VAULTINUM

SINCE 1976

TECH DUE DILIGENCE SOLUTION

Introduction

1 Introduction

2 Our focus

3 Our methodology

Vaultinum – Technology as a Service

About us

- Technology provider combining automated tools and experts
- Protecting IP and source code for over 40 years
- Providing Equipped Cyber and Tech Due diligence
- For Investors, Vendors and Corporates
- Meeting the need for assessment, compliance and monitoring

- 40 employees - 50% in IT and R&D
- Hosting 250,000+ source codes
- Proprietary technology
- Holistic Approach to Tech DD

ISO 27001

eIDAS READY

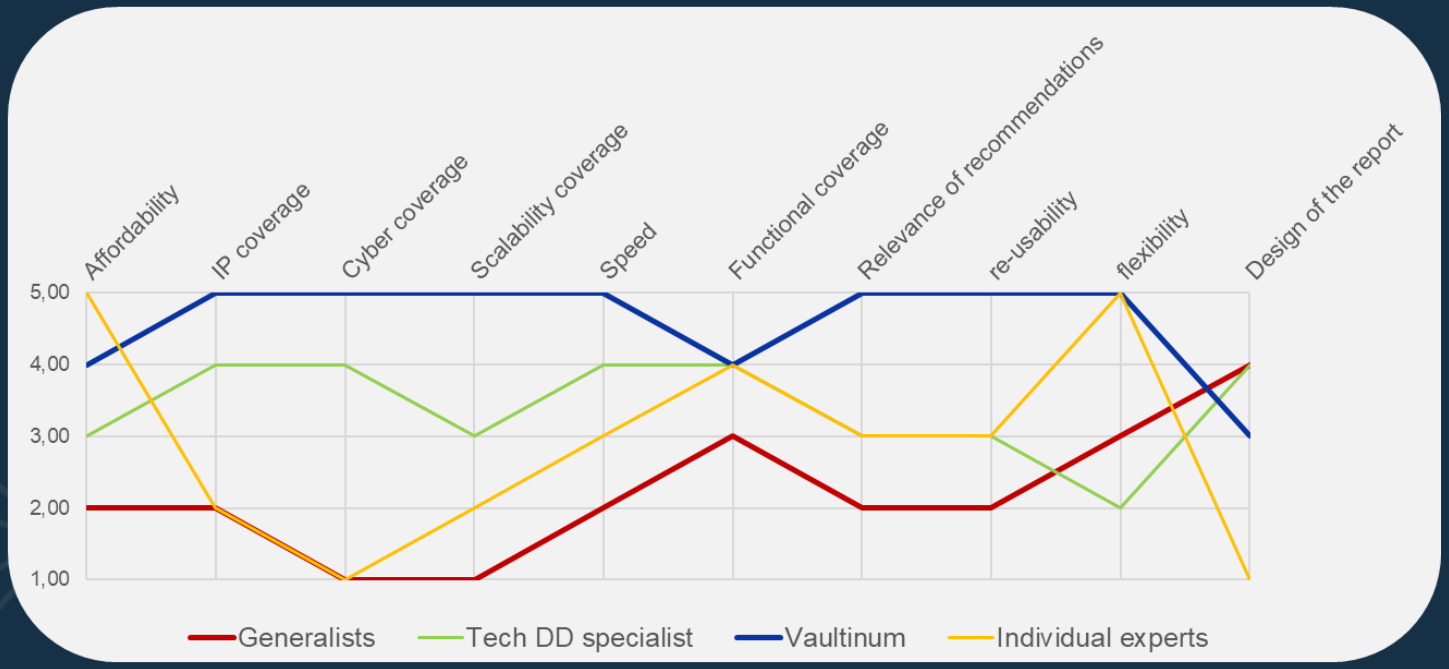
Vaultinum – Technology as a Service

- A comprehensive, data-driven approach to technology due diligence
- Unique scanning technology to detect threats
- Expert contextualization of data and actionable recommendations
- Identifying technical debt and reducing risk
- Verifying the technology aligns with the business objectives
- Monitoring, de-risking and enhancing your tech portfolio

The combination of DATA + TOOLS + EXPERTS makes our approach unique on the market

W. Edwards Deming,

“Without data, you’re just another person with an opinion”



