Chameleon Company

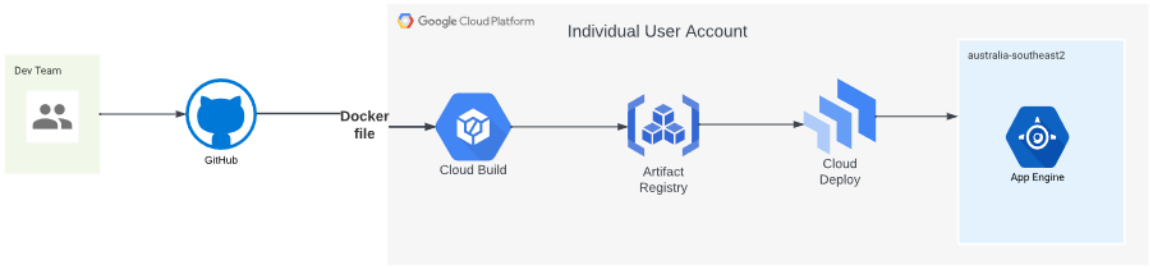
Infrastructure Security Report

Purpose

The purpose of this report is to highlight the need to develop a DevSecOps Security approach for the Chameleon company operations, by Integrating application security principles into software development and the deployment lifecycle will not only strengthen the collaboration between the Chameleon development and security team but prioritise security with deployment. Currently the security team has no visibility into the deployment lifecycle and Cloud Security Settings.

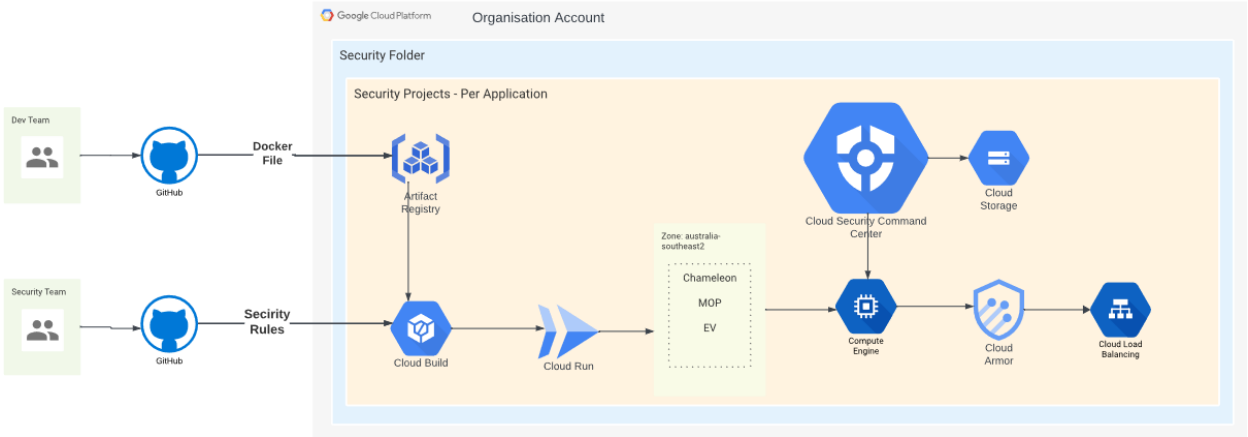
Current DevOps and security operations.

The below image illustrates the current development and deployment for the Chameleon Company web applications, further information including the current security controls can be found in Chameleon Security plan by Leon Netto. The security team is not involved in managing the current infrastructure model and conducts ad hoc automated and manual security tests on either hosted or self-hosted web applications. The hosted web applications are currently on Google Cloud Platform (GCP) under an individual student account where none of the GCP security features are enabled. The security team repeats multiple tasks without the required insights and knowledge of how each of the companies' applications works and what cloud security measures are currently in place to mitigate any type of attacks or weaknesses, currently the web application tests conducted on old web applications not in use.



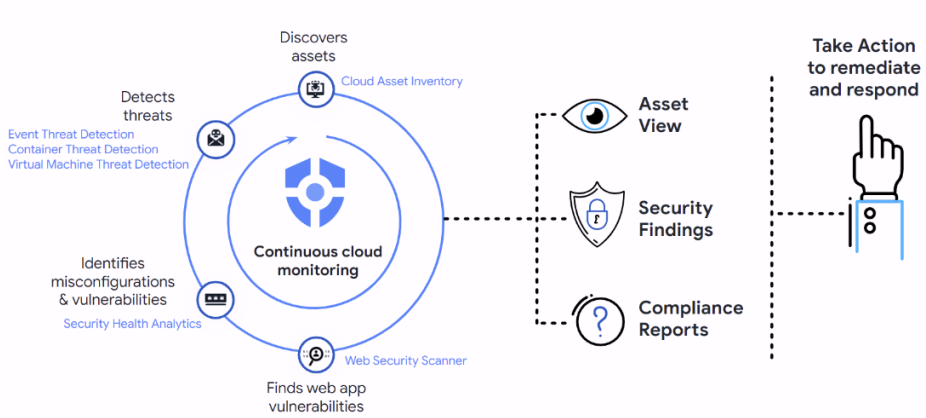
Moving to a DevSecOps model.

