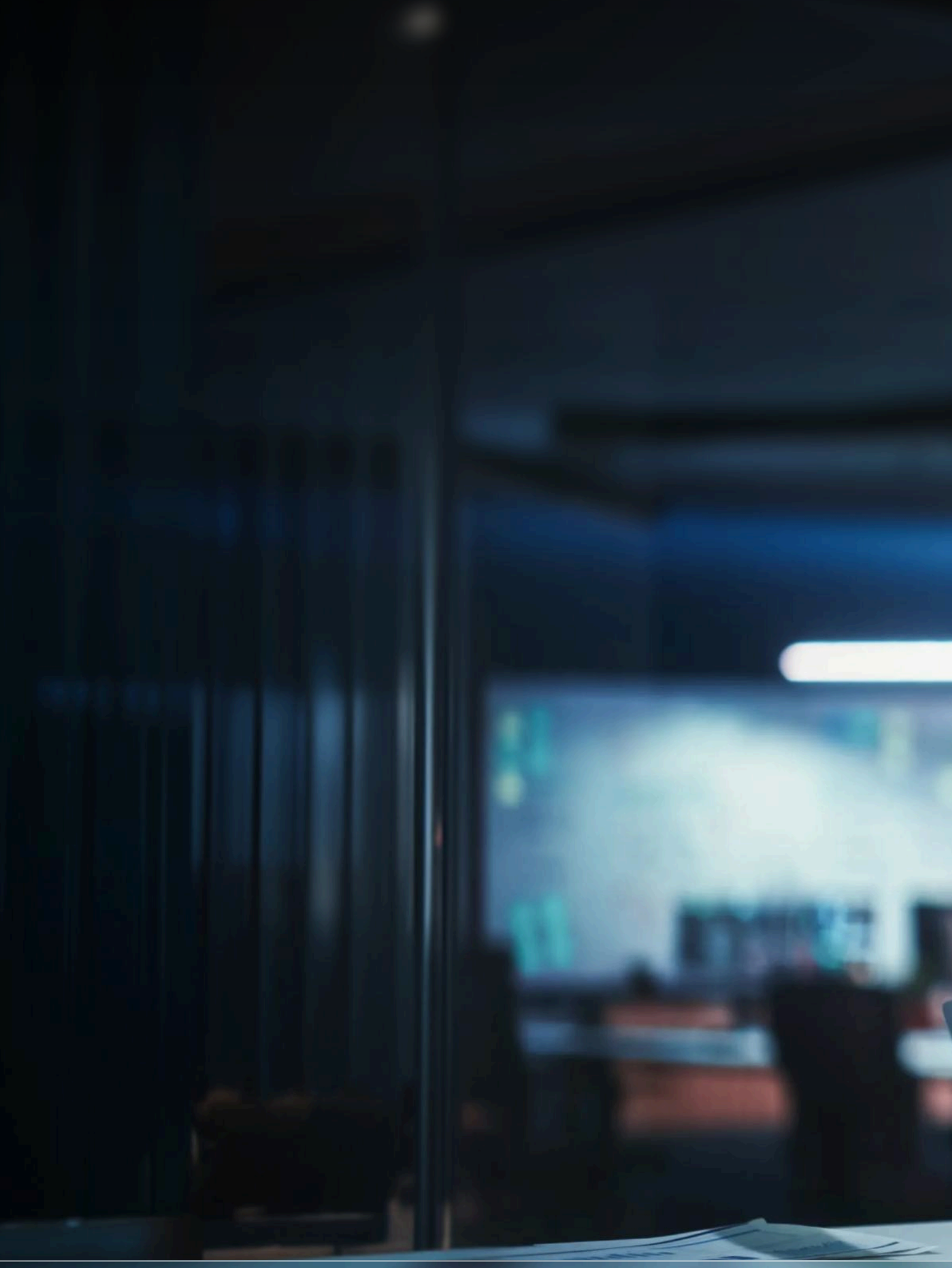
immersive

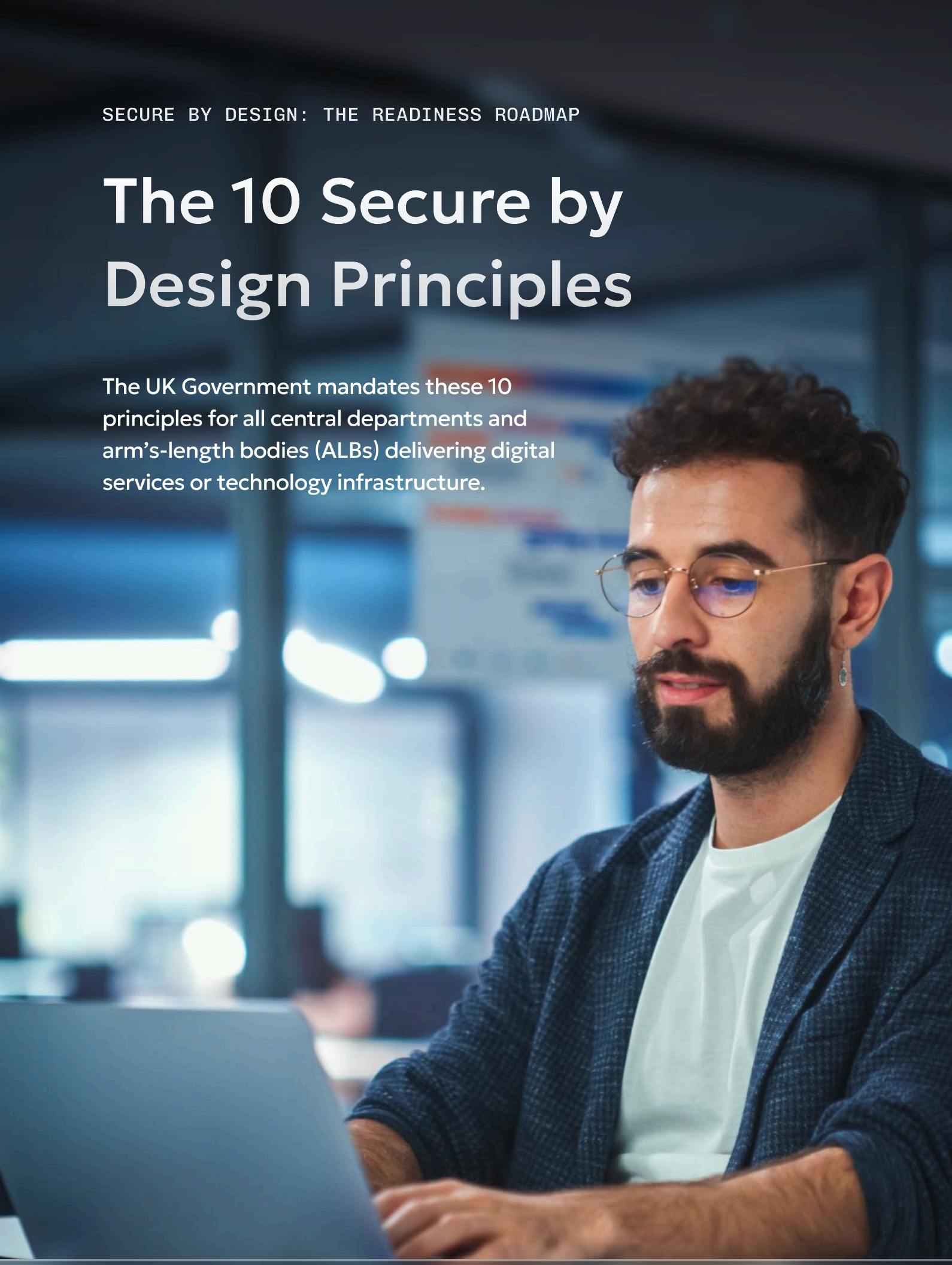
SECURE BY DESIGN

The Readiness Roadmap



The 10 Secure by Design Principles

The UK Government mandates these 10 principles for all central departments and arm's-length bodies (ALBs) delivering digital services or technology infrastructure.



001 CREATE RESPONSIBILITY

Establish senior-level accountability for cyber risk. Security is a business risk, not just a technical one.

002 SOURCE SECURE TECH

Ensure security is considered during the procurement of third-party products and services.

003 ADOPT A RISK-DRIVEN APPROACH

Use continuous threat modelling and risk assessments to prioritize impactful interventions.

004 DESIGN USABLE CONTROLS

Security measures must be intuitive to prevent staff from using "workarounds" that increase risk.

005 BUILD DETECT-AND-RESPOND

Shift focus from just "prevention" to the ability to identify and mitigate active incidents.

