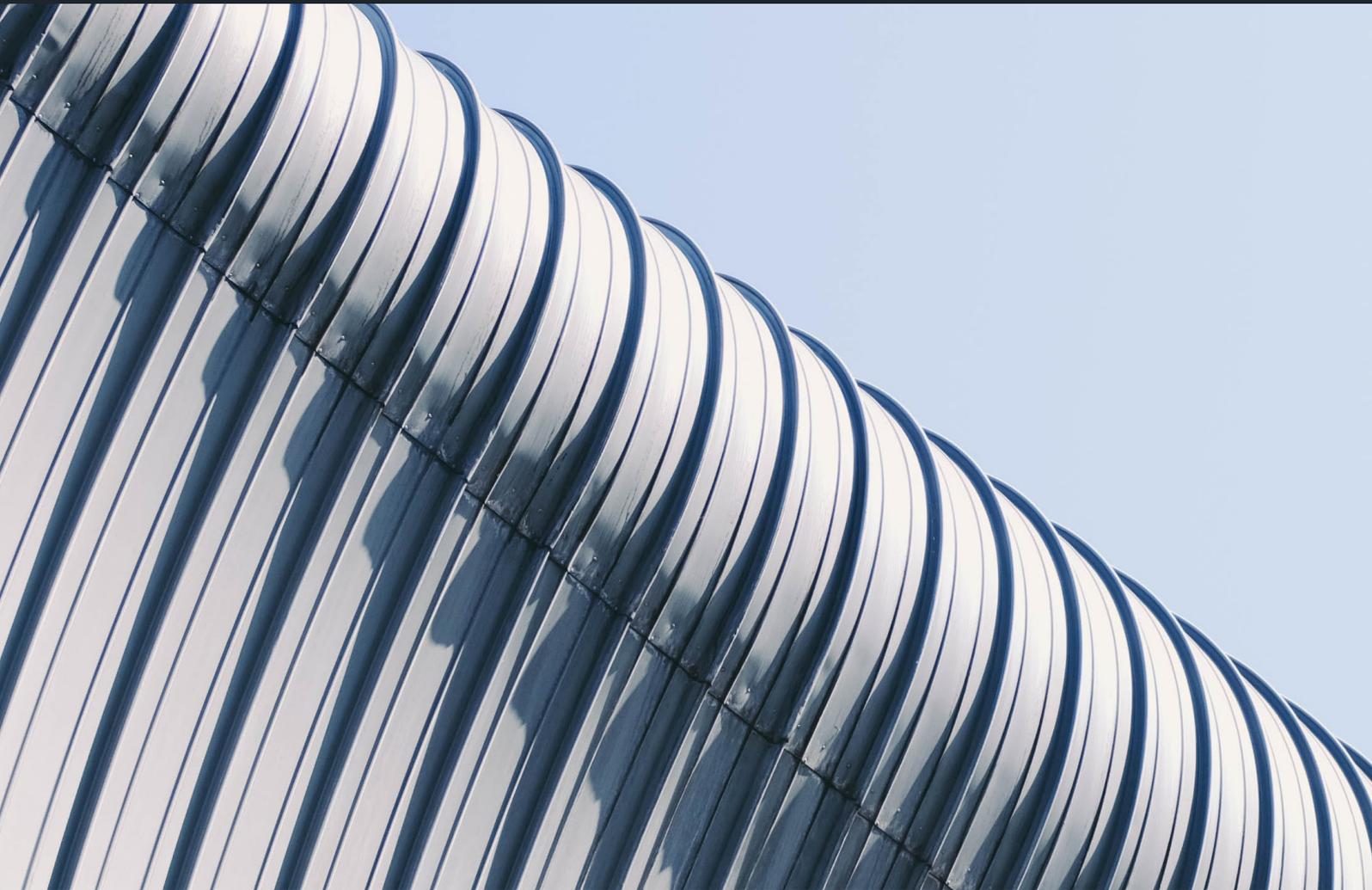


Security solutions  
you can see

TALION





Talion is a UK-headquartered Managed Security Service Provider (MSSP) born out of BAE Systems, the UK's largest defence contractor. Originally created to protect a major sporting event in 2012, our Security Operations Centre, based in Leeds, UK, is considered one of the most advanced in the country. We are experts in understanding the threat landscape and designing security monitoring solutions to meet the specific needs of each individual client.

We create cyber security programmes that are woven into the fabric of an organisation. We take the time to understand each client's unique challenges and ambitions, which enables us to minimise the relevant threat and place control firmly back in their hands, safeguarding their business and empowering their people to press on and do what they do best.

The threat from cyber-attacks is relentless. For organisations, it hinders their ability to make plans, succeed and grow. Even without a breach, the threat alone robs businesses of control and autonomy.

**This isn't right. And it is why we do what we do.**



Everything we do, we share with our clients. We do not provide black box solutions. We form relationships. Relationships built on trust, transparency, and an intimate, human understanding of the way our clients work and the potential risks that come with it. This allows us to deliver solutions that address the critical issues facing our clients, providing real value.

# Total Transparency. Complete Control.

At Talion we believe in transparency, collaboration, and handing control back to the customer.

