Alert and log optimization

So far, you've learned how alerts provide security teams with real-time information about potential threats in their environment. Remember, not every alert signals an actual threat. An alert may be a false positive, which is an alert that incorrectly detects the presence of a threat.

In this reading, you'll explore how to set up alerts and notifications and how to use them in Google Cloud. You'll also learn about the advantages of metrics and some of the challenges that can happen with alerts.

Cloud Monitoring and alerting policies

Cloud Monitoring collects data from cloud resources in a Google Cloud project. It then monitors the health, performance, and availability of your cloud resources to create insights about your cloud environment through metrics like central processing unit (CPU) utilization, memory usage, and network traffic.

In Cloud Monitoring, you can set up alerting policies to create the alerts triggered when these metrics exceed certain thresholds. An alerting policy specifies the conditions that you want to be alerted on and how you want to be notified when those conditions are met. In Cloud Monitoring, there are two types of alerting policies you can configure depending on the metrics you choose to monitor: metric-based and log-based.

Metric-based alert policy

Metric-based alerting policies are most useful for monitoring the health and operations of cloud resources. For example, you can set an alert to trigger when CPU utilization on a particular virtual machine (VM) instance exceeds 80%. Here are some steps to create, configure, and test a metric-based notification system:

Create the metric-based alert policy

1. Go to the Google Cloud console: https://console.cloud.google.com.
2. Click the **Navigation** menu (three horizontal lines) in the top left corner.
3. Click **Monitoring.**
4. Click **Alerting.**
5. Click the **Create policy** button.

Configure the metric-based alert policy

1. In the **Resource type** field, select **VM instance**.
2. In the **Metric** field, select **CPU utilization.**
3. In the **Condition type** field, select **Threshold.**
4. In the **Threshold** field, enter **80%.**
5. In the **Aggregation** field, select **Average.**
6. In the **Per** field, select **1 minute.**
7. In the **For** field, select **5 minutes.**

Test the metric-based alert policy using the console notification system

1. In the **Test notification** section, select the notification channel that you just configured.
2. Click the **Send test notification** button.
3. If you receive the email test notification, then the notification system is configured correctly.

Test the metric-based alert policy manually

1. Manually increase the CPU utilization of VM instance vm1 to more than 80%.
2. Wait for the alert policy to trigger and generate an alert.
3. Verify that you receive an email notification.

Get more information on metric-based alert policies

- How to create an alerting policy in Google Cloud Monitoring: https://cloud.google.com/monitoring/alerts
- Cloud Monitoring documentation: https://cloud.google.com/monitoring/docs

Log-based alert policy

Log-based alerting policies are most useful for monitoring security-related events since they monitor log data. You can use them to notify you anytime a specific event appears in a log. For example, you could create an alert that's triggered when a user account accesses the security key of a service account. Here are some steps to create, configure, and test such a log-based notification system:

Create a log-based metric

1. In the Google Cloud console, select **Logging > Logs Explorer.**
2. To create a log-based metric, click **More > Create log-based metric.**
3. Enter this information:
    - **Name:** Security Key Access
    - **Description:** Tracks the number of times a user account accesses the security key of a service account
    - **Filter:** `resource.type="service_account" AND protoPayload.service_account.email=([YOUR_SERVICE_ACCOUNT_EMAIL]) AND protoPayload.event_type="security_key_access"`
    - **Value extractor:** `count(*)`
4. Click **Create.**

Create a log-based alert

1. Click **More > Create alert** from metric.
2. In the **Alert details** pane, enter this information:
    - **Name:** Security Key Access Alert
    - **Description:** Alert when a user account accesses the security key of a service account
3. Click **Next.**
4. In the **Choose logs to include in the alert** pane, select the **Security Key Access** metric.
5. Click **Next.**
6. In the **Configure conditions** pane, select these conditions:
    - **Condition:** Value above threshold
    - **Threshold value:** 1
7. Click **Next.**
8. In the **Configure notifications** pane, select the notification channels that you want to use for the alert.
9. Click **Next.**
10. In the **Review and create** pane, review the alert details and click **Create.**

Test the alert

1. Open the Cloud Shell and run this command:
   `gcloud logging write logs SERVICE_ACCOUNT_EMAIL security_key_access "Accessed security key"`
2. In the **Logs Explorer,** click the **Security Key Access** metric. You should see a data point for the current time.

