Google Cloud

Automation to improve cloud security efficiency

So far, you've learned that automation is the use of technology to improve the efficiency of tasks. For example, you can use automation to build and deploy containers. Automation also helps you enforce policy as code (PaC), and manage resources, which can change often in the cloud. In this reading, you'll learn more about automation, and explore some examples.

What is automation?

Automation is the use of technology to perform common and repetitive tasks, and reduce the need for human interaction. Automation helps reduce human error by completing repetitive tasks the same way every time. Since automation always completes tasks in exactly the same way, it doesn't change the way processes are carried out.

Types of automation

There are many different types of automation you might use in your professional career, including: resource allocation, configurations, development and deployment, tagging, security, and logging and monitoring.

- **Resource allocation:** Resource allocation is one of the cores of cloud computing. This type of automation lets you scale resources up and down to match demand. With resource allocation, you can also scale networking resources, compute resources, or memory resources up and down. Resource allocation helps you manage your resources, keeps you from using and paying for too many, and ensures you have enough resources for what you need.
- **Configurations:** These automations are automatically implemented configuration of your assets. You can define configurations by using code, or by using templates that have already been made.
- **Development and deployment:** Developers use automation to scan code for errors and vulnerabilities. They also use automation for version control. They rely on automation for testing, and to help develop some of their assets.
- **Tagging:** You can add tags that identify assets based on context, criteria, and operation conditions. Automation can help you to create and maintain tags for assets. These tags also help security tools know which assets to secure.
- **Security:** You can set up cloud environments with automated security controls. These security controls can have several functions, like scanning for known indicators of

compromise (IoCs), searching for vulnerabilities, or identifying when configurations are changed to a potentially insecure state.

- **Logging and monitoring:** You can set up automated cloud tools to log all activity going through your cloud. You can use automation to monitor all the services and workloads in your cloud environment. You can also set up monitoring filters to look for unexpected events or anomalies, and alert users.

Infrastructure as code (IaC)

Infrastructure-as-code (IaC) is the provisioning and managing of infrastructure through reusable scripts. You can create your own IaC templates, or use templates from your cloud provider. These templates have many environments and asset configurations already defined, and give automation the instructions it needs to build IaC assets.

Scanning for vulnerabilities

As a cloud security professional, you need to scan all of your assets for vulnerabilities. Automation can help you save you time by:

- Scanning for vulnerabilities to prevent human error.
- Monitoring all the assets in the environment, and scanning everything coming in.
- Defining rules and policies.
- Evaluating assets according to your rules and policies, and enforcing them.

Key takeaways

Automation can perform tasks, save you time, and prevent human error. And, there are many different types of automation to choose from. You can also use automation for building IaC, and a variety of security tasks, like scanning for vulnerabilities, and monitoring your cloud environment.