littlefish
Cyber Security Services

LITTLEFISH CYBER MANAGED XDR

Are you looking to ensure your information & infrastructure is protected? Our managed XDR service will provide you with subject matter experts to design, build, maintain and leverage multiple security solutions in order to provide you with 24x7x365 detection & response capabilities against your ever-changing threat landscape.

littlefish
Cyber Security Services

WORLD-CLASS, AWARD WINNING MANAGED IT AND CYBER SECURITY SERVICES. DELIVERED ONLY FROM OUR 24/7 UK SERVICE CENTRES

Offering a truly tailored, user-centric approach that achieves tangible value for our customers.

Contents

in *- Littlefish* f *- Littlefish* *- @littlefishuk*

> “We ensure that our customers consistently receive a ***market-leading service***

littlefish
Cyber Security Services

SERVICE OVERVIEW

Welcome to Littlefish.
Where cyber security is done a little bit differently…

Since 2010, we’ve challenged the managed IT market, offering organisations a credible and people-focused alternative to the faceless, monolithic service providers that often fail to perform.

Alongside our technical excellence and proactive threat-monitoring activities, we believe that cyber security should be delivered in a personalised, user-centric, and authentic way.

Managed XDR
An overview

Littlefish’s managed XDR (eXtended Detection and Response) service provides peace of mind that your IT infrastructure is monitored for cyber-attacks and that your data integrity is maintained and safe from compromise or theft. We provide guidance, planning, and protection – all carefully tailored to your risk profile and organisational needs.

Our highly qualified, UK-based support teams, housed within our CREST-certified Cyber Security Operations Centre (CSOC), offer proactive monitoring and response capabilities to mitigate and contain threats, allowing you to maintain focus on other core business activities.

The Littlefish managed XDR team will also augment and optimise threat detection for your organisation, building a service tailored to your IT environment and specific concerns and offering investigation, response, and hunting across the business’s entire IT ecosystem.

Gain the support and expertise necessary to close skills gaps and build a mature security program with 24x7x365 detection and response from Littlefish.

Sterling

“Information security was becoming a bigger and bigger concern for the company, with pharmaceuticals being a highly regulated industry. For us, data security is paramount and cannot be underestimated – we needed a partner we could trust, one that could come in and hit the ground running and that was Littlefish.”

Paul Southam, Sterling Pharma Solutions, CIO

CROYDON
www.croydon.gov.uk

“We ran a full procurement exercise to choose a supplier for our service desk and end user computing, and Littlefish were the clear winners. What came across was the culture of Littlefish aligning with what we wanted to be able to do with the Croydon Digital Service.”

Dave Briggs, London Borough of Croydon, Head of Digital Operations

MANAGED XDR KEY TECHNOLOGIES

The Littlefish approach to managed XDR is intelligent because we will build 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.

Wherever possible, we'll also leverage your existing technologies and licensing to maximise service effectiveness while simultaneously minimising cost.

Littlefish's managed XDR service provides a wide range of reactive and proactive security capabilities to help your organisation mature its security posture and adopt a layered defence strategy. Our experienced and knowledgeable engineers and security-cleared analysts are certified across various security solutions, such as Microsoft's Sentinel and Defender suite. This means we can offer our customers a wealth of experience in designing, planning, and delivering a tailored and ongoing cyber security strategy, allowing your organisation to get on with the job at hand, just as it should be.

Through investment in security-specialised people, processes, and tools, we ensure that our customers consistently receive an effective and collaboratively managed cyber security service delivered along with service excellence. As your partner, we're always available to provide support, consultancy, and open communication whenever you need us.

Our managed XDR service compromises several key technologies, frameworks, and abilities to provide visibility and response in both a proactive and reactive manner.

> ***"Gain the support and expertise necessary to close skills gaps and build a mature security program with 24x7x365 detection and response from Littlefish."***

Together, this results in a service that facilitates the following:

Enhanced SIEM Visibility

Utilising the industry-leading Microsoft SIEM/SOAR solution, our dedicated transition team will build a bespoke solution tailored to your environment and the data sources requiring monitoring. With over 120+ data connectors at our disposal, we can optimise the ingestion and parsing of your security data based on your specific security concerns and risks.