They trust Vaultinum

Our clients

CAPZA
EURAZEO
bpifrance
Five Arrows Principal Investments
ARMEN
B&Capital
andera PARTNERS
4 ACCURAFY4 — INVEST FOR GOOD —
SUMMIT PARTNERS
MEANINGS
ICG
eoden GRANDISSONS LE FUTUR
idiCo
AIRBUS
Consilience Ventures
cnrs
SIEMENS
RIOTS
partech
BNP PARIBAS
TERRANOHA
VIVALTO PARTNERS
QUANTIC DREAM
SURGAR Surgical Augmented Reality
Jo-Mei GAMES
MedyCare
QuantHouse
ALSTOM
TOTAL
HORIZON SOFT COMMODITIES
elettromil transformers and reactors
Kids&Us.
THALES
formind
ul invest
CATHAYCAPITAL
FOODICS
R3
borwell
Propellant.digital
Holy Dis

Our partners

netsystem make IT clear
akvize
greyspark partners
DIGITAL VALUE Data Analytics for Business
INDEFI
APPROACH
YDES Société d'Avocats
CARLER
ICV FINANCE
racine AVOCATS
MoneyOak
SOCIETE GENERALE
CIC BANQUES
sMyPatent
DS AVOCATS
PAUL HASTINGS

Our focus

1 Introduction

2 Our focus

3 Our methodology

Understand software risk and impacts

Our Tech Due Diligence Assesses:

Cybersecurity

- Vulnerabilities in the code (data leak, password etc..)
- Cyber defence tooling
- Pen tests
- Network Footprint scan
- Processes and governance

Intellectual Property

- Inventory of OSS
- Categorisation of OSS risks
- Value of the IP of the software
- Domain names
- OWASP

Scalability – IS maturity

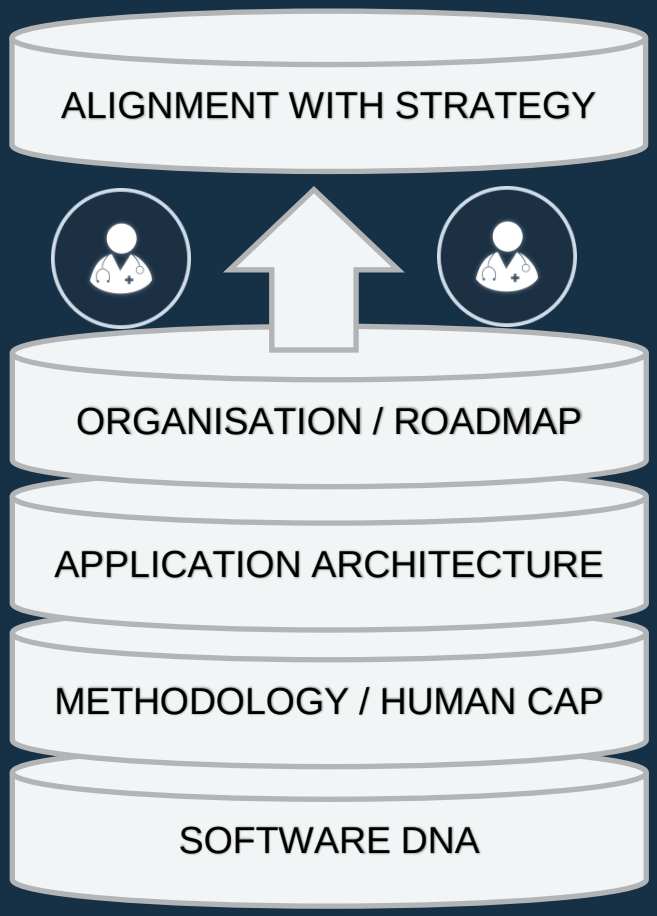
- Architecture
- Human capital / Key people
- Information Systems
- On premise SaaS
- Infrastructure
- Best practices / language
- Process and Tooling

