CASE STUDY

# Keeping data safe and sound

## How a security health check can give you the confidence to scale your business

EQUAL EXPERTS

This case study explores the benefits of a 2 week security health check delivered by Equal Experts. Our client had built a successful data analytics platform using a new cloud provider, but because of the rapid pace of delivery of the new technology, the Infosec team had struggled to actively engage with the project.

As a result, both the development and information security (Infosec) teams lacked confidence in, and evidence of the security of the system. They felt they had a security blind spot that they needed to resolve.

We were asked to carry out an assessment to provide a snapshot of the effectiveness of current security controls, identify any missing controls, recommend effective controls and help the client create a prioritised remediation plan based on severity and business impact.

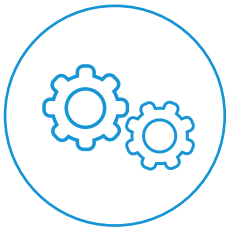
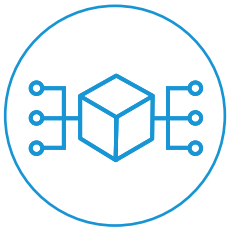
We also reviewed their security processes, to understand why they reached a situation where they lacked confidence in the security of the platform, and to help them improve security engagement and capabilities in future projects.

## In 2 short weeks:

- A comprehensive overview of security health
- Specific high-risk security issues identified
- New, bespoke technical security standards and workflow improvements.

# About the client

Our client is a major provider of digital payments infrastructure to businesses and banks. They deliver card schemes, payment methods, fraud screening tools and other essential payment products through a cloud-native tech stack, to support their customers to optimise and scale their payment services through one connection.

| INDUSTRY | ORGANISATION SIZE | LOCATIONS | SERVICES |
| --- | --- | --- | --- |
|  |  |  |  |
| Financial | 500+ employees | Europe | Deliver / Scale |

# Establishing the system context to lay the foundation of an effective review

The first thing we did was hold a stakeholder workshop to understand the client's vision and requirements. This was key to ensuring the report we delivered would provide value to all involved parties, and wasn't just an off-the-shelf security scan.

The key requirements were to increase the Infosec team's confidence in the system's security controls, help the delivery teams understand and prioritise fixes for any gaps, and help to build a self-serve capability so the delivery teams were empowered to secure their systems and provide assurance on an ongoing basis.

Our team consisted of two technical specialists "on-site" with the client for two weeks to perform review activities, and a security principal who was engaged for 4 days to establish the scope and value proposition and collate and produce the final report.

We identified the specific areas of the client's systems and processes that were under review. Agreeing the scope of the review in this way was essential to ensure we had enough time, and the right expertise to achieve a comprehensive and deep technical review.

# Gathering in-depth information for secure and compliant systems

Next, we carried out review activities to fully understand the system in scope; how it works, how it's managed and what type of data it processes. We used a variety of techniques, both manual and automated, to discover all of the required information.

**Asset and Data Identification:** We identified all of the high-level assets within the system, including their function, the sensitivity of data they process and store, and the perceived business impact if confidentiality, availability or integrity were subverted.

**Architectural Security Review:** We mapped the flow of data through the system, identified the principals with access to perform operations then reviewed the security of all components based on security principles such as authentication and access controls, data protection, and monitoring. This informed a shortlist of priorities for action, with severity weightings based on business impact.

**Cloud Security Compliance Scan:** Automated scanning tools analysed the configuration of the team's cloud estate against industry (Centre for Internet Security) benchmarks, and triaged the results to understand where configuration of resources presented a genuine security threat.

**Secure SDLC Maturity Review:** Mapping the existing software delivery lifecycle (SDLC) workflows helped us understand how security was embedded in terms of release management, security reviews, scanning tools and system operation. Again, we scored these against an industry standard benchmark.

# Comprehensive reporting to lock down security risk and increase confidence to scale

As a result of our extensive review process we were able to provide a set of clear and comprehensive reports which gave the client's Infosec team confidence that many security controls were already effective.

We also highlighted specific security issues with impact assessments, and highlighted areas where improvements could be made with clear, practical and technical recommendations prioritised by impact severity.

An important approach we took was to work collaboratively with the client's engineering teams to ensure we understood and highlighted the good work already achieved in building effective controls in some areas, and then to identify and design improvements that were practical and technically sound.

We also provided an easy-to-use technical checklist to help them build security into future projects and proactively provide evidence of effective security. The full set of outputs included:

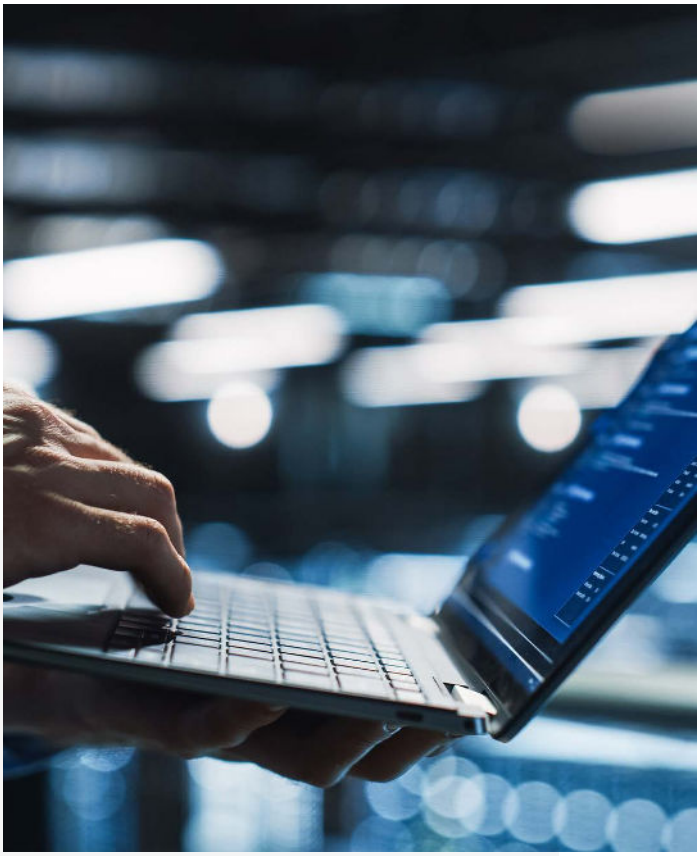
**Overall Security Findings Report:** An inventory of assessed systems and principals, with a matrix of identified issues and their corresponding business impact, providing an overall understanding of current security levels.

**Security Program Maturity Report:** This identified current secure delivery maturity, including recommended approaches to reach an agreed maturity level in terms of processes, policies and security tools.

**Compliance Benchmark Recommendations Report:** A triaged report showing compliance with benchmarks such as CIS, including a recommended remediation path based on impact.

**Architectural Control Recommendations Report:** A set of security requirements and implementation recommendations to remediate any large-scale architectural findings, allowing engineers to understand the impact of control deficiencies.

# The value of confidence to scale



Our client not only felt that this two-week collaborative exercise delivered on what they needed, but also commented on how enjoyable it was.

Their Infosec team gained confidence and evidence of the security of their system; the engineering team got both validation and a practical set of technical recommendations; and both teams benefited from learning how to improve ways of working together, to build in security and avoid blind spots in the future.

They particularly appreciated having a risk-based, prioritised backlog of improvement work based on industry standards. They also enjoyed the opportunity to gain expertise from our consultants, in terms of how to perform their own security reviews, specific technical best practices and our recommendations on their security workflows.

# Want to know more?

Are you interested in this project?

Or do you have one just like it?

Get in touch. We'd love to tell you more about it.