

DATA SHEET

Digital Resilient Security Operations

► SECURITY OPERATIONS EXCELLENCE FOR IMPROVED DETECTION AND RESPONSE

Benefits

- Optimisation of existing security investments
- Improved threat identification and response
- Greater agility to respond to changing attacks
- Identification of hidden attackers and open threat vectors
- Reduction in attacker dwell time
- Holistic view of security with actionable threat intelligence

Cybersecurity needs to scale and transform in tandem to address growing risks. To achieve this and ensure digital resilient security operations, your organisation needs to integrate capabilities such as automation, machine learning and analytics into a robust platform that will boost security threat detection and response. A transformational approach to digital resilience will also require these capabilities to be bolstered by expert threat hunting and incident response to ensure that your organisation remains vigilant and stays ahead of potential threats and compromise.

Threat Detection and Response Consulting

Organisations are constantly looking for ways to optimise existing security investments to [increase threat detection and response capabilities](#), and to be agile enough to address the rapid changes in modern attacks. With a proven methodology in security operations centre (SOC) design and build, backed by years of experience, we can help you transform your organisation's security capabilities to meet these needs. We will work with you to develop digital resilient security operations with a tailored approach that enhances your threat detection and response capabilities, and help create an agile go-forward plan that includes skills augmentation and capability build up.

Trustwave SpiderLabs Proactive Threat Hunting

[Trustwave SpiderLabs Proactive Threat Hunting](#) helps organisations to fortify your security defences by identifying hidden attackers in the environment and open threat vectors that can lead to a breach. Unlike threat hunting services that use only automated, indicator-centric detection methods, the SpiderLabs service is human-led with an emphasis on analysing clues and developing hypotheses. It leverages SpiderLabs' renowned cadre of threat hunters, a purpose-built threat hunting platform, and best practices and recommendations to help eliminate threats in the environment. The combination of human-driven and automated threat hunting augments the organisation's existing security tools and capabilities, enabling you to maintain vigilance against unforeseen threats.

Managed Threat Detection and Response powered by Trustwave Fusion

[Trustwave Managed Threat Detection and Response](#) leverages our global network of SOCs and experienced security analysts to conduct advanced threat detection, analysis, investigation and response based on your organisation's security needs. It is powered by Fusion, a cloud-based platform that consolidates and normalises data from disparate security tools and integrates with Trustwave's data lake and analytics to deliver a holistic view of security across the organisation's ecosystem and provide actionable threat intelligence.