AI Maturity

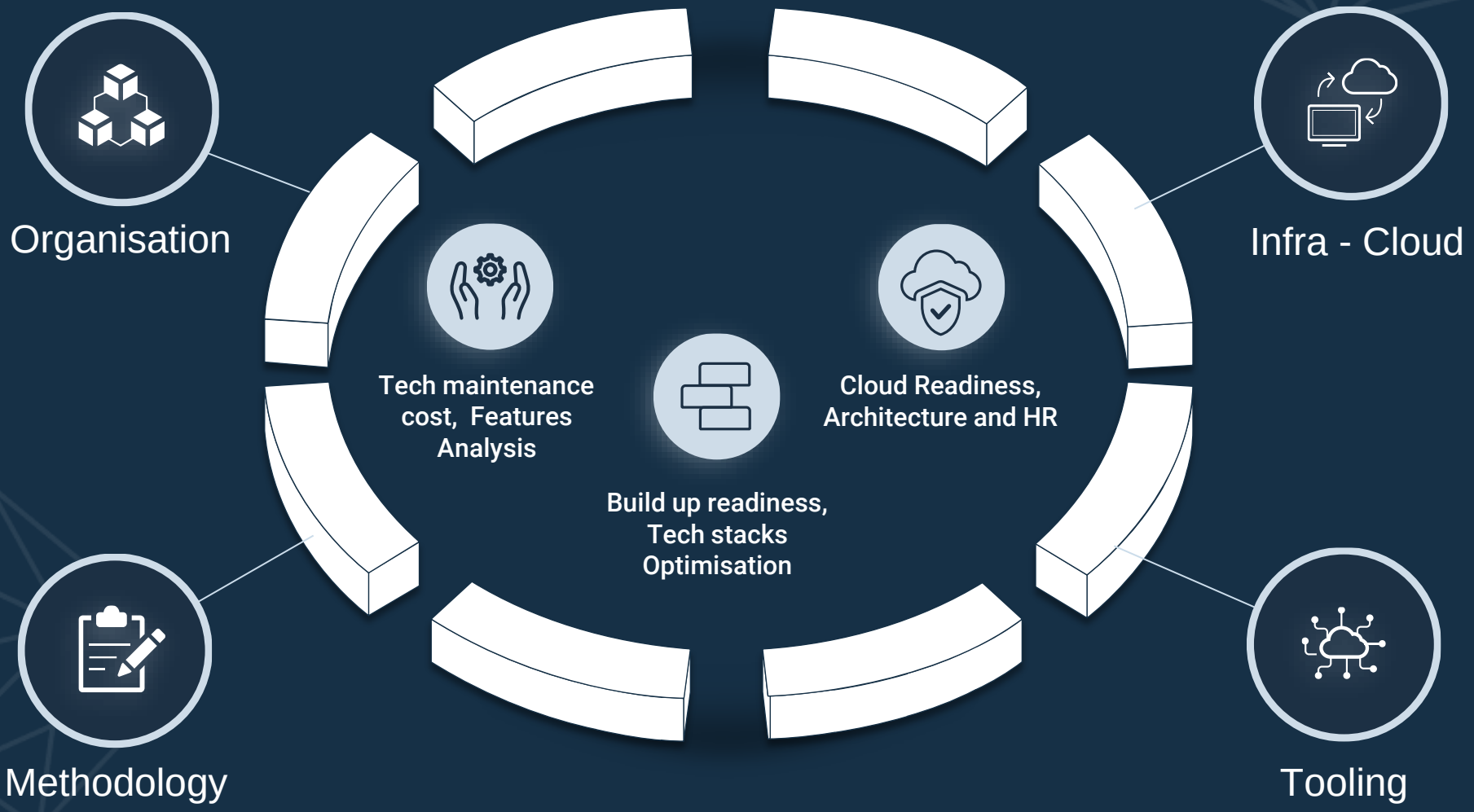
- AI business model
- Complexity and maturity
- Framework and machine learning
- Risks associated with data
- Analysis of the roadmap and team
- Tooling and efficiency
- AI exploitation and scalability

Vaultinum Through 360 Audit

- Adding Expertise to have a full comprehensive view on the business
- Understanding the Industry and the positioning
- Allowing matching analysis with Business expectations



360° view of the IT environment



Our Methodology

1 Introduction

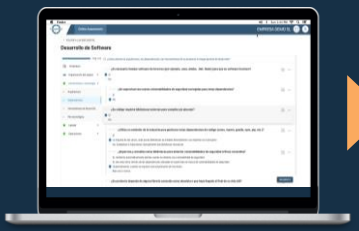
2 Our focus

3 Our methodology

From quantitative data to expert guidance

What we do: Using data to go deeper, faster

Online Questionnaires

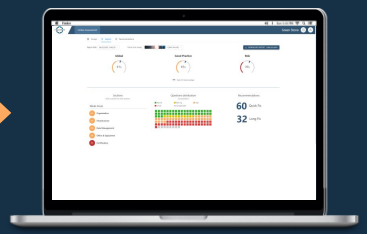


Source code scan

IT and Legal expert contextualization

Recommendations, Estimated time & costs

Performance Monitoring



What we deliver: operational insights for impactful decisions and better exit value

- Thorough analysis of the tech's strengths and vulnerabilities
- Report focusing on the main areas of risk and how to address them
- Action plan with estimated time of fix and costs
- Dashboard to track and monitor performance over time

