

littlefish GROUP

Incident Response

Document Control

Attribute	Value
File name	Incident Response service
Author	Rowan Troy
Status	Published
Classification	Unclassified
Date	23/01/2026

Table of Contents

Service Overview 4
Key Features and Activities 4
Rapid Response Mobilisation 4
Swift Containment Methodology 4
Eradication of Persistence 4
Recovery and Reporting 5
Customer Benefits 5
About Littlefish 6

Service Overview

The Incident Response Service will provide dedicated resource as and when an Incident Response engagement is required to Identify, Contain, Eradicate and Recover from an array of high priority verified incidents, ranging from business email compromise to widespread ransomware attacks.

The Littlefish Incident Response team leverage the industry recognised SANS PICERL (Preparation, Identification, Containment, Eradication, Recovery & Lessons Learned) framework in order to establish effective process throughout the engagement, as well as bespoke forensic applications.

Key Features and Activities

Rapid Response Mobilisation

Littlefish will deploy a rapid response team virtually to investigate and contain the incident as quickly as possible, minimising the potential harm or loss from the event, whilst ensuring the chain of custody is always maintained.

Swift Containment Methodology

Conduct containment activities to reduce the attack surface across the client estate, which includes but is not limited to:

- Disabling of both on-premises and cloud-based accounts, until such a time that their activity is reviewed and they are considered safe for use.
- Implementation of security tooling and monitoring, where applicable, both to assist in the investigation phase of the engagement and to provide detection & response capabilities for attack vectors.
- Short term or permanent removal of IT Infrastructure ingress points, where appropriate and authorised to do, whilst containment actions are ongoing.

Eradication of Persistence

Any identified persistence mechanisms found within the investigation that would allow any further compromise, as well as proactive measures, such as resetting of user account authentication information, executed to further reduce the likelihood any such compromise.

Recovery and Reporting

Littlefish will support the customer through the recovery stages, providing experienced and timely advice to ensure that the business operations can return to a normal run state and produce detailed reporting highlight areas that require improvements to prevent a repeat occurrence.

Customer Benefits

- **Timely Incident Response:** Rapid deployment of dedicated incident response personnel who can quickly identify, contain, eradicate and support the recovery process.

- **Standardised Process Driven Approach:** Following the industry recognised SANS PIRCEL model, a process driven approach to ensuring that each stage is planned, executed, recorded and reported on, providing an overview of activities and results to support the organisation during their incident.

- **Seamless real-time collaboration:** During an incident communication is critical, incident response personnel will create and follow a clear and rigid communication plan to ensure that the organisation and possible 3rd parties are fully informed of any discoveries throughout the investigation, allowing for synchronous collaboration and a rapid reliable response.

- **Comprehensive Analysis:** Incident response personnel will leverage all available data sources as well as available cyber threat intelligence with the goal of deriving the full scope of the incident, the root cause and any actionable insights for future containment, prevention and mitigation. This is done to provide the organisation with a complete understanding of the incident which will be provided in the form of a final incident report.

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