

Managed Endpoint Detection & Response (EDR)

Endpoint Detection & Response

The complexity of attacks and threats continues to develop at a pace that exceeds the ability of the tools and defenders to keep pace.

Due to their proximity and association with user's endpoint detection and response (EDR) is ideally placed to detect and respond to advanced threats in a timely and effective manner.

Talion's Managed EDR service

Our Managed EDR service provides sophisticated detection and remediation capabilities at the endpoint, all delivered as a fully managed and monitored service.

We build, manage and monitor the solution so our customers don't need to worry about providing a 24/7 SOC capability or the need to attain/maintain the skills required to install and manage the technology.

Securing the modern enterprise means protecting a complex mix of endpoints spread across on-site, remote and cloud locations. We have partnered with CrowdStrike and their Falcon platform to provide the technology at the heart of our Managed EDR service.

Using our Managed EDR service means we can detect threats, investigate incidents, and stop breaches fast—before they can compromise your business.

The main features of our Managed EDR Enterprise service are:

Technology

- CrowdStrike's Falcon EDR platform – industry leading endpoint protection and detection capability.
- Managed SOAR platform – reducing false positives, enables the orchestration of security events and the automation of remediation response.

People

- Experienced cyber security engineers, project managers and 24/7 security operations centre.

Process

- Security monitoring, orchestration, and automation capabilities that underpin the Managed EDR service.

To help customers maximise their existing investments our Managed EDR service can also be deployed to customers who already have an endpoint solution in place.

Managed Endpoint Detection & Response

Managed EDR Service Levels

- **Managed EDR Essential** - is designed for clients who would like us to provide enhanced monitoring around their EDR technology but where the customer manages the EDR technology.
- **Managed EDR Remediate** - is designed for clients who would like us to provide enhanced monitoring, and automated remediation around their existing technology but where the customer manages the EDR technology.
- **Managed EDR Enterprise** - is a managed service for clients who would like us to provide enhanced monitoring, and automated remediation around a CrowdStrike Falcon deployment that is managed by Talion.

Why Talion?

We work as an extension of your security team:

- As an independent MSSP we are not tied to product vendors; we only work with best of breed security technologies and partners.
- Our team of Solution Architects, Project Managers and Security Engineers provide the skills around design, deployment, and management of the CrowdStrike's technology, so you do not need to train and maintain the know-how needed to effectively operate the underlying EDR technology.
- Our team of Security Analysts and Engineers have years of experience in creating highly efficient, accurate and effective threat detection content to keep you safe from cyber threats.
- Our team of SOAR Engineers have years of experience in creating highly automated playbooks to speed up the triage and diagnosis of security cases.
- Our 24/7 Security Operations Centre (SOC) provides security monitoring, triage and alerting around the clock, every day.
- Complete service transparency: we give you 100% visibility into our service, enabling us to form an effective partnership to best protect your business against increasing cyber threat.
- We operate a defence-grade managed security service using SOAR technology. We protect a global base of enterprise customers in the Defence, Legal, Financial Services, Technology, Construction, Energy and Social Care sectors.

About Talion

At Talion, we're changing the way organisations interact with their Managed Security Service Provider. Born out of BAE Systems, our service is built on first-hand knowledge of military engineering and defence-grade security, together with an in-depth understanding of the threat landscape facing the commercial world today.

When it comes to cyber security, we believe every organisation deserves full visibility and complete control over how threats are monitored, how decisions are made, and how their business is protected. That's why we prioritise transparency and collaboration across our service lines, implementing security programs that give businesses the control and freedom to pursue ambitions and realise goals, safe in the knowledge that we've got their back, 24 hours a day, 7 days a week.

HQ

The Hub, Fowler Avenue
Farnborough GU14 7JF

Security Operations Centre

Marshall's Mill
Marshall Street
Leeds LS11 9YJ

Engineering Centre

Unit 32-01, Level 32
The Vertical Corporate Office
Tower B, Avenue 10
Bangsar South, No 8
Jalan Kerinchi, 59200
Kuala Lumpur, Malaysia

Copyright ©2021 SY4 Security Limited trading as Talion.
All rights reserved.