whitespider®

Managed Cyber Protection Services

Service Definition

Executive overview

Cyber security is a critical operational and strategic concern for organisations operating in an increasingly complex and hostile threat landscape. For CIOs and IT leaders, the challenge is not simply deploying security tools, but ensuring continuous protection, visibility, and response across a growing and distributed digital estate.

WhiteSpider's **Managed Cyber Protection Services** provide a comprehensive, intelligence-led security capability designed to detect, investigate, and respond to threats across networks, users, endpoints, and cloud environments. Delivered as a fully managed service, this offering reduces cyber risk, strengthens resilience, and enables organisations to meet security and compliance obligations without the need to build and retain large in-house security teams.

The service integrates **Network Detection and Response (NDR), User Detection and Response (UDR), Cloud Detection and Response (CDR)**, and **Extended Detection and Response (XDR)** into a unified operating model that delivers proactive protection and rapid incident response.

Managed cyber protection capability

WhiteSpider's Managed Cyber Protection Services are built around continuous monitoring, advanced analytics, and expert-led response. By correlating signals across multiple domains, the service provides early detection of threats that traditional, siloed security tools often miss.

Network Detection and Response (NDR)

NDR focuses on identifying malicious or anomalous activity within the network. By analysing network traffic patterns and behaviours, NDR enables the detection of threats such as lateral movement, command-and-control activity, and data exfiltration.

For CIOs, NDR provides deep visibility into east-west and north-south traffic, helping to identify threats that bypass perimeter controls and reducing the risk of undetected compromise within the network.

User Detection and Response (UDR)

UDR monitors user behaviour to identify compromised accounts, insider threats, or misuse of privileges. By establishing behavioural baselines, the service can detect deviations that indicate potential security incidents.

This capability is particularly valuable in environments with remote or hybrid working models, where identity has become a primary attack vector. UDR helps protect critical systems and data by identifying risk early and enabling timely response.

Cloud Detection and Response (CDR)

CDR provides visibility and protection across public and private cloud environments. It detects misconfigurations, suspicious activity, and threats targeting cloud workloads, platforms, and services.

By continuously monitoring cloud control planes and workloads, CDR helps organisations maintain secure cloud operations while supporting agility and scalability. This is essential for organisations adopting hybrid and multi-cloud strategies.

Extended Detection and Response (XDR)

XDR unifies telemetry and response across network, endpoint, user, and cloud domains. By correlating data from multiple security layers, XDR provides a holistic view of threats and enables faster, more accurate incident detection and response.

For CIOs, XDR delivers improved security outcomes through reduced alert fatigue, faster investigation, and coordinated response actions across the entire digital estate.

WhiteSpider managed services

WhiteSpider Managed Cyber Protection Services deliver continuous, expert-led security operations aligned to organisational risk profiles and operational requirements.

The service provides 24x7 monitoring and analysis of security events across NDR, UDR, CDR, and XDR domains. Advanced analytics and threat intelligence are combined with human expertise to identify genuine threats and reduce false positives.

When incidents are detected, WhiteSpider security specialists investigate, contain, and coordinate response actions in line with agreed runbooks and escalation procedures. This ensures rapid mitigation while maintaining clear communication and governance.

The service also includes ongoing tuning, optimisation, and reporting to ensure security controls remain effective as the threat landscape and organisational environment evolve.

Key features and benefits

WhiteSpider's Managed Cyber Protection Services are designed to deliver measurable security and operational value.

For CIOs, the service reduces cyber risk by providing continuous visibility and response across critical attack surfaces. It removes the operational burden of running a Security Operations Centre (SOC) internally, addressing skills shortages and reducing cost and complexity.

From an organisational perspective, faster detection and response limit the impact of security incidents, reducing downtime, data loss, and reputational damage. Unified visibility and reporting support governance, audit, and compliance requirements, while enabling informed security decision-making.

Use cases

Managed Cyber Protection Services support a wide range of organisational security needs.

Organisations seeking to strengthen their cyber resilience benefit from continuous threat detection and expert-led response without the overhead of building in-house SOC capabilities.

Hybrid and cloud-first organisations gain consistent security monitoring across on-premises, cloud, and remote environments, reducing blind spots and improving control.

Public sector and regulated organisations benefit from improved visibility, auditability, and governance, supporting compliance with security and data protection obligations.

