

Service Definition – Misco Managed Cyber Security Services

Service Overview

Misco Managed Cyber Security Services provide organisations with ongoing operational support to prevent detect respond to and recover from cyber security threats the service focuses on delivering continuous assurance expert oversight and practical risk reduction rather than standalone software deployment it is designed to complement existing security tooling and organisational processes.

This service is vendor agnostic and can incorporate multiple security technologies platforms and data sources depending on each individual customer's requirements.

Service Scope

the service covers the day-to-day operational management of cyber security controls and incidents including:

- Continuous monitoring of security alerts and events.
- Threat investigation and incident triage.
- Coordinated response and remediation guidance.
- Security posture reviews and risk visibility.
- Advisory support aligned to organisational priorities.

The service is tailored to each call-off and may vary dependent on the customer environment maturity and risk profile.

What the Service Includes

- Continuous monitoring of security alerts and events
- Incident triage, investigation, and response guidance
- Severity-based prioritisation of security incidents
- Operational security reporting and visibility
- Advisory support aligned to organisational risk and priorities
- A named service or technical account manager

Service Delivery

The service is delivered remotely using secure tooling and integrations with customer environments. Delivery is aligned to the agreed scope at call-off and may include business-hours support or enhanced coverage for critical incidents.

Misco works collaboratively with customer teams to provide clear communication, escalation, and coordinated response when security incidents occur.

Support Model

Support is provided using a severity-based model. Critical incidents are prioritised for rapid response, with lower-severity issues handled in line with agreed service levels. Support coverage and response targets are defined contractually.

Commercials

Pricing is based on the agreed service scope, coverage level, and complexity of the customer environment. All costs are defined at call-off, with no additional onboarding fees unless explicitly agreed.

Exit and Offboarding

On service termination, access to customer systems is withdrawn in a controlled manner. Any customer data handled during service delivery is securely removed in line with contractual and data protection requirements.

Summary

This cyber security services provide practical ongoing cyber security capability focused on operational resilience expert response and continuous improvement enabling organisations to manage cyber risk effectively without reliance on a single technology or vendor.