Utilizing Cloud Computing Log Events for Security Automation

by

Khalid Farrag

A creative component submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

Master of Science

Major: Information Assurance

Program of Study Committee:

DOUG JACOBSON, Major Professor

The student author, whose presentation of the scholarship herein was approved by the program of study committee is solely responsible for the content of this dissertation. The Graduate College will ensure this creative component is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2019

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

NOMENCLATURE

AWS	Amazon Web Services
VM	Virtual Machines
SDK	Software Development Kit
JSON	JavaScript Object Notation
SOC	Service Organizations Control
HTTPS	Hypertext Transfer Protocol Secure
SNS	Simple Notification Service
IAM	Identity and Access Management

ACKNOWLEDGMENTS

I would like to thank my major professor, Doug Jacobson, for his guidance and support throughout the course of this research.

ABSTRACT

The rising use of cloud computing and deploying and managing applications and services on a large-scale demand researcher to utilize cloud-logs to achieve greater continuous of security and compliance. Cloud security auto-remediation not only essential for preventing a potential breach, but also essential to prevent system frailer or accidents, and for complying with compliance requirements or legal actions. However, now most of cloud hosting services provide cloud trails or logs to identify and track security incidents. But that isn't enough without acting at the event time.

In this research, I present a novel approach for automatic security remediation that can be built from a noisy and unstructured cloud logs. The approach utilizing cloud trails logs. Examining the records syntax will provide the complete picture of actions taken by a user, role, captured API calls for systems events.

Also, it is necessary to understand how log events can be constructed to build a strong remediation policy. In some parts, cloud providers have had little incentive to provide broad administrative access to the set of information, and that often do not provide the adequate log that can be used for security auditing or compliance. However, the ultimate goal of this research is to connect the dots of deferent events to build a strong cloud security auto-remediation policy.

CHAPTER 1. INTRODUCTION: STATEMENT OF THE PROBLEM

Introduction to Cloud Computing

For many years, individuals use different ways of dealing with information, writes them in long pages, storing them in data centers or recently in the cloud. In today world the off-premise term is shifting our direction towards Cloud Computing. The term cloud computing is not just accessing a storage device through the internet, but it is a way of reaching data or application over the Internet. Cloud computing enables convenient, on-demand network access to a shared pool of configurable computing resources, servers, storage, applications, and services. With all those different models of cloud computing, one of the most important first step is understanding what the cloud types are. In general, there are three primary cloud delivery models IaaS, PaaS, and SaaS:

Platform as a Service (PaaS):

Platform as a Service is a mechanism for combining infrastructure as a Service (IaaS) with an abstracted set of middleware services, software development, and deployment tools that allow the organization to have a consistent way to create and deploy applications on a cloud or on-premises environment [21]. PaaS is mainly being used for applications, for example like AWS Elastic Beanstalk, Google App Engine, Heroku, etc.

Software as a Service (SaaS):

In this model, the cloud provides the user with access to varieties of databases, software, and applications. According to Wikipedia SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee. In the SaaS model, cloud providers install and operate application software in the cloud and

cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. [20]

Infrastructure as a Service (IaaS):

On this project, our main focus is utilizing infrastructure as a Service (IaaS) cloud services model. The IaaS model is the common usable cloud version for most business and government sectors. Also, this model is agile and enables users with great infrastructure assets to analyze the log and build an effective auto-remediation policy.

The National Institute of Standards and Technology defines IaaS as the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. According to Zeal Vora on his book *Enterprise Cloud Security and Governance* "the consumer does not control the underlying infrastructure, such as virtualization software, physical security, and hardware. It is the cloud provider's responsibility to handle the reliability of hardware and virtualization software used and the physical security of the servers" [1].

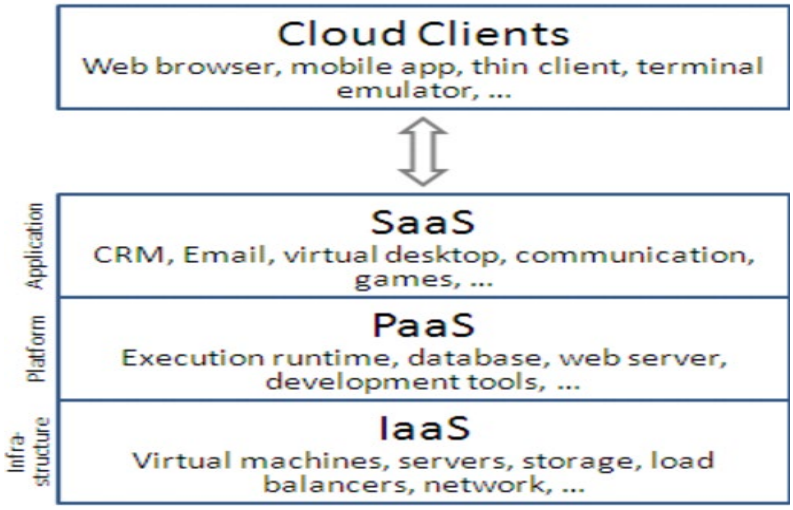


Figure (1.1): Cloud Computing Service Models [2]

Security Concerns

For many businesses leaving private data centers and move Public clouds is considered a risky operation. A recent study performed by Tim Greene showed that overall, security concern was the major deterrent to adoption, with 41% of respondents indicating it's a worry. But nearly as many, 40%, say cost is a concern as well. Coming in a distant third with 26% was privacy and compliance concerns [19].

