Technology Due Diligence

Dare with care

VAULTINUM

1 **Dare with Care**

2 Technology Due Diligence at Vaultinum

3 Our methodology

4 Our experts & tools

Vaultinum, Technology As A Service

- A unique approach, combining automated tools, data and experts
- Meet the needs of investors and tech companies for assessment, compliance, monitoring
- A team of senior experts, with experiences rooted in business & technology
- Protecting & auditing source code for over 40 years
- Offices in Geneva, Paris, London, Madrid, Dubai
- eIDAS-qualified and ISO 27001 organization

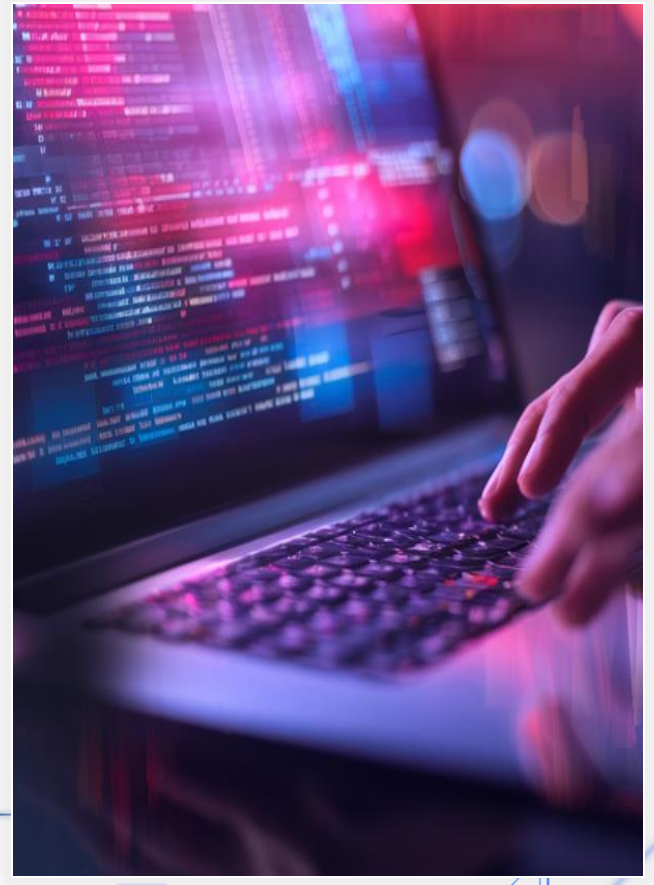
>100
Audits per year

>20
Countries around the world

30
Senior Tech experts

250 000
Source codes on our servers

Vaultinum differentiators

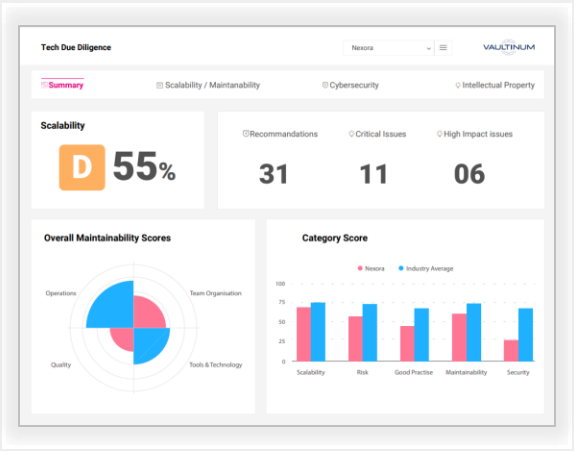


- Unique scanning technology to collect data and insights
- Experts giving actionable recommendations
- Identifying risks and downsides, enhancing scalability and upsides
- Adding tech value creation to support portfolio companies

