Google Cloud

Security monitoring key concepts

So far, you've learned that security monitoring is a systematic process of surveilling systems to detect and handle potential security breaches or incidents. In this reading, you'll learn about the role that security professionals play in security monitoring. You'll also examine proactive monitoring and how it differs from reactive monitoring.

Cloud security monitoring

Cloud security monitoring is a process that allows security professionals to review, observe, and manage alerts and possible security threats in their cloud environments. It allows them to inspect systems and identify potential threats. Cloud security monitoring also helps security professionals recommend remediations, address issues, mitigate damage, and identify existing threats or vulnerabilities.

How cloud security monitoring works

Cloud security monitoring tools collect log data from across all cloud resources. Then, the log data is aggregated. Next, the data is analyzed and correlated. During this process, the monitoring tool searches for anomalous activity. If it finds any, it sends an alert to start an incident response.

Security and risk management platforms

Cloud security monitoring can be conducted using a security and risk management platform, providing cloud security professionals visibility into their cloud resources.

These platforms help cloud security professionals detect external threats, including malicious activity that targets resources, and any unauthorized behavior occurring within the organization.

Examples of security and risk management platforms include Google Security Command Center and Chronicle SIEM.

Benefits of monitoring services

Tools for cloud security monitoring may be offered by a cloud service provider. Along with a cloud service provider's security tools, cloud security professionals can also use third party security solutions called monitoring services.

A monitoring service offers:

- **Visibility:** Cloud security professionals can use a dashboard to monitor user, file, and application behavior.
- **Scalability:** Cloud security professionals can monitor large amounts of log data with cloud security monitoring.
- **Auditing and monitoring capabilities:** Cloud security professionals can identify malicious activity quickly, which helps prevent attacks.

More about monitoring

There are two main types of security monitoring: proactive and reactive.

Proactive monitoring

When practicing proactive monitoring, cloud security professionals continuously monitor their applications, infrastructure, and systems. This is sometimes called threat hunting. Threat hunting is the process of proactively searching for cyber threats that may have evaded traditional security controls. Security professionals use a variety of tools and techniques to search for threats, including:

- **Log analysis**: Threat hunters can analyze logs from a variety of sources, like network devices, endpoints, and applications to look for suspicious activity.
- **Network traffic analysis**: Threat hunters can analyze network traffic to identify anomalies that may be indicative of a threat.
- **Endpoint analysis**: Threat hunters can analyze endpoints to identify malware, suspicious processes, and other indicators of compromise.
- **Threat intelligence**: Threat hunters can use threat intelligence to learn about new threats and vulnerabilities, and to prioritize their hunting activities.
- **Identity and access management**: Threat hunters can examine IAM logs and data to identify suspicious access patterns, unauthorized access attempts, and changes to user permissions.

The goal of threat hunting is to monitor for indicators of compromise (IOC). IOCs include any anomalies that appear suspicious, and any abnormal activity from users or systems that require investigation.

Security professionals can also use various tools and data sources to gather and analyze data. Some of these tools include:

- Application Performance Monitoring (APM) tools for monitoring applications for performance and availability

- Analysis and log management tools
- Infrastructure monitoring tools
- Cloud monitoring tools
- Synthetic monitoring tools

Some data sources used to gather and analyze data include:

- System alters
- Performance metrics
- Event logs

Reactive monitoring

Reactive monitoring is very similar to the classic model of troubleshooting. If the system works, leave it as it is and focus on adding features. The goal is to quickly respond to problems after they're found. Since reactive monitoring involves reacting to incidents instead of preventing them, it can lead to disruptions. It also takes more time to troubleshoot incidents that have already happened.

Proactive vs reactive monitoring

The main difference between proactive monitoring and reactive monitoring is that reactive monitoring focuses on addressing issues after they're discovered, while proactive monitoring focuses on preventing problems before they occur. For example, A predictive alarm that warns you that something may happen instead of warning you when it has already happened is proactive monitoring. An alarm that tells SecOp team members about something that has already happened and needs to be fixed is an example of reactive monitoring.

Key takeaways

Cloud security monitoring allows organizations to review, observe, and manage operational workflows in their cloud environments to identify and address threats. Cloud security professionals can use security and risk management platforms and monitoring services to streamline their monitoring process. They can also use proactive or reactive monitoring depending on the needs of their organization. Proactive monitoring continuously monitors applications, infrastructure, and systems using tools like system alerts and event logs. Reactive monitoring addressed issues that have already occurred. Being familiar with these monitoring strategies can help you prepare to respond to threats and incidents more readily.