Google Cloud

Guide to risk assessment and compliance management with Security Command Center

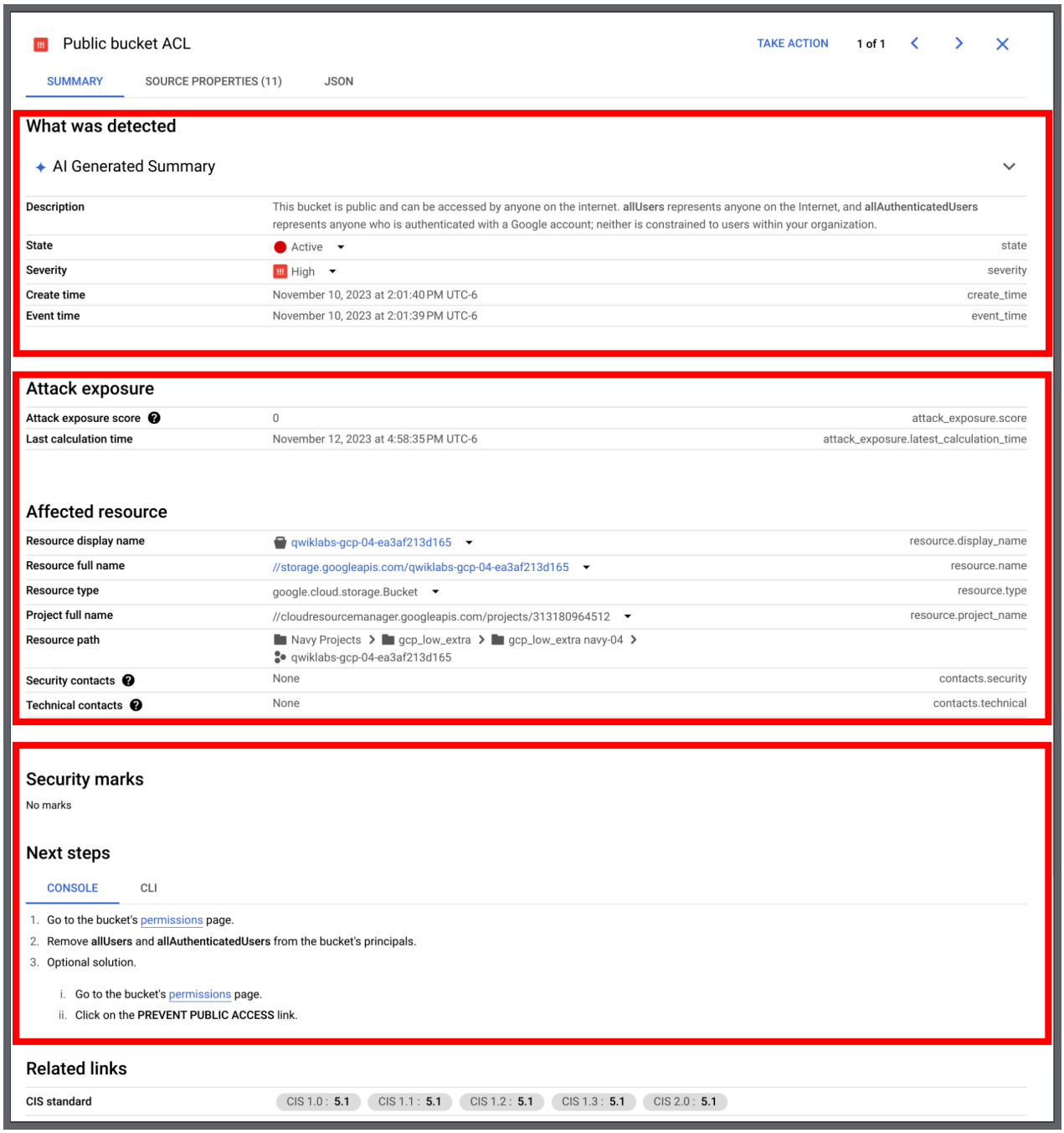
You've learned about vulnerability management frameworks which are used to identify and classify vulnerabilities. You've also explored key cloud tools used in managing risk and compliance. In this reading, you'll learn about how to leverage Security Command Center to help identify and remediate threats.

Security Command Center (SCC)

Security Command Center (SCC) is Google Cloud's centralized vulnerability and threat reporting service. SCC can help organizations strengthen their security posture. SCC does this through *services* which detect security issues in an environment. Through services, SCC scans resources on Google Cloud to help identify threat indicators, vulnerabilities, and misconfigurations.