Security is considered a key requirement for cloud computing consolidation as a robust and feasible multi-purpose solution [2]. The complexity of cloud computing requires many organizations to utilize multi-tools environments to monitor and fix the cloud security risks.

However, the increasing demand on the cloud computing has led to a huge investment from security companies to digest and analyze security logs to identified security holes and offer possible solutions. Amazon Web Services (AWS) for example provides Security Hub that is designed to accommodate users with a high-level security view. Security Hub is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Security Hub [3]. However, Security Hub provides a solution for the obvious security incidents, but it lacks the dedication of zero-day vulnerabilities. It also comes with a huge cost that isn't always suitable for small businesses.

To maintain high level of security, availability and reliability, AWS has designed it is environment to log most of the actions that are happening on the cloud. This log is very critical to build a strong remediation policy. However, the log files itself are generated in many different formats by a plethora of devices and software. The analysis of log files comes with some extra challenges. Since many systems are distributed and heterogeneous, logs

from a number of components must be correlated first. Moreover, maybe there are missing, duplicate or misleading data that make log analysis more complex or even impossible [4]. In Infrastructure as a Service like on AWS the extraction and analysis of the log file is based on CloudTrail or VPC Flow Logs, that consist of aggregation and correlation of streaming data from multiple sources.

In general, the advance on cloud technology opens the door for more dependable security automation. The availability and a better understanding of the log data can be used to enhance our security automation. Therefore, this will lead to more cloud usage and lower security operation costs.

Security Operation Costs

Cloud computing technology allows users to build resources and expand their operations quickly. With new features and extended functionality of cloud computing, the developing teams increase the speed by adding new services to the environment. That has led to creating new security holes. Therefore, this comes with an additional security operations cost that grows day after day.

CHAPTER 2. LOG ANALYSIS IN THE CLOUD

What is a Log in the Cloud?

In computing, a log file is a file that records either events that occur in an operating system or other software runs [5]. The log in cloud computing has the same functionally which used for automatically captures the type, content, or time of transactions made by a user using the cloud system. Overall in a computer system the log "analysis (or system and network log analysis) is an art and science seeking to make sense out of computer-generated records (also called log or audit TrailRecords). [6]. In a short explanation the log is like a text message that is being generated by the systems based on an event.

Log analysis is an effective approach to illustrate usage patterns, in particular how users interact with digital libraries. Digital libraries were not frequently used compared with other types of online resources, especially in the early age of digital library development. In a study in 1996, 35% of users accounted for 80% of the usage. [7].

Log Integrity

Log integrity can be questioned when a malicious user is able to modifies or intercepted the log file, this will significantly impact the forensic work. The threat arises when messages are intercepted and altered by a malicious service agent, thereby potentially compromising the message's confidentiality and or integrity [8]. Several researchers as Josiah Dykstra and Alan T. Sherman [8] have indicated that evidence acquisition is a critical issue with cloud forensics. The malicious actor can change the evidence to clear the tracks of the attack. Figure (2.1) shows an attack that carried by an intermediary hacker.