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 substantial efficiency savings. This means alert dwell time is significantly reduced, allowing the "time to initial resolution" KPI metric to be vastly improved.

Consistent Threat Landscape Assessment

Littlefish's dedicated threat-hunting team leverage intelligence feeds and reporting to alert upon attack infrastructure through monitoring indicators of compromise (IOCs). This means we can also evaluate the attacker's behavioural tactics, techniques, and procedures (TTPs) and map these within your security solution, allowing for detection and response action.

Priority-Based Vulnerability Management

Leveraging leading vulnerability management solutions, Littlefish's CSOC will provide context and advice about security vulnerabilities within your IT estate to help inform and prioritise security improvements.

Furthermore, we'll regularly provide comprehensive security reports about the XDR service and offer 'at a glance' trend analysis; these reports make it simple to measure the effectiveness of your security solution and track improvements.

littlefish
Cyber Security Services

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 detect, investigate, prevent, and respond to advanced threats. This is achieved through the use of advanced TTP-based detection, automated response, and web content filtering, as well as the leveraging of DFE-specific features, such as Attack Surface Reduction policies, to implement proactive controls and mitigate security weaknesses within your environment.

Microsoft Defender for Office 365 - (DFO-365)

Used to provide your organisation proactive control and enhanced detection and response capabilities against malicious threats posed by email messages, the infrastructure used to send these emails, links within these messages, and other collaboration tools. This solution allows for the creation of tailored security policies which focus on areas such as anti-spam and phishing and safe attachment and link scanning. It also allows our team of analysts to take response actions, such as removing malicious emails from mailboxes within your environment and blocking attack infrastructure used in active campaigns against your organisation.

Microsoft Defender for Identity (DFI)

A cloud-based security solution that leverages both 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 achieved via evaluation of user (and other entities') behaviours to establish a baseline of expected activity which means any anomalous/suspicious activity is alerted-to. If found, Littlefish will take responsive actions to contain the account over both your cloud and on-premise environments.

Microsoft Defender for Cloud Apps (DFCA)

DFCA is a Cloud Access Security Broker (CASB), which allows us to implement policies and leverage the application catalog to provide your organisation with a list of in-use applications across your estate. This will then allow us to work with you to discover potential shadow IT operations and build a list of "sanctioned" and "unsanctioned" applications to be enforced in order to mitigate data loss and exfiltration from areas that you may not be aware of.

Microsoft Defender for Cloud (DFC)

The DFC solution is both a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) solution. Proactive mitigation is achieved through the continuous assessment of your Azure, AWS, or Google cloud environments, which allows for recommendations to be raised. The solution also allows for reactive measures since detailed alerts are raised directly to the Littlefish CSOC.

Microsoft
Solutions Partner

The above solutions provide the Littlefish team with the ability to improve your detection capability as well as carry out authorised containment and eradication actions upon your behalf.