Step 1: Online assessment

Evaluate organisation & management of

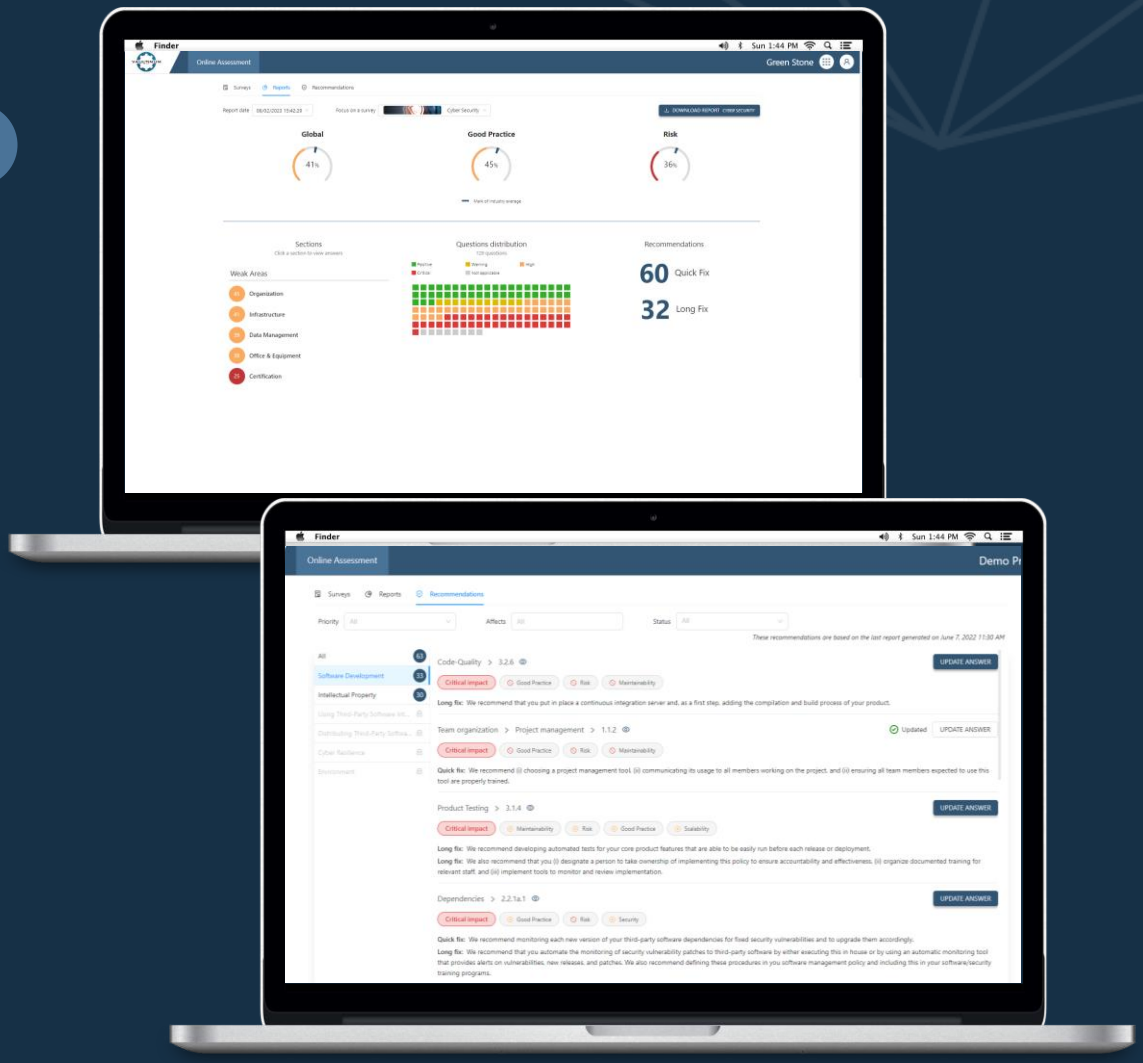
- Cybersecurity practices
- Intellectual Property Protection
- Software development and IT infrastructure organisation
- GDPR processes

Created by international experts - Vaultinum collaborative Platform

Step 1: Online assessment

Control Panel for rapid view of

- Identified opportunities and vulnerabilities
- Scoring compared to industry average
- Report with expert recommendations



Step 2: Source code scan

Unique proprietary methodology gathering data analysis from 7 scanners

- Cyber vulnerabilities scan
- Code hygiene and maturity
- OSS dependencies scan
- OSS copy/paste scan
- OSS modifications scan
- Git analyzer for scalability
- Analysis of quality and security
- Access security risk
- Optional Pen testing
- Tooling efficiency

Step 3: Contextualization with Experts

Interview with IT & Legal Experts to

- Review findings in context of business objectives
- Identify mitigating factors
- Understand technology environment and end use
- Assess timelines to formulate action plan

