Connected Research - KDD Google Cloud Software Delivery Shield

DACI Decision

Status	REJECTED
Impact	This decision affects the development process and to a great degree the tools, that should be used by the LabBooster team.
Driver	KRONTIRAS-ext, Pavlos
Approver	KRONTIRAS-ext, Pavlos
Contributors	
Informed	Roscetti, Nicolas MENGHETTI, Matteo SIMAO-ext, Vitor
Due date	
Outcome	Will not proceed with general implementation at this time. Decision made on 13 Dec 2024

Tips and info

Recommendations

Contributors

Contributors: I am seeking the right people to get involved in the decision. Add your comments to this page, let's get the conversation started.

Please add:

- ***The people** directly impacted by this so we can include them.*
- ***Any references** to previous work and investigations that we can leverage.*
- *Any **constraints and challenges** we need to consider to make this decision and following action plan.*

Impact rating

Here's an example you can use as a guide.

Decision characteristics	
• The decision will have a material impact on the customer experience OR • will significantly impact the roadmap OR • will adversely disrupt an internal business process.	HIGH
• The decision will involve a less than material change to customer experience OR • will impact the roadmap OR • will impact an existing internal business process	MEDIUM
• All other decisions	LOW

Background

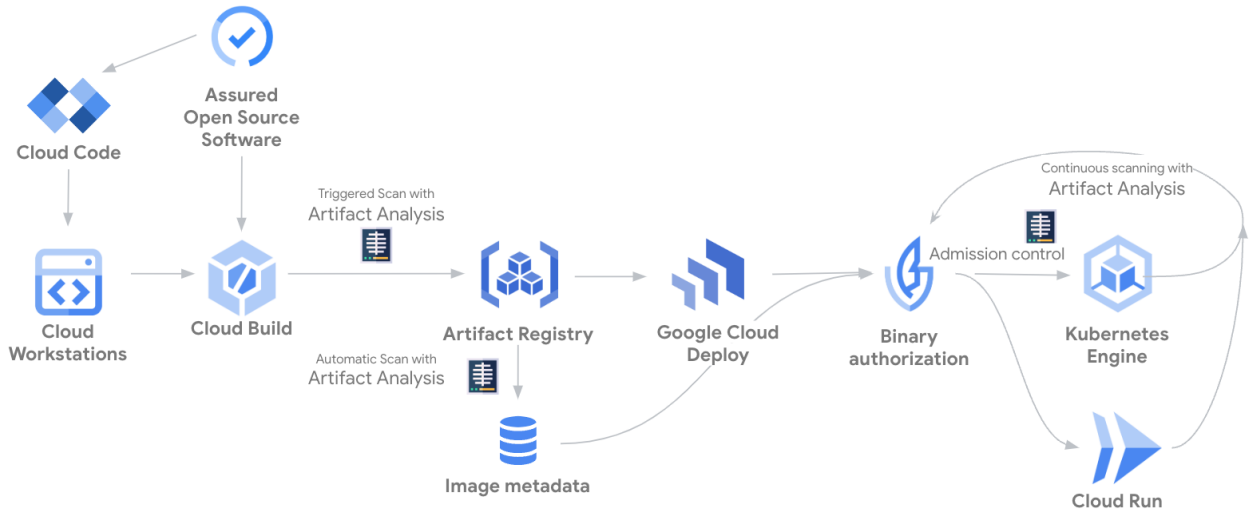
The Google Cloud Software Delivery Shield is a set of tools and services that offer a secure cloud-hosted development environment with end-to-end security built-in, that prevents any unauthorized code or data exfiltration from the organization's GCP estate.

Current state

All development is done locally on individual computers with full access to upload/download files and data.

Data for decision support

High level Architecture of GCP Software Delivery Shield



Options considered

	Option 1: Do nothing	Option 2: Use GCP Software Delivery Shield
Description	No change	Implementing this framework will require the activation and use of several new GCP tools & services and will change the current development and software build and delivery processes.
Rollout plan	No change	• Request new development GCP project in Syensqo landing zone with all required APIs and network configurations enabled • Create Artifact repositories for source code management and Assured Open Source Software • Create development VMs with necessary software tools installed • Create build pipelines • Test and validate framework • Create user documentation • Scale up the rollout to developers

Pros and cons	⊕ No change to current development process ⊕ No additional cost or effort required ⊖ Higher on-boarding time for new team members ⊖ Potential for lost time and inefficiencies due to development environment ⊖ Continued security risks & inefficiencies	⊕ Secure development with validated secure 3rd party libraries and automatic scanning of containers for security vulnerabilities ⊕ Digitally signed containers for verifiable build provenance ⊕ Prevents data loss/exfiltration by enforcing a security perimeter with resources contained within GCP ⊕ Standardizes development environment and tools, minimizing errors and lost time troubleshooting problems due to misconfiguration or configuration differences ⊕ Accelerates on-boarding time for new team members ⊕ Potentially reduces hardware costs with reduced performance requirements for developers' physical hardware ⊖ Requires fast and reliable Internet connectivity ⊖ Increases GCP consumption costs with use of new tools & services ⊖ Would require additional GCP skills to support framework ⊖ Libraries currently in use in DataLab code may not be security validated ⊖ Introduces a completely new development process ⊖ May require significant amount of time to deploy, validate, and rollout ⊖ May not be easily transferable to other cloud platforms, e.g. Azure
Risks	• Continued risk of data exfiltration • Continued risk of including security vulnerabilities in delivered product	• Resistance from developers that want to maintain their own independent development environment • Additional costs are not acceptable • Skills are not available in team to support the framework
Estimated cost and effort		

FAQ

Q1.

A1.

References

Relevance	Link
Official documentation of the GCP Software Delivery Shield	https://cloud.google.com/security/solutions/software-supply-chain-security?hl=en
Review of test implementation	

Follow-up action items

- [ ]

Learn more: https://www.atlassian.com/team-playbook/plays/daci