Bring the Threat into the Light

Gain greater visibility into your external attack surface, reduce your risk exposure, and strengthen your cyber resilience with Sapphire's Managed Threat Intelligence service.

Our 24/7 managed service empowers your team to act decisively, protect your brand, and stay ahead of emerging threats - without the need for in-house threat intelligence expertise.

The Challenge

Organisations today face a complex and evolving threat landscape. Cyber threats stem from direct attacks, indirect collateral damage, and brand impersonation that defrauds customers. Without visibility into these threats, businesses are vulnerable - risking financial loss, operational disruption, and reputational damage.

Compounding the issue, many organisations lack the time, expertise, and skilled resources needed to effectively manage and act on threat intelligence. This gap leaves them exposed, unable to interpret signals from the threat landscape or respond proactively to emerging risks.

An overwhelming 70.6% of dark web-related news and discussions are focused exclusively on the United Kingdom, highlighting the country's prominence as a key target for cybercriminal activities, and the importance of threat intelligence.

Sapphire can help.

Key Benefits

- Credible Threat Identification
- Brand and Reputation Protection
- Operational Efficiency
- Strategic Insight
- Compliance Support
- Customer Trust

The Sapphire Difference

Sapphire's 24/7 Managed Threat Intelligence (TI) service provides continuous digital risk protection. We monitor multiple intelligence sources to detect, predict, and respond to threats targeting your business, operations, and people. Our approach combines automation with expert human analysis to deliver contextualised, actionable insights tailored to your organisation. By integrating and refining intelligence, we reduce false positives and focus on credible threats - enabling faster prioritisation and response.

We continuously fine-tune our detection systems to align with your evolving risk profile, ensuring relevance and accuracy over time.

We monitor the surface, dark and deep web for threats that may impact your security and your brand: data breaches, phishing threats, brand impersonation, data leakage, exposed credentials and cyber fraud, and more, protecting your brand and operational integrity, and helping you maintain your customers' trust.

Keep ahead of the threat. Remove the barrier to visibility.

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Our threat investigations are backed by takedown services, helping you swiftly neutralise malicious content and protect your digital identity.

One vendor identified 2,126 threat actors on the Dark Web, posting over 18,537 times in the last 12 months. Those activities predominantly involved selling compromised data and unauthorised access credentials.

Through our customer-centric service delivery, you will benefit from:

Credible Threat Identification
Actionable intelligence filtered for relevance, enabling your team to focus on real risks and respond decisively.

Brand and Reputation Protection
Proactive detection of impersonation and phishing threats, supported by takedown services to protect your public-facing assets.

Operational Efficiency
Reduced noise and false positives mean your teams can focus on the real threats and strategic priorities.

Strategic Insight
Context-rich reporting supports informed, risk-based decisions—helping leadership align security investments with business goals.

Compliance Support
Continuous monitoring helps meet regulatory requirements such as GDPR, ISO 27001, and NIS2, with transparent reporting for audit readiness.

Customer Trust
By protecting your digital assets and identity, you maintain customer confidence and reduce the risk of reputational damage.

Integrated Value for Existing Customers

Existing customers of Sapphire's managed services benefit from a unified, expert-led approach. With one dedicated team delivering a range of integrated services, the addition of Managed Threat Intelligence extends the capabilities and value of your existing solution. This seamless integration unlocks deeper insights, stronger protection, and greater operational efficiency - maximising the return on your investment across both services.

Service Enhancements

Third-Party Monitoring
Gain a better understanding of the cyber threats posed to you by your third-party suppliers. This module extents to monitoring your third-party suppliers for events such as breaches, ransomware extortion, or malicious communication with threat actors.

Attack Surface Management
Through the addition of the Attack Surface Management module, we offer a comprehensive and proactive approach to identifying, monitoring, and securing your external digital assets. ASM provides additional visibility and context into the risks presented by your internet-facing assets, shadow IT, open-port monitoring and more. Our continuous 24/7 monitoring of your attack surface ensures we're aware of new assets and emerging threats.

Anti-Phishing/Canary Tokens
Cloning a website is scarily easy. That extends the risk to your employees and customers, making them vulnerability to fraud and credential theft. Real-time monitoring and alerting for unauthorised cloning of your website(s), helps identify phishing attempts.

Remove the barrier to greater visibility of the threat. Speak to us today.

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001