test change observed.

5. Finding Summary

Alert: Unauthorized IAM Permission Change (simulated)

Detection: Wazuh generated an alert when the AttachUserPolicy CloudTrail event matched the custom cloud detection rule for the soclab test account.

Investigation: The user, source IP, timestamp, affected IAM resource, API action, policy, AWS region, and severity were reviewed in the SIEM.

Response: The temporary permission was removed and the DetachUserPolicy response event was verified.

Status: Resolved

6. Conclusion

The cloud monitoring and alerting workflow operated successfully. AWS activity was collected through CloudTrail, processed by Wazuh, and evaluated by the custom detection rule. The IAM permission change generated a high-severity alert, the event was investigated using centralized cloud metadata, and the temporary permission was removed. The lab therefore demonstrated the complete detect → investigate → respond workflow required by the exercise.

7. Recommendations

- Continue monitoring IAM permission changes and other administrative CloudTrail events in Wazuh.
- Use least-privilege permissions for cloud users and service accounts.
- Enable MFA for cloud identities wherever supported by the training environment and production policy.
- Review unexpected AttachUserPolicy, DetachUserPolicy, PutUserPolicy, and privilege-related actions promptly.
- Retain CloudTrail logs in centralized storage long enough to support investigations and audit requirements.

8. Task 7 Completion Checklist

Requirement	Status
Alert ID recorded	Complete
Alert name recorded	Complete
User and resource identified	Complete
Source IP recorded	Complete
Severity recorded	Complete
Permission-change action documented	Complete
Defensive response documented	Complete
Final status recorded	Resolved

9. Analyst Sign-Off

Analyst / Student	_____
Date	_____
Instructor / Reviewer	_____