FUJITSU

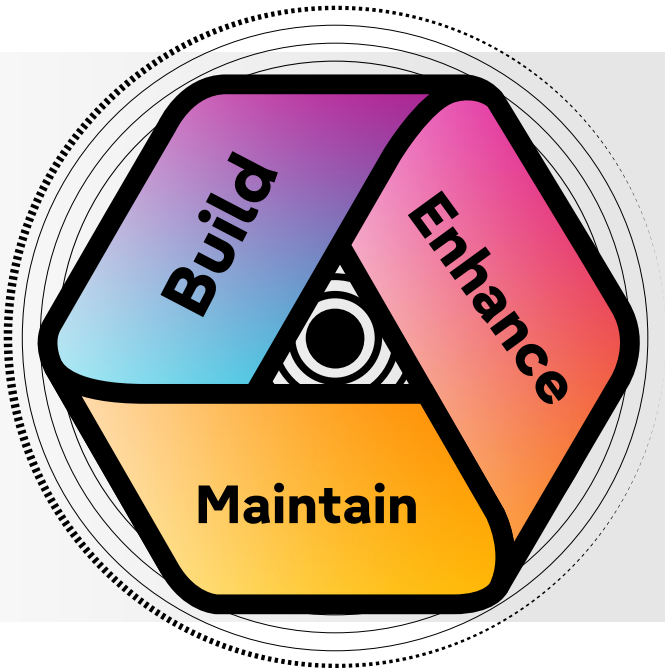
Detection Engineering Services

Cyber security that never sleeps

Modern attackers evolve daily. Your detections should too.

Our Detection Engineering Services provide continuous development, tuning, and uplift of your detection logic. Fujitsu's Advanced Cyber Intelligence & Response Team (ACIRT) ensures that your rules mature over time, become more accurate, and remain aligned with the threat landscape.

Our build, enhance, and maintain lifecycle approach treats detection as a living capability - continuously adapting your defences to keep pace with real-world adversaries.



Outcomes

Improved coverage

Detect threats earlier and more accurately through expanded, high-fidelity detection logic.

Reduced noise

Minimise alert fatigue and missed threats through continuous tuning and refined triage.

Threat alignment

Keep detections aligned to the threat landscape through ongoing, intelligence-led enhancement.

Confidence

Maintain confidence as detections mature across build, enhance, and maintain phases.

Through this lifecycle, we establish a strong detection foundation aligned to your environment and priority risks, expand coverage using threat-intelligence-led use cases and hardened logic, and sustain detection quality through tuning, triage feedback, and targeted threat hunting. The result is improved signal quality, reduced operational noise, and consistently high-fidelity detections over time.

In line with ASD guidance, SIEM and SOAR platforms require continuous tuning and oversight and are not "set and forget" solutions.

Build

- Develop collection strategies tailored to your environment
- Assist with deployment and integration of cyber threat detection tooling

What you gain:
Establishes a strong detection foundation aligned to your environment and priority risks.

Enhance

- Create detection use cases informed by cyber threat intelligence
- Develop complex detections aligned to threat models
- Harden detection engines by identifying bypasses and improving logic

What you gain:
Expands detection coverage and resilience against advanced adversary techniques.

Maintain

- Tune alerts to reduce fatigue and improve fidelity
- Review triage outcomes to refine detection accuracy
- Action detection/exclusion requests and conduct threat hunts based on emerging CTI

What you gain
Sustains high-fidelity detections over time, reducing noise while minimising missed threats.

Fujitsu's ACIRT (Advanced Cyber Intelligence & Response Team) advances threat-informed defence by integrating intelligence, detection, and response into a unified capability. ACIRT operates as an extension of the SOC, supporting detection content development and tuning, strategic threat modelling and hunting, and escalated incident response.

How we protect you

Engineering Detection-as-Code across SIEM, XDR, and EDR platforms.

Threat informed development incorporating adversary techniques and behavioural patterns.

Automated quality assurance and logic validation, reducing drift and preventing silent detection failure.

Application of adversarial testing to confirm rule effectiveness.

Continuous tuning cycles to improve precision, fidelity, and reduce noise as detections mature.

Integration with threat intelligence and purple team findings to validate and refine detection logic.

Why choose us?

Human-led threat detection powered by cognitive and integrable AI models (DTEX, Nuix), ensuring contextual decision-making.

Seamless extension of your SIEM with specialised insider-threat capabilities for deeper monitoring and faster insights.

An end-to-end approach that helps your organisation prepare, respond, and recover from security incidents with confidence.

Ready to strengthen your cyber resilience?
Contact us today.