Supporting Private Equity firms from acquisition to exit

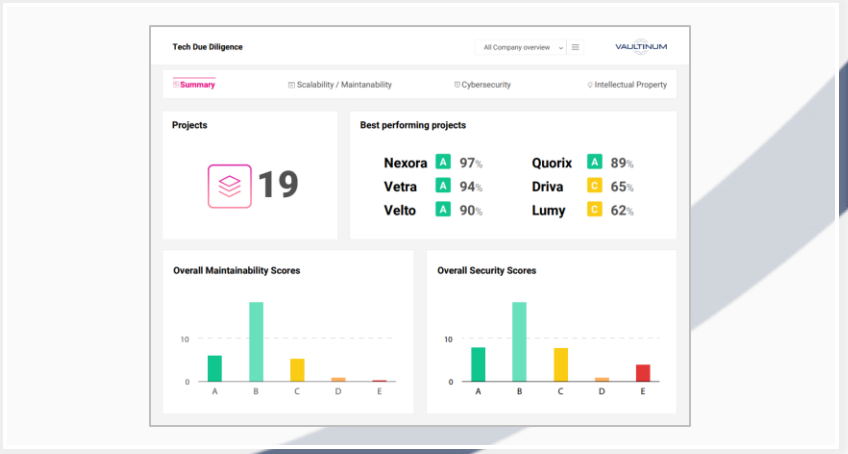
1 Acquisition

Tech Due Diligence



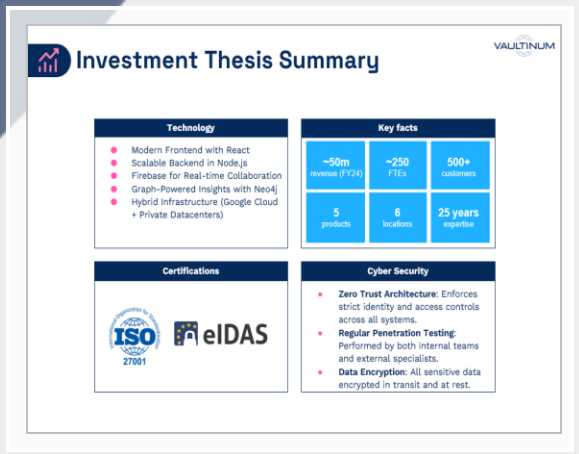
2 Continuous Diligence

PE visibility/reporting



3 Exit

Vendor Due Diligence



VAULTINUM

They trust Vaultinum

Clients

Partenaires

VAULTINUM

1 Dare with Care

2 **Technology Due Diligence at Vaultinum**

3 Our methodology

4 Our experts & tools

We assess Technology in several areas

Software Scalability
- SDLC
- Roadmap
- Tech Debt
- Process & Tooling
- Automation

Ops & Client Support
- Efficiency
- Process
- Tooling
- Implementation and support

Cybersecurity software
- Code Scan
- CVEs and CWEs
- General consideration

Infrastructure scalability
- Enterprise/Saas
- Architecture
- Cost optimisation
- Internal IT

AI Maturity & Disruption
- AI code readiness
- Initiatives & Roadmap
- AI product Integration
- AI Moat

Cybersecurity hardware
- Network Footprint
- @host exposure
- Pen test
- Equipment and tools

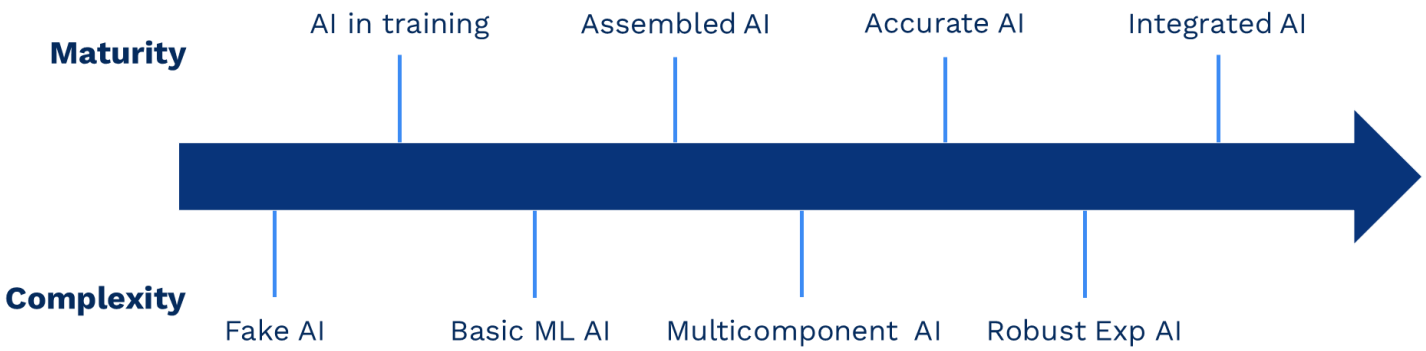
Organisation
- Talents
- Governance
- Key people

IP & 3rd party dependency
- Open Source
- Third Party
- OWASP

Data
- Data value chain
- Cost Optimisation
- Data Privacy (GDPR)

Focus on AI Readiness Assessment

- Assess AI usage in SDLC (Code generation, tooling maturity)
- Evaluate AI product integration (framework, ML models)
- Analyse AI governance and enterprise adoption
- Measure defensibility and competitive positioning (tech angle)
- Review AI Initiatives and Roadmap and produce a SWOT Analysis



Focus on Cybersecurity

General consideration

- Understanding the level of cybersecurity-readiness
- Looking at phishing email response, employee training, level of equipment and tooling
- Offering recommendations and best practices to avoid hacking, spoofing, data leaks

