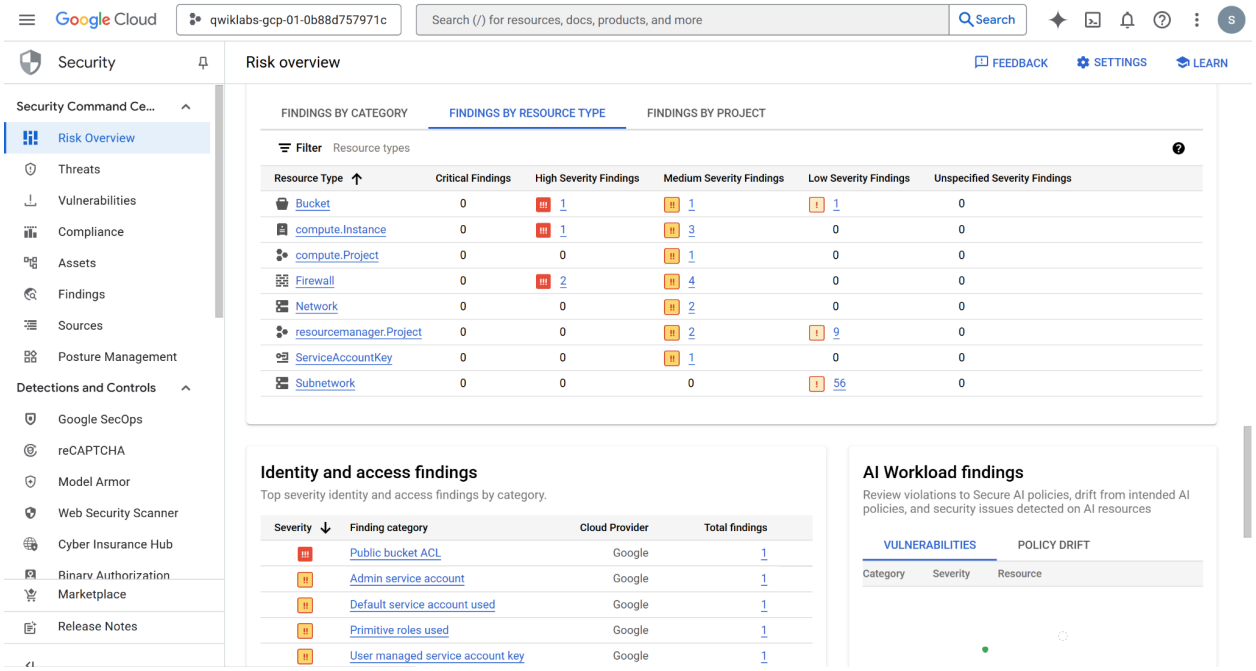
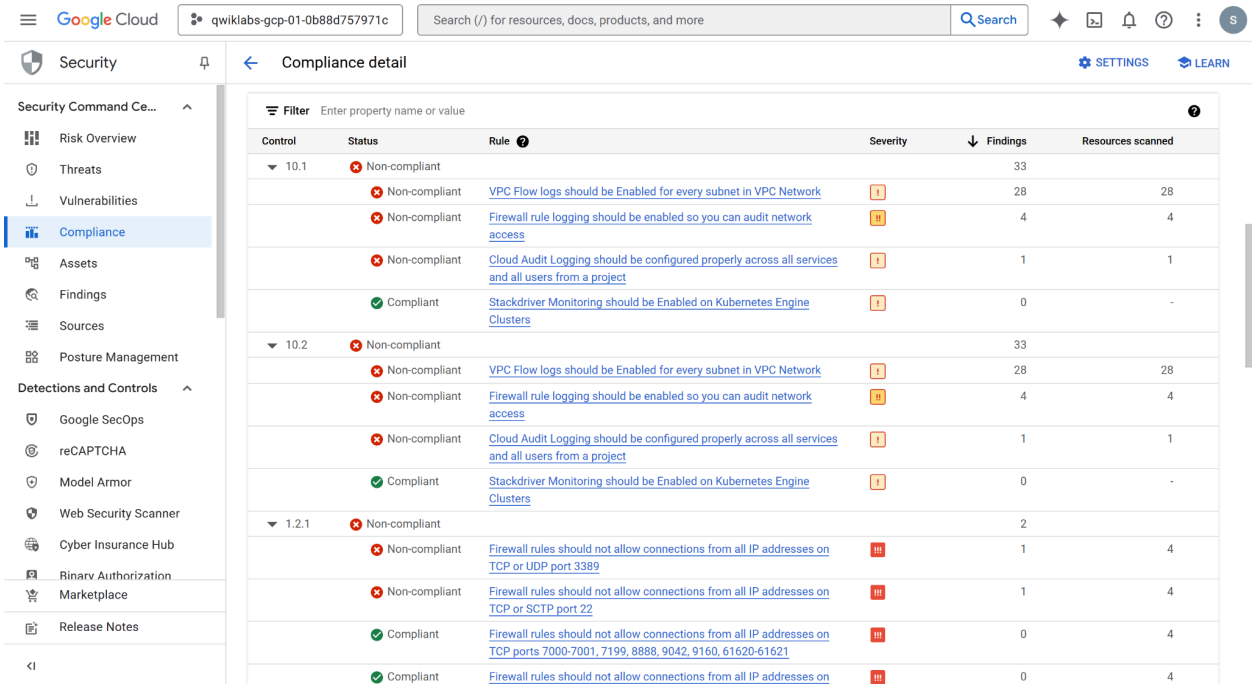
Visual Report:

