Security Project for QGIS

Oslandia

Open source GIS

- 🎂 Born 2009
- 🐓 French SME
- 🔧 high technology
- 🔐 open source
- 🌍 Geographical information systems
- 💯 Open Source “pure player”

At a glance

- 👩‍💻 100% remote company
- 👥 ~30 team members
- 🔬 R&D investment
- 🔗 100% independant
- 🚀 projects from small to large
- 🤾‍♀️ team play (consortiums, partnerships, community…)

Expertise

open source Geomatics (FOSS4G)

Reknown expertise

- consulting
- audit
- training
- development
- maintainance
- assistance (helpdesk)

pdal

GDAL

PROJ

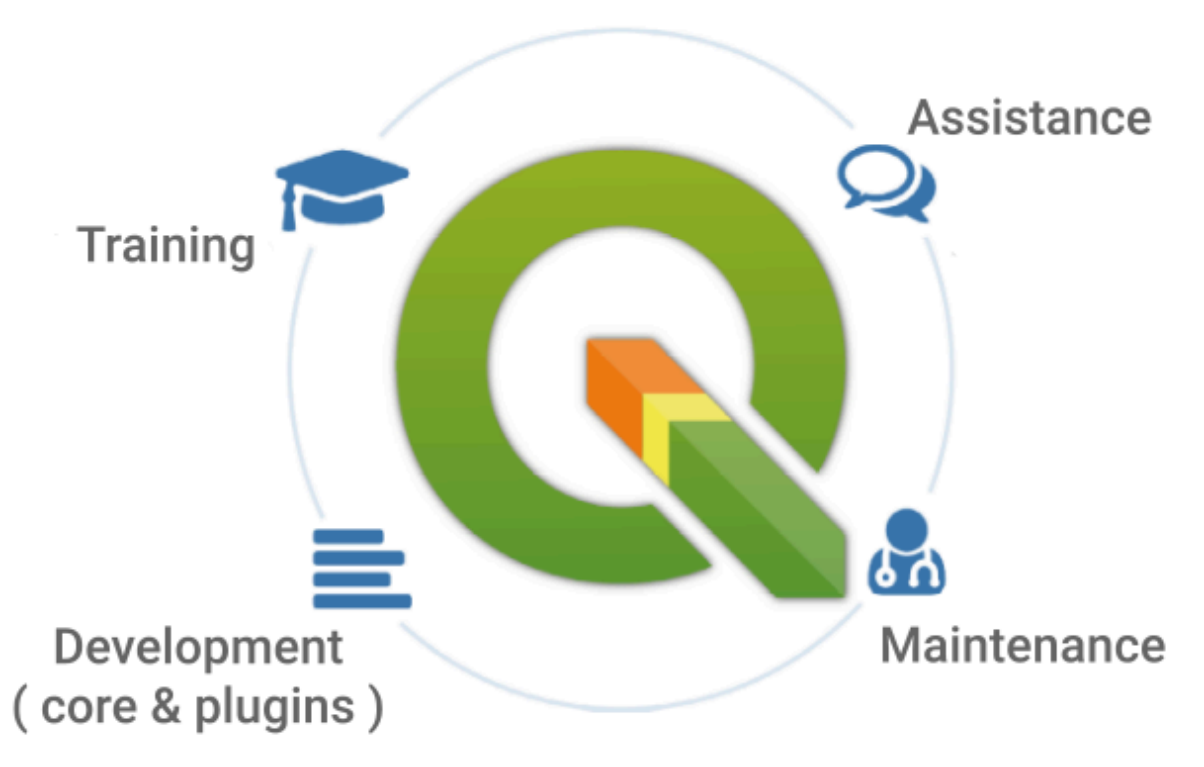
3DTiles

GEOS Geometry Engine Open Source

PostGIS

ANSIBLE

QGIS Editor


Assistance
Training
Development
(core & plugins)
Maintenance

Security Project for QGIS

Strong growth of cyber threats & regulations

- *Cyber Resilience Act* (CRA - EU)
- *Network and Information Security* directive (NIS2 - EU)
- *Cybersecurity and Infrastructure Security Agency* (CISA - USA)

Impacts :