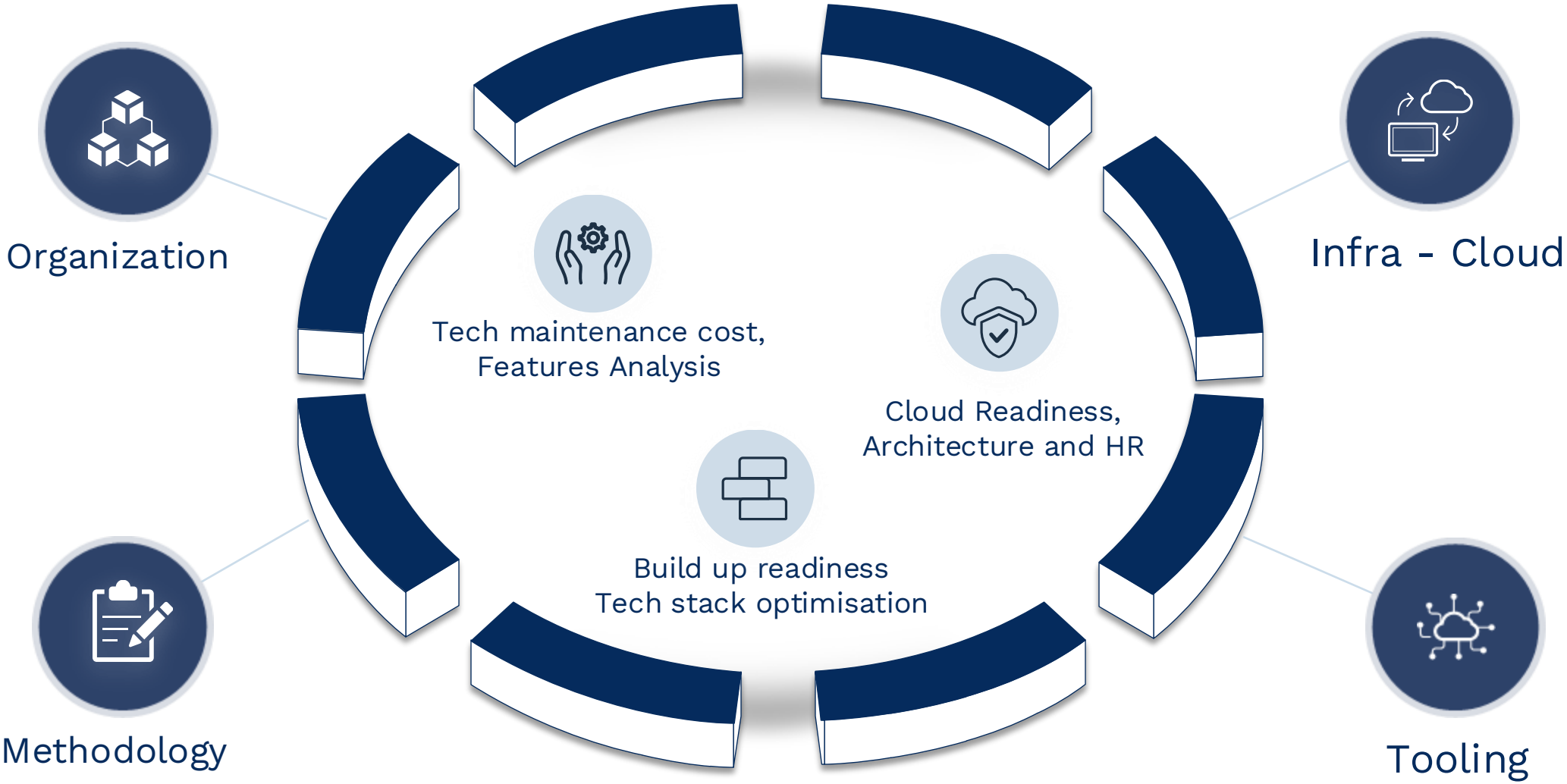
Software Scan

- Source code scan and OWASP compliance
- Detecting CVEs (Common Vulnerabilities & Exposures)
- Detecting CWEs (Common Weaknesses Enumeration

Network Footprint and Pen test

- Scanning the host exposures
- Testing the resiliency of Hardware equipment
- Verifying data leak to Dark Web
- Black Box, Grey Box, & Pen testing optional