This is a document demonstrating how I addressed and remediated vulnerabilities in the Cloud of Cymbal Bank using Google Cloud's Security Command Center. Screenshots throughout the report showcase each step of the remediation process, providing a visual walkthrough of how I improved the security posture of the environment.

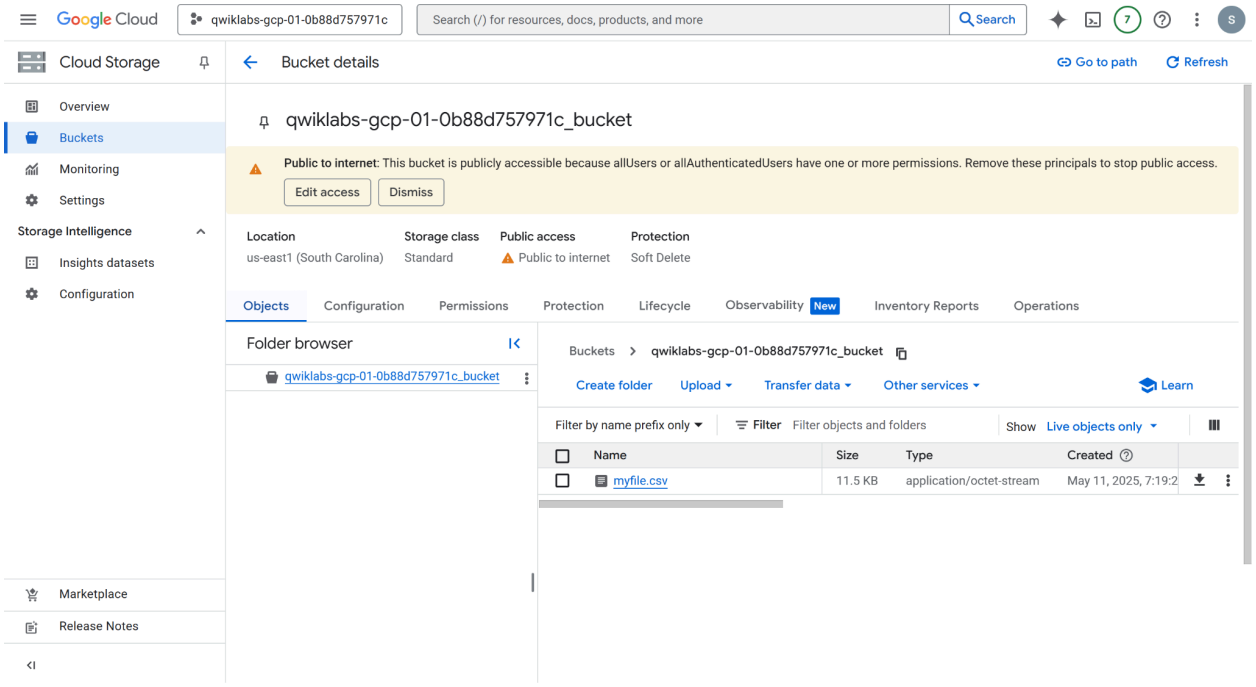
I began the investigation by leveraging Security Command Center's Risk Overview panel to assess the simulated bank's current threat exposure. I prioritized findings based on severity and focused on public bucket access, overly insecure firewall rules, and under-protected service accounts. This critical triage step aligns with security best practices in asset risk classification.



