Google Cloud

Vulnerability management

So far, you've learned that vulnerability management is the practice of identifying and mitigating weaknesses in your cybersecurity infrastructure and architecture. Various organizations, like MITRE and OWASP®, have created vulnerability management frameworks that organizations can use to help support the vulnerability management process. To pick the right frameworks, it's important to match the strengths of each framework to your organizational needs. In this reading, you'll learn more about the different frameworks and tools that support vulnerability management.

Vulnerability management

Vulnerability management tools and frameworks guide good security decision making. While risk management focuses on guiding the process of identifying, assessing, and managing risk, vulnerability management is more focused on the ways in which a system may be compromised, regardless of the level of impact on the system, or its role in the organization. Vulnerability management focuses on the likelihood of a compromise on the system instead of the impact the compromise might have. Tools like MITRE ATT&CK® help security teams think about the threats to a system, so they can find the right controls to apply to lower the likelihood of compromise or failure.

Vulnerability management and modeling: MITRE ATT&CK®

MITRE is an unbiased, nonprofit organization that was established to provide engineering and technical guidance to the federal government. Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) is the threat modeling framework that was developed as part of a MITRE research project. MITRE ATT&CK® outlines 14 tactics used by threat actors:

Tactic	**Attacker(s) Objective**
1. Reconnaissance	Gather information they can use to plan future operations
2. Resource Development	Establish resources they can use to support operations
3. Initial Access	Get into your network
4. Execution	Run malicious code
5. Persistence	Maintain their foothold

6. Privilege Escalation	Gain higher-level permissions
7. Defense Evasion	Avoid being detected
8. Credential Access	Steal account names and passwords
9. Discovery	Figure out your environment
10. Lateral Movement	Move through your environment
11. Collection	Gather data of interest to their goal
12. Command and Control	Communicate with compromised systems to control them
13. Exfiltration	Steal data
14. Impact	Manipulate, interrupt, or destroy your systems and data

One of the major benefits of MITRE ATT&CK® is its ability to help organizations stay up-to-date with the latest threats and attack techniques. The framework is regularly updated with new techniques and tactics as they emerge, so that organizations are aware of the latest threats, and can take proactive steps to mitigate them. MITRE ATT&CK® also helps organizations identify and prioritize the most relevant threats, and put controls in place to reduce the risk of a successful attack.

Vulnerability management frameworks

MITRE CVE®, OWASP® Top 10, and the National Vulnerability Database (NVD) are all frameworks that cloud organizations can adopt to help manage and increase awareness about vulnerabilities.

MITRE CVE®

CVE® stands for Common Vulnerabilities and Exposures. The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. It does this by providing a method for publicly sharing information about cybersecurity vulnerabilities and exposures. Each identified vulnerability has its own record in the CVE® catalog. Cybersecurity professionals can use CVE® Records to coordinate their efforts to help prioritize and address vulnerabilities.

OWASP® Top 10

Every year, OWASP® publishes its Top 10 threats and vulnerabilities to increase awareness of the most common risks. The OWASP® Top 10 can be used as a basis for scans and alerts.

National Vulnerability Database (NVD)

NVD is a publicly accessible repository of data about known system and software vulnerabilities created and updated by the National Institute for Standards and Technology (NIST). The NVD is updated regularly with information from researchers, vendors, and other security organizations.

Key takeaways

Knowing about the different vulnerability management frameworks will help you be aware of common, new, and emerging threats, so you can improve your organization's security management posture.

Resources for more information

Learn more about vulnerability management by clicking these links:

- OWASP Top 10 for 2023
- NVD Homepage
- VulnDB
- DoD DISA IAVA
- MITRE CVE®