Vaultinum’s thorough 360° Audit



VAULTINUM

1 Dare with Care

2 Technology Due Diligence at Vaultinum

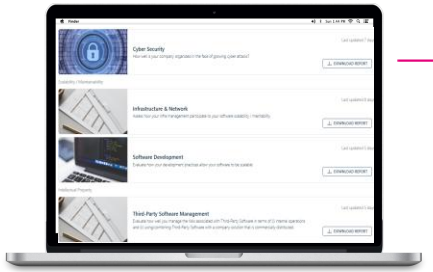
3 **Our methodology**

4 Our experts & tools

Combining data and expert guidance

Using data to go deeper and faster

Online Assessment



Source code scan + Data Room

Interviews - Expert contextualisation

TDD report, Recommendations

Operational insights for impactful decisions and better exit value

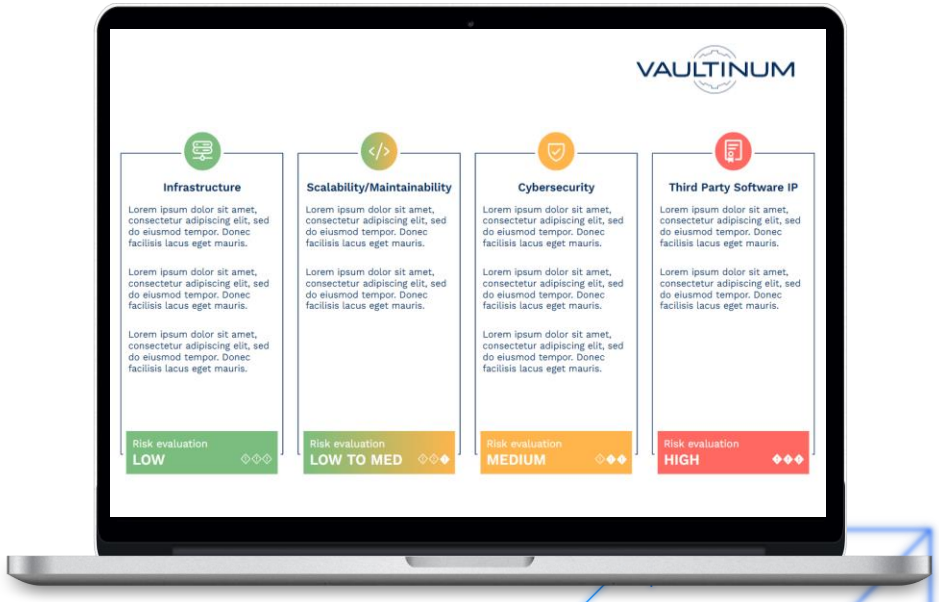
Thorough analysis of the tech's strengths and vulnerabilities

Report focusing on the main areas of risk and how to address them

Action plan with estimated time of fix and costs

360 Assessment of the technology in hand

Vaultinum’s available reports



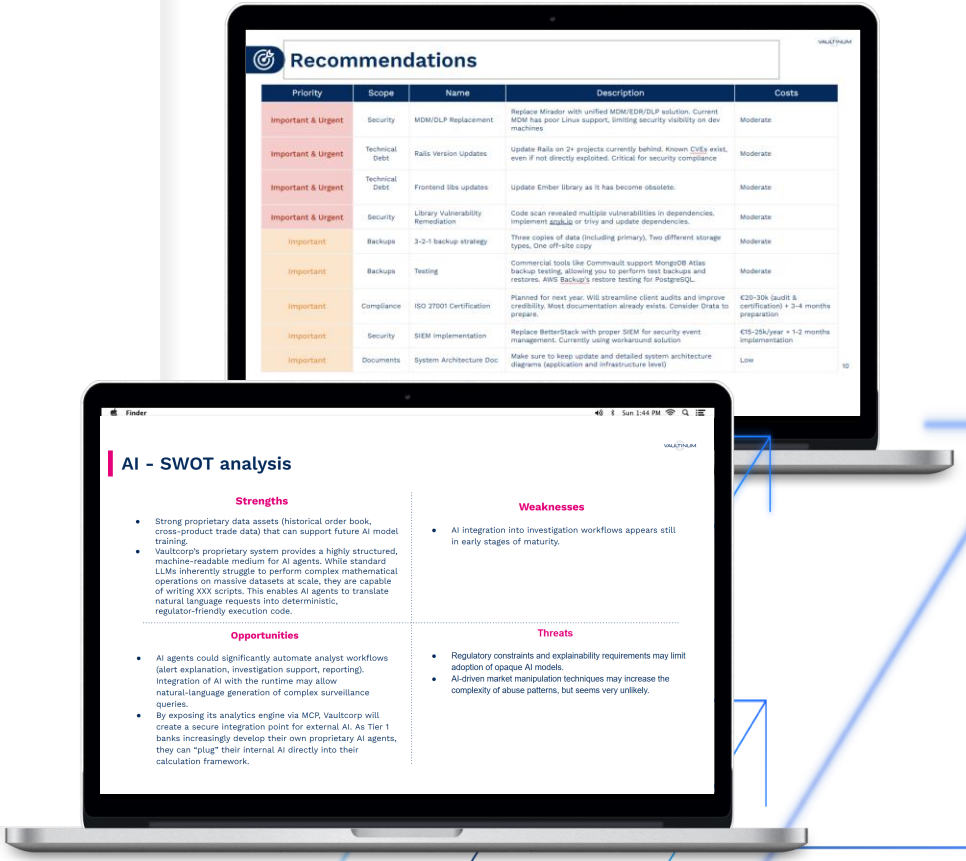
3 reports available

- Red Flag report with first assessment
- Code Scan report with all technical details of vulnerabilities, open-source licenses, and maturity insights -> very useful for the audited company
- Investor report with executive summary, observations, industry contextualisation, and tactical & strategical recommendations