- ➡️ Systems resilience
- ➡️ User's sovereignty
- ➡️ Economic & community ecosystem

🔍 Context

- Increased security requirements
  - CRA (Cyber Resilience Act)
  - Cybersecurity and Infrastructure Security Agency (CISA)
  - NIS2
- Growth in requests via security@qgis.org
- Estimated cost of CRA impact on an open-source projects : +30%
- Risk of IT departments blocking QGIS installation if vulnerabilities are present

💪 Improving QGIS Security

- Adaptations to CRA and NIS2 directives
- Overall strengthening of QGIS and QGIS Server security

👉 Current Situation

- QGIS security processes are too light
- Existing openSSF score page
- Identified security team
- Funded studies for occasional QGIS Server code audits

🔗 Software Components

- QGIS
- QGIS Server
- Underlying libraries:
  - GDAL/OGR
  - PROJ
  - GEOS

Additionally, according to available resources:

- QGIS Web Client
- QField

Impact on OSGeo Scope

Approach relative to other OSGeo software:

- Advance the QGIS project
- Make QGIS a model project for security
- Replicate the approach in other projects

🏗 Proposed Actions

- 1. Builds reproducibility and Build Systems
- 2. Binary and Docker Image Signing
- 3. Code Analysis and Dependency Management
- 4. External Security Audit and Global Analysis

- 5. GitHub Processes and Contribution Management
- 6. Plugin Security
- 7. Artifact Security Analysis
- 8. Security Training, Documentation, and Visibility
- 9. Improve Memory Safety

🎯 Benefits

- Compliance with CRA and modern requirements
- Security risk reduction
- Improved user/organization trust
- Defined and documented security processes
- Enhanced reliability and traceability
- Easier enterprise/IT systems integration
- Better control of the software supply chain
- QGIS as a GIS security leader and OSGeo model

⚠️ Risks

- Resistance to change from long-time QGIS community members
- Managing technical debt (e.g., incompatible dependencies, unavailable resources to upgrade deps…)
- Increased technical entry barriers for contributions
- Insufficient long-term resources to address vulnerabilities

Work packages, Challenges, and Actions

WP A : Security foundations

Budget : 290 000 €

- A.1 Code Analysis and Dependency Management (50K€)
- A.2 Build Reproducibility (45K€)
- A.3 Binary and Docker Image Signing (35K€)
- A.4 GitHub Processes and Contribution Management (35K€)

- A.5 Plugin Security and specific Audit (45K€)
- A.6 Basic Training and Documentation (15K€)
- A.7 Advanced Access Management (15K€)
- A.8 Improve Memory Safety (50K€)

WP B: Strengthening and Compliance

Additional Budget: € 190,000
Cumulative Budget (WP A + B): € 480,000

- B.1 Advanced Code Analysis
- B.2 Advanced Vulnerability Management
- B.3 Optimization of Windows Installation System
- B.4 Security Analysis of Artifacts
- B.5. Extended Training and Visibility

WP C: Continuous Improvement and Advanced Research

Additional Budget: € 170,000

Cumulative Budget (Priorities A + B + C): € 650,000

- C.1 Comprehensive External Security Audit
- C.2 Advanced Code and Security Analysis
- C.3 Community management

📝 Budget Summary

- Work package A: € 290,000
- Work package B: + € 190,000 (Cumulative: € 480,000)
- Work package C: + € 170,000 (Cumulative: € 650,000)

Modalities

- Shared Funding: Focus on large accounts
- Execution: By Oslandia + OPENGIS.ch + security experts + community partners as needed
- Collaboration: Work closely with the QGIS community
- Additional Funding: Explore European grants or other sources

📅 Timeline

- Start actions as early as 2025 Q1
- Progress based on funding availability: Work packages A, B, C in order
- WP A Completion Target: 2025-2026
- WP B and C: 2025-2026
- CRA Application Deadline: From 2027

Proposed Funding Sources

- Solicitation of French ToSIT association
- Open call for funding
- Investment from Oslandia and OpenGIS
- Potential support from OSTIF, OpenSSF, NGI, or other organizations
- Solicitation of QGIS.org

