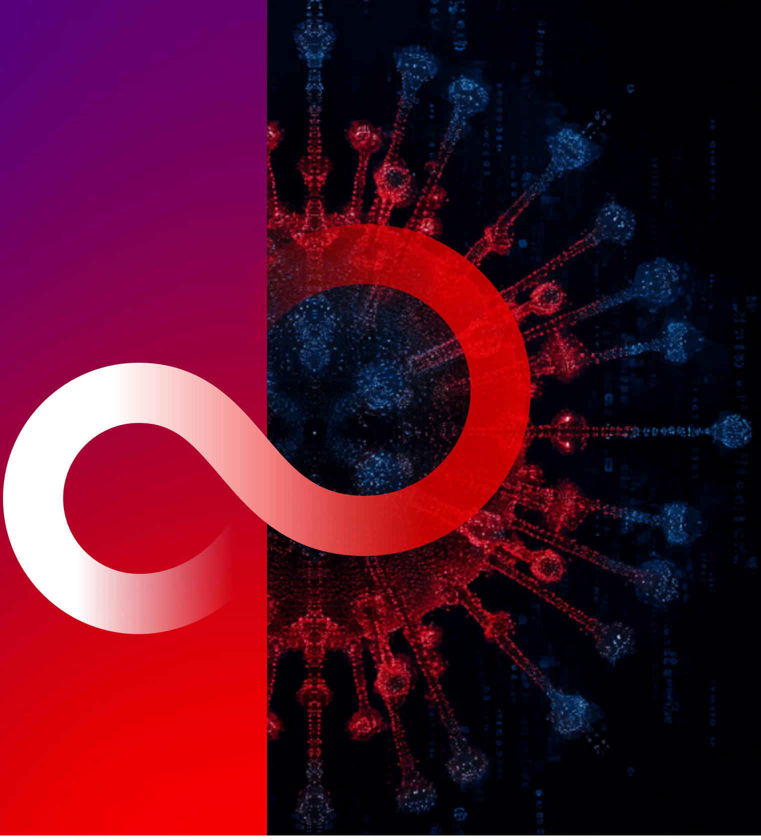
Threat Detection Strategy Consulting

Clarity, capability, and confidence



Build a detection capability that keeps pace with your business - and ahead of attackers.

Our experts help you overcome ineffective threat identification, management, and response by bringing greater clarity, structure, and measurable uplift to your security operations. We work closely with your teams to simplify complexity, sharpen focus, and elevate the performance of your detection capability.

With an independent, practitioner-led view, we strengthen your security posture and ensure it proactively supports your business goals.

Is your organisation set up to detect threats before they become incidents?

Outcomes

Strategic clarity on detection priorities.

Improved operational workflows.

Roadmap for measurable uplift in detection maturity.

Greater confidence in your organisation's ability to detect emerging threats.

The sound of silence

Enterprises invest heavily in Security Information and Event Management (SIEM), Extended Detection and Response (XDR), and Endpoint Detection and Response (EDR). These platforms are critical, yet the detection rules that power them can fail quietly.

While the industry is obsessed with the noise of false positives, the real danger lies in the silence of false negatives, the successful attacks that expensive tools never see.

The industry has no shared way to describe how detection rules fail. Rules differ across vendors, formats, and platforms, and that inconsistency multiplies risk.

The Adversarial Detection Engineering (ADE) blueprint ... created by us

Our experts created the Adversarial Detection Engineering (ADE) framework to address one of the biggest gaps in modern detection: **silent failure**. ADE provides a shared way to identify, classify, and reduce false-negative risk in detection rules, giving organisations greater confidence that their controls work as intended.