Built-in services include: Security Health Analytics, Event Threat Detection, Container Threat Detection, and Web Security Scanner. In this reading, you'll focus on Security Health Analytics. Security Health Analytics helps find and report misconfigurations of resources such as excessive identity and access management (IAM) permissions or publicly exposed resources.

When these services detect a threat, vulnerability, or misconfiguration, they create a *finding*. A finding is a report that describes the security issue, the affected Google Cloud resource(s), and provides solutions for fixing the issue. You can access these findings within SCC.



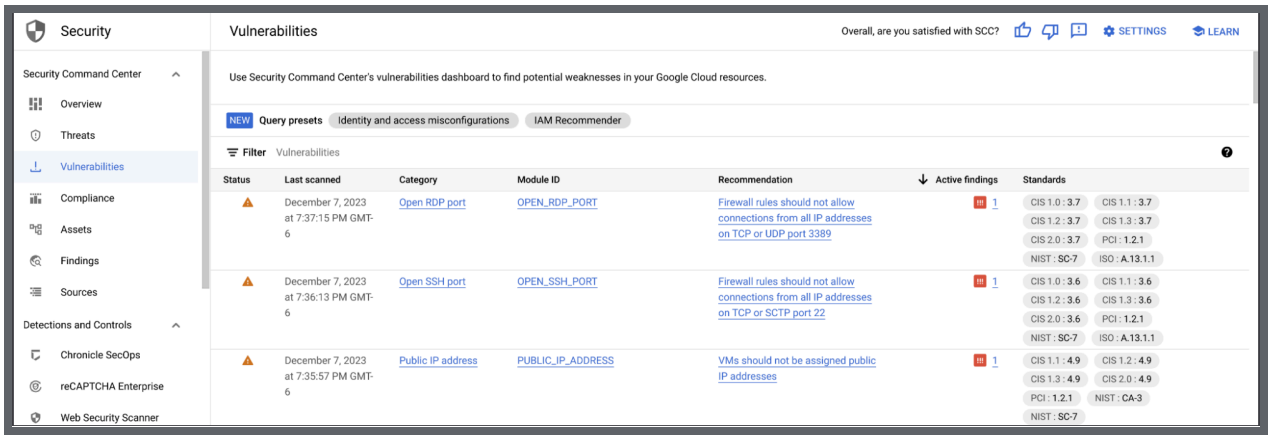
Note: Security Command Center has two service tiers: Standard and Premium. The tier type determines which built-in services and their features are available to use. In this program, the labs provide you with access to the Premium tier.

Pro tip: You can use the SCC query editor to build queries to retrieve and filter findings.

Vulnerabilities

The Security Health Analytics service generates vulnerability findings that are available to access in the **Vulnerabilities** page in SCC. Security Health Analytics uses *detectors* to help identify vulnerabilities and misconfigurations. Each detector coincides with a finding category. For example, the storage vulnerability findings category uses detectors that detect vulnerabilities relating to Cloud Storage buckets. Here are some examples of detectors from the storage scanner type and their importance in helping maintain the security of a cloud environment:

- **Public bucket ACL**: Detects if a Cloud Storage bucket is publicly accessible. Publicly accessible buckets are not secure because they allow public access to data in the buckets.
- **Bucket policy only disabled**: Detects if uniform bucket-level access isn't configured. Uniform bucket-level access is a security suggestion for bucket access. It enforces a single set of permissions on the bucket and its objects which helps simplify IAM management and improve security by reducing the potential for misconfigurations.
- **Bucket logging disabled**: Detects if there is a storage bucket without logging enabled.



Compliance

SCC can also measure your Google Cloud environment against standards and regulations such as Center for Information Security (CIS), Open Web Application Security Project (OWASP®), and more. You can also generate compliance reports to help identify whether your cloud resources have any compliance violations. The SCC compliance reports not only map security categories to the applicable standards and regulations, they also provide you with actionable insights and recommendations to help you address and comply with specific requirements. You can access these compliance reports in the **Compliance** section.

Key takeaways

SCC services include key cloud tools that a cloud security team can use for compliance and vulnerability management. The team utilizes the services to help quickly identify and address vulnerabilities in a cloud environment before they can be exploited and maintain a robust security posture.

Resources for more information

- For more information on detectors, check out Overview of Security Health Analytics.
- If you'd like to learn more about Security Command Center's Compliance page, check out Manage and monitor for compliance.