TALION

SIEM Platform Management

Managing a SIEM

Security Information and Event Management (SIEM) technology emerged 20 years ago to address the need to meet regulatory requirements and to detect IT security threats.

SIEM solutions have struggled to keep pace with the evolving security landscape and the risks posed by cyber-attackers. The need to manage your SIEM platform effectively is now a key requirement. Integrating your SIEM platform management with a 24x7security capability is a necessity.

SIEM Platform Management

Any investment in a SIEM platform is a considered decision and getting the most value from the platform is key. Managing the SIEM platform has become as important as the data it is processing. Finding the right resources to maintain your SIEM platform 24 hours a day, 7 days a week is a challenge.

Our SIEM Platform Management is designed to alleviate the resource headache and security challenges of effectively operating your SIEM platform. Our expert team of SIEM Engineers manage your SIEM platform as part of a Managed Security Service, enabling you to maximise your technology investment. SIEM Platform Management provides the ongoing support, management, and maintenance of your SIEM platform.

We support:

- On-premises SIEM deployment within customer owned or co-located environments.
- Cloud based SIEM deployment in a public/private cloud under customer ownership.

The service provides management and maintenance of the SIEM Platform with the main features defined as:

- Assurance that the SIEM platform is maintained to agreed version and patch levels
- Assurance that the availability of the SIEM platform is in line with agreed service levels
- Assurance that the performance and capacity of the SIEM platform aligns with the business needs
- Day to day management of the security monitoring functionality
- Day to day configuration and optimisation of the SIEM platform
- Security information normalisation/transformation
- Provision of monitoring services to ensure supplier and customer are made aware of events that may affect the performance or availability of the SIEM platform
- Facilitation of the following ITIL processes: (Major) Incident Management, Service Request Management, Change Management, and Event Management

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

SIEM Platform Management

- Provision of an agreed Service Request Catalogue covering agreed, pre-approved tasks. This may include such activities as:
  - User management
  - Onboarding of log sources
  - Additional monitoring
  - Ad-hoc reporting/data export
  - New query requests
  - Service/solution integration based upon a pre-defined list of integrations offered by Talion
- Provision of first, second and third-line support levels relating to the delivery of the Service
- Engagement with customer support teams, vendors or other customer 3rd party suppliers in relation to the support and delivery of the SIEM platform

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 Engineers have years of experience across leading SIEM platforms.
- Our SIEM Platform Management service is designed to integrate with your SIEM; we can also provide SIEM Content 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