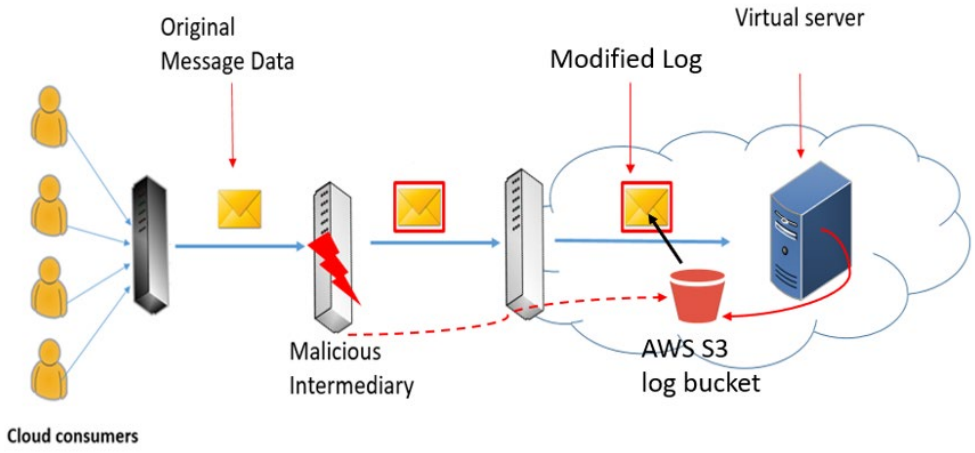


Figure (2.1): Log Integrity

Challenges of volatility can affect the integrity of the log file. The volatility refers to the loss of content in memory or storage when the power is turned off. This is a big issue from a forensic point of view because if the server goes down, all processes in memory and CPU will disappear. This problem increases in complexity when the case involves Virtual Machines (VM). For example, IaaS VM have no persistent storage; therefore, all volatile data may be lost if the VM goes down [9]. This problem has been reported as a zero-day vulnerability on AWS could environment. In particular, when AWS hypervisor allows an untrusted EC2 instance to read the memory of neighbor instance.

Processing the Log on Cloud Computing

In the cloud environment, the log is often stored and delivered to virtual storages or buckets. On AWS the users can provide log files from multiple regions to a single S3 bucket for a separate account. When using CloudTrail, any event occurs that matches our trails settings it will be delivered to Amazon S3 bucket and Amazon CloudWatch Logs log group. It is essential to understand that we need all cloud logs should be preconfigured before any

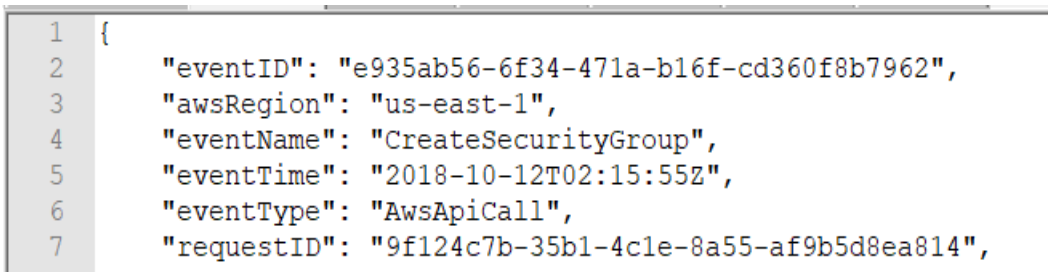
work on the automation policy. The following trails options provide by AWS to cover all logs events:

- Data events: These events provide insight into the resource operations performed on or within a resource. These are also known as data plane operations.
- Management events: Management events provide insight into management operations that are performed on resources in [the] AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account. [10]

Analyzing a Log file on AWS

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. [11]

The CloudTrail stored on JSON format. The log use file name that consist of "account ID, CloudTrail, region name, and unique string file name format." The log file can be delivered to Amazon S3 bucket. The log consists of multi-attributes and array data types corresponding to different events. Figure (2.2) shows a log file example of a security event.



```
{
    "eventID": "e935ab56-6f34-471a-b16f-cd360f8b7962",
    "awsRegion": "us-east-1",
    "eventName": "CreateSecurityGroup",
    "eventTime": "2018-10-12T02:15:55Z",
    "eventType": "AwsApiCall",
    "requestID": "9f124c7b-35b1-4c1e-8a55-af9b5d8ea814",
```

Figure (2.2): Log Example

On this JSON format, the “eventID” represents a particular event. The ID is a unique identifier for each event. The “awsRegion” refers to the region where our services are deployed.

CHAPTER 3. CLOUD COMPUTING SECURITY AUTOMATION

Security automation is about letting machines do the task instead of human work. But, overall, security automation is about 10 years behind the automation of other technology processes, said Ariel Tseitlin, partner at Foster City, Calif.-based investment firm Scale Venture Partners. Cloud security automation, on the other hand, is requiring integrated functions to automate tasks across products through workflows, while also allowing for end-user oversight and interaction. Neely continues that more automation enables the SOC to stay abreast of endpoint-related threats, while addressing a major issue cited by respondents: Lack of staffing and resources to manage and monitor their many endpoint-related toolsets [14].

Why do we need automation?

Security automation can be used to eliminate the use of repeated security tasks. If we do all of [security work] manually, it will take more time, and there will also be a chance of human error. So, we automate the repetitive set of tasks to hasten the process and save some time as well as repetitive tasks [22]. From a cloud security standpoint, there many easy tasks that can be automated, like upgrading a firewall rule on specific incidents or blocking some services from communicating based on specific log criteria. This automation will also limit the human error on those easy tasks.

Data loss and leak on the cloud is a common security risk; the data cloud be deleted by mistake, an unauthorized user or attacker. Data loss can have a significant damage on an organization; especially when there isn't any backup. For a business standpoint, data leakage is an important, especially when it contains a sensitive information or company secrets. Through virtualization technologies an operating system can be repeatedly booted from exactly the same image on a variety of machines. By simply changing the one image, many

machines can be modified to address patching issues, apply configuration changes, or do wholesale operating system upgrades. In the event of a compromise, virtualization allows sysadmins to quickly recover to a known good state. [12]. Let's summarize the benefits of automation:

- Time and cost saving
- Faster deployment and delivery
- Elimination of the chance of human error
- Improved collaboration
- Easy to implement security [22]

To conclude, besides all the mention benefits of the security automation building auto-remediation environment offers brief answers to prevent and remediate the cloud security issues by analyzing and incorporate virtualization security incidents logs. Also, Security automation in cloud computing, could, in theory, enable organizations to investigate incoming threats and react to them quickly, without human intervention, at least, for the most popular, labor-intensive types of attacks. That also can save a lot of time and effort to recover from a potential attack.

