TALION

SIEM Content Management

25% of a cyber security analysts time is managing false positives as a result of poor content[1]

Managing a SIEM

Security Information and Event Management (SIEM) technology is designed to help organisations monitor and detect threats to their IT security.

Since their emergence SIEM solutions have struggled to keep pace with the evolving security needs of today's enterprises. The need to develop and maintain high quality detection content for SIEM platforms has never been more important. If your SIEM does not have high quality detection content that is up to date and well maintained the risk of a cyber-attack drastically increases.

SIEM Content Management

SIEM Content Developers are a rare resource who are difficult to attract and retain. We have been developing SIEM content for the last 10 years; our SIEM Content Developers deliver and maintain the detection content that powers our 24/7 security monitoring services. Our Content Developers work closely with our security analysts and threat intelligence teams, to ensure we offer a defence grade content capability. Our business relies on the capability of our Content Development team and the quality of the detection content they create. We believe that this experience and knowledge can help our customers with their detection content on their own SIEM platforms.

Our SIEM Content Management service provides our people and processes to create and manage custom detection content for the customer's SIEM platform. This custom detection content is designed to enhance the protection and monitoring of the customer's IT estate. Better content means better detection, improved outcomes and higher quality alerts passed to your security analysts.

Where customers need assistance we can also provide Staff Augmentation services for your security analyst team.

Throughout the service lifecycle, we will ensure full transparency through regular, performance driven reporting and the delivery of supporting documentation enabling the customer to understand their content coverage against cyber threats.

1 Exabeam and the Ponemon Review 2020: https://solutionsreview.com/security-information-event-management/25-of-infosec-professionals-time-wasted-on-false-positives/

SIEM Content Management

SIEM Content Management

We build content on the following SIEM Platforms:

- Devo
- Sentinel
- Splunk
- Arcsight

The main features of the Service are defined as:

- Management of new custom SIEM content creation from security use case analysis, through to release in a production environment
- Advise on existing SIEM content
- Maintenance of content to ensure threat relevance cater for new techniques
- Retirement of obsolete content, that is:
  - Inefficient
  - Replaced
  - Duplicated/Conflicting
- Management of the TTP process to review Security Use Cases, evaluate against current threats and prioritise new content accordingly
- Reporting against content planned in roadmap and delivered

Why Talion

Working with us has the following advantages:

- Being technology-agnostic we are free to make technology choices independent of our ties to product vendors. This means we can change quickly to respond to new threats and adapt to new technologies.
- Our team of SIEM Content Engineers have years of experience across leading SIEM platforms.
- Our SIEM Content Management service is designed to integrate with your SIEM; we can also provide SIEM Platform Management and Managed SOAR services.
- We are seen as a market leader in Threat Intelligence and detection content development, ensuring you maximise your SIEM investment.
- Complete service transparency: we give our customers 100% visibility into our service, enabling us to form an effective partnership to best protect their 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