Managed Detection & Response Services

The cyber threat is unrelenting, ever evolving, and it is our job to anticipate, respond to and protect you against the threat, whatever form it takes.

TALION

Total Transparency. Complete Control.

As your cyber security partner, we work closely with you, ensuring you have full visibility and complete control over how cyber threats are monitored, how decisions are made, and how your business is protected.

Our mission is to be the most transparent and collaborative MSSP in the market, giving control back to businesses.

With our innovative flexible model, you can choose the level of interaction with our dedicated security team.

Transparency

In contrast to standard black-box security solutions, Talion shows you everything that goes on in the SOC, 24 hours a day, 7 days a week with completely customisable dashboards.

Control

We believe in giving control back to businesses, that's why, unlike many MSSPs, we give you total visibility of your security cases.

With this unrestricted view you maintain control of your security, whether that's making decisions on remediation actions, or having visibility of all your security incidents.

TALION

"Talion have been a fantastic partner to work with and I really see them as an extension of our team. Having the skillset and agility of a growing organisation but the talent and capability of a much larger organisation from which they were formed, BAE Systems, has proven a great combination. The team work hard to continuously demonstrate and add value to their customers and are always receptive to feedback".

Senior Director – Security Operations
Large UK Technology Company

Benefits:

Automate remediation

Quickly remove devices or systems from the network before they can cause damage.

Investigate & detect threats rapidly

Network traffic analysis improves network traffic visibility and in turn delivers rapid investigation and threat detection.

Understand your threat coverage

Our proprietary Threat Coverage Modelling enables customers to understand their security monitoring coverage in the context of the methods a cyber attacker would use.

Expose new threats

Using our data lake capabilities and our analysts skilled knowledge of how threat actors work we can perform automated and manual threat hunts across our entire data set.

Detect anomalous user behaviour fast

User and Entity Behaviour Analytics (UEBA) utilises machine learning and artificial intelligence to detect anomalous user behaviour that may pose an insider threat.

Understand the threat of high-risk insiders

Enhanced user monitoring detects the threats posed by high-risk insiders.

The Detail

Managed Detection & Response

Managed Detection and Response enhances your ability to detect and respond to cyber threats faster and more accurately, thus reducing risk to your business and improving your security posture.

We pride ourselves on offering a fully transparent service, from our unique threat coverage modelling to visibility of the analyst workbench and customisable dashboards across any datapoint in the SOC. Our threat-led MDR service detects threats and suspicious events on your network and correlates multiple related security events into a single security case with the contextual information and security-valuable sources our analysts require to immediately provide insight and allow resolution of any security issue.

Our service is underpinned by the following core components:

- We provide all the tools, people, and processes to monitor and detect attacks before real damage is done.
- Security Information and Event Management (SIEM) platform which collects security event data and processes it using security logic developed and maintained by our analysts.
- Security orchestration, automation, and response (SOAR) platform that provides workflow management to drive up the speed, efficiency, and accuracy of security alert triage.
- 24x7 security analyst team who are on hand to ensure your networks and systems are secure. The team use the SIEM and SOAR platforms as well as our threat intelligence team's input to analyse security events and alerts. If anything goes wrong the analysts alert you.
- IT Service Management (ITSM) platform which provides secure management, including auditable logs of all actions and clear communication of any alerts we pass to you.

MDR Features:

- 24x7x365 service
- UK based Security Operations Centre and Senior Leadership Team
- Our MDR service has featured in the Gartner Magic Quadrant for 6 consecutive years
- We are experts in Security Orchestration & Automation, we have developed over 200 orchestration playbooks over the last 5 years
- We continually develop threat relevant content, backed by threat intelligence & measured against SLAs
- Transparent service giving control back to businesses
- Threat Coverage Modelling: a transparent way to understand where you are most vulnerable
- Third party integrations to ensure coverage across your estate
- Our MDR service is underpinned by a market leading threat intelligence team
- We operate a "Benefit one, benefit all" service
- Dedicated Service Delivery Manager

TALION

Extended Detection & Response

XDR is a service enhancement to our MDR service. XDR allows clients to start to automate remedial actions around their key security infrastructure. For example, by applying the XDR service to an endpoint solution we can detect an issue on an endpoint and then use our Orchestration and Collaboration Platform to perform remedial actions, such as isolate the endpoint or block a misbehaving process, all automatically. This approach means that at risk endpoints can be quickly and at any time of day taken off the network before they can cause damage. XDR is being expanded to provide the same levels of automation on other protective security solutions such as firewalls, cloud, and identity access systems.