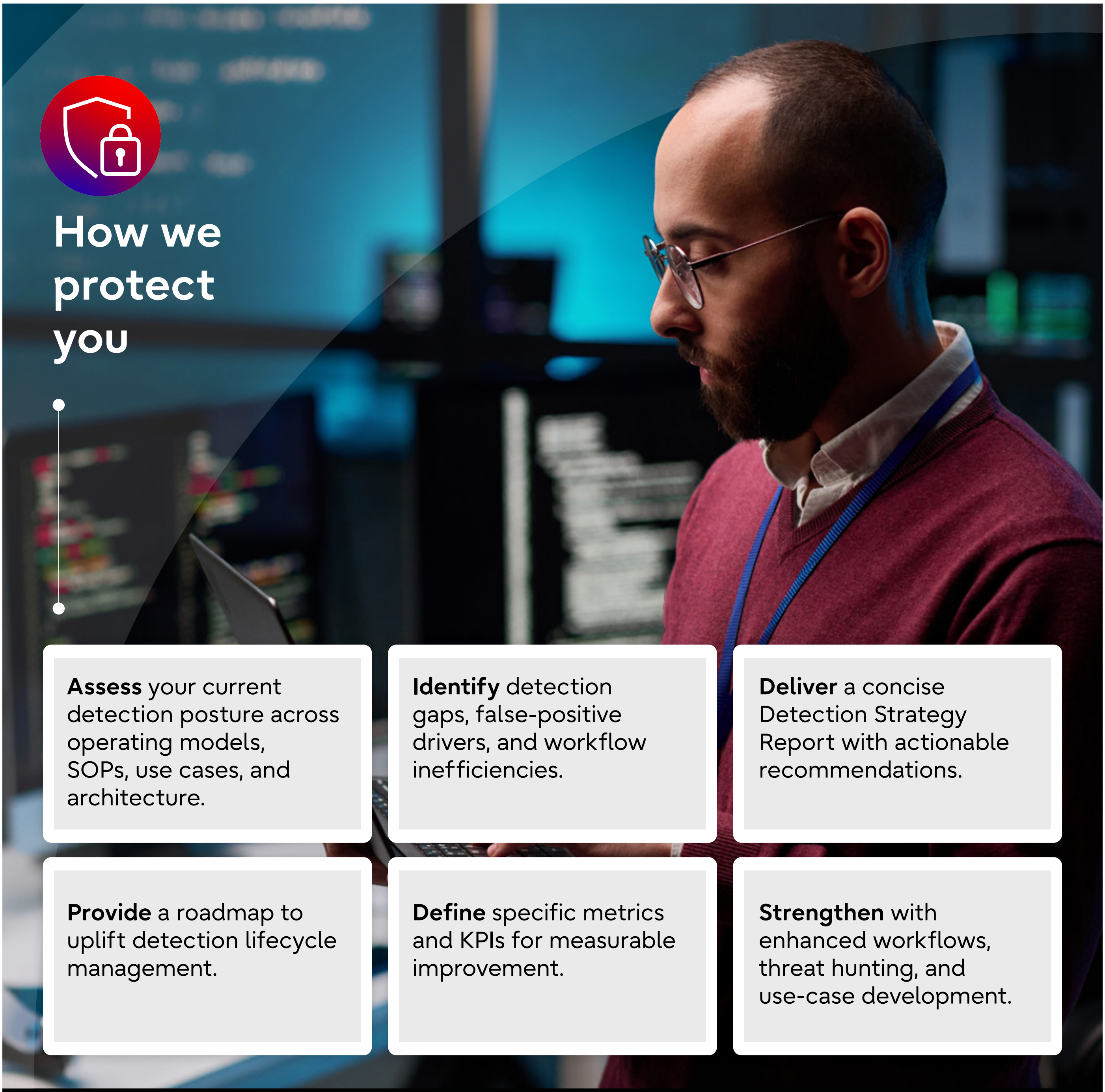
In plain terms, it provides:

- A taxonomy for detection logic bugs
- A method to classify and reason about false negative risk
- A shared standard that enables uplift across the ecosystem.

At Fujitsu, ADE underpins our detection engineering and managed operations. For our customers, this means:

- Higher assurance that rules detect what they claim
- Faster remediation and hardening cycles
- Improved audit and reporting due to the shared ADE taxonomy.

Learn more about ADE here



How we protect you

Assess your current detection posture across operating models, SOPs, use cases, and architecture.

Identify detection gaps, false-positive drivers, and workflow inefficiencies.

Deliver a concise Detection Strategy Report with actionable recommendations.

Provide a roadmap to uplift detection lifecycle management.

Define specific metrics and KPIs for measurable improvement.

Strengthen with enhanced workflows, threat hunting, and use-case development.

Why choose us?

Expert guidance that turns fragmented practices into a unified, effective capability.

Proven methods that reduce complexity, boost efficiency, and accelerate response.

Tailored strategies aligned to your environment for measurable, lasting improvement.

Practical advice that empowers teams and maximises existing security investments.

Ready to strengthen your cyber resilience?
Contact us today.