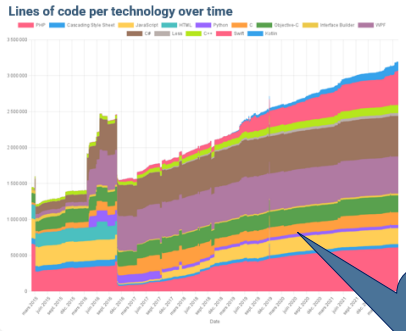
Step 4: Delivering a risk report and action plan

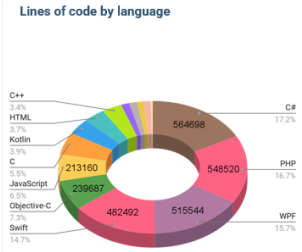
A risk report and action plan that shows

- Scalability of the tech asset, cloud readiness, build up readiness
- OPEX and CAPEX estimated risk
- Bottom-up analysis leading to better accuracy
- Deep tech background to factualize risks and recommendations

The power of data, leading to insightful recommendations

Analysis - Maintainability





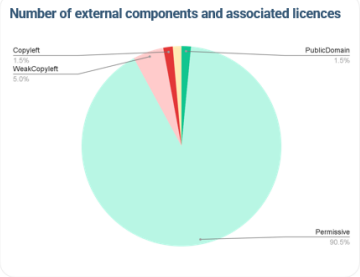
Too many coding languages presents scalability challenges. Reengineering to be planned immediately to address scalability issues .

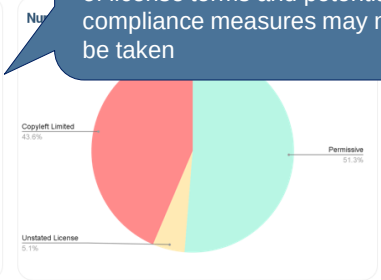
Observations

The number of lines of code is significant at 3.281.478 (note: the inclusion
inflates the actual number of supported lines of code). PHP is the most gr
diversity of technologies can be found within the source code presenting a challenge in terms of skills required to maintain.

Licence usage

Presence of restrictive open-source software requires a further analysis of license terms and potential compliance measures may need to be taken

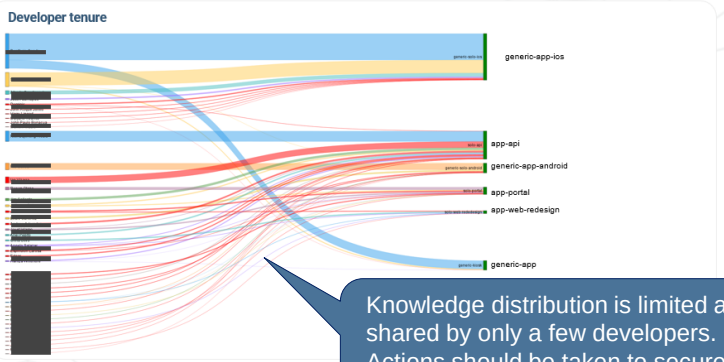




Main observations

The source code analysis identified three types of limited copyleft licenses attached to 17 components. The strict copyleft licenses require that any changes be released as free software, while the limited copyleft licenses require this only in certain cases. For example, the Mozilla Public License (MPL) only requires publication of changes to existing files, while added files can be licensed in any way. The LGPL (Lesser General Public License) for program libraries requires only that changes to the library itself be licensed under the LGPL.

Analysis - Knowledge distribution



Knowledge distribution is limited and shared by only a few developers. Actions should be taken to secure key personnel.

Main observations

The vast majority of contributions are made by the Country 1 team with 100% ownership for all mobile applications. Some redundancy with the team in Country 2 exists on the two most critical repositories Web + API

Analysis - Human capital

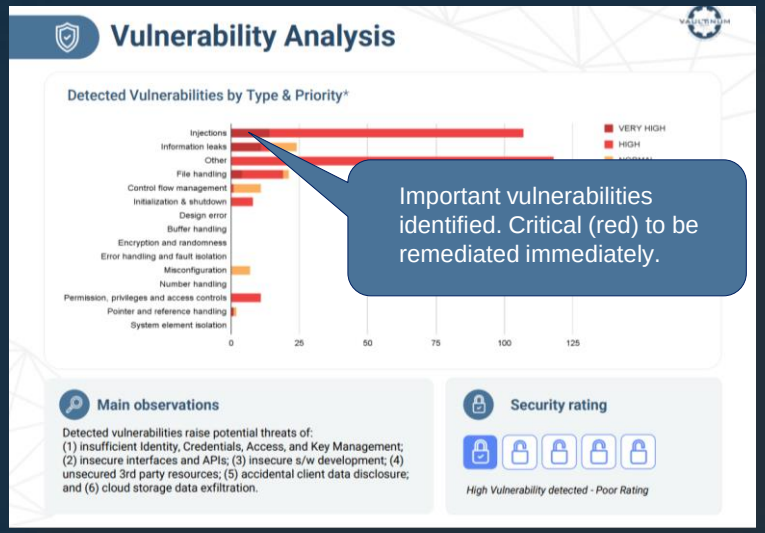
High turnover of developers puts into question the management of the team