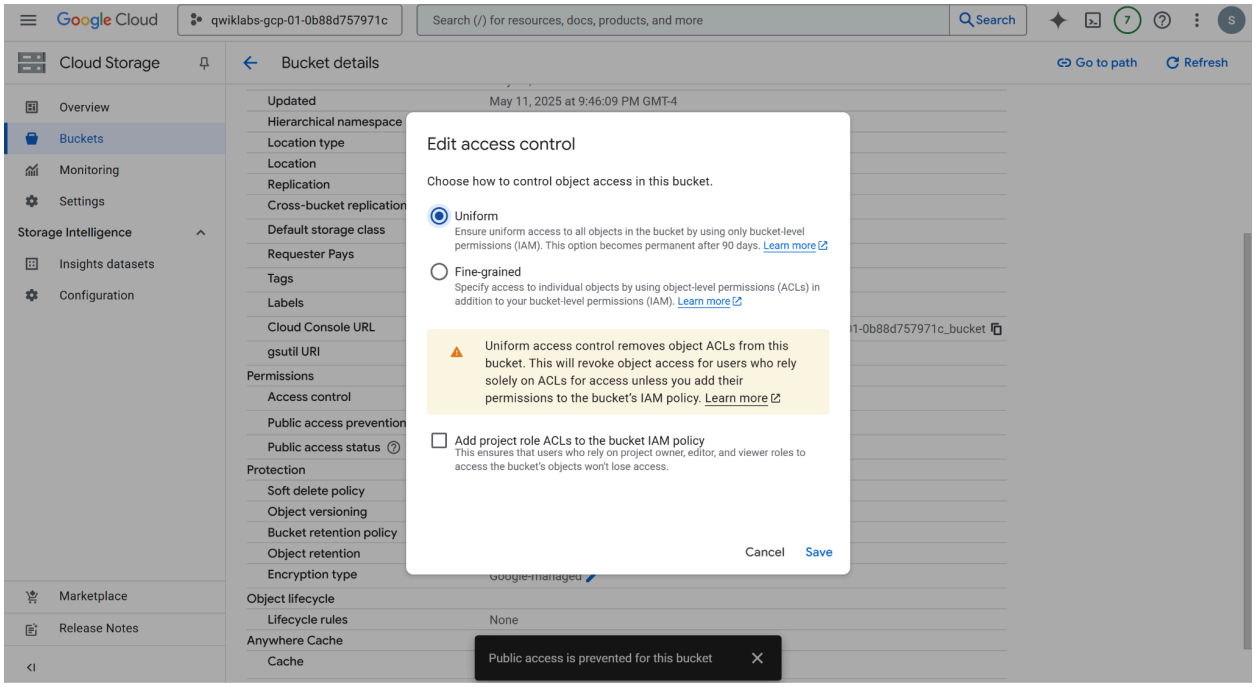
I reviewed the Compliance tab in Security Command Center to identify all failed control checks across the environment. These included missing VPC Flow Logs, disabled firewall logging, and overly permissive inbound rules.



