Orchestration & Collaboration Platform

TALION

Total Transparency. Complete Control.

Benefits:

- ✓ 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.

The Challenge

Organisations operating Security Information and Event Management (SIEM) technology are being overwhelmed with alerts, which need to be organised, 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 Orchestration & Collaboration Platform

We offer a cloud-based Orchestration & Collaboration Platform that ingests the alert data from your SIEM and applies our playbooks to correlate multiple alerts into single security cases. We enrich the security case with contextual information from other sources directly relating to the event, thus allowing the analyst to make faster and better decisions. These sources could be applications on your network, or more generally available security sources, such as VirusTotal. This improves the quality of the information available to you in your security cases, further reduces false positives, and frees up your analysts to focus on higher priority security needs or reduce your costs. Finally, the service offers automated remediation, speeding up your ability to act against security risks. This is done through the playbooks with your approval, delivering a fully auditable set of actions.

The Orchestration & Collaboration Platform 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 in The Orchestration & Collaboration Platform.

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.

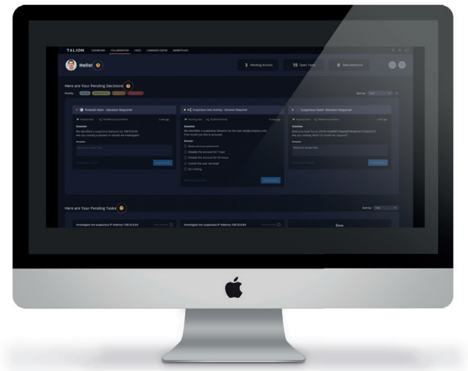

Fig 2: Collaborate directly with Level 3, Talion analysts

3. CONTROL ▸
See the whole picture

The Orchestration & Collaboration Platform 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.

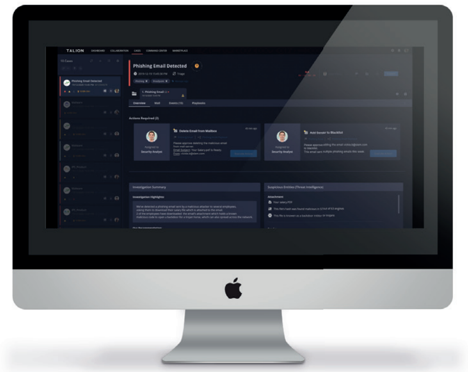

Fig 3: View your entire security case including an investigation summary, suspicious entities, alert highlights, and events.

The cloud-based Orchestration & Collaboration Platform integrates with multiple SIEM platforms and utilises Talion's advanced playbooks to correlate and prioritise security cases. The platform allows the integration of enrichment sources and security tools with the ability to perform remedial actions such as isolate, block or quarantine.

Orchestration & Collaboration Platform

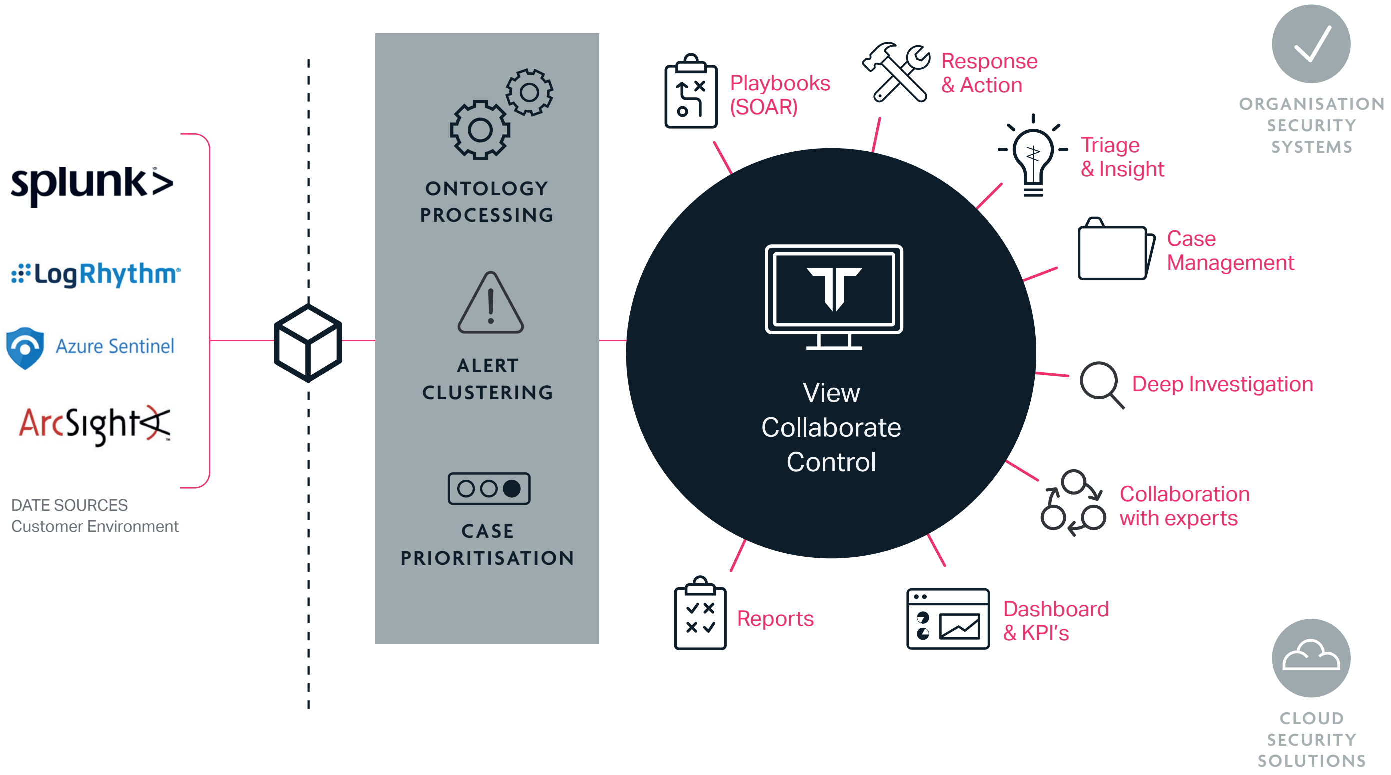

Fig 4: Orchestration & Collaboration Platform Architecture

Automated Remediation

When the Orchestration & Collaboration Platform 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:

- Content Management: SIEM content consultancy, SIEM content development, SIEM management
- Bespoke 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.

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

Keven Knight
COO, Talion

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