Main observations

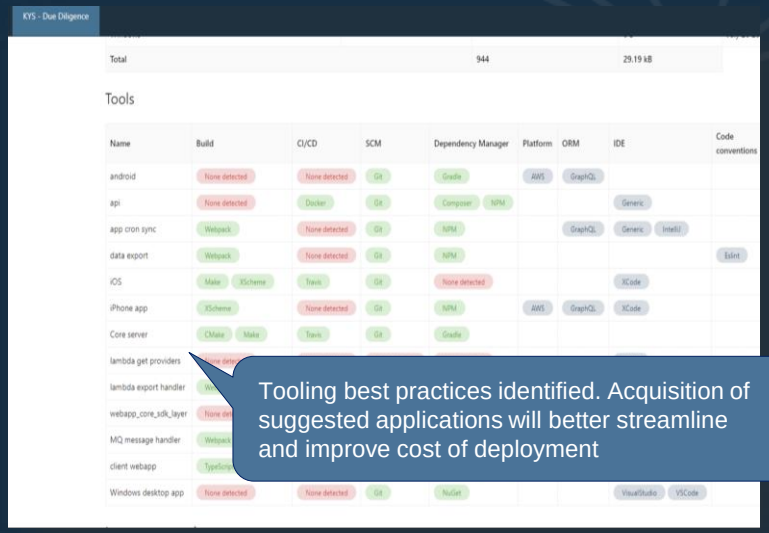
A high turnover rate can be observed with more than half of contributors staying less than 1 year. This can have a negative impact on the code quality.

Country 1 team: 14 active developers [53 no longer active]
Country 2 team: 2 active developers [7 no longer active]

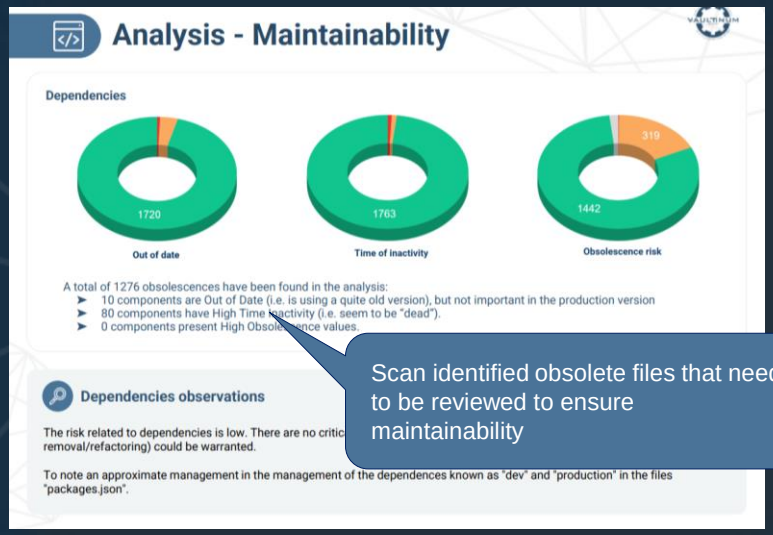
An illustrated overview of detailed data



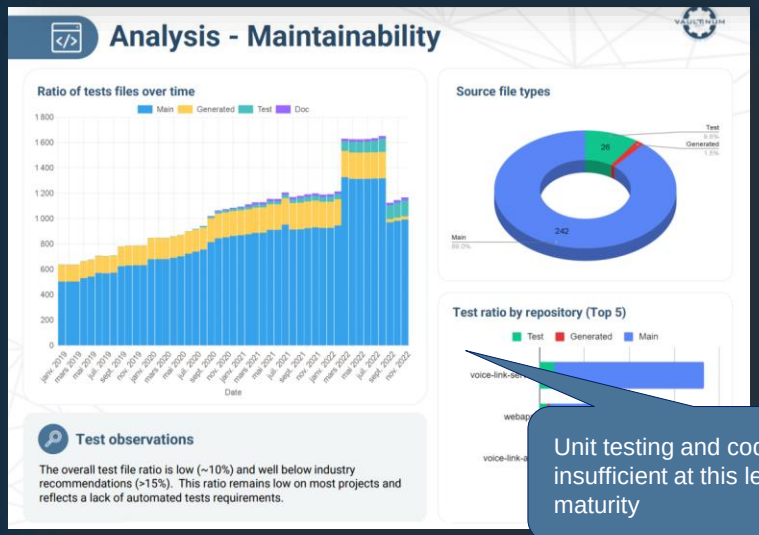
Important vulnerabilities identified. Critical (red) to be remediated immediately.