Security Automation Using Open Sources and Commercial Tools

Many different open-source tools offer solutions to auto remediate security risks such as T-Mobile’s "PacBot" and Netflix’s Security Monke. For example, the PacBot platform continuous security and compliance assessment. It also offers reporting functionality. However, AWS and some other cloud service provider, have the perfect environment to host the open-source tools. Some of those security tools are heavily driven by small, serverless resources to automate security, which is suitable to work on most cloud environments.

On the other hand, many commercial tools can be obtained to help automate security work. They can help with speeding the process of detecting and take actions, but they still have drawbacks. With better learning the log analysis concept and the cloud environment, commercial tools can give outstanding results and save a lot of time and effort for the security teams. Commercial tools also would address some open-source tools problems like lack of support and outdating problems.

CHAPTER 4. CLOUD SECURE CONFIGURATION GUIDELINES

Security automation is critical factor to mitigate cloud risks. The diversity and quantity of endpoints in the modern enterprise are driving the need for more automation and predictive capabilities [13]. Generally, the auto-remediation policy should follow International Organization for Standardization (ISO) recommendation, which to outline the required steps to investigate process classes and activities. In general, the log provided by the cloud service provider consists of a series of timed events that can be scaled against ISO recommendations. ISO/IEC 27037 has published seven activities that are essential for the forensic investigation. Those play a major rule of defining a sold security automation policy. The security incident investigation would start with examining the condition before the incident takes place, then followed by what changed after the event. The following Figure (4.1) shows the activities before and after an incident has been identified.

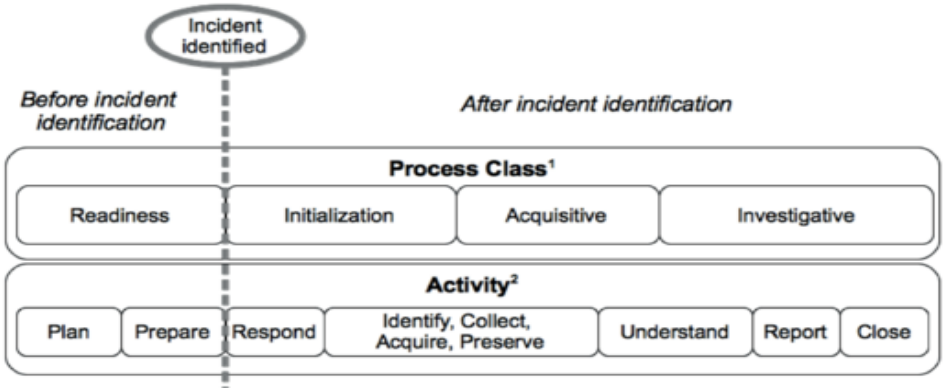


Figure (4.1) Investigation Process Classes and Activities [10]

IT open standards play critical rule for security engineers to set up an effective automation policies and procedures. Therefore, major cloud platforms like AWS are complying with standard like ISO 9001:2015 to maintain feature's ability to satisfy the requirements of confidentiality, availability, integrity, and security.

Once the system administrator understands the security goals [or standards], she must then map these goals into the configuration of all the servers. This requires first knowing the configuration state of each system, and then understanding how to modify the configuration to meet the desired goals [12].

AWS Secure Configuration Guidelines

AWS, for example, provides prescriptive guidance for configuring AWS security. AWS follows CIS benchmarks, which "consensus based secure configuration guidelines applicable to a variety of operating systems, middleware and software applications, and network devices, designed to assess Member's network cybersecurity [16]. The CIS Amazon Web Services Foundations focus on foundational, testable, and architecture agnostic settings. The CIS document covers the following:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- AWS CloudWatch
- AWS Simple Notification Service (SNS)
- AWS Simple Storage Service (S3)
- AWS VPC (Default) [16]

CHAPTER 5. AUTOMATION POLICY ARCHITECTURE

Policy Architecture

Cloud architecture applies various components in terms of resources, software capabilities, and applications. Architecture mainly is a precise method to integrate different key elements to show how our environment documented and constructed. On this project, I aim to simplify the definition of many policy components as well as the relationships between them. I propose a modified solution to setup an automated response to an event that occurs within a CloudTrail event. The automatic response is generated from a Python Lambda function by utilizing AWS Config rules that will automatically update the effected resources.

