

littlefish GROUP

Managed eXtended Detection and Response (M-XDR)

Document Control

Attribute	Value
File name	Managed eXtended Detection and Response (M-XDR)
Author	Rowan Troy
Status	Published
Classification	Unclassified
Date	23/01/2026

Table of Contents

Service Overview 4
Key Features and Activities 4
Enhanced SIEM Visibility 4
Security Orchestration & Automated Response 4
Consistent Threat Landscape Assessment 4
End-to-End Reactive Tooling 5
Microsoft Defender for Identity (DFI) 5
Microsoft Defender for Cloud (DFC): 5
Service Management 6
Service Review 6
Customer Benefits 7
About Littlefish 8

littlefish GROUP

Service Overview

The Managed eXtended Detection and Response (M-XDR) service is based on Microsoft's Sentinel platform and will deliver a centralised view of information security activity. The SIEM provides automated collection and management of audit logs from the Monitored Infrastructure and Security Event analysis, alerting and reporting and is our preferred solution.

The Littlefish approach to M-XDR provides a service tailored to your unique environment. Along with the core components of the service, including solution implementation, alert detection and reporting and compliance services, we also offer optional components which may be built into the service as required.

Key Features and Activities

Enhanced SIEM Visibility

Utilising the industry-leading Microsoft SIEM/SOAR solution, our dedicated transition team will build your solution bespoke to your environment and the data sources within your IT infrastructure that require monitoring, leveraging the 120+ data connectors at our disposal to ensure that the ingestion and parsing of your security data are achieved efficiently.

Security Orchestration & Automated Response

Utilising capabilities created by Littlefish's Development team to ensure a more agile approach to triaging and resolving the alerts. This capability enables efficiency savings, significantly reducing alert dwell time and allowing for faster fulfilment of the "Time to Initial Resolution" KPI metric.

Consistent Threat Landscape Assessment

Littlefish's dedicated threat-hunting team leverages intelligence feeds and reporting to not only alert upon attack infrastructure through the monitoring of IoCs but also evaluate the adversary's behavioural Tactics, Techniques & Procedures (TTP) to assess the methods used against organisations within your emerging threat landscape. This approach will ensure that these TTPs are mapped within your security solutions, allowing for detection & response action to be taken to further harden your environment against such threats.

End-to-End Reactive Tooling

The Littlefish teams are extensively trained to Implement, enhance, monitor and leverage additional security solutions required within your environment; these tools sit within the Microsoft Defender suite and are specialised in key areas such as:

- **Microsoft Defender For Endpoint (DFE):** An advanced endpoint security solution designed to assist your organisation in detecting, investigating, preventing and responding to advanced threats.

- **Microsoft Defender for Office 365 (DFO-365):** Used to provide your organisation with proactive control and enhanced detection & response capabilities against malicious threats posed by email messages, the infrastructure used to send these emails, links within these messages and collaboration tools.

- **Microsoft Defender for Cloud Apps (DFCA):** DFCA is a Cloud Access Security Broker (CASB), which allows the Littlefish team to implement policies, leverage the application catalogue and provide a list of in-use applications across your estate.

Microsoft Defender for Identity (DFI)

A cloud-based security solution leveraging your Azure and on-premises Active Directory environments to identify, detect and investigate advanced threats, compromised identities and malicious insider actions directed at your organisation. This is accomplished by evaluating users and other entities' behaviour to establish a baseline of expected activity.

Microsoft Defender for Cloud (DFC):

The DFC solution is both a Cloud Security Posture Management (CSPM) and a Cloud Workload Protection Platform (CWPP). Proactive mitigation is achieved by continuously assessing your Azure, AWS or Google Cloud environments, allowing recommendations to be raised.

Service Management

Ongoing engagement and dialogue are key to a successful partnership, which is why Littlefish provide structured reviews with the customer on a regular basis.

Service Review

A monthly report will be provided detailing feedback on the service's performance and effectiveness during the period. The report will summarise Security Incident information against relevant monitoring controls. Additionally, service performance management information is included, summarising the following:

- Security alerts
- SOC Security Incident volume
- SOC Security Problems
- SOC availability
- SOC Service Requests

The report will be provided by the 10th working day of the month for the previous monthly reporting period per the current schedule. The SOC service will be reviewed as part of a quarterly Service Review chaired by the Cyber Security Service Delivery Manager and delivered via video conference.

