Google Cloud

Vulnerability scanning, penetration testing, and tabletop exercises

In this reading, you'll explore more about vulnerability management, including vulnerability scanners, penetration testing, and tabletop exercises.

Vulnerability management

Cloud environments are complex. There are many different components found in each layer such as network, data, users, and applications, which can all contain potential vulnerabilities. It's vital for organizations to address them using **vulnerability management,** which is the process of scanning, identifying, and prioritizing vulnerabilities. As a cloud security professional, you must work to identify, categorize, and prioritize your organizations cloud security vulnerabilities in order to properly fix them. You can use several different tools and processes, such as vulnerability scanners, penetration testing, tabletop exercises, and more.

In incident response, security teams can use vulnerability scanners to automatically detect underlying vulnerabilities and exposures that may have contributed to the security incident. Vulnerability scans can help SecOps teams prioritize their remediation efforts.

When you find vulnerabilities, you first address them through patching using patch management, which is the process of remediating vulnerabilities. In incident detection and response, once you discover the vulnerability associated with the incident, you patch it to prevent it from being exploited in the future. For example, you can use patch management tools in Google Cloud to patch operating system vulnerabilities for virtual machines (VMs).

Vulnerability scanners

A **vulnerability scanner** is software that automatically compares known common vulnerabilities and exposures against the technologies on the network. There are many different vulnerability scanners that you can use to identify vulnerabilities in different layers of a cloud environment such as the network, web applications, containers, API keys, and more.

Examples of vulnerability scanners in Google Cloud Platform include:

- **Security Command Center (SCC)**: Security Health Analytics is built into SCC and uses specialized detectors built into the Google Cloud infrastructure to help detect vulnerabilities and threats.
- **Rapid Vulnerability Detection**: Operates as a network and web application scanner that scans endpoints to help detect vulnerabilities such as weak credentials, incomplete

software installations, exposed administrator user interfaces, and other critical vulnerabilities that have a high likelihood of being exploited.
- **Web Security Scanner**: Scans applications, compute instances, and Kubernetes containers to help identify vulnerabilities.
- **Artifact Analysis**: Provides vulnerability scanning and metadata storage for containers on Google Cloud. You can use it to scan container images, Docker files, and other artifacts for known vulnerabilities

Penetration testing

Vulnerability scanners provide an *automated* way to help identify vulnerabilities. They are not perfect and can't catch all vulnerabilities. Manual methods can be used to complement vulnerability management. One manual method is **penetration testing** (**pen testing**) which is a process where a red team simulates cyber attacks to help identify vulnerabilities in an organization's security infrastructure. Organizations can use third party suppliers to perform penetration testing, or have their own red team with pen testers. **Red team** is a generalized term for a team of ethical hackers whose main role is to mimic potential adversaries to thoroughly examine the security defenses of an organization.

Note: Penetration tests are not only useful for vulnerability management, you can also use them to help meet regulatory standards and requirements such as PCI DSS.

Tabletop exercises

Tabletop exercises are scenario-based exercises that involve an organization's security team and other stakeholders. They are commonly performed by members of the **blue team,** who are responsible for defending the organization's systems and networks from simulated attacks.

Tabletop exercises should include a list of participants' roles and responsibilities, an outline of the exercise, key facts about the security incident, and discussion questions. Tabletop exercises must not be performed in isolation from other departments. Security is a team effort. Including the right people ensures that the exercise is effective and that participants are better prepared to respond to a security incident. In addition to the security team, this includes members from executive leadership, IT teams, business units, public relations, legal, human resources, and application and data owners.

Key takeaways

Vulnerability management is a key part of cloud security. Cloud environments are complex and always changing. Understanding the tools and processes behind vulnerability management will help you, as a cloud security professional, better protect organizations from security incidents.