Delivering a TDD report with recommendations

A risk report and action plan that shows

- Scalability of the tech asset, cloud readiness, build up readiness
- Cyber estimated risk
- AI SWOT analysis, bridging technology and future strategy
- Deep tech background to factualise risks and recommendations



VAULTINUM

1 Dare with Care

2 Technology Due Diligence at Vaultinum

3 Our methodology

4 **Our experts & tools**

Our senior experts on hand to help

Scalability Infra	Scalability Software	Cyber security	Intellectual Property	AI Disruption	AI Maturity	Data Value Chain	Product Strategy	Project Manager	GDPR
Jonathan Berdah	Frédéric Ollivier	Steeves Deloustal	Marina Chanian	Jean Albert	Julien Weissenberg	Stéphane Père	Jonathan Berdah	Juliette Cazenave	Kristin Avon
Francois Hervieux	Guillaume Acard	Olivier Clef	France Charruyer	Thomas Solignac	Adam Votava	Jer Jang	Henry Seabright	Kristin Avon	
Mickaël Franck	Richard Kershaw	Johann Romefort			Radouane Oudhriri		Hervé Couturier	Sara Terraz	
Boydlee Polentine	Fernando Nunez	Steeves Mihy					Kevin Monserrat		
Simon Morley	Radouane Oudrhiri	Jeremy Berast							
Oleg Podsechin	Jonathan Berdah								
	Merlin Gore								

Example of AI SWOT

AI - SWOT analysis

Strengths

- Strong proprietary data assets (historical order book, cross-product trade data) that can support future AI model training.
- Vaultcorp's proprietary system provides a highly structured, machine-readable medium for AI agents. While standard LLMs inherently struggle to perform complex mathematical operations on massive datasets at scale, they are capable of writing XXX scripts. This enables AI agents to translate natural language requests into deterministic, regulator-friendly execution code.

Weaknesses

- AI integration into investigation workflows appears still in early stages of maturity.

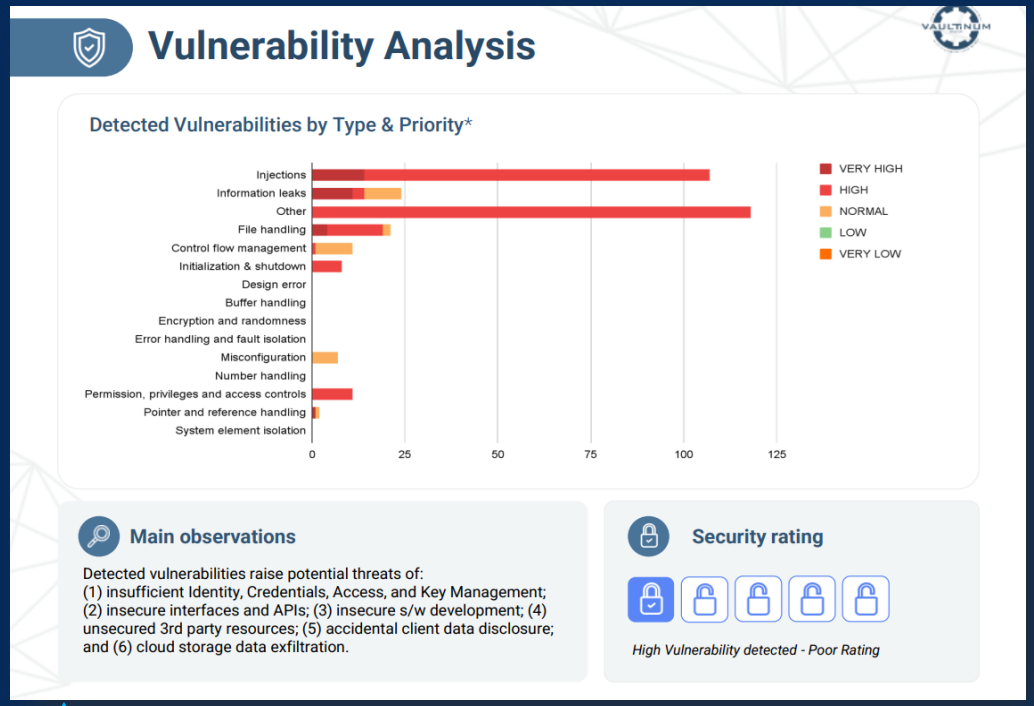
Opportunities

- AI agents could significantly automate analyst workflows (alert explanation, investigation support, reporting). Integration of AI with the runtime may allow natural-language generation of complex surveillance queries.
- By exposing its analytics engine via MCP, Vaultcorp will create a secure integration point for external AI. As Tier 1 banks increasingly develop their own proprietary AI agents, they can "plug" their internal AI directly into their calculation framework.