006 DESIGN FLEXIBLE ARCHITECTURES

Build systems that can adapt and be updated easily as the threat landscape changes.

007 MINIMISE ATTACK SURFACE

Reduce the number of potential entry points for attackers by disabling unnecessary features.

008 DEFEND IN DEPTH

Use multiple layers of security so that the failure of one control does not lead to a total breach.

009 CONTINUOUS ASSURANCE

Replace "point-in-time" accreditation with a model of ongoing, evidence-based security tracking.

010 MAKE CHANGES SECURELY

Embed security into the entire lifecycle, including CI/CD pipelines and the retirement of old systems.

Addressing the Critical Gaps

While all ten principles are mandatory, most organizations face systemic failure in these three areas. These gaps represent the difference between compliance and true readiness.

PRINCIPLE 1 // THE ACCOUNTABILITY VACUUM

THE PROBLEM

Organizations often treat security as a cost center task for the IT department.

THE RISK

Without executive buy-in, security becomes a bottleneck. Leaders who don't understand cyber risk can't justify the investment needed to stay ahead of AI-driven threats.

THE REFLECTION

If your C-suite views security only as a checkbox for an audit, who is actually owning the risk when a real-world breach occurs?

PRINCIPLE 9 // THE POINT-IN-TIME ILLUSION

THE PROBLEM

Traditional assurance relies on a static certificate that might be three years old.

THE RISK

In a landscape of zero-days and rapid AI advancement, a snapshot from even six months ago is obsolete. Legacy accreditation creates a false sense of security while vulnerabilities drift into your production environment.

THE REFLECTION

Can you provide evidence right now that your teams have the skills to handle an incident, or are you waiting for the next scheduled audit to find out?

PRINCIPLE 10 // THE VELOCITY-SECURITY PARADOX

THE PROBLEM

Secure by Design requires embedding security into Agile Development. However, many teams still treat security as the final gate before launch.

THE RISK

Adding security at the end leads to expensive redesigns, missed deadlines, or—worse—launching with known flaws in the name of meeting a deadline.

THE REFLECTION

Is your secure change process a dynamic part of your CI/CD pipeline, or is it a manual hurdle that your developers are incentivized to bypass?

THE SHIFT:

How to Move from Legacy Accreditation to Secure by Design

FEATURE	LEGACY ACCREDITATION (POINT-IN-TIME)	SECURE BY DESIGN (CONTINUOUS)	HOW IMMERSIVE SUPPORTS SBD PRINCIPLES
CADENCE	Every 3–5 years; often static and quickly outdated.	**Ongoing;** security is embedded in the daily SDLC.	**Continuous Readiness:** Hands-on labs and micro-exercises build muscle memory in short bursts without disrupting daily operations.
AI RISK	Often ignored or treated as an isolated, manual technical silo.	**Integrated;** securing the AI life cycle and defending against AI-enabled threats	**AI Threat Readiness:** safe, sandboxed labs for RAG and Agentic AI build technical fluency and ethical awareness to mitigate AI-powered risks.
FOCUS	Compliance checklists and theoretical documentation.	**Capability;** proving teams can actually defend against live threats.	**Proven Performance:** Cyber Drills and Ranges test detection and response speed, turning passive playbooks into practiced action.
CULTURE	Security as a final gate or a burden on project delivery.	**Security-First Culture;** reducing friction between Dev, Sec, and Ops.	**Security-Aware Engineering:** role-specific upskilling helps developers embed secure coding into daily workflows to stop vulnerabilities before production.
REPORTING	Fragmented, anecdotal, and reactive reporting.	**Visual & Evidence-based;** delivering board-ready data on demand.	**Stakeholder-Ready Insights:** on-demand reports and heatmaps map readiness to DORA, NIST, and MITRE ATT&CK to justify investment.

immersive

Can you prove you're Secure-by-Design compliant? Don't miss our upcoming webinar

Immersive is trusted by the world's largest organizations and governments, including Citi, Pfizer, Humana, HSBC, the UK Ministry of Defence, and the UK National Health Service. We are backed by Goldman Sachs Asset Management, Ten Eleven Ventures, Menlo Ventures, Summit Partners, Insight Partners and Citi Ventures.

WWW.IMMERSIVELABS.COM | SALES@IMMERSIVELABS.COM