Log Analysis Technology through Account Management Incident Analysis in OpenStack-based Cloud Environment

Yunyoung Jung, Minhui Seo, Yeeun Kim, Jungjoo Oh,
Il-Gu Lee, Seongmin Kim and Wonhyung Park*

Department of Convergence Security Engineering, Sungshin Women's University, Republic of Korea.
{20211097, 20211066, 220224005, winteroot,
iglee, sm.kim, whpark}@sungshin.ac.kr

Abstract

Recently, as infrastructure operations have begun to shift from on-premises to the cloud, cyberattacks have also increased dramatically in the cloud environment. As this has emerged as a new security issue, it is necessary to analyze logs in the cloud environment differently from those in the on-premises environment. This paper analyzes account management hacking incidents, which account for the largest proportion of hacking incidents in the cloud environment and proposes a new log analysis technique.

Keywords: Cloud Incident Analysis, Account Management, Log Analysis

1 Introduction

Recently, digital transformation has been accelerated by artificial intelligence and metaverse environments, changing the way IT infrastructure is operated. These changes have led to new security challenges, as cloud computing environments, unlike on-premises environments, distribute roles and responsibilities between cloud service providers (CSPs) and users, increasing new security threats. As result, it is necessary to analyze security incidents for these new threats with new technique in the cloud environment differently from those in the on-premises environment. Therefore, we propose a log analysis technique to analyze and effectively respond to hacking incidents caused by account management, which accounts for the largest proportion of cloud security incidents.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No. P-8
*Corresponding author: Department of Convergence Security Engineering, Sungshin Women's University, Republic of Korea, Seoul, 02844, Email: 20211097@sungshin.ac.kr

2 Analyzing of Hacking Incidents

Security incidents due to lack of identity, credential, and access management (account management) have been consistently occurring since before 2016 and account for the highest percentage of incidents. Therefore, we analyzed account management cases from the perspective of log analysis with CloudTrail.

2.1 Incident Case Analysis of Account Management Vulnerability

Table 1 : CloudTrail Analysis Results

Action log	Action Description	Number of calls	Time	Charged	Etc
event_id.iaas.**floating_ip.attach**	Associate Instance Floating IP	2	**12:49:52** **12:50:07**	Unable to verify	-
event_id.iaas.**floating_ip.create**	Create Floating IP	2	**12:49:10** **12:49:14**		
event_id.iaas.**instance.create**	Create Instance	2	**12:48:19** **12:48:58**	Unable to verify	-
event_id.iaas.**keypair.create**	Create Keypair	1	**12:47:48**	-	-
event_id.iaas.**project_selected**	Access the project	2	**12:46:57** **12:57:48**	-	-

1. At 12:46, access to the project by an unauthorized person was confirmed.
2. A PEM key for instance access was created at 12:47.
3. Two instances were created over approximately 40 seconds from 12:48, and at 12:49, two floating IP connections were created, and instance connection was performed.

2.2 Log Analysis Technology through Accident Analysis

Besides the examples, the logs in the table below can be used for incident analysis. CloudTrail allows you to check specific event logs to understand the attack behavior of an instance, but it is difficult to check events that occur within an instance. Therefore, after identifying malicious behavior with these logs, tracking malicious activity inside an instance should be done in the same way as on-premises.

Table 2 : Specific Logs Utilized in Incident Analysis

Action log	Action Description	Action log	Action Description
event_id.iaas.**instance.create**	Create Instance	event_id.iaas.**floating_ip.create**	Create Floating IP
event_id.iaas.**instance.delete**	Delete Instance	event_id.iaas.**floating_ip.attach**	Associate Instance Floating IP
event_id.iaas.**project_selected**	Access a project	event_id.iaas.**keypair.create**	Create Keypair
event_id.iaas.**metadata.create**	Initialize Windows PW	event_id.iaas.**security_group.create**	Create Security Group
event_id.iaas.**image.create**	Create Image	event_id.iaas.**security_group.delete**	Delete Security Group
event_id.iaas.**image.delete**	Delete Image	event_id.iaas.**floating_ip.delete**	Delete Floating IP
event_id.iaas.**image.update**	Change Image Information	event_id.iaas.**keypair.delete**	Delete Keypair
event_id.iaas.**instance.update**	Change Instance Information		

3 Conclusion

In order to react quickly when an incident occurs, you need to anticipate the flow by checking behavior against specific logs in CloudTrail, then verify the infection with security equipment, and track the malicious behavior by checking in-instance logs.

References

[1] NIST(2020.08), *NIST Cloud Computing Forensic Science Challenges*, NIST IR 8006
[2] CSA(2021), *Cloud Incident Response Framework*, pp 1-36.
[3] Pichan, A. and Lazarescu, M. andSoh, S.T.(2018), *Towards a practical cloudforensics logging framework*, Journal of Information Security andApplications, vol. 42, pp. 18-28.