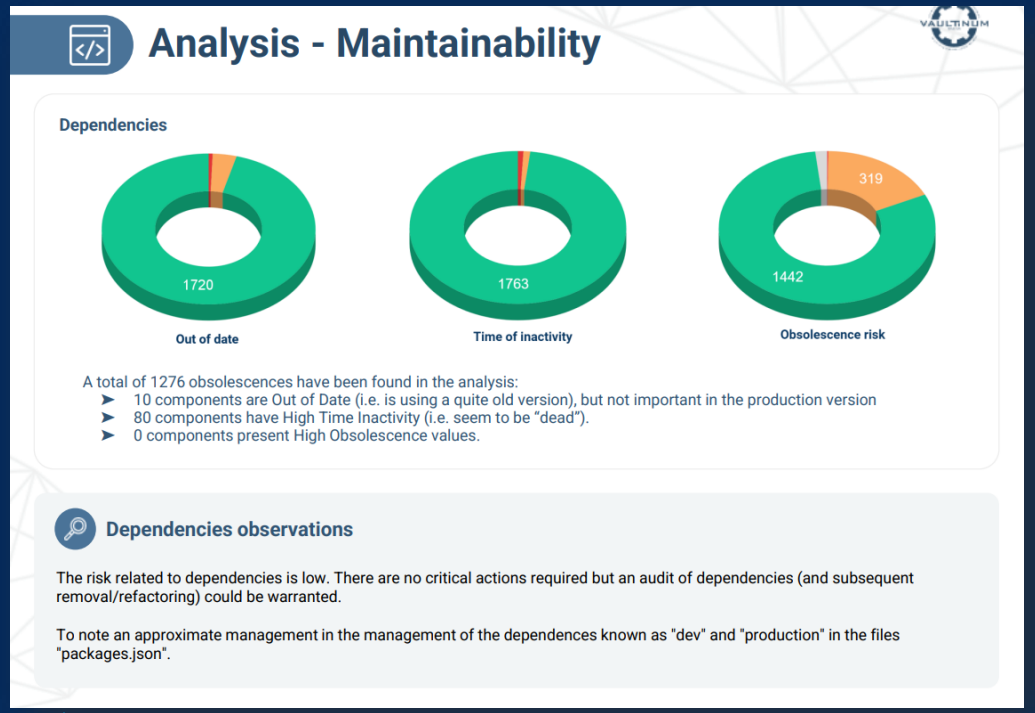
Threats

- Regulatory constraints and explainability requirements may limit adoption of opaque AI models.
- AI-driven market manipulation techniques may increase the complexity of abuse patterns, but seems very unlikely.

Illustrated view of code scan insights

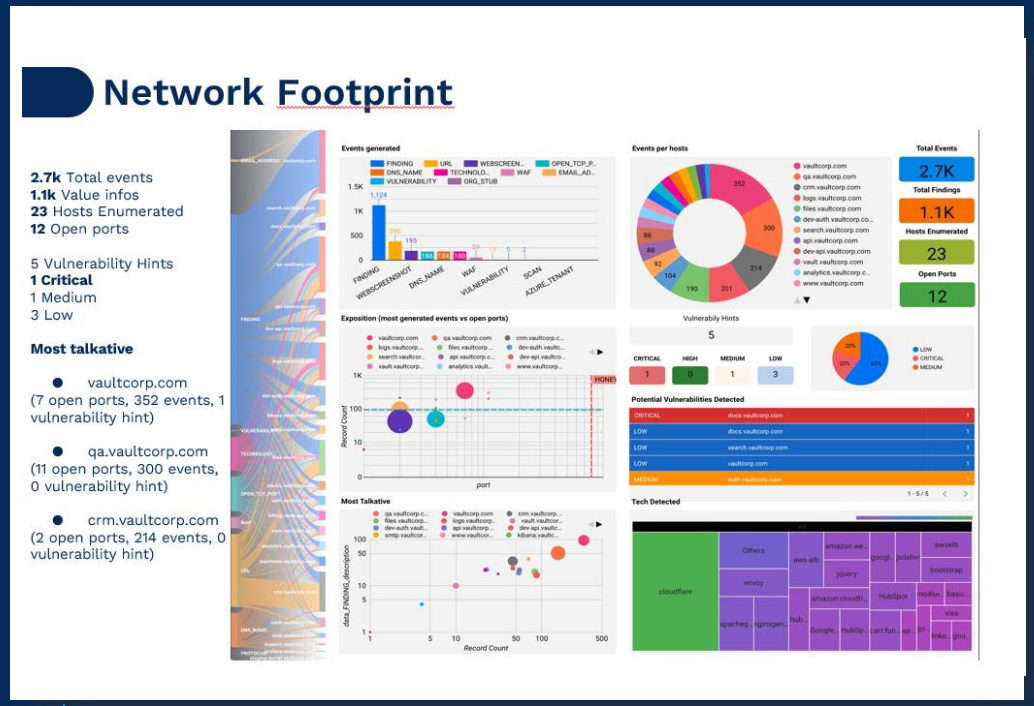


Important vulnerabilities identified.
Critical (red) to be remediated.