Network Detection & Response

Organisations are turning to Network Detection and Response (NDR) solutions to complement or replace traditional security tools. Many enterprises have a blind spot inside the network. NDR uses network traffic analysis to provide improved network traffic visibility that in turn delivers rapid investigation and threat detection. Talion have partnered with ExtraHop to deliver a service based around their Reveal(x) product set. Reveal(x) provides a full-spectrum detection capability powered by advanced machine learning, rules, and custom models to detect suspicious behaviours, prioritise high-risk threats, and automate/augment response activities.

Threat Coverage Modelling

The adoption of the "attack" or "kill chain" idea means that the cyber security industry now has a common model of understanding how attacks take place. This means we can better position security controls to defend against any attacks. The "kill chain" idea was adopted by MITRE ATT&CK and has since gained wide adoption as it provides descriptions and models that are vendor agnostic and objective.

Talion's Threat Coverage Modelling (TCM) tool has been designed with the MITRE ATT&CK model at its heart. Using the work from our Tactics, Techniques and Procedures (TTP) group, TCM helps our customers understand their security monitoring coverage in the context of the methods a cyber attacker would use.

TCM allows our customers to:

- Validate monitoring already in place
- Asses the gaps in their security monitoring strategy
- Make informed decisions on how to enhance their protection and where to spend their security budget

Threat Hunting

Threat Hunting is the practice of proactively searching for threats on a network by detecting anomalies in normal user and network behaviour. This approach to cyber security is driven by the premise that it is impossible to prevent every single intrusion on a client's estate. This approach drives the two main objectives for Threat Hunting:

1 Identify previously unknown or ongoing threats
2 Gain a deeper understanding of the client's technical landscape to provide additional security value

Using our Azure-based data lake capabilities and our analysts skilled knowledge of how threat actors work we perform automated and manual threat hunts across our entire data set which complements our existing monitoring service.

Insider Threat Detection & Response

Attackers are bypassing traditional perimeter defences and insiders are, by definition, already on the network. Businesses need to maintain a much closer watch on user behaviours. Talion have developed two approaches:

User and Entity Behaviour Analytics (UEBA)

As part of our MDR service we have developed an Azure-based service for orchestrating and automating UEBA.

The UEBA service integrates:

- Talion's Threat and Content Teams
- Talion's SIEM and SOAR platforms for event collection, correlation, and automation
- Microsoft's Azure Data Factory and Data Explorer to move, transform and analyse data

Enhanced User Monitoring Service (EUM)

EUM is an additional monitoring and detection service for the threats posed by high-risk insiders. Enhanced User Monitoring uses specific detection use cases which are mapped to the MITRE ATT&CK cyber threat framework.

Vulnerability Management

Security vulnerabilities remain one of the main causes of serious data breaches.

Talion's Vulnerability Management Service (VMS) helps customers implement a vulnerability discovery capability without the need for software, hardware, or staff.

VMS delivers a managed service for:

- External and internal scanning
- Active scanning
- Daily vulnerability checks and updates
- Authenticated and unauthenticated scanning
- Compliance scanning for PCI-DSS, HIPAA and other frameworks

VMS also has advanced functionality to help customers prioritise their remediation efforts:

- Likelihood prediction - machine learning to establish the likelihood of exploit
- Threat context - Talion's threat intelligence to understand how attackers are using a vulnerability

Why Us?

- Protecting our customers is our number one priority, always.
- We form relationships. Relationships built on trust, transparency, and an intimate, human understanding of the way our customers work and the potential risks that come with it.
- We provide full visibility into the processes and decisions that are keeping you safe.
- We integrate best of breed technology; we are technology agnostic.
- With 12 years of experience, we are leading experts in SIEM and Security Orchestration, Automation & Response technologies.
- We have built a partner community of experts and innovators, to tackle the threat from all angles.
- We operate a high performing, threat-led security operations centre from Leeds, UK.
- We are cyber experts, we invest heavily in threat intelligence, detection content and orchestration playbook development, and are considered to be one of the best in the MSSP industry.

TALION

TALION.NET

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.

Speak to one of our experts today

hello@talion.net
+44 (0) 800 048 5775

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

Managed Detection & Response Services