Managed Security Orchestration, Automation & Response (SOAR) Service

TALION

Total Transparency. Complete Control.

Benefits:

- A single cloud-based platform that gives you full visibility into your security operations, from customisable dashboards to individual, detailed security cases.
- Your analysts receive comprehensive security cases, rather than disparate alerts. Each case is enriched with contextual information, a case summary and recommended remediation actions, making it quicker and easier for analysts to make better decisions.
- Through expertly designed and curated playbooks improve process consistency, reduce human error, speed up mundane tasks, remove the need to log into other applications and reduce the amount of training required on both your SOAR and SIEM platforms.
- Benefit from up to **70% reduction** in triage volumes without missing any actionable security alerts.
- Improve your security case handling with a **300% increase** in time available for triage.
- Reduce your analyst resources by up to **65%,** whilst addressing the same level of security alerts.
- Get greater contextual information allowing you to more accurately prioritise risks.
- Increase efficiency with automated response.

The Challenge

Organisations operating Security Information and Event Management (SIEM) technology are being overwhelmed with alerts, which need to be prioritised, analysed and acted upon. Security analysts are prone to alert fatigue which leads to mistakes and real alerts being missed. The round-the-clock threat of cyber-attacks is leaving organisations facing a high-cost solution, covering unsocial hours, with a potentially diminishing value in return.

If cyber security is not already challenging enough, the high attrition rate of security analysts, added to the scarcity of skills, makes it difficult to accumulate an experienced, efficient, and resilient analyst team.

But help is at hand. Security orchestration, when deployed correctly, substantially improves Security Operation Centre (SOC) precision and performance as well as reducing analyst burn out.

Talion's Managed SOAR Service

Managed SOAR is the hub of your security operations, it's a single platform that bridges the gap between your disparate security tools, the data they produce and your visibility across your IT estate. Rather than working across multiple technologies such as SIEM, EDR and NDR, our platform unifies these systems so that your analysts have one single work bench from which they can detect, investigate, and respond, with a complete picture of the threats facing your business.

But this alone does not solve the problem, we layer over this a library of carefully curated playbooks to further enhance efficiencies, and as a Managed SOAR customer, you recieve custom playbooks designed, tested, and deployed specifically for your use case on a monthly basis. Your analysts utilise the same interface as Talion analysts allowing real time collaboration, investigation, and remediation. Managed SOAR is more than just a technology platform, it is a collaborative space where analyst can operate at their absolute best, utilising advanced playbooks to speed processes, improve consistency, remove human error and enrich security cases, meaning the analyst can make much better decisions, fast. Our experience has shown that this reduces attrition, and improves efficiency, efficacy and ultimately job satisfaction within your security team.

Managed SOAR offers the right combination of technology–yours and ours, integrations, and road-tested orchestration, automation & repsonse playbooks, coupled with security expertise, which enables your security team to accurately prioritise the threats posing the highest risk to your organisation.

Managed SOAR is accessed via a user-friendly interface covering three key components:

1. VIEW ▸
Your Data, Demystified

Customisable dashboards give you one unified view of all data points across the platform, allowing you to generate insights like never before. You can understand the true performance of your security operations with full visibility of key metrics. You can also view dashboards for your various security use cases including, but not limited to, Endpoint Detection, Insider Threat and Vulnerability Management.

Fig 1: Customisable dashboards

2. COLLABORATION ▸
Side-by-side support

Collaboration functionality allows you to chat to Level 3 Talion analysts at any time, day or night. You can ask questions and get clarity on an investigation while approving or rejecting recommended remediation actions with the click of a button. Leave no room for error when collaborating on investigations.

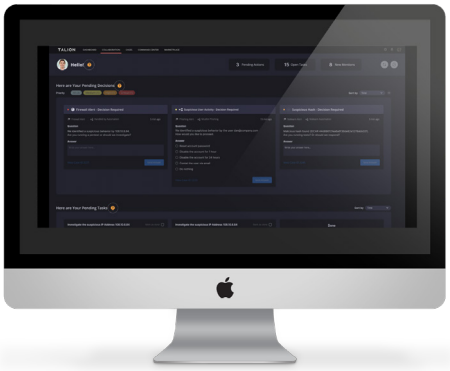

Fig 2: Collaborate directly with Level 3, Talion analysts

3. CONTROL ▸
See the whole picture

Managed SOAR gives you full visibility of your security operation and allows you to stay in control of all security decision, while avoiding the need to manage a platform and create the content needed to derive value from it. You see the whole picture allowing your analysts to prioritise better, resolve cases faster and ensure better security outcomes.

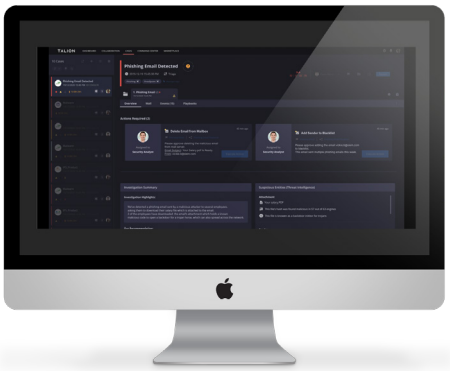

Fig 3: View your entire security case including an investigation summary, suspicious entities, alert highlights, and events.