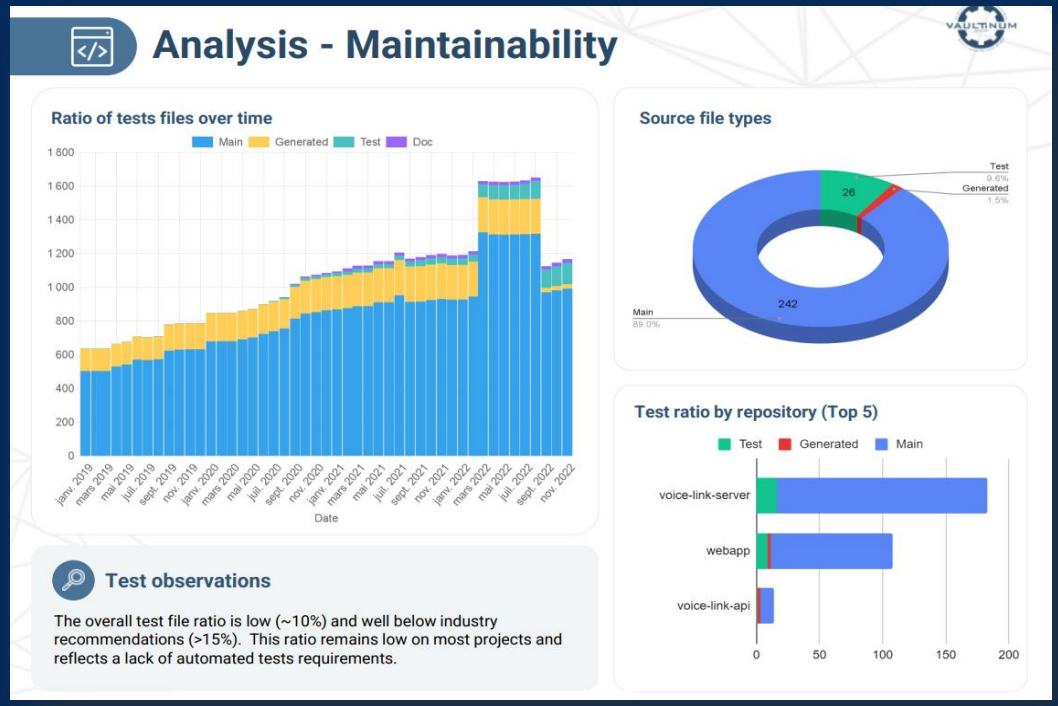


Scan identified obsolete files that need to be reviewed to ensure maintainability.

Illustrated view of code scan insights

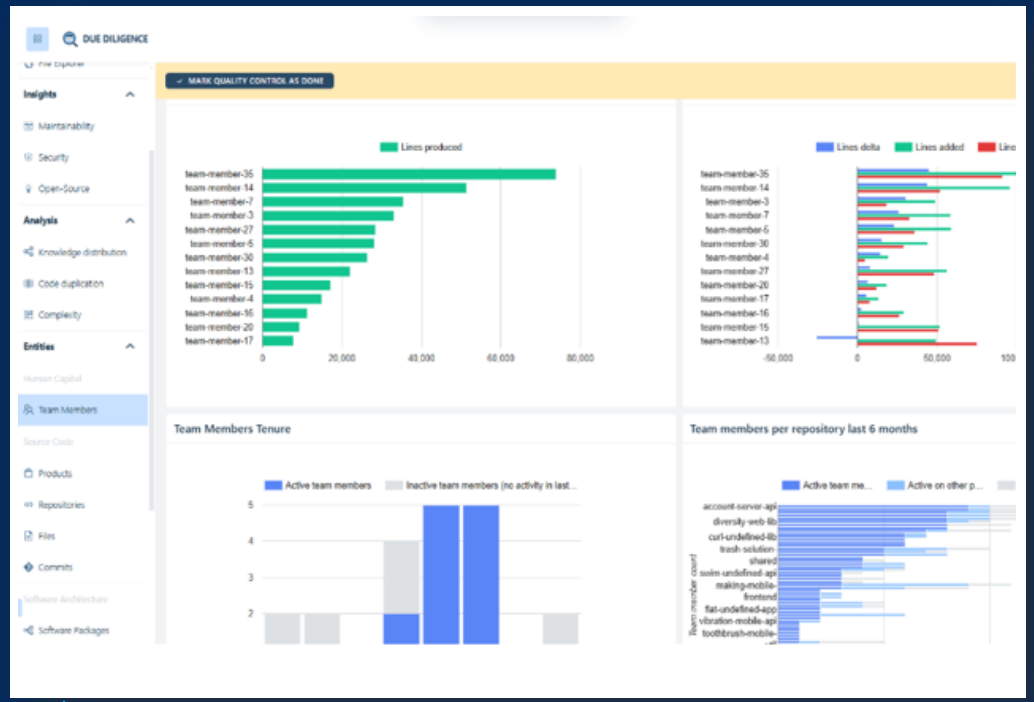


Some corporate emails have leaked and are available on the web. This constitutes an easy entry into the IT system.



