RIVERSAFE

CLIENT CASE STUDY:

BREAKING DOWN SILOS – HOW EMBEDDED SECURITY ENGINEERS TRANSFORMED SOFTWARE SECURITY IN A GLOBAL ENERGY GIANT

THE CHALLENGE: A SILOED SECURITY APPROACH SLOWING DEVELOPMENT

A major oil and gas organisation faced a critical challenge in securing its applications at scale. With a vast, globally distributed technical organisation, security and development teams operated in isolation, each focused on their own priorities. This siloed approach created significant bottlenecks, leading to slow vulnerability remediation, missed security risks, and frustrated developers.

A Common Problem in Large Enterprises

In large, complex organisations, security is often seen as a gatekeeper rather than an enabler. Security teams are tasked with identifying vulnerabilities but lack the mechanisms to ensure fixes are implemented effectively. Meanwhile, development teams are under pressure to deliver features rapidly, often seeing security as an external function rather than a core part of their workflow. This misalignment results in:

- **Backlogs of Unresolved Security Issues**
  Security vulnerabilities piled up because developers had no direct accountability for remediation. Without embedded security expertise, fixes were delayed or deprioritized in favor of feature development.
- **Slow, Inefficient Security Processes**
  Security was treated as an external check-point rather than an integrated function. Developers had to hand off security-related work, leading to long lead times between identifying and resolving vulnerabilities—sometimes spanning multiple sprints.
- **Lack of Clear Ownership**
  Security was considered “someone else’s problem,” rather than a shared responsibility. Without direct security support within development teams, security best practices were inconsistently applied, increasing risk across the organisation.
- **Developer Resistance to Security Processes**
  Developers often saw security as a blocker rather than a partner. Security reviews felt like an extra burden, slowing down releases rather than enabling a more secure development process.

The organisation knew it needed a different approach—one that would embed security into the development lifecycle without slowing down innovation.

THE SOLUTION: EMBEDDING SECURITY ENGINEERS INTO DEVELOPMENT TEAMS

To break down silos and improve security efficiency, the organisation introduced RiverSafe's Embedded Security Engineers within development teams. This approach ensured that security expertise was always available where it was needed, eliminating bottlenecks and enabling a proactive security culture.

Key Changes Implemented:

1: SECURITY ENGINEERS BECAME PART OF DEV TEAMS

- Instead of working as an external function, security engineers were placed directly into development teams.
- This eliminated handoffs and competing priorities, ensuring security expertise was built into day-to-day development.

2: SECURITY BECAME SEAMLESS AND DEVELOPER-FRIENDLY

- Security engineers worked alongside developers to automate security checks and integrate them into existing workflows.
- Hands-on support was provided to help developers understand why security fixes mattered and how to address them efficiently.

3: FASTER VULNERABILITY REMEDIATION

- With security engineers embedded, vulnerabilities were now identified, triaged, and resolved within the same sprint.
- The organisation moved from reactive, end-of-cycle security interventions to continuous security integration.

4: BUILDING LONG-TERM SECURITY CAPABILITY

- Developers were trained to proactively manage security in their codebases, reducing dependency on external security teams.
- Teams created and maintained their own threat models within a few sprints, enabling self-sufficiency in secure development.

5: MINIMISED DEPENDENCY ON EXTERNAL REVIEWS

- Security was no longer an afterthought that required costly external audits or last-minute fixes.
- By shifting security “left” into development, teams could proactively manage risks before they became critical issues.

THE OUTCOME: SECURITY AS AN ENABLER, NOT A BARRIER

By embedding security engineers within development teams, the organisation achieved:

1: FASTER SECURITY FIXES

- What once took multiple sprints to resolve was now often fixed within a single sprint.
- Security became an enabler of fast, secure development rather than a blocker.

2: STRONGER COLLABORATION BETWEEN DEV AND SECURITY

- Security was no longer a separate function - it was part of the team.
- Developers had immediate access to security guidance, leading to better, more secure coding practices.

3: REDUCED BOTTLENECKS AND HANDOFFS

- Security was no longer a slow-moving external review process.
- Developers had real-time security support, eliminating delays in identifying and fixing vulnerabilities.

4: A SCALABLE, SELF-SUFFICIENT SECURITY CULTURE

- Developers took ownership of security, reducing reliance on a stretched central security team.
- Teams became security champions within their own projects, ensuring security was integrated into every stage of development.

CONCLUSION: A MODEL FOR LARGE-SCALE SECURITY INTEGRATION

This transformation enabled the organisation to scale its security practices without slowing down development. By embedding security engineers within development teams, they shifted from reactive security fixes to proactive security integration, ensuring a faster, more resilient approach to securing applications.

For large enterprises struggling with security silos, this case study demonstrates that security doesn’t have to be a roadblock—it can be a seamless, empowering part of the development process.