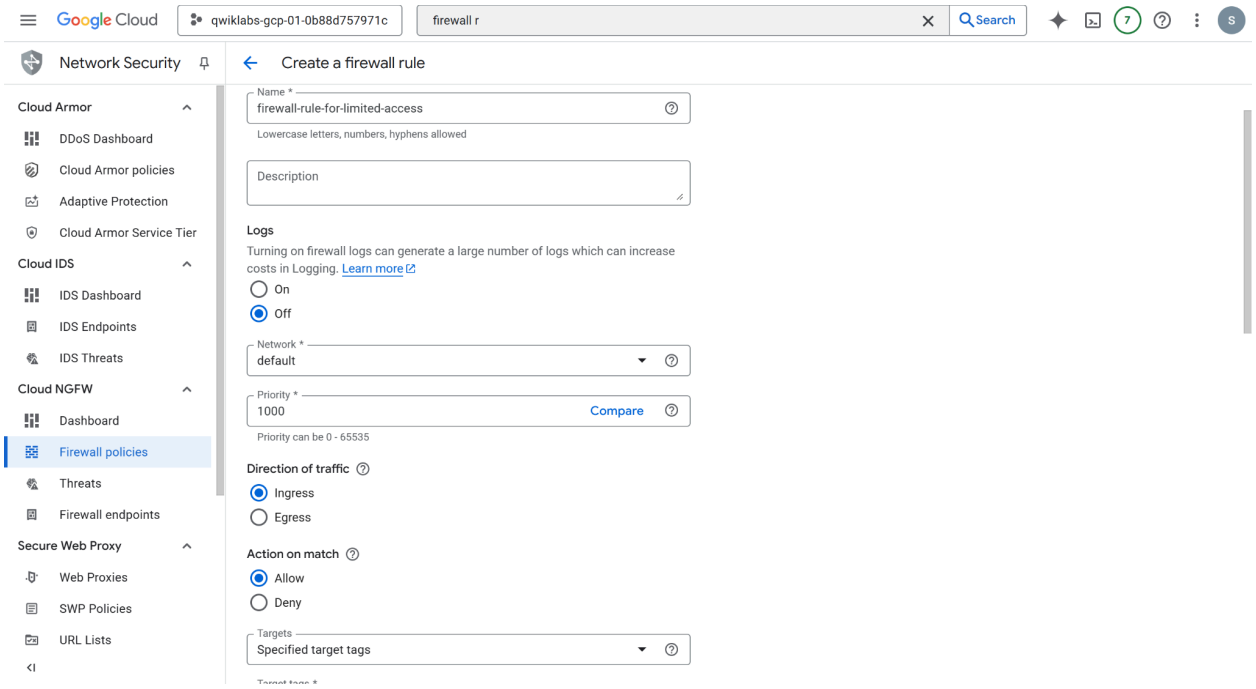
I discovered that the cloud storage bucket was publicly accessible, creating a major data exposure risk. Buckets accessible to *allUsers* without restriction pose a high likelihood of sensitive data leaks which violates the principle of least privilege (PoLP).

