Google Cloud

Core cloud security analyst responsibilities

As you've learned, cloud security analysts have many responsibilities. Each responsibility contributes to protecting cloud assets and preventing cyber threats. Your role as a cloud security analyst is important in defending your organization against these threats. In this reading, you'll review the different types of responsibilities common in the cloud cybersecurity field.

Key responsibilities

Cloud security analysts have a variety of responsibilities that contribute to protecting cloud environments.

Map security concepts to cloud products

Cloud security analysts gain practical experience working with a variety of cloud products relating to compute, networks, and storage. It's their responsibility to identify the potential attack vectors for each product, and know how to protect them from threats. For example, analysts are knowledgeable about different networking concepts, like how to identify suspicious network traffic. When a networking threat is identified, analysts know which product or tool to use to remediate the issue.

Use tools

An exciting aspect of cloud security is the opportunity to work with different tools, like Linux, Terraform, and many Google Cloud offerings. Cloud security analysts use tools to help facilitate the checking of virtual machines (VMs), containers, and networks. Tools help analysts keep track of assets and identify misconfigurations that require remediation.

Tools are also used to analyze threat detection and security compliance reports. An important part of an analyst's job is to consider how regulations might impact their cloud environment.

An intrusion detection system (IDS) is one type of tool analysts can use. An IDS is an application that monitors system activity and alerts on possible intrusions. An IDS is a valuable tool because it can detect abnormal system behavior and unauthorized logins. Analysts use an IDS to identify threats across resources and take necessary action.

Communicate the security of cloud environments

Cloud security analysts are expected to communicate with a variety of people. For example, analysts use written communication to prepare status reports to share with management and other team members. Analysts are also responsible for conveying information about the health and security of their organization's cloud environment.

Cloud security professionals should have the ability to tailor their communication to their intended audience. For example, analysts need to explain complex security concepts in an understandable way to non-technical audiences or stakeholders.

Pro tip: One way analysts can develop communication skills is by recognizing and avoiding jargon. Jargon is technical language that people outside of the specific field won't understand.

Monitor and respond to potential security incidents

Cloud security analysts monitor their organization's infrastructure for potential security incidents. They use threat detection and compliance reports to help mitigate risks. They use cloud logging tools to gather information about user and system activity. They also identify errors as they appear.

Knowing how to monitor these types of events is crucial. It's an analyst's responsibility to identify suspicious or unusual activity in the infrastructure's network, VMs, containers, and other cloud products.

When analysts detect a suspicious event, it's also their responsibility to respond to these incidents, and escalate incidents to the appropriate parties. Analysts respond to a variety of threats, including malware infections and security breaches.

Test new security products

Cloud security analysts have the opportunity to test new security products to determine if they're suitable for their organization to adopt. Also, after adopting new security products, they'll regularly test those products to ensure they perform correctly within their cloud environment.

Analysts also test new applications that will be added to their cloud infrastructure. Testing applications first is important so that the security team can ensure the addition isn't introducing new risks.

Stay current with the latest security advancements and cyber threats

Keeping up with the latest security trends and cyber threats is essential for cloud security analysts. Analysts can stay updated by checking out online resources like security blogs and

journals. A helpful website is the Open Source Foundation for Application Security (OWASP) ® Foundation that annually releases the top 10 cybersecurity threats. This OWASP® list is a resource analysts can use to keep track of current and new security risks. Cloud security analysts monitor and prevent these new threats from damaging their organization's infrastructure.

Key takeaways

Cloud security analysts have a lot of responsibilities, each important for maintaining and improving a cloud environment's security posture. Analysts must know how to map security concepts to a wide range of cloud products. They use tools to help identify threats to these products, and also must also communicate these alerts to different parties. Analysts monitor and respond to security incidents. They also have the opportunity to test new security products and stay ahead of new trends in the cybersecurity space.