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

An illustrated view of performance and costs



R&D efficiency per individual is reported here through several criteria.

View on delivery per project and lines of code per technology to check the active project.

An illustrated view of performance and costs

Defense & Monitoring tools

Grafana · Prometheus · FORTINET · CLOUDFLARE · Bitbucket · aqua trivy

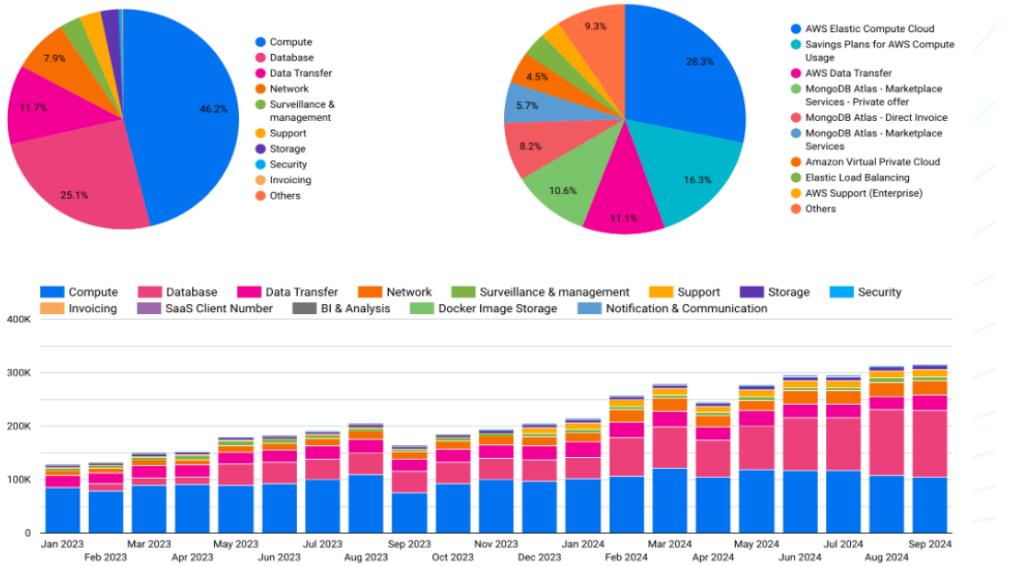
Log Aggregation and Monitoring
Grafana to visualize the aggregation of logs from Prometheus. This includes system metrics and logs pushed by Loki into a bucket.

IPS/IDS on Fortigate
Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) activated on Fortigate. While Zero Trust Network Access (ZTNA) is currently not activated, there is potential to migrate to Cloudflare's ZTNA.

Continuous Integration and Continuous Deployment (CI/CD)
Bitbucket Pipelines: Utilized for managing their CI/CD processes, including tasks such as dispatching jobs, vulnerability scanning with Trivy, and we internally check the exploitability of identified vulnerabilities.

Tooling issues identified. Acquisition of suggested applications will improve cost of deployment.

Usage of Cloud Services



The company could save 300K by making EC2 commitments on AWS.

VAULTINUM

Vaultinum is a provider of technology due diligence services for private equity investors. We support tech-driven value creation and risk mitigation across the full investment lifecycle.

From pre-acquisition to post-deal optimisation, through a combination of proprietary scanners and expert insights, our assessments deliver a clear, data-driven view of a target's technology assets, covering scalability, cybersecurity, team performance, data compliance, intellectual property, FinOps, AI maturity and AI disruption risks.

Contact us

vaultinum.com

Vaultinum Switzerland - Rue de l'Ecole-de-Médecine 10, 1205, Geneva	Vaultinum Paris - 25 rue de la plaine 75020 Paris, France	Vaultinum Italy - Corso di Porta Romana, 61, 20122 Milano MI, Italia
Vaultinum London - Spaces, Mappin House, 4 Winsley St, London, W1W 8HF, United Kingdom	Vaultinum Madrid - Spaces Avalon, Calle de Santa Leonor, 65 ,Edificio D, 28037, Madrid, Spain	Vaultinum Dubai - Spaces, C1 Building, Level 1, Trade Centre 2

Dare with care