Tooling best practices identified. Acquisition of suggested applications will better streamline and improve cost of deployment



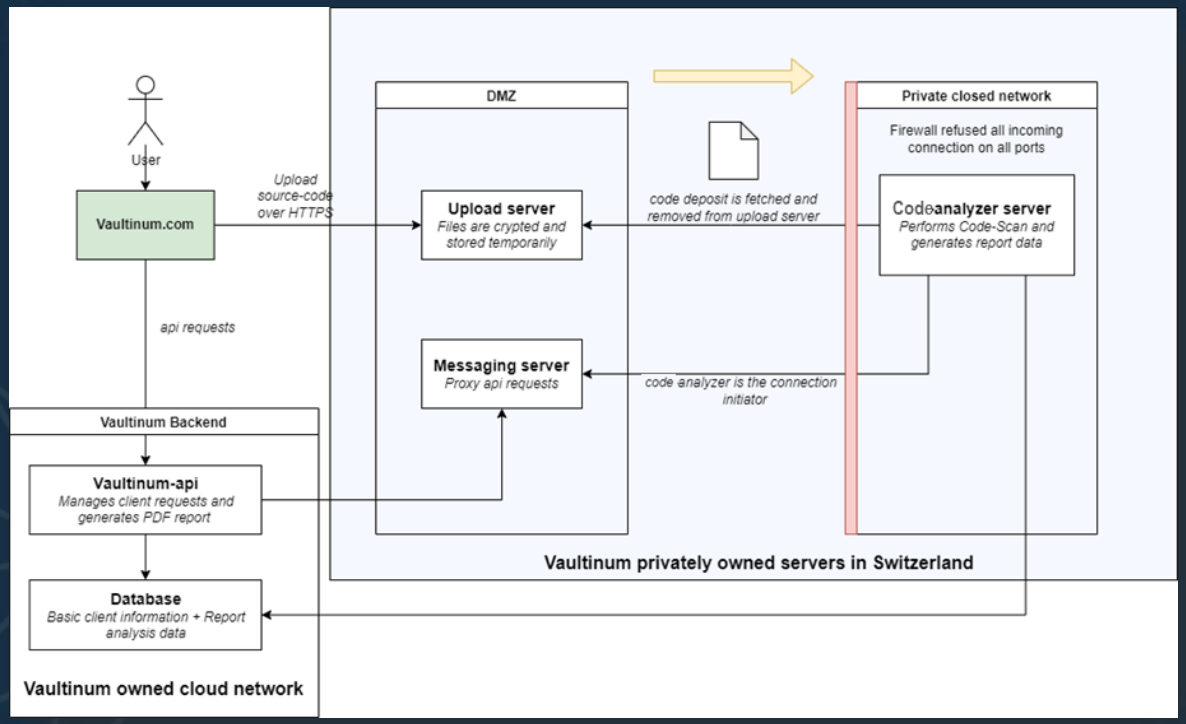
Scan identified obsolete files that need to be reviewed to ensure maintainability



Unit testing and code review still insufficient at this level of maturity

100% secure - 100% of the time

- Securing source code for 40 years with the biggest European software vendors
- Secrecy of the source code assured through a strict workflow
- No human access to the source code
- Letters of guarantee and certificate of destruction



- **Temporary** presence on our server with immediate **auto-deletion** post scan
- **No access** by external parties. Only the scanner can read
- Upload made through **secure server** (no email, no SFTP)

- Trusted third party since 1976
- Sovereign servers in Switzerland
- ISO27001
- eIDAS READY

Meeting your needs

FOR A TECH COMPANY

1. Run a full tech health check
2. Ensure compliance with industry best practices
3. Unveil vulnerabilities and obtain recommendations prior to a sell
4. Obtain operational recommendations on action plan, timeline and cost