The below architecture diagram illustrates how a DevSecOps approach will ensure security plays an integrated role in the lifecycle of the Chameleon companies' application deployments, which has been built on top of the existing technologies in use to incorporate application and infrastructure security.

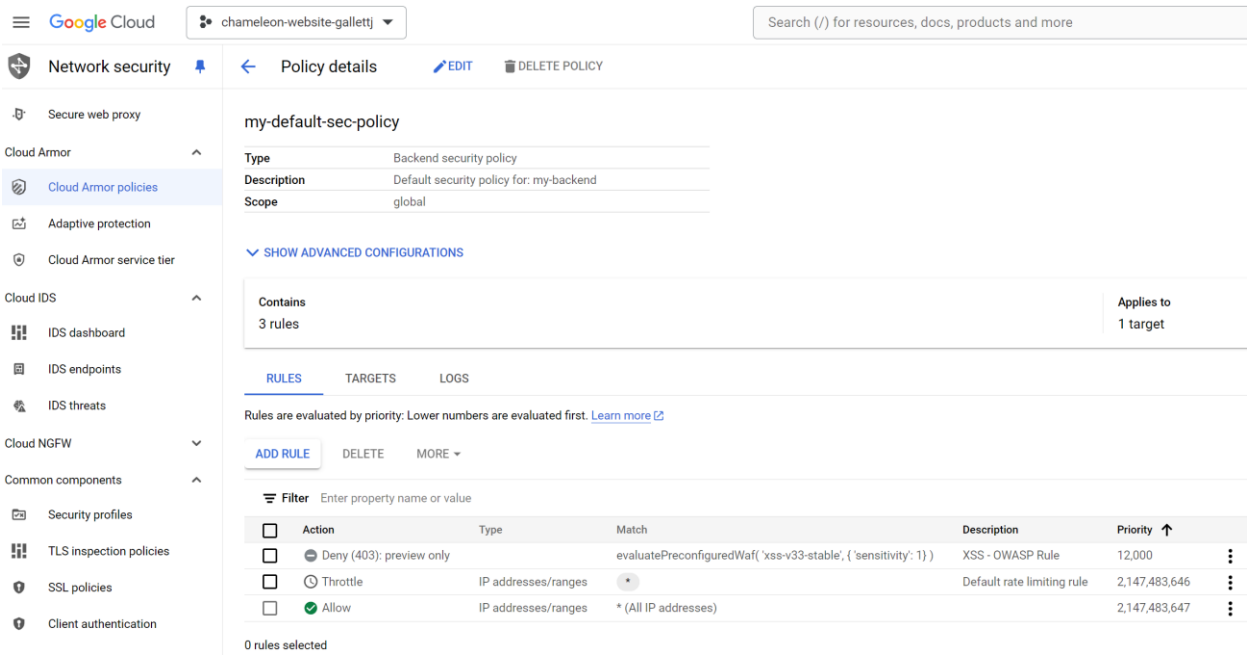


The main new items to be added to the DevOps model above are the GCP Security command centre, the Security command centre will enable the Chameleon security team to collaborate within multiple areas

including (SOC) analysts, Vulnerability analysts and compliance, to investigate and mitigate any security issues or threats across all Chameleons cloud web applications and environments and



Cloud Armor: Cloud Armor provides protection against the common OWASP top 10 attacks, including Cross Site Scripting (XSS), SQL injection (SQLi) and distributed denial of service (DDoS) attacks, security rules are required to be manually configured, Cloud Armor has a set of preconfigured WAF rules for ease of use, a security policy can be implemented by the Chameleon Security team to suit the current applications and environments and managed using infrastructure as code through terraform. Managing a security policy has additional advantages for the Chameleon Security team as custom rules can instantly be written to mitigate against any zero-day attacks or tuned to suit the current application environment, example limiting traffic from specific countries. The below image demonstrates adding the OWASP Cross-Site-Scripting (XSS) rule to the Cloud Armor policy.



Recommended Roles for Chameleon Security Team

In DevOps roles and responsibilities are shared across the development and operations, adding a security component to the existing model will require the Chameleon security team to take a proactive approach to not only assess potential security risks through extensive testing but to build and maintain the infrastructure required. The operations in DevSecOps should focus on building secure infrastructure at every level, the following roles and responsibilities would be recommended.