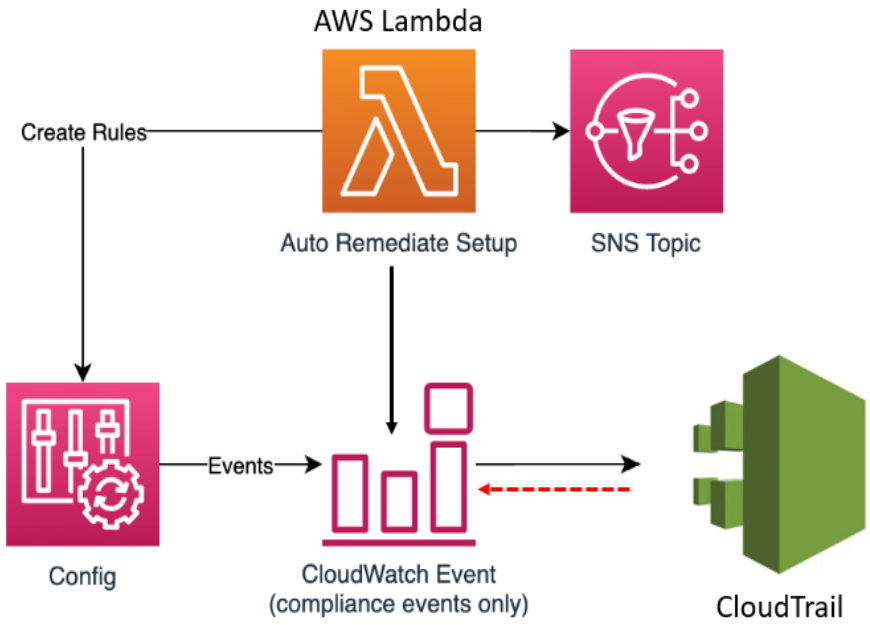


Figure 5.1: Policy Architecture

Lambda Function

AWS Lambda is a serverless compute service that runs your code in response to events and automatically manages the underlying compute resources for you. You can use AWS Lambda to extend other AWS services with custom logic or create your own back-end services that operate at AWS scale, performance, and security [15]. Figure (5.2) show the first part of lambda function, which is responsible of calling the configuration rule "MY_POLICY_RULE." Lambda is using BOTO3, which is the Amazon Web Services software development kit (SDK). That allows python developers to write software, which makes use of services like Amazon EC2 or AWS Config.

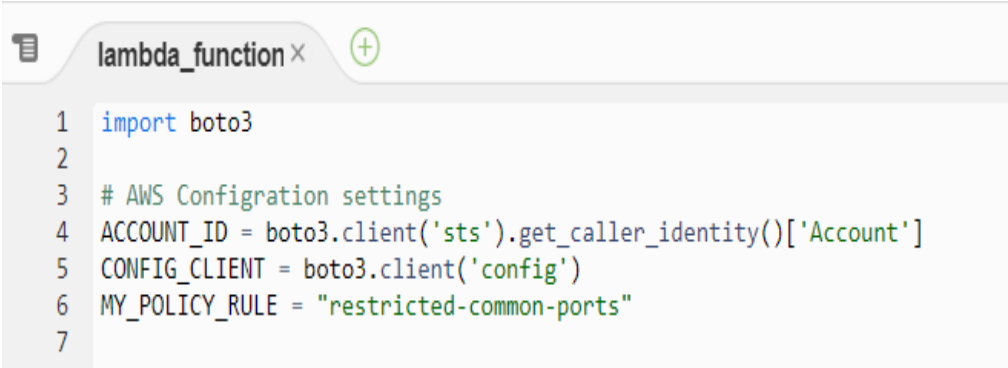


Figure (5.2): Lambda Function

CloudTrail

As we have explained in chapter (2), CloudTrail is basically our central log repository. All log events will be delivered to the CloudTrail. Therefore, if an attacker or user is updating a cloud resource, the event will generate CloudTrail log that will be processed and analyzed by CloudWatch. However, both data and management events will provide us with a virtual diagram of what is happening in our environment.

CloudWatch

For quickly recovering our related logs, I used Amazon CloudWatch, which is a log monitoring and management service that collect and access all performance and operational data in the form of logs and metrics from a single platform [13]. Often CloudTrail logs quantities are considerably large, but with a precise search using CloudWatch service combined with a specific time range search to identify the log file related to our investigation. Overall, CloudWatch provides us with customized dashboards and a simple diagram of our entire policy. It will show the lambda function invocations. This chart can track the effectiveness of our lambda response over time, as shown on Figure (5.3).

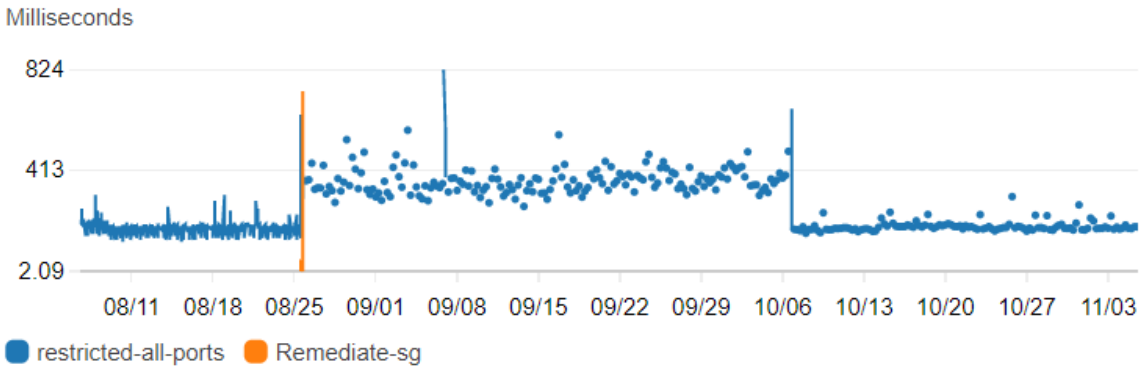


Figure 5.3: Lambda Function Invocations Time

AWS Config

AWS Config is a service that enables you [the user] to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations [17]. AWS Config rules is used to auto-remediate of noncompliant resources. It is using either the console or API, that can add a rule to fix noncompliant support when it is found automatically. This functionality depends on AWS

Systems Manager Automation documents, which is a set of arrangements referenced by the Config rules and provide guidelines for actions taken on resources. On our experiment we have define a configuration policy called “MY_POLICY_RULE.” This rule is responsible of restricting common ports that used by hackers to target servers. The rule is triggered and creating CloudTrail log when any port is added to our security groups. The rule works only on ports (20, 21, 22, 3306 and 4333) as showing on Figure (5.4).

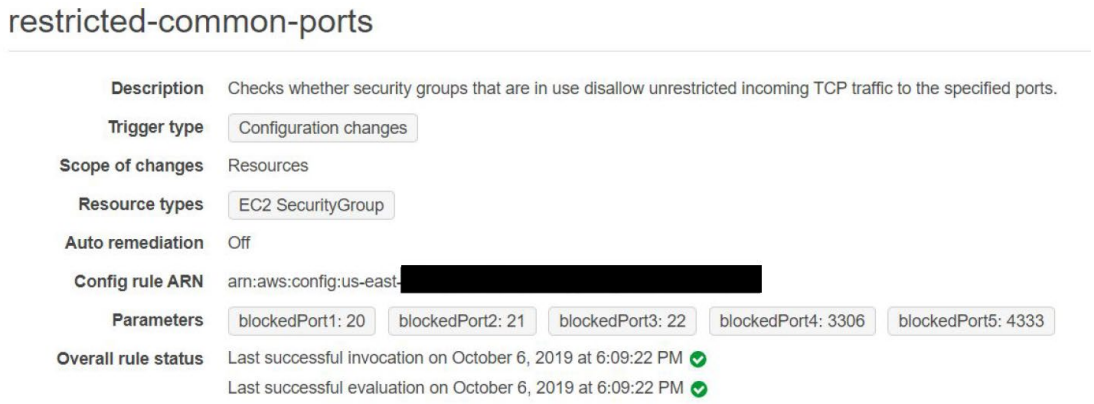


Figure (5.4): Restricted Common Ports Rule

Amazon SNS Topic

An Amazon Simple Notification Service (SNS) topic is a logical access point which acts as a communication channel. A topic lets you group multiple endpoints (such as AWS Lambda, Amazon SQS, HTTP/S, or an email address) [18]. Our policy applies the SNS topic to send email notifications to users when any dangerous security changes happen in our environment. After subscribing to the SNS topic, we need to confirm it via HTTPS endpoints email addresses as AWS resources require this confirmation. However, we need to note that the SNS topic integration is a very important part of our policy. Those broadcast messages are critical for early alerting on a potential security breach. SNS topic also has the ability to send SMS messages, but SMS is not configured on our experiment.

CHAPTER 6. EXPERIMENTAL EVALUATION

To create an automation policy, I have utilized a target system that is hosted in the AWS cloud. The flexible nature of cloud computing, in some cases, will involve a criminal act who commits a crime and then quickly destroys the evidence. However, that situation is not considered in the case study. The goal of this research is to evaluate the efficacy of using cloud logs to track a security event, then build an Auto-remediation policy that acts in a timed manner to different security events.

A. Creating A Security Event

To build the scenario of a security event and trigger the remediation policy, I have performed a risky change. Our scenario assumes the attacker has an AWS configuration access. The attacker (Root) on the first step will update the Security Group, which acts as a virtual firewall. According to AWS, the rules of a security group control the inbound traffic that's allowed to reach the instances that are associated with the security group and the outbound traffic that's allowed to leave them [11]. By editing the inbound rule and allowing the incoming traffic from the attacker-controlled IPs, the attacker simply reaches our secure resources. The attacker then can sniff the traffic that coming through the security group or simply exploit any of the resources controlled by this security group.

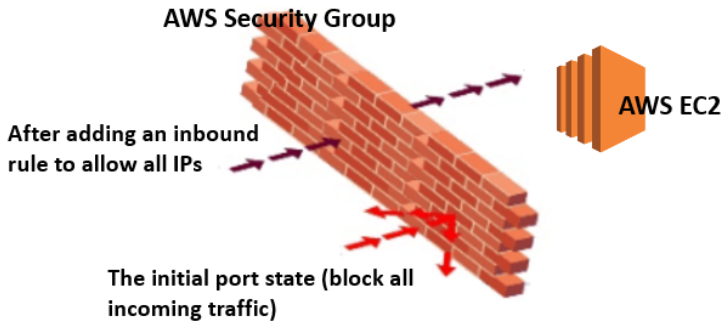


Figure (6.1): Editing Security Group's Inbound Rule

Now, editing the security group rule will create a log event. All log events on the security group are significant to investigate authorized server access. By reconstructed data events, we can draw the relation between the CloudTrail log event and the automation policy responses. Table (6.1) summarizes different events before and after the policy action. The Event ID "**-bb08-ceada01f9b01" is the initial "root" AWS console access before any change takes place. While event ID "**-8dd4-3caf16b46db2" indicating the server's IP was changed by a user or attacker. Event ID: "**-bc57-16ed684f79a3" shows that we have an EC2 instance running using the security group.

Table (6.1) Events Before and After the Policy Actions

Event ID	Event Time	Username	Event Name	Remarks
**-9261-fcc80be9a4f5	2019-10-06, 12:53:51 PM	configLambdaExecution	PutEvaluations	The automation policy reviews different log events after removing the rule
**-aa6b-dfe469ddf37b	2019-10-06, 12:53:51 PM	configLambdaExecution	PutEvaluations	The automation policy reviews different log events
**-87dc-18b9f3fc690b	2019-10-06, 12:51:24 PM	restricted-all-ports	RevokeSecurityGroupIngress	Lambda function will be triggered to remove the violated rule
**-9729-586604b44ba7	2019-10-06, 12:51:23 PM	configLambdaExecution	PutEvaluations	The automation policy reviews different log events
**-bdfd-4ae61f74812b	2019-10-06, 12:51:23 PM	configLambdaExecution	PutEvaluations	The automation policy reviews different log events
**-a3a5-696a8c3a84d4	2019-10-06, 12:51:23 PM	restricted-all-ports	CreateLogStream	CloudTrail log is being created for the violated resource
**-bc57-16ed684f79a3	2019-10-06, 12:49:05 PM	Root	RunInstances	This event shows that we have an EC2 instance running
**-8dd4-3caf16b46db2	2019-10-06, 12:49:03 PM	Root	AuthorizeSecurityGroupIngress	On this event we have added an inbound rule to allow traffic to port 22
**-8818-b730f69af82b	2019-10-06, 12:49:03 PM	Root	CreateSecurityGroup	This our first event for creating a Security Group
**-bb08-ceada01f9b01	2019-10-06, 12:20:05 PM	Root	ConsoleLogin	The initial AWS console access (root is AWS account that has default access)

B. Automation Policy Analyze

The automation policy reviews different log events by closely analyzing those events; then, the policy will effectively deliver tasks and responses. Now the automation policy would analyze our risky event ID "**-8dd4-3caf16b46db2." This will trigger "policy_non_complinance" function, which is responsible for checking our configuration policy "MY_POLICY_RULE." Then the policy will move to perform actions against the violated resource.

C. Automation Policy Action

Automation workflows will follow the sequence outlined in the automation policy architecture (figure 5). Lambda function allows the policy service to perform actions on behalf of us. There are two main actions are performed by the policy:

1. **Send an SNS Topic Email**

   First the policy will send an email to notify the users about the violated resource. This service will be triggered from our Lambda function by utilizing SNS topic services. Figure (6.2) shows a non-compliance notification is sent to indicate that our security group is updated.

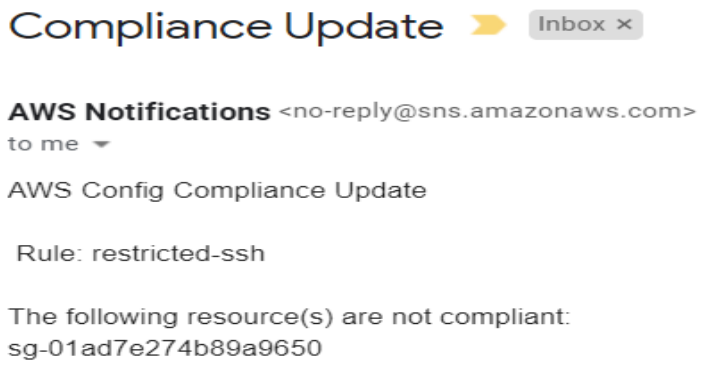


Figure (6.2) Non-Compliance Email Notification

2. Remove and Add an Inbound Rule

Secondly, when a noncompliant action occurs, the Lambda function will be triggered to remove the violated rule as showed on event ID "**-87dc-18b9f3fc690b." This will be followed by adding an inbound rule for port 22. This rule would add a private IP address to our security group to auto-remediate our violated security group resources. Now our security group will have 10.0.0.0 IP, that is not open to the public.

CHAPTER 7. CONCLUSION AND FUTURE WORK

With the rapid development of service-less applications on the cloud, the auto-remediation policy offers enormous benefits to automate the security work. The system can be used to comply with different security standards, as well as can be utilized to safeguard our cloud resources. The cloud security log is very effective in constructing an effective automation policy.

In this research, we able to utilize different cloud resources to build an automation policy that could analyze and summarizes various log events then act based on a specific security event. By constructing a log-event table, we able to draw a complete picture of how the policy will analyze and automate action workflows. This policy is able to perform a series of actions by sending an email notification, then removing the violated rule, and finally adding a new inbound rule to our violated resource.

The automation policy can help spot attacks before they begin and therefore save a lot of time and money that can organization spend after a successful attack. While the cloud log can draw a complete picture and evaluation of the security automation, the potential downside for security automation is that a one-size-fits-all approach to cybersecurity crowds out human judgment and control. Also, the automation policy will require a constant update for the new security threats as they come. In the end, it makes human efforts needed to maintain the accuracy and effectiveness of the auto-remediation policy.

Future Work

This policy proves the hypothesis that it would be possible to automate some security work on the cloud to achieve a higher level of security automation. The policy is open for future improvement. Adding more actions is possible to achieve by adjusting the lambda

function limitation to some ports. In the feature, the policy can be enhanced to cover actions based on user behaviors instead of relying on logs to analyzing only. While the auto-remediation policy satisfies securing security groups, the policy can be enhanced to cover AWS Identity and Access Management (IAM). This can be achieved with proper implementation of the automation policy.

REFERENCES

[1] Vora, Zeal, and Safari, an O'Reilly Media Company. Enterprise Cloud Security and Governance Vora, Zeal. 1st ed. 2017. Web.
[2] IDC: Cloud Computing 2010 – An IDC Update. 2009. slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update.
[3] https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-ct.html
[4] Mavridis, Ilias ; Karatza, Helen, The Journal of Systems & Software, March 201, Vol.125, pp.133-15. Web. 5 August 2019
[5] DeLaRosa, Alexander (February 8, 2018). "Log Monitoring: not the ugly sister". Pandora FMS. Archived from the original on February 14, 2018. Retrieved February 14, 2018. Web. 21 August 2019
[6] https://en.wikipedia.org/wiki/Log_analysis
[7] Iris Xie PhD, Krystyna K. Matusiak PhD, in Discover Digital Libraries, 2016
[8] Thomas Erl, Mahmood, Puttini "Cloud Computing Concepts, Technology & Architecture." read.amazon.com Amazon, n.d. Web. 7 May 2019
[9] Damshenas, M.; Dehghantanha, A.; Mahmoud, R.; Shamsuddin, S.B. Forensics investigation challenges in cloud computing environments. In Proceedings of the 2012 International Conference on Cyber Security,Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 26–28 June 2012; pp. 190–194. Web. 20 October 2019
[10] https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-management-and-data-events-with-cloudtrail.html
[11] https://aws.amazon.com/cloudtrail/
[12] Potter, Bruce. "Security Automation." Network Security 2007.9 (2007): 18-19. Web.
[13] "Logicworks Unveils Cloud Security Automation Framework on AWS." Wireless News (2016): Wireless News, May 20, 2016. Web. 15 June 2019
[14] "Endpoint Security Automation Top Priority: Results of the 2018 SANS Endpoint Security Survey." Journal of Engineering (2018): 447. Web. 2 October 2019
[15] https://aws.amazon.com/lambda/feature
[16] https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/
[17] https://aws.amazon.com/config/
[18] https://docs.aws.amazon.com/sns/latest/dg/sns-tutorial-create-topic.html
[19] Greene, Tim. "Private Clouds Hold a Wide Lead over Public Clouds among IT Pros Polled; Biggest Roadblocks to Cloud Adoption Are Security and Cost, CDW Poll Says." Network World (2011): Network World, June 1, 2011. Web. 7 October 2019
[20] Zhang · Lu Cheng, Boutaba "Cloud computing: state-of-the-art and research challenges." homeworkmarket.com. n.d. Web. 2 November 2019
[21] http://rapidscale.net/cloud-collaboration-is-the-new-normal/
[22] Priyam, Prashant, and Safari, an O'Reilly Media Company. Cloud Security Automation Priyam, Prashant. 1st ed. 2018. Web. 2 October 2019