Cisco EDR

WhiteSpider Managed Services

whitespider®

Endpoint Detection & Response

Endpoint detection and response (EDR) solutions detect threats across your environment, investigating the entire lifecycle of the threat, and providing insights into what happened, how it got in, where it has been, what it's doing now, and what to do about it. By containing the threat at the endpoint, EDR helps eliminate the threat before it can spread.

Endpoint Detection and Response (EDR) and Managed EDR (MEDR) are not the same thing. Many organisations have purchased and deployed EDR. Great! But unless you have staff with the skill, experience and time to actively review the ocean of telemetry being produced by an EDR platform, you really are not getting your money's worth. And, worse, you are definitely not that much more secure.

WhiteSpider's EDR service

WhiteSpider's Managed Endpoint Detection and Response (MEDR) is a service that focuses on safeguarding endpoint devices — such as computers, mobile devices, and servers — from cyber threats. By combining advanced technology with expert oversight, MEDR offers a dynamic approach to detect, investigate, and neutralize threats at the endpoint level.

Service benefits

Real-Time Monitoring

MEDR solutions continuously monitor endpoint activities, ensuring immediate detection of suspicious behaviour. This proactive approach is crucial for stopping threats before they escalate.

Threat Detection and Analysis

Leveraging sophisticated algorithms and threat intelligence, MEDR tools identify potential security incidents. They analyse patterns and anomalies to differentiate between benign activities and genuine threats

Incident Response and Remediation

Upon detecting a threat, MEDR services facilitate swift response actions. This includes isolating affected endpoints and mitigating threats to prevent spread and damage.

Expert Guidance

Many MEDR solutions come with the backing of cybersecurity professionals who provide expertise in managing and responding to incidents. This human element ensures that nuanced threats are not overlooked.

Cisco XDR

WhiteSpider Managed Services

whitespider®

Extended Detection & Response

Extended Detection and Response (XDR) is a unified security solution that integrates and correlates data from multiple security products across an organisation's networks, cloud, endpoints, email and applications. It helps security operations teams to detect, prioritise and respond to threats more efficiently and effectively. It reduces false positives and enhances threat detection and response through clear prioritisation of alerts and providing the shortest path from detection to response. With threats becoming increasingly sophisticated, the old detection and response model, built upon self-contained point security solutions, which are then pieced together, doesn't go far enough. This is where XDR comes in.

Effective XDR solutions are comprehensive, providing prioritised and actionable telemetry across all vector, improving visibility and creating context across your environment. They should also enable unified detection from a single investigative viewpoint that supports fast, accurate threat response, with opportunities to elevate productivity even further through automation and orchestration. XDR solutions typically include features such as playbook-driven automation, guided incident response, threat hunting, alert prioritisation and breach pattern analysis to empower security operations.

WhiteSpider's XDR service

What if you could get XDR as a service through an managed services with highly trained in-house staff specialised in Cisco XDR? At WhiteSpider we deliver a managed services approach to cybersecurity, essentially putting the powerful capabilities of XDR into the hands of a team of highly experienced cybersecurity professional.

Service benefits

Centralises data sources

Centralises and normalizes data from all connected sources, including users, the network, and wherever data and applications reside.

Correlate data and alerts

Correlate all security data and alerts and provide a centralized incident detection and response.

Integrate tools

Integrates a range of investigative tools, behavioural analytics and automated remediation capabilities into a single platform.

Advanced threat detection

Focus on advanced threat detection and tailored responses, has comprehensive monitoring across the entire attack surface.

Why WhiteSpider

WhiteSpider combines deep security expertise with proven managed service delivery to provide a cyber protection capability that is both effective and operationally practical. Our services are designed to integrate with existing security investments while delivering improved outcomes through unified detection and response.

By partnering with WhiteSpider, organisations gain a trusted security partner focused on reducing risk, improving resilience, and enabling the secure operation of modern digital environments.

Next steps

WhiteSpider Managed Cyber Protection Services can be tailored to organisational size, risk profile, and regulatory requirements. Engagements typically begin with a security assessment to define scope, priorities, and service alignment.

whitespider®

Telephone: +44 20 3773 2380
E-mail: info@whitespider.com
Website: www.whitespider.com

/whitespider

CYBER ESSENTIALS PLUS

bsi ISO/IEC 27001 Information Security Management CERTIFIED

bsi UKAS MANAGEMENT SYSTEMS 0003