3. If you have configured notifications, you should receive an email notification that the alert has triggered.

Get more information on log-based alert policies

- Create and manage log-based alerts: https://cloud.google.com/logging/docs/alerting/log-based-alerts

Using metrics to improve incident response processes

One way to measure the effectiveness of an organization's incident response process is through the use of metrics. By tracking metrics, organizations can identify areas where they are doing well and areas that need improvement. Metrics help security teams make informed decisions supported by data that can be used to improve the incident response processes.

There are different types of metrics that can be used depending on what you need to measure. For example, the number of incidents per day is a time-based metric. Time-based metrics provide data over a period of time and can be useful in tracking variations that occur within a time frame. Time-based metrics can also be used to benchmark your cybersecurity program against other organizations.

There are many different cloud monitoring operations metrics that you can use for security operations in apps, like Chronicle SOAR and Chronicle SIEM's Cloud Monitoring for log ingestion health. There are also metrics for cloud operations available in Chronicle itself. Here is a list of some common metrics:

Cloud Security Monitoring Metrics

- **Failed login attempts:** The number of failed attempts to log in to your cloud console or other cloud resources
- **Login attempts:** The number of attempts to log in to your cloud console or other cloud resources
- **Security alerts:** The number of security alerts that have been triggered
- **Unusual activity:** Any activity that is outside of the normal patterns of your cloud usage

General Cloud Operations Monitoring Metrics

- **Application errors:** The number of errors that occur in your applications
- **Application latency:** The time it takes for an application to respond to a request
- **API call errors:** The number of API calls that fail
- **API call latency:** The time it takes for an API call to be processed
- **API call volume:** The number of API calls made to your cloud resources
- **CPU utilization:** The percentage of CPU time that is being used

- **Disk utilization:** The percentage of disk space that is being used
- **Memory utilization:** The percentage of memory that is being used
- **Network traffic:** The amount of data that is being transmitted over the network
- **System logs:** The number of system logs that are generated

Additional Cloud Monitoring Metrics

- **Cache metrics:** Metrics for cache servers, like hit rate and miss rate
- **Container metrics:** Metrics for Kubernetes containers, like CPU usage, memory usage, and network traffic
- **Database metrics:** Metrics for database servers, like query latency and connection count
- **Load balancer metrics:** Metrics for load balancers, like request throughput and response time
- **Messaging metrics:** Metrics for messaging queues, like message throughput and latency

Get more information on cloud monitoring metrics

- Google Cloud Security Command Center (SCC): https://cloud.google.com/security-command-center

Note: Metrics differ from key performance indicators (KPIs). Metrics track the status of a workflow or business process, while KPIs are specific, measurable values that quantify the effectiveness of a workflow in achieving critical initiatives, objectives, or goals.

Pro-tip: Many security solutions provide you with the ability to create personalized dashboards to display data in one place. For example, Chronicle SIEM provides a high-level summary of information related to security events over time. Cloud Monitoring also provides you with the ability to create dashboards using metrics.

The challenge with alerts

Security analysts can receive hundreds of alerts per day, and processing all of these security alerts can be resource intensive and time consuming. One of the biggest challenges that security teams currently face is false positive alerts. A **false positive** is an alert that incorrectly detects the presence of a threat. False positives increase the workload of a security team and can contribute to slower performance and productivity because of the time the team spends investigating a wrongly categorized alert.

Along with the issue of false positives, security analysts commonly experience alert fatigue because of the overwhelming volume of alerts and the intensive time it takes to process each one of them. Alert fatigue contributes to desensitization, which can cause analysts to overlook real threats.

As a result, one of the primary goals of security teams includes implementing strategies that aim to reduce the number of alerts that are received in SIEM platforms, especially the amount of false positive alerts. In cybersecurity, this is also known as noise reduction where the noise is excessive false positive alerts. There are many strategies that you can use to do this like refining the detection capabilities of security solutions and improving alert ticket workflows through automation.

Key takeaways

Alerting provides timely awareness about problems in your cloud environment. As a cloud cybersecurity analyst, you'll create, configure, and manage alerts and notifications. By having a solid understanding of alerts and notifications, you can play a vital role in keeping cloud environments safe and secure.

Resources for more information

If you'd like to learn more about alerting policies in Google Cloud, check out these links:

- Google Cloud documentation about setting up alerting policies
- Google Cloud security foundations guide