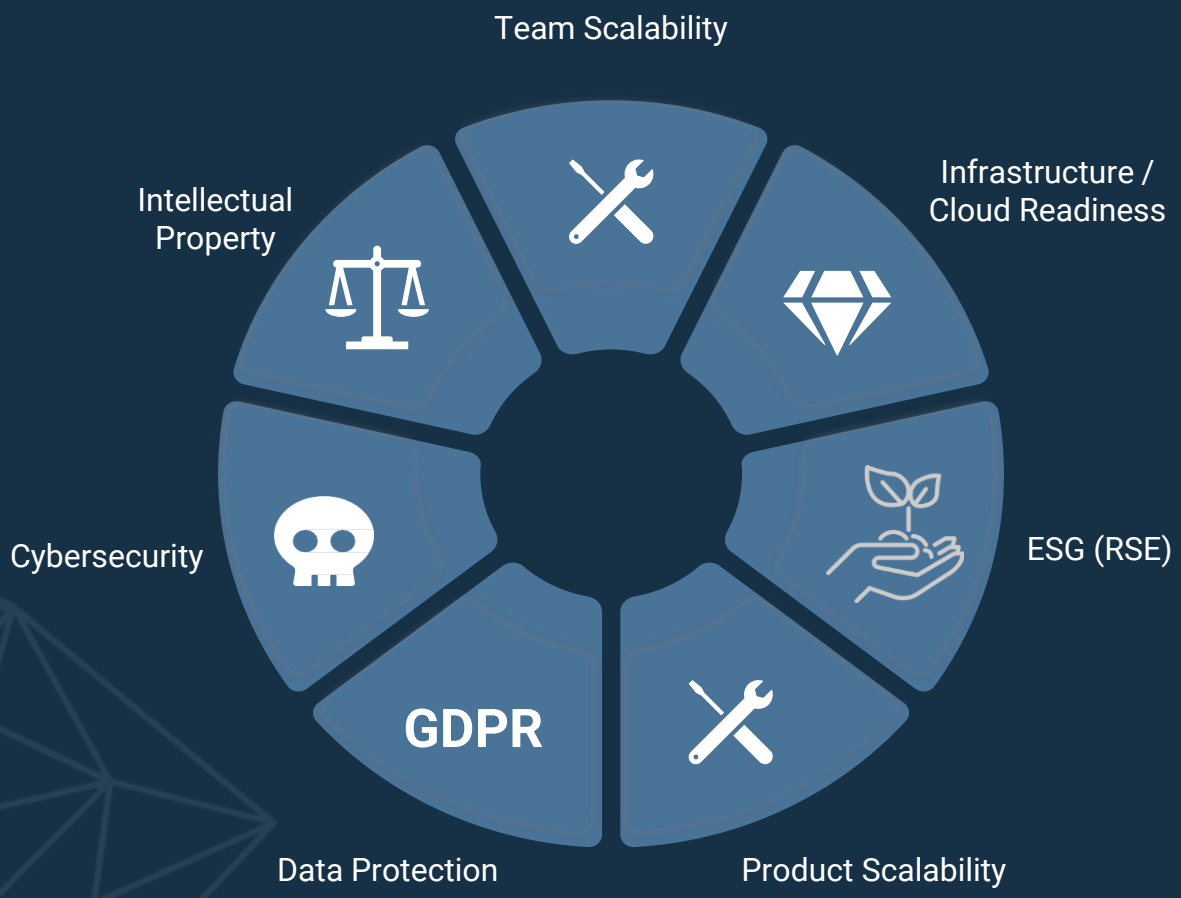
FOR INVESTORS

1. Gain critical insights about the value of the tech asset
2. Validate the scalability and cybersecurity of the asset
3. Identify short and long-term main areas of risk
4. Obtain operational recommendations on action plan, timeline and cost

Monitoring Progress

TECH to Value – Ongoing progress monitoring

Ongoing Assessment– What does it cover ?



- **Online and Collaborative**
- **Scoring within Industry**
- **Expert Recommendations**
- **Performance Monitoring**
- **Exit Readiness**

About **Vaultinum**

Vaultinum is a trusted independent third party specialized in the protection and audit of digital assets.

Since 1976, Vaultinum has enabled thousands of digital creators and investors secure their innovations by :

- protecting their intellectual property
- ensuring the continuity of their business activity
- mitigating cyber and software risks

Double expertise IT and Legal • ISO 27001, eIDAS Ready

Contact us

Address

World Trade Center
Route de Prés-Bois 29
1215 Meyrin, Switzerland

Mail

contact@vaultinum.com

Phone

+41 41 511 82 08

Website

www.vaultinum.com

Linkedin

www.linkedin.com/company/vaultinum