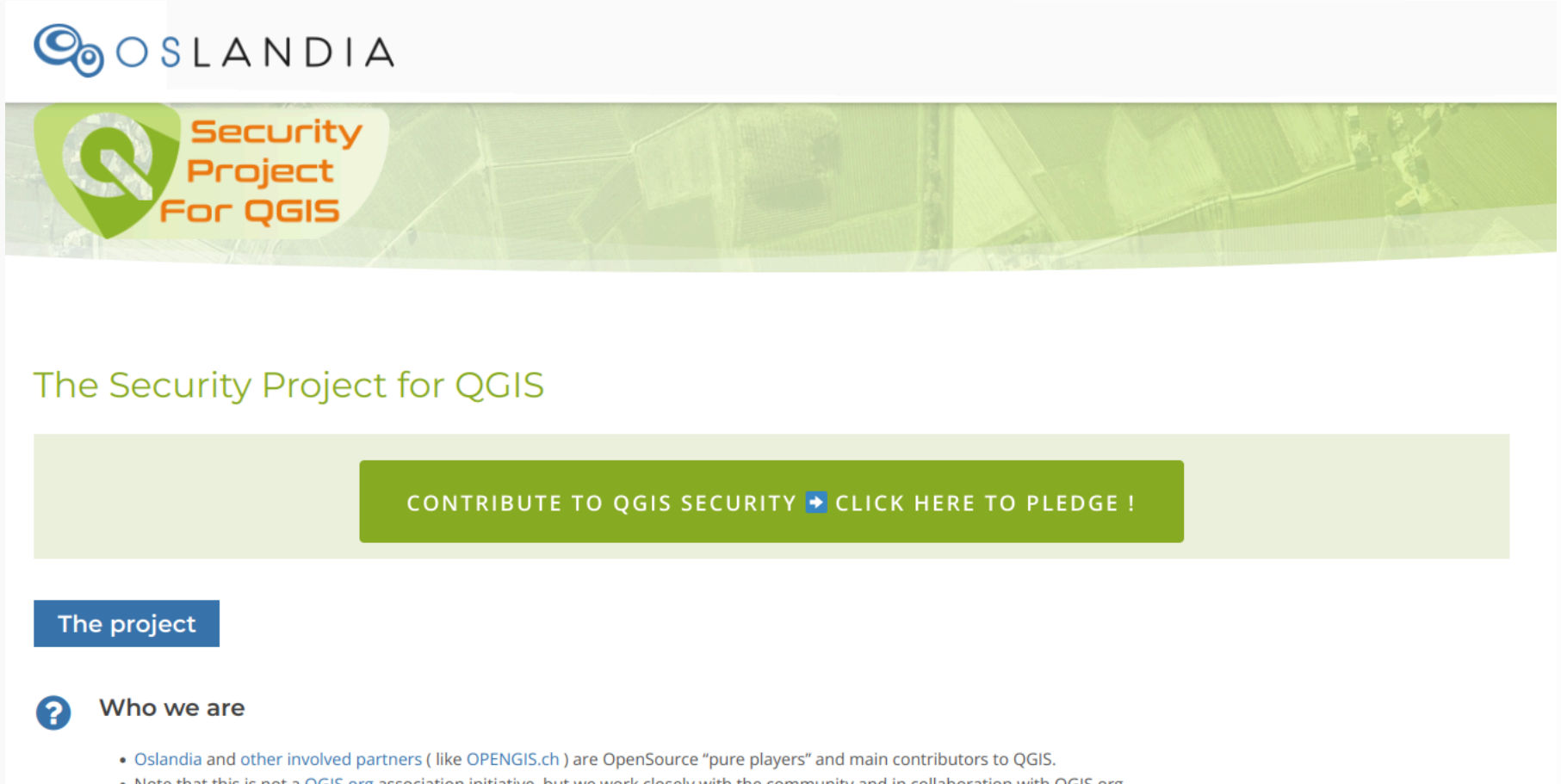
💶 Current contributors

- Orange group
- Grenoble Métropole
- SNCF Réseau
- Oslandia
- OPENGIS.ch
- …

Pledge !

🙏 Pledge to help the project !

https://security.qgis.oslandia.com



Questions ?

qgis+security@oslandia.com