Governance Board

In addition to the service reviews, Littlefish and the customer may periodically convene a Governance Board to assess:

- Overall Service Performance.
- Customer Business Strategy.
- Suitability of the service agreement.
- Opportunities for Littlefish to further enhance the customer's business objectives.

Through a blend of tools, processes and personnel development, Littlefish consistently endeavours to elevate the services delivered to our customers. As part of the monthly Service Review process, Littlefish demonstrates to the customer the steps taken to enhance services and, when applicable, showcases improvements through enhanced service reporting metrics.

Customer Benefits

- Comprehensive Security Oversight: 24x7 highly skilled team of cyber security analysts to detect unwanted behaviours without the need to hire and train internally.
- Early Threat Detection: Holistic detection capabilities of the organisation's network and systems, capable of reviewing thousands of log entries daily and separating the security and non-security relevant data to provide true oversight of operational activities.
- Rapid Incident Response: Powered by highly trained and skilled individuals, following detailed and timely processes and utilising the latest technology that will support an organisation in quickly isolating an incident before escalation or breach occurs.
- Incident and Trend Reporting: Providing trends and patterns can help determine where potential weaknesses reside and how to improve or build additional controls to mitigate risk.
- Greater visibility of Activity and Behaviours: Helping to understand how users interact with the networks and systems and provide near-real-time alerting to changes in those behavioural standards.

This approach allows the team to improve your detection capability and carry out authorised containment and eradication actions on your behalf, ensuring that your IT infrastructure and sensitive data are protected when an attack occurs.

About Littlefish

- Littlefish is an award-winning Cloud based Manage d IT Services Provider. Through our capability and delivery of service excellence we have become an established and credible alternative to the 'usual suspect' large Multi £Billion Managed Service Providers and IT Outsourcers in the mid-market and enterprise.

- Our purpose is to disrupt the conventional Managed IT Services models – where the usual suspects typically fail to perform – by delivering service solutions that are tailored to the precise needs of your organisation and which are communicated in clear and straightforward language. Our people (and users) first approach delivers a higher quality experience and will add tangible business value to your organisation.

Our service solutions are designed to consider and deliver tangible outputs in terms of improved business performance. The IT experience of your users can be enhanced to promote more agility and improved quality output. Furthermore (but often overlooked), highly available, better performing IT services, with expert support on hand when it's needed to get your users working again, can engender employee health and well-being. Because of these deliverables, workforce productivity levels are increased, and it's likely that our highly attuned service model will also enable you to effect cost-efficiency gains. What's not to like!

littlefish.co.uk



MICROSOFT SPECIALISATIONS AND DESIGNATIONS

Microsoft Solutions Partner
Digital & App Innovation
Azure

Specialist
AI Platform on Microsoft Azure
Low Code Application Development
Intelligent Automation

Microsoft Solutions Partner
Modern Work

Specialist
Modernize Endpoints
Copilot
Adoption and Change Management

Microsoft Solutions Partner
Security

Specialist
Cloud Security
Threat Protection
Copilot

Microsoft Solutions Partner
Business Applications

Specialist
Copilot
Intelligent Automation
Low Code Application Development
Small and Midsize Business Management

Microsoft Solutions Partner
Data & AI
Azure

Specialist
AI Platform on Microsoft Azure

Microsoft Solutions Partner
Microsoft Cloud

Microsoft Solutions Partner
Infrastructure
Azure

Get in touch:
0344 848 4440
sales@littlefish.co.uk

CRN CHANNEL AWARDS 2025
MSP OF THE YEAR

MSP CHANNEL AWARDS
MSSP OF THE YEAR 2025

CREST SECURITY OPERATIONS

CYBER ESSENTIALS CERTIFIED PLUS

ISO 27001 ISOQAR REGISTERED

ISO 9001 ISOQAR REGISTERED

ISO 14001 ISOQAR REGISTERED