FUJITSU

Threat Hunting

Proactive detection.
Real-world validation.
Actionable security.

Threat hunting is a proactive approach to cybersecurity. Instead of waiting for alerts, it actively searches for hidden threats, vulnerabilities, and detection gaps that automated systems may miss.

Threat hunting isn't just about finding threats, it's about proving your defences work. It gives you the confidence to act, the insight to improve, and the resilience to stay ahead.

Our team of experienced threat hunters leverage advanced techniques and threat intelligence to proactively identify and locate hidden threats within your environment, reducing dwell time and minimising potential damage.

Our detailed report

Our Threat Hunting assessment delivers a detailed report of hidden threats, vulnerabilities, and detection gaps, providing clear, actionable recommendations to strengthen your defences, with our team available to support you beyond the assessment if needed.

You'll receive a comprehensive report including:

- Threat findings and Indicators of Compromise (IOCs)
- Adversary profiles and tactics
- Security control effectiveness
- Actionable recommendations

Identify threats early, before they escalate into breaches.

Expose blind spots in your environment that attackers could exploit.

Validate your security controls to ensure they're working as intended.

Strengthen your resilience with expert-driven, actionable recommendations.

How we hunt threats

We combine threat intelligence, behavioural analytics, and adversary emulation to uncover:

- Hidden malware and APTs
- Misconfigurations and anomalies
- Gaps in detection and response
- Real-world adversary behaviours

Adversary profiling

Adversaries are profiled based on your geolocation, industry, and internet footprint.

Security control validation

Threat actors often exploit vulnerabilities present through malware or other means. To assess the effectiveness of existing security controls, attack scenarios are emulated in a controlled environment with an Endpoint Detection and Response solution in place. This enables validation of detection and response capabilities against real-world adversary behaviour.

Vulnerability identification

Vulnerabilities are identified through threat intelligence sources and endpoint telemetry. This includes known CVEs (Common Vector Exposure), misconfigurations, or behaviours anomalies observed within the environment.

Our intelligence-led methodology combines global threat intelligence, advanced hunting techniques, and real-world attack simulations to deliver clarity, confidence, and control. We don't just find threats, we provide actionable insights and partner with you to strengthen resilience.

Duration: Typically, 2-4 weeks

Advanced threat hunting

Delivered by seasoned threat researchers using global intelligence feeds, ensuring cutting-edge protection and continuous improvement.

Clarity on your security controls

Understand the strengths and weaknesses of your current security setup, enabling you to focus resources where they'll have the greatest impact.

End-to-end guidance and support

We guide you throughout, so you're never left to navigate challenges alone.

Start your threat hunt today and gain clarity, confidence, and control over your security environment.