Whether you are looking for a fully outsourced managed security service, or you operate your own SIEM and are our looking to make performance improvements to your security operation, we offer a flexible range of services that provide you with the right level of transparency, collaboration, and control for your business.

Our high performance SOC defends some of the world's most highly targeted organisations. Since its inception, we have honed our skills in content development and security orchestration and automation, as well as developing a world leading threat intelligence capability that tracks hundreds of the world's most dangerous threat groups.

## UK-Based Security Operations Centre (SOC)

Features of our SOC include:

- Based in Leeds, UK.
- With 12 years of experience, we are leading experts in developing SIEM detection content and Security Orchestration, Automation & Response technologies.
- We continually develop threat-relevant content, backed by threat intelligence & measured against SLAs.
- Our services are underpinned by market leading threat intelligence.
- We deliver a "Benefit one, benefit all" service.
- Our Managed Detection & Response service has featured in the Gartner Magic Quadrant for 6 consecutive years.



# Our Services

## Managed Detection & Response (MDR)

MDR 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. Components of our MDR service include:

- **Managed Endpoint Detection & Response (EDR)** enables at-risk endpoints to be quickly and automatically taken off the network before they can cause damage.
- **Managed Network Detection & Response (NDR)** analyses network traffic behaviour and uses machine learning techniques to detect attacks that may have evaded traditional perimeter security technology.

- **Threat Coverage Modelling (TCM)** is an objective, standards-based method of assessing the coverage of a customer's current and future security monitoring.
- **Threat Hunting** identifies previously unknown or ongoing threats and allows us to gain a deeper understanding of the client's technical landscape to provide additional security value.
- **Insider Threat Detection & Response** utilises machine learning to undertake User and Entity Behaviour Analytics (UEBA) as well as our Enhanced User Monitoring Service which uses specific detection capabilities to monitor key or high value users.

## Hybrid SOC & Collaboration Services

### Managed Security Orchestration, Automation & Response (SOAR)

We bring simplicity to a complex problem. Disparate security technologies producing vast volumes of data overwhelm analysts, draw heavily on security engineering resources and distract security leaders.

Talion's Managed SOAR service overcomes this challenge by integrating with your security technologies to provide a simple to use security management platform that gives comprehensive visibility of the threats facing your business and improves efficiency through a library of expertly crafted and tested

orchestration, automation & remediation playbooks. This allows analysts to focus on what matters, freeing up engineering resource and allowing security leaders the time and space they need to think strategically about protecting the business.

#### Other Hybrid services include:

- SIEM Platform Management
- SIEM Content Management
- Custom Playbook Development
- Additional Enrichment Sources
- Additional Remediation Integrations
- Staff Augmentation

## Security Advisory & Testing

There are a broad range of capabilities required to effectively and efficiently protect an organisation from cyber security threats. Our consulting services help you to understand the security risks you face and the effectiveness of your existing policies, processes and technologies. We will help you understand where you are exposed and design a programme to help you mitigate, reduce, or remove risk to ensure you have the optimal security posture, specific to your organisation's operating factors and risk tolerance.

### Cyber Risk Assessments

We take time to understand your organisation, working with your senior leadership to understand the risks to your business, and enable you to make better cyber security decisions.

### Cyber Maturity Assessments

We help you to understand the strengths and weaknesses of the controls you have in place by examining the policies, process, technology and data you use.

### SOC Performance Assessments

We help you identify where efficiency, performance and resiliency can be improved and give you practical options to get there.

### Penetration Testing

Our threat-led penetration testing provides a structured and effective approach for companies to mitigate their cyber risk, avoid cyber-attacks and understand the real effectiveness of key technical security controls they have put in place.

---

## Threat Intelligence

Our Threat Intelligence team investigate and track many of the world's most dangerous threat groups, against which we risk assess each of our clients. Understanding these threat actors and their tactics, techniques and procedures underpins our security operations. Our unique Threat Coverage Modelling, leveraging the MITRE ATT@CK model, allows us to identify the top threats relevant to your business, the techniques used by specific threat groups and how our rules defend against these techniques. This is how we deliver a threat-led service.

### We also offer:

- **Threat Advisory Bulletins:** Our Threat Intelligence team produce regular threat advisory bulletins alerting you to new or evolving threats and vulnerabilities your team may need to address. All bulletins include actions our SOC are taking and recommendations for the client.
- **OSINT Glass:** Our open source intelligence service keeps you one step ahead of the attackers by revealing what information they can obtain about your company and its employees, that could increase risk to your business.

---

## Incident Readiness & Response

Our teams use proven tools, proprietary analytics, and unique knowledge of the tactics employed by over 200 of the world's most advanced threat groups to uncover the critical facts fast. We offer strategic guidance to ensure your organisation makes the right decisions at the right time.

We support you every step of the way so you can get back to doing what you do best.

## T-LABS

T-Labs is a tight-knit, highly skilled team of Talion threat intelligence analysts, detection content and playbook developers, pen testers, incident responders, architects, engineers, and researchers developing innovative ways to stay ahead of the cyber threat.

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