Managed SOAR ingests alert data from your security technologies such as EDR, NDR & SIEM. It then acts as a centralised hub for analysing, correlating, processing, and consolidating your security cases. Managed SOAR leverages advanced playbooks designed, tested, and curated by our expert team to provide the analyst with a much richer picture of what is happening across the estate, enriching cases, and automating mundane tasks so they can make better decisions more efficiently. Once triaged by the analyst, Managed SOAR helps to automate the remediation of the security incidents, meaning your incidents are resolved fast. If Staff Augmentation is purchased alongside Managed SOAR, the customer's security team can hand off to, or collaborate with, Talion Level 3 analysts utilising the exact same system, so information between the teams is complete and seamless.

Managed SOAR Architecture

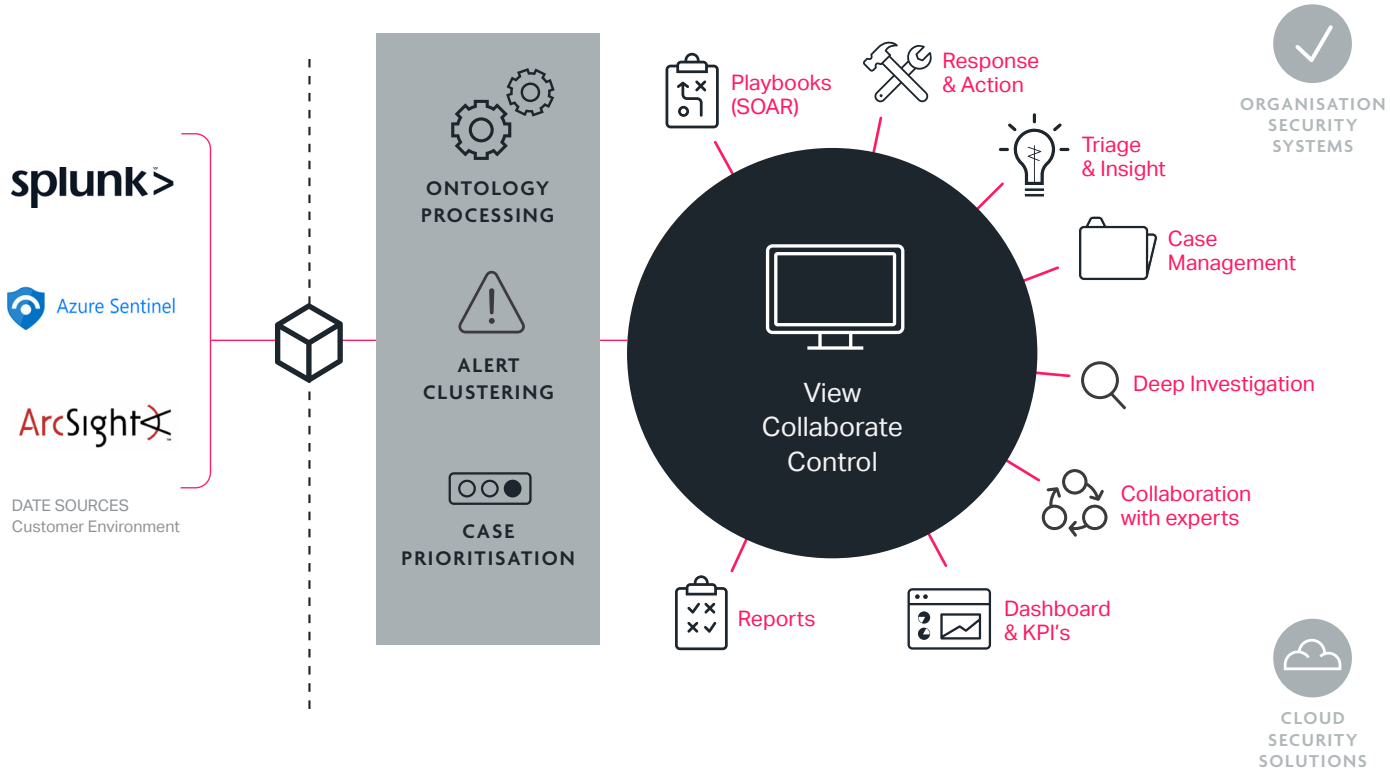

Fig 4: Managed SOAR Architecture

"Our Security Operations Centre defends some of the world's most highly targeted organisations. Since its inception in 2012, we have honed our skills in content development and security orchestration and automation - improving the efficiency, effectiveness, and resiliency of our global customer base. Managed SOAR is ideal for a security team running their own SIEM, EDR or NDR technology, likely drowning in alerts and failing to deliver the value they had hoped. Managed SOAR allows you to improve security outcomes while maintaining visibility and control."

Keven Knight
COO, Talion

TALION

Automated Remediation

When the Managed SOAR service identifies a security event that requires action, we have automated remediation processes leveraging your security tools to quarantine a device or block a suspicious process, without you losing control.

Our Automated Remediation solution places the control of approving the remediation in the hands of your security owners. Once approval is given our platform (rather than an individual) interacts with your security consoles and completes the agreed remediation.

Additional add-on services include:

- SIEM Platform Management
- SIEM Content Management
- Custom playbook development
- Additional enrichment sources
- Additional remediation integrations
- Threat Coverage Modelling
- Threat Intelligence Advisory Bulletins
- Staff Augmentation: on-demand analysts and out of hour triage service

For further information and pricing of additional services please speak to your Talion representative.

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

Orchestration & Collaboration Platform