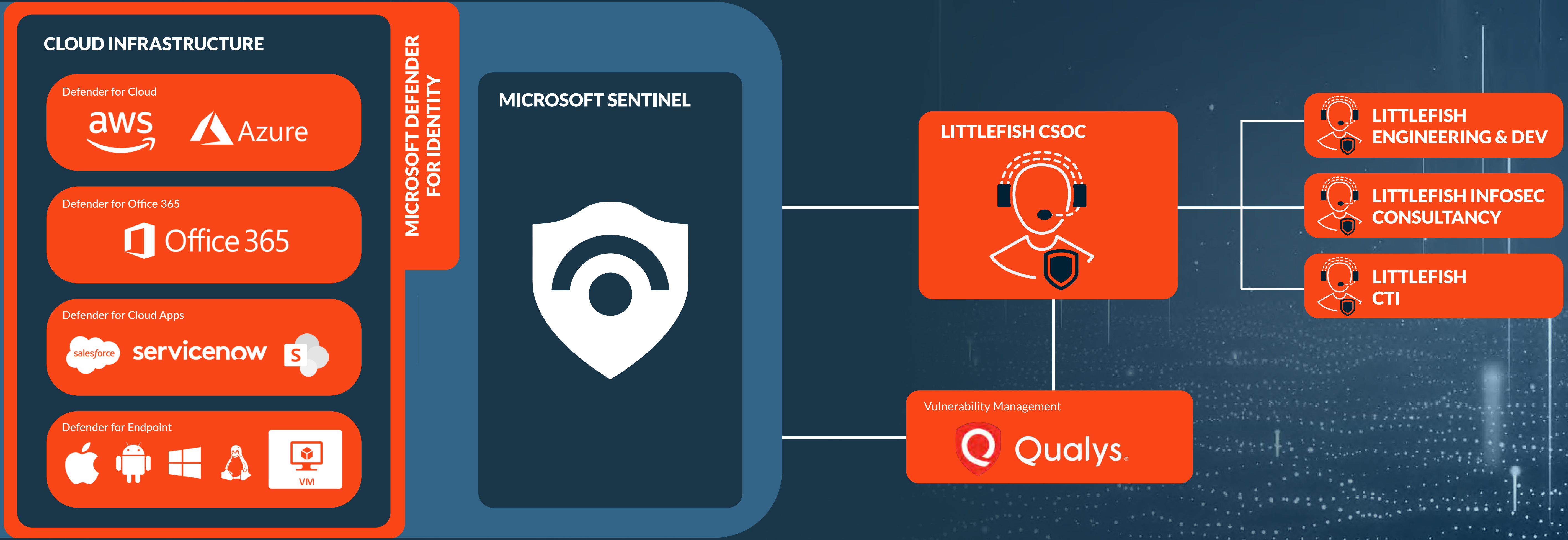
Together, these capabilities ensure that, when an attack inevitably occurs, your IT infrastructure and the sensitive data held within will be protected.

CONFIGURING THE XDR SERVICE

littlefish
Cyber Security Services

There are various ways to breach IT systems and different organisations will naturally have differing security concerns and vulnerabilities to address through their Managed XDR service. As such, Littlefish will outline the best options and optimal XDR configuration for you during the service transition period and in close collaboration with your team. This discussion will also cover any optional components you may wish to add to your service.

With the above in mind, below is an example of what a Managed XDR service might look like:



ABOUT LITTLEFISH

CRN CHANNEL AWARDS 2022 WINNER MSP of the Year

British Business excellence Awards 2022 Winner Mid-Market Business of the Year

megabuyte PRIVATE 50 2022

The Littlefish Difference

Littlefish is an award-winning cloud-based managed 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 user) 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.

We provide market-leading managed IT service solutions that fit flexibly around your business's exacting needs. Whether you're looking to fully outsource, or collaboratively co-source alongside your existing resources, we will deliver a service that enhances business performance.

SECURITY AND ASSURANCE

Information Assurance

Littlefish are an ISO9001 and ISO27001 certified organisation (copy of certificates available on request). We are accredited to Cyber Essentials and Cyber Essentials Plus.

The service is currently suitable for covering a GSC Security Level of OFFICIAL (and OFFICIAL- SENSITIVE).

All Littlefish personnel are BPSS checked as standard. With a significant number of our security teams are NPPV2, CTC and SC cleared.

As previously stated all solution data is kept within your environment and as such is subject to your data security requirements and overall ownership. Additionally, where possible, appropriate encryption will be used for any data in transit to the in use component solutions and also at rest.

Microsoft Solutions Partner

CREST. | SOC

CYBER ESSENTIALS PLUS

ISO 14001 ISOQAR REGISTERED www.alcumusgroup.com

ISO 27001 ISOQAR REGISTERED www.alcumusgroup.com

ISO 9001 ISOQAR REGISTERED www.alcumusgroup.com

littlefish
Cyber Security Services

A LITTLEFISH WITH A BIG DIFFERENCE

Discover how Littlefish's managed XDR service complements your existing teams with the information security skills required to protect your IT & data infrastructure:

info@littlefish.co.uk

0344 848 4440