Connected Research - KDD Code Security Tools

DACI Decision

Status	NOT STARTED
Impact	This decision affects the level of security protection built into the application code developed and deployed by the Lab Booster team.
Driver	KRONTIRAS-ext, Pavlos
Approver	KRONTIRAS-ext, Pavlos
Contributors	
Informed	
Due date	
Outcome	

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 application code developed for Lab Booster (DataLab) includes 3rd party libraries that are widely used in the industry but may still include vulnerabilities. Also the business logic within the code along with the application design may itself create vulnerabilities that could expose the Syensqo systems and data to potential bad actors. Including security tools as part of the application code build, and the development practice itself can significantly reduce this risk.

Current state

No standardized security tools are used.

Data for decision support

Options considered

	Option 1: Do nothing	Option 2: Aikido	Option 3: Snyk	Option 4: SonarQube	Option 5: HCL AppScan
Description		https://www.aikido.dev/	https://snyk.io/	https://www.sonarsource.com/	https://www.hcl-software.com/appscan
Rollout plan					
Pros and cons	⊕ No change, BAU ⊖ Code quality remains questionable ⊖ Security vulnerabilities can continue to be added to the application ⊖ Additional effort spent on debugging problems that might have otherwise been caught during the build/scanning of the code ⊖ Potential disruption to service if Security team blocks application due to security risks	⊕ Developer-first tool ⊕ Multiple integrations with IDEs and Ci/CD tools ⊕ Real-time scanning during development ⊕ Context-aware, AI-powered analysis, reduces false positives ⊕ Easy to setup/deploy ⊕ Focus on cloud-native security, especially microservices architectures. ⊕ ⊖ Young company (2yo)., not enough track record ⊖ SaaS only ⊖ AI reduces false positives but accuracy is unknown ⊖ SAST only, no DAST capability ⊖	⊕ Scans code, library dependencies, containers, and IaC. ⊕ Integration with IDEs and CI/CD tools. ⊕ Strong open-source vulnerability detection ⊕ Regular updates to address the latest vulnerabilities ⊕ ⊖ SaaS only ⊖ Can be expensive ⊖ Complex setup and confusing UI/UX ⊖ Difficult customization ⊖	⊕ Support for multiple programming languages ⊕ Integration with popular CI/CD tools ⊕ Ease of use & deployment ⊕ Detailed reports ⊕ Plugin can scan code in real time during development ⊕ Customizable rules ⊕ Comprehensive service with code quality + security analysis ⊕ SaaS and on-prem self-managed ⊖ Can be difficult to integrate ⊖ Not very user friendly UI ⊖ Only static analysis ⊖ Learning curve can be steep ⊖ Can be resource intensive for scans of large projects ⊖ SAST only, no DAST ⊖	⊕ Combines static, dynamic, and interactive security testing ⊕ Detailed reporting ⊕ Supports frameworks like OWASP, GDPR, and PCI-DSS ⊕ Feature-rich and stable (has been on market for many years) ⊕ ⊖ Multiple different modules, choosing the right one can be confusing ⊖ Steep learning curve and high maintenance ⊖ Expensive ⊖ Complex CI/CD integration ⊖ Outdated UX/UI ⊖
Risks		New product and community knowledge/skills/support may be limited AI classification may not be very accurate		May not address all use cases	High cost and complexity to maintain
Estimated cost and effort		From € 299/mo for 10 users https://www.aikido.dev/pricing	$25 per dev/product /month (minimum 5 devs / $1,375 annually) https://snyk.io/start/team/	Limited functionality for free Developer license $160 /year https://www.sonarsource.com/plans-and-pricing/	On demand, not publicly shared

FAQ

Q1.

A1.

References

Relevance	Link

Follow-up action items

- [ ]

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