ADARMA

SIEM Consulting Services

A Security Information and Event Monitoring (SIEM) platform is a vital component of any organisation's cyber defence. So getting the best out of your SIEM platform is critical to monitoring and analysing security events effectively.

We provide our customers with the skills and expertise to maximise their value of SIEM through effective strategy, assessment, design, implementation, ongoing management and training.

We help our customers to identify and implement a baseline set of use cases based on initial threat modelling. This creates a ruleset sophisticated enough to allow customers to identify their most significant threats in real time.

Adarma advise on the best data to onboard, how to onboard it and how to normalise the data. This is so the SIEM platform can utilise powerful correlation searches and anomaly detection mechanisms properly. And this allows customers to deploy data analytics and visualisations to ensure they can quickly identify events of interest and trends in their data.

We have years of experience helping a broad range of clients including some of the largest and most complex enterprise companies.

What are the advantages of SIEM Consulting Services from Adarma?

We are dedicated to helping our customers prepare for attack, and provide a range of consulting services designed to achieve that aim.

Our customers benefit from:

- Unlocking the true potential of your SIEM by ensuring it is setup and performing optimally
- Faster time to value. We've been doing this for a long time and we understand the potential pitfalls to avoid
- A methodology that will help you clearly define and monitor your significant threats.
- A holistic approach to security event monitoring, covering all aspects of technology infrastructure, process development and organisational and cultural change.
- A collaborative approach. We work alongside your team, building peer relationships, transferring knowledge and helping teams prepare their cyber defence capabilities.

What challenges are addressed?

The value of Security Monitoring can only be realised by the extent to which it enables organisations to respond in an accurate and timely manner to threats.

- Creating an initial threat baseline delivers a solid foundation from which to build monitoring capabiltiies. The quality of this initial htreat modelling can have significant long term impacts on the effecitveness of the SIEM. It's vital the threat modelling is tailored to the organisation, broad in coverage and an accurate reflection of current threats.
- Many organisations have made a significant investment in SIEM technology, but have not been able to realise the full protective value of their solution. Increasing false positives and out of date use cases end up directing too much resource onto lesser or irrelevant threats.
- SIEM solutions can sometimes end up as an interesting technology project, but one that integrates poorly with business processes, leaving analysts to make difficult judgement calls about what to deal with what to ignore.

The Adarma way

We believe that all SIEM platforms need to achieve three mandatory objectives;

- They must have the broadest possible coverage in terms of the data sources they collect events from,
- They must have the breadth in terms of the common threats modelled into them.

© 2019 Adarma Ltd

- They should be built with a fundamental understanding of the unique threats each organisation face.

We think the perfect SIEM platform is a powerful tool to assist each organisation's threat management processes. Every company is different, market sector and scale, along with a host of other factors, shape the approach to security monitoring. We believe every SIEM platform should be built to adapt to each unique environment, not demand the the organisations tries to fit in with a one size fits all approach.

We build SIEM platforms to last. This is not just about the scalabilty and robustness of the platform. It's about developing the SIEM for known threats and unknown threats. We engineer in powerful correlation searches and anomaly detection techniques. We can automate response actions to events and incidents. We can even design and deploy a full Security Orchestration, Auromation and Response (SOAR) solution for you.

Powerful dashboards and visualisations are really effective to track security related KPIs. They give an analyst powerful visual indicators of anomalies.

The broader the number of data sources, the better the SIEM will become. Being able to enrich and provide better context to investigations along with integrated threat intelligence feeds and vulnerability management feeds.

The detail

We've developed a set of tried and tested steps for SIEM consulting engagements based around the most common customer needs -

SIEM Assessment and Direction

"If you don't know where you are, how can you make a plan to get where you need to go?"

During the Assessment and Direction phase, we undertake a thorough review of current status, including existing SIEM capabilities and their effectiveness, met and unmet use cases, utilised and unutilised data sources and SIEM security and operational procedures.

This enables us to produce a gap analysis and provide the best advice to help the customer move their security monitoring capabilities in the direction they want to go.

SIEM Architecture and Design

"A goal without a plan is just a wish"

We provide consultancy services to build out the necessary plans, designs and procedures which will be the map and guide to successfully implementing a SIEM capability.

Using a proven methodology based on our toolkit, we help our customers build a plan containing;

- High Level Designs intended to give a complete view of the whole solution and the primary functions of core components.
- Low Level Designs providing detailed plans for all aspects of the solution.
- Process Frameworks outlining the core functions that make up the capability
- RACI documentation assigning critical roles and responsonbilities in support of the capability

SIEM Implemenation and Enhancement

During this phase of any program of work, we are focused on turning plans into reality. We work collabortatively with our customers through the various technology, process and human elements needed to achieve the specified goals.

We provide services to build or enhance the SIEM platform, implement use cases, develop reporting and analytics views, test the platform and create build documentation.

We help our customers develop Service Operating Procedures ensuring the SIEM platform will not only work effectively on day one, but continue to operate successfully for the long term as a result of effective maintenance procedures.

We ensure a smooth and effective handover of the technology and procedures to BAU operations.

© 2019 Adarma Ltd

We also deliver services in support of the most common and recurring SIEM operational tasks -

Data Source Onboarding

As IT Infrastructures evolve, the potential data sources for events change with them. Our Data Source Onboarding Consultancy helps customers to streamline the process of integrating new data sources into their SIEM plaform, and reduces the risks of gaps in monitoring coverage.

Use Case Development and Implementation

The threat landscape is dynamic. SIEM platforms and Security Monitoring capabilities need to be equally dynamic if they are to remain effective. Use Case Development and Implemenation Consulting help customers identify and implement new use cases as threats evolve.

Support and Management

A reliable and robust SIEM platform is critical to effective security incident management. Gaps in support and management capabilities lead to inefficiencies and ultimately increase the risk associated with security incidents.

We therefore provide services to support, manage and maintain a SIEM infrastructure within a cloud or customer data centre environment.

Health Check

Our SIEM Health Check is useful either as a recurring engagement to ensure the SIEM platform is functioning as intended, or as an ad hoc exercise to address a SIEM platform which may not be performing as required.

We follow a structured methodology and provide a report which covers all of our findings and recommends any corrective actions we believe would be beneficial.

Training

Trained and certified staff are more confident and better able to successfully perform their job roles. We believe this is a critical component of security monitoring and therefore provide training for all aspects of SIEM platform configuration, operation and maintenance.

Why Adarma?

We are Adarma, one of the largest independent security services companies in the UK. As a business formed and run by veteran senior security leaders, we know security and how to deliver real value in the real world. This is why our clients are successful FTSE 250 organisations from all industry sectors.

See us as your true partner in security. We have the experience, proven track record and industry recognition, to provide best-of-breed services for all our clients. Our team are specialists in Threat Management including SOC design, build & operation. And we always tailor our cybersecurity services to your needs.

Contact us to discuss your SIEM requirements enquiries@adarma.com

www.adarma.com