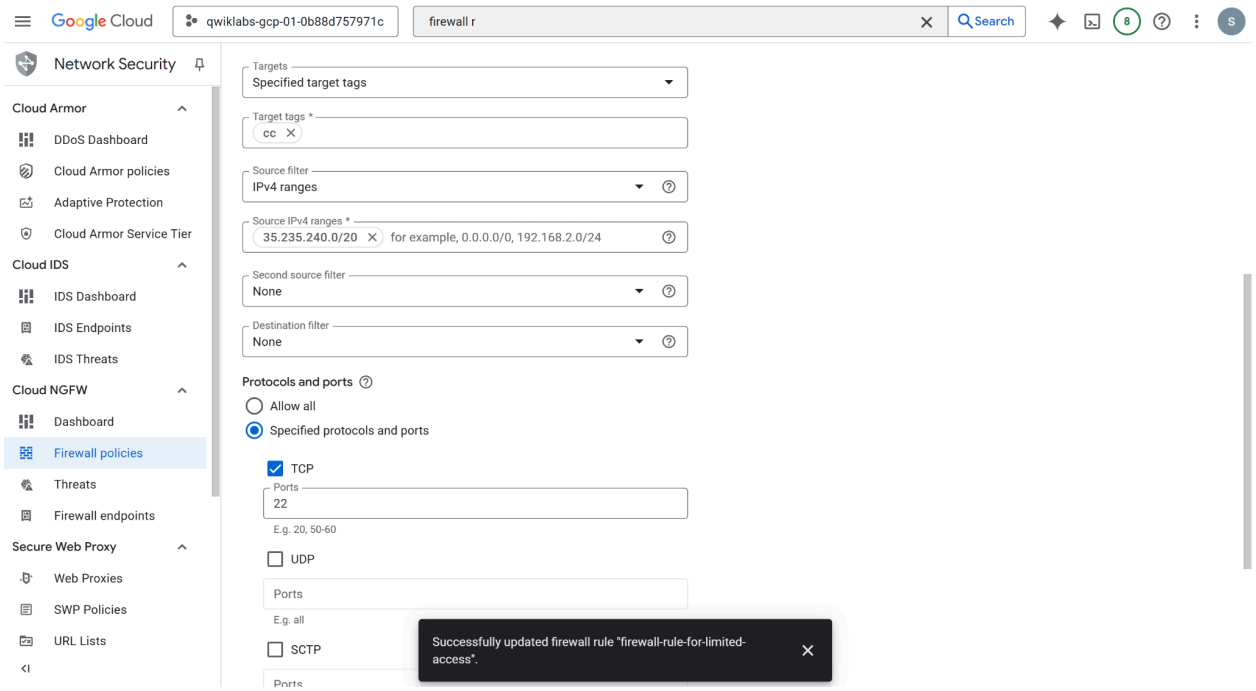


To mitigate the storage threat, I enforced uniform bucket-level IAM policies and revoked object-level ACLs (Access Control Lists) that granted public access.

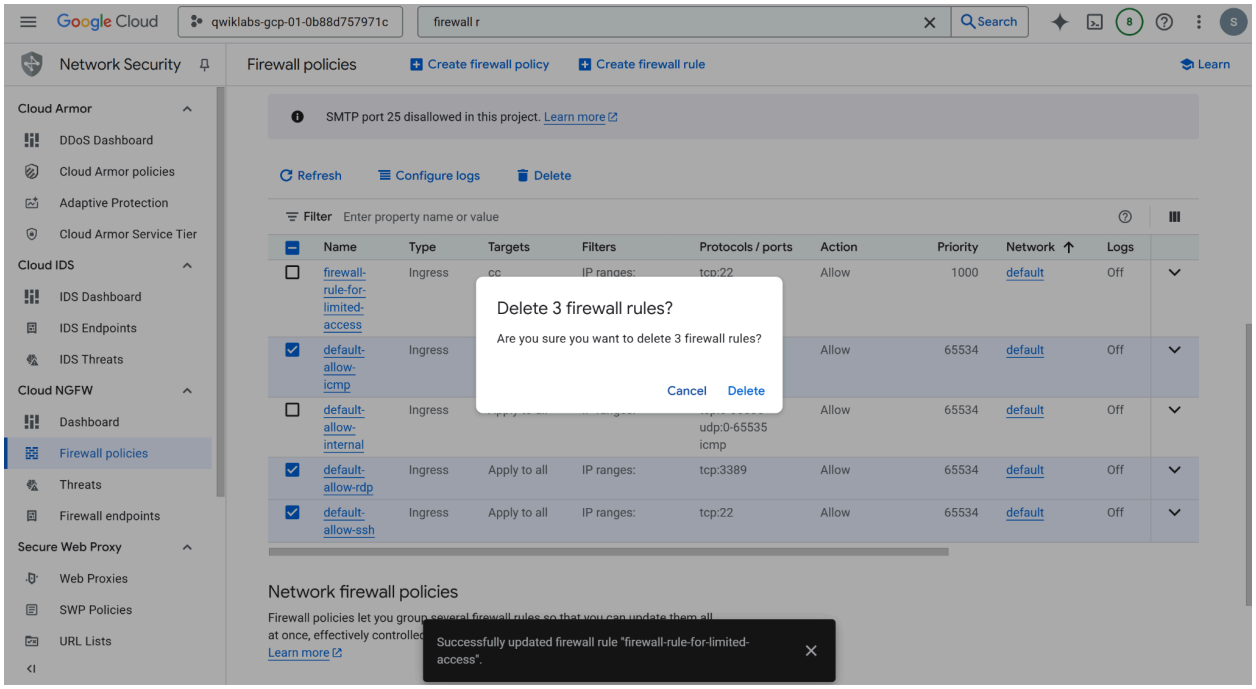


To reduce exposure, I created a custom rule that allows SSH (TCP port 22) only from a trusted IP range (35.235.240.0/20). Instead of using Google Cloud's default rules, I specified exact parameters: source IPs, target tags, direction, protocols, and ports, essentially enforcing least privilege and zero trust principles to restrict access to just what's needed.





I removed default firewall rules (allow-ssh, allow-rdp, allow-internal) that permitted unrestricted traffic across dangerous ports. These broad rules often leave cloud environments vulnerable to scanning, unauthorized access, or pivoting during post-exploitation stages.



I turned on firewall logging to record all incoming connection attempts matching my firewall rules. This allows for real-time monitoring and threat detection as patterns can be easily monitored through log records.