Google Cloud

Threat and vulnerability management assessments

So far, you've learned that a threat management strategy (TMS) is a comprehensive plan that addresses the various types of cyber threats an organization may face. Conducting regular cloud security audits is strongly recommended and should be part of your threat management strategy. These audits can help you improve cyberattack prevention by identifying weaknesses in the organization's cloud infrastructure. They also identify potential points of entry within the infrastructure.

In this reading, you'll learn more about conducting regular cloud security audits as part of a TMS. You'll also explore the role of enhanced AI and how it can help monitor cloud infrastructure systems.

Regular cloud security audits

As a cloud security professional, you and your team should regularly conduct cloud security audits that cover a comprehensive set of resources, like network permissions and operating processes.

Your audit team should also give your organization recommendations to help recover from a breach quickly.

A security audit includes these steps:

1. The team interviews the teams related to IT, SecOps, DataOps, and Compliance. Then, the team conducts a document review based on the interviews. This helps the team know what security controls are in place and understand the organization's architecture, environment, and what changes the team plans to make to the environment. This review also helps the team establish an enterprise baseline.
2. Next, the team runs tools to collect information, like identity misconfigurations and possible attack chains. This process helps the team establish an environment baseline.
3. Then, the team creates recommendations.
4. Finally, the team presents its findings to the stakeholders, makes recommendations, and answers questions.

AI-based threat management

Much like people, artificial intelligence (AI) can gain new intelligence through experience. AI learns from repetition and developing predictions and correlations about behavior. AI can help with security analysis in several ways, including:

- Detecting unusual behaviors in events that people might overlook
- Detecting when certain events in the cloud could indicate the potential of a suspicious event or attack
- Modeling and reporting on the monitored assets
- Making correlations between known and potentially unknown attack strategies that have potentially inappropriate behavior or actions
- Creating initial relationships and weakening or strengthening them, based on continuously analyzing—so a single, unnoticed event can become relevant to the AI when it can establish other connections

Pro tip: When building your security strategy, consider incorporating AI to enhance monitoring between regular cloud security assessments. AI is continually evolving and can significantly augment various aspects of security, including monitoring.

Note: While AI can't completely replace certain critical security tasks, like basic security measures, real-time analysis, and cyber forensics conducted by security analysts, it can provide valuable support in enhancing your security posture.

Using AI together with regular audits

Even though you conduct audits at regular times, things can still happen in the time between audits you should know about. This is one use case where AI can help you continuously identify problems in-between regular audits.

Key takeaways

Regular cloud audits are important in your security strategy. They help you make sure you've properly secured your network resources. Audits can also indicate what you need to fix and what problems you can prevent in the future.

As technology keeps moving forward, AI is constantly developing. As it does, it will continue to be more helpful in monitoring your infrastructure's security. By using it together with other security techniques, you'll know more about your infrastructure's security condition in-between regular cloud audits.