FUJITSU

Purple Teaming as a Service

Strengthen your cyber defence through collaborative adversary emulation

We evaluate your organisations threat detection and response capability.

Purple Teaming combines the offensive expertise of Red Teams with the defensive insight of Blue Teams to evaluate and enhance your organisation's threat detection and response capabilities.

We leverage the latest threat intelligence and our own research to emulate real-world adversaries, observe your team's response, and work collaboratively to transform your defence from reactive to proactive.

Turn real-world threats into actionable improvements for your security posture

Blind spots in detection and alerting

Recent threat research discovered that the SoaPy attack tool can evade default detection rulesets, highlighting the need for custom detection logic.

Gaps in incident response workflows

Recent threat research helped develop proprietary processes for uncovering SIEM rule logic bypasses, enabling organisations to close critical detection gaps.

Misconfigured or underutilised tools

Recent threat research identified attack paths in Azure cloud environments not covered by standard Defender rulesets, enabling tailored cloud defence strategies.

Our workshop provides confidence, capability, and a clear path forward:

Enhanced resilience

Improved detection, response and containment processes.

Empowers your teams

Equip your team with practical insights and best practices.

Actionable maturity plan

Receive a detailed report with prioritised recommendations.

Build confidence

Build confidence against industry-specific threat actors.

Our approach

Coordinated attack simulation

We execute multiple threat intelligence informed scenarios according to your industry's threat actors, while observing your security team's detection and response capability.

Workshop detection and response

Our adversary emulation and defence team meets with your team to collaboratively transfer knowledge and review opportunities to improve your organisation's detection and response capabilities.

Detection and response enhancement

Continuous feedback during the engagement leads to immediate improvements, and a final report is provided detailing key areas and strategies for your organisation to mature its defences.

This workshop is designed for organisations that want to strengthen their cyber resilience by improving detection and response capabilities. It's ideal for security operations teams, incident responders, and IT professionals responsible for defending against advanced threats. Whether you're looking to validate existing controls, identify gaps, or accelerate maturity, this collaborative engagement empowers your team with practical skills and actionable insights.

Collaborative engagement

The workshop is focused on guidance, not criticism.

Tailored threat scenarios

Based on your industry's adversary profiles.

Rapid security uplift

Immediate improvements during the engagement.

Contact us

Ready to strengthen your cyber resilience? contact us today.