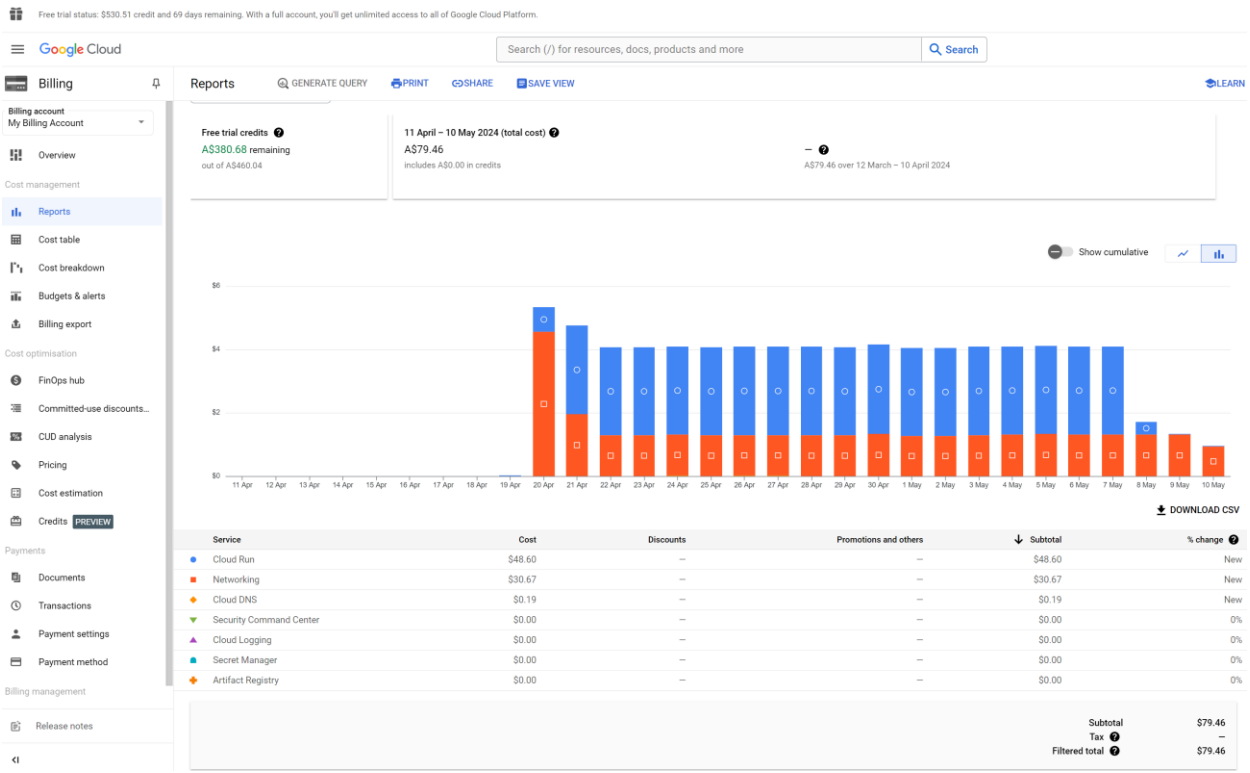
Role	Responsibility
Security Engineers	Security infrastructure as code, GCP, CI-CD, GitHub, Terraform
SOC analysts	Penetration testing, WAF rules, Monitoring
Analysts	Log Analysis, Billing, Monitoring, Research, IAM
Leadership Team	Strategic direction, communication facilitation, compliance,

Current deployment cost analysis.

Building your own lab in GCP currently offers new users a $300 AUD credit for 90 days usage, by signing up for Cloud Identity as a Google Cloud Admin you can register a Domain name (still using free GCP credits) and receive an additional $160 AUD Credit, after 3 weeks I also received an organisational free trial bonus of $152.70, the total credits equals $612.70 AUD for 90 days.

After a few weeks of running penetration tests, DDoS attacks and automated web scans on the hosted Chameleon static web application running a warm instance the cost was approx. $4.20 per day, moving to a cold instance reduces the cost less than $1.40 per day. The security infrastructure build time was approximately 4-6 hours, this could be improved using Infrastructure as code through Terraform. The below table provides options how the Chameleon Security team could maintain the infrastructure each trimester hosting multiple web applications still within the free trial credits and periods.

Application	Static/Dynamic	Usage Estimate Cost	Number of days	Total Cost
Chameleon	Static	$2.00 per day	80 (Cold start)	$160.00
Mop	Dynamic	$4.00 per day (Est only)	80 (Cold start)	$320.00
WAF Rules		$15.00 per month		$45.00
Domain Name		$15.00 one time		$15.00



References

https://www.quadrasystems.net/blogs/take-control-of-security-and-risk-management-with-google-cloud

https://dev.to/rushi-patel/deploy-react-app-to-google-cloud-run-with-github-actions-cicd-a-complete-guide-52pf

https://www.cloudskillsboost.google/paths/419?utm_source=cgc&utm_medium=website&utm_campaign=evergreen

https://medium.com/@expertopinionsa12/devsecops-vs-devops-a-comparison-of-roles-and-responsibilities-9d00b54b16f1

https://cloud.google.com/security-command-center/docs/concepts-security-command-center-overview

https://github.com/Chameleon-company/Chameleon-security/blob/master/trimester_3_2023/Chameleon%20System%20Security%20Plan.pdf

https://github.com/GallettiJ/cloudArmor/blob/main/cloudArmorStandard/cloudArmor-backendPolicy.tf

https://owasp.org/www-project-cloud-native-application-security-top-10/

https://cloud.google.com/armor/docs/cloud-armor-overview

https://cloud.google.com/armor/docs/waf-rules

https://developer.hashicorp.com/terraform/tutorials/gcp-get-started