Datasheet

ADARMA

SOAR Consulting Services

Security Orchestration, Automation and Response (SOAR) aims to improve the efficiency, effectiveness and speed of response of a range of security tools through integrations between them and more coordinated use of the data they collect.

According to Gartner, "By 2021, 70% of enterprise organisations with a dedicated SOC will include SOAR capabilities, up from less than 5% in 2018 and only 1% in 2017." With its ability to address some of the major challenges that security teams face today – alert overload, disparate tools, manual processes and the cybersecurity skills shortage – SOAR is undeniably a solution that enterprise security teams should be considering to assist in responding to cyber-threats across any environment.

But, SOAR is not simply an opportunity to save time and cost by automating existing processes. SOAR should be considered a transformational technology that will alter the way security services are delivered. Orchestration and automation are well proven within the wider IT industry and a good SOAR product, implemented well, will deliver significant benefits to a security function and the wider business.

Challenges that lead to a SOAR requirement

There are a number of challenges that a well-planned, modular approach to SOAR deployment can address including:

- Increased workloads together with constrained budgets and the ongoing cyber skills shortage force organisations to do more with less.
- Valuable analyst time is consumed by routine tasks and investigations causing analyst fatigue
- Security incidents are becoming more frequent and costly. Organisations need to find new ways to reduce the mean time to detection and the mean time to resolution.
- High staff turnover, typical in SOC environments leading to loss of tribal knowledge and personnel challenges.
- Security operations are increasing in complexity making it difficult to measure and manage effectively.
- Customer's need to ensure consistent responses to incidents to help build confidence in cyber defence teams and to assist with audit and compliance requirements.

Deploying orchestration and automation can very quickly become complicated and costly unless managed well.. Successful deployments typically come from sound planning and design, and incremental implementation that proves change or, where necessary, fails fast.

SOAR Consultancy from Adarma

SOAR requires a broad range of skills, from the inherent technical complexity associated with API's across a broad range of security tools to the challenge of building the right SOAR strategy and roadmap of capabilities. Our team of specialists help with all aspects.

Our SOAR consultancy services include:

- Assessment and Direction.
- Architect and Design.
- Build.
- Configure & Update.
- Health Check.
- Training.

These services are intended to assist our customers at any stage of their SOAR project. We provide:

- Assistance in developing a strategic approach to SOAR, understanding how your existing platforms can enable SOAR and defining the most valuable use cases within your organisation.
- Resources to customers who do not have the skills, capacity or capability to design a SOAR framework for your organisation using either your existing, or new tools.

- Assistance in increasing the scope of your SOAR framework where you have outstanding use cases which have not been implemented.
- Integration assistance with existing systems that would enhance the overall SOAR solution.
- Improving the performance of existing SOAR capabilities and solving common problems which result in inconsistent results and failures.
- Guidance on system performance improvements where SOAR integrations create excessive load.
- Resolution of issues where SOAR integrations are no longer productive or fit for purpose.

The Adarma way

We work with our customers to develop a strategic plan for SOAR, helping you to both define and realise your objectives.

We help build out a foundation of tools and infrastructure to support a broad range of future SOAR use cases.

We also help our customers prioritise use cases and develop a roadmap of future orchestration, automation and response capabilities based on your threats and operational challenges.

We provide the expertise to allow you to integrate a broad range of security technologies to enable your SOAR strategy.

We work alongside our customer's team, building peer relationships, transferring knowledge and helping you prepare for incoming attacks.

Why Adarma?

SOAR is a world of new possibilities for many organisations. The opportunity to configure security technologies to work together creates the potential to transform many aspects of security operations, and of course, the potential to expose new risks.

At Adarma, we help our customers to implement and maintain systems and processes that reduce residual risk to be within your defined appetite. Our SOAR consultants' guiding principle is to help our customers people achieve more thorugh the use of technology. We can increase job satisfaction, improve response and remediation times and ensure consistency through SOAