Real-time Log Monitoring is Essential for Effective Cloud Security

June 15, 2020

Prepared By:
Set Solutions, Inc.
1800 West Loop South
Houston, TX 77027
Phone: (713) 956-6600
setsolutions.com

Contributing Authors:
Nick DiPasquale, Senior Security Solutions Architect
Brandt Varni, Practice Manager - Data & Analytics
Jon Young, Senior Security Engineer
INTRODUCTION

Cybersecurity is a significant challenge for organizations today. No matter how large or small a company is, or the industry it is in, networks and data are under virtually constant siege. Moving to the cloud provides a variety of benefits in terms of performance, availability, scalability, and cost savings, but it also creates a more complex infrastructure to try to protect against a massive and expanding threat landscape.

Preventive security measures only go so far. There is no amount of security that will guard against 100% of attacks. Attackers are also aware of the increasingly complex network environments and are constantly looking for weak points to infiltrate without being detected. There will be attacks that slip through your defenses. What is important is your ability to quickly detect and respond so you can avoid—or at least minimize—damage from those attacks. Real-time logging and monitoring play a crucial role in protecting a dynamic network environment.

REAL-TIME LOGGING AND MONITORING

Log data has always been a valuable source of information for IT and IT security teams. The difference between now and 5 or 10 years ago is that it's no longer good enough to just log data for periodic analysis or archiving. Continuous, real-time monitoring is essential for identifying anomalous or suspicious activities that require further attention.

Real-time logging and monitoring enable you to quickly identify indicators of compromise or potential breaches. It also provides you with the information you need for thorough incident response forensics. The ability to correlate and analyze log data in real-time is essential for detecting and remediating threats like unauthorized privilege escalations, suspicious access activities, brute force attempts, and malicious actions. Identifying and responding to incidents as quickly as possible helps reduce dwell time—the amount of time between initial compromise and detection of an attack—for successful attacks and minimize the potential consequences.

SECURITY ON AWS

When it comes to cloud computing and cloud security, it’s important to understand the shared responsibility model. Many organizations make the mistake of assuming that the cloud platform provider assumes all responsibility for security, but that is simply not the case. The cloud provider—whether it is AWS, Azure, Google Cloud, or some other platform—is responsible for securing and protecting the backend infrastructure that its platform is hosted from, and ensuring the security and integrity of the hardware and software it is offering as a service. The organization, however, is responsible for securing and protecting everything they run in or store on that platform.
The cloud platform provider typically provides security controls that can be configured and managed by customers, but it is imperative that organizations understand that it is their responsibility to use them properly. It is also good to understand the limitations of the available tools and how to augment or leverage the tools provided as part of a more comprehensive cybersecurity strategy.

AWS provides a variety of tools and services that customers can use to secure the workloads and protect the data they have in AWS. AWS CloudTrail is a web service organizations can use for real-time logging and monitoring. By observing AWS CloudTrail logs, a customer can determine activity data such as requestor identity, request time, source IP address, as well as the elements provided by AWS in response to the request.

AWS CloudTrail helps organizations with regulatory compliance reporting requirements, but it is a relatively basic service. It can record and log relevant activities, but that is all it can do with the data. Fortunately, it can also be configured to feed into security information and event management (SIEM) platforms or other third-party tools for deeper analysis.

BUILDING VISIBILITY INTO THE CLOUD ARCHITECTURE

What does effective cloud security look like? Let’s use a fictional company to represent an average organization and take a closer look at how to achieve effective cloud security, and what some of the common attack scenarios and responses look like.

Our fictional company is just starting their migration to the cloud—moving from an on-premise datacenter to AWS. The company has a relatively mature IT security program—complete with a vulnerability management solution, content filtering, edge security, and other core security best practice tools and policies. Their primary platform for correlating and analyzing data is Splunk, and they have a handful of playbooks developed for Splunk Phantom—their SOAR (security, orchestration, automation, and response) solution to handle events.

As this organization navigates its cloud migration efforts, the cloud team and IT security team also need to coordinate to ensure there is visibility into the AWS environment, while also pulling logs and telemetry data from the cloud platform into Splunk.

The organization can leverage the information from AWS CloudTrail and ingest it into Splunk with the right configuration. The following steps are performed to feed AWS CloudTrail logs into Splunk, and the accompanying architecture diagram represents the final example build out:

1. Configure Splunk Heavy Forwarders behind an Elastic Load Balancer in the production AWS account. These heavy forwarders will be used to receive the logs from AWS, perform the necessary parsing, and forward the events to the indexers.

2. Install the Splunk Add-on for Amazon Kinesis Firehose on each of the Heavy Forwarders and Search Heads so that Splunk can properly parse the CloudTrail events.

3. Configure the HTTP Event Collector on the Heavy Forwarders to receive the data from the Kinesis Firehose and to send the CloudTrail logs into the “aws” index.
4. Configure a trail in CloudTrail to send logs to CloudWatch Logs.

5. Configure the Amazon Kinesis Firehose stream to send CloudTrail data to the Elastic Load Balancer address.

6. Configure CloudWatch Logs to send logs to the Kinesis Firehose stream.

**DETECTING AND RESPONDING TO SECURITY INCIDENTS**

With the AWS CloudTrail data flowing into Splunk, the IT security team has the same visibility into the AWS cloud environment as they have for the on-premise infrastructure, enabling them to conduct real-time logging and monitoring and take quick action when incidents are detected.

Having real-time logging and monitoring in place is an important step, but the value is also a reflection of the operational tactics you employ. Logging everything for the sake of logging results creates an overwhelming amount of information and a lot of unnecessary noise. It's important to consider what attack scenarios your business is most likely to see in order to determine the information you should be logging, what events or activities are you looking for, and how should you respond if anomalous or suspicious activity is detected.

Let's take a closer look at three common scenarios, and how real-time logging and monitoring of the AWS environment is essential for effective detection and response.

**ATTACK SCENARIO 1: ODD SOURCE IP CONNECTING**

Using the source IP address in the CloudTrail events, the security team uses the geolocation functionality in Splunk to flag activities from an unexpected location. One of simplest ways to detect anomalous or suspicious activity is by monitoring where the activity is originating from. Most activity will generally occur from IP addresses in the office that are managed by IT. There may be some external IP addresses from users working from home or logging in from a local coffee shop, or even from employees who are traveling. However, when you detect activity from a source IP address in an unusual region, that should raise a red flag.
The screenshot below is from a Splunk dashboard that shows suspicious activity coming from an unexpected source IP out of China. Our fictional example company does not have any resources or customers in China, so the traffic is immediately suspicious.

Below is a visual example of a Splunk Phantom playbook that can be employed when an odd source IP is detected. As shown, the company can either automatically block the IP address at the edge (top portion of the workflow), or it can alert IT security for investigation and remediation (bottom portion of the workflow).
ATTACK SCENARIO 2: BRUTE FORCE LOGIN ATTEMPT

Attackers will often try to gain access through brute force—essentially trying every possible username and password combination until valid credentials are discovered. This method is very noisy and results in a hundreds, or possibly thousands, of failed login attempts. As seen in the screenshots below, real-time logging and monitoring can quickly detect a spike in failed login attempts. In this example, there were several failed login attempts into our fictional company’s AWS Console from a single user account. This is classic brute force behavior.

As in the previous attack scenario, Splunk Phantom playbooks can be used to thwart the attack in several ways:

- Blocking any further activity from the source IP address (see the Phantom playbook visual in Attack Scenario 1 above)
- Deactivation of the suspicious user
- Resetting the password of the suspicious account (see the visual below for a simple example of a password reset playbook)
ATTACK SCENARIO 3: UNAUTHORIZED CHANGES MADE TO IAM

In Splunk, the security team configures an alert to identify suspicious provisioning activities within their cloud accounts. The security team can now proactively detect any rogue AWS resources in their account and quickly identify the compromised credentials. Additionally, Splunk Phantom playbooks can be created to respond to the suspicious activity by blocking the source IP at the edge, resetting the credentials of the user in question in AWS IAM (identity and access management), snapshotting and terminating the suspicious VM (virtual machine), or any combination of these.
There is no such thing as perfect security. Technology constantly evolves, and attackers constantly adapt and develop innovative new techniques and strategies to bypass or circumvent security measures. Preventive security measures only go so far, which is why it is crucial to quickly detect and respond to security incidents that slip through.

The damage and fallout from an attack rarely occur from the initial compromise. Minimizing dwell time prevents attackers from gaining more of a foothold and limits their ability to conduct further reconnaissance and propagate across your network to other vulnerable assets. Real-time logging and monitoring gives you the visibility you need and automated response playbooks help ensure swift action to stop attacks cold.

**MINIMIZE DWELL TIME WITH QUICK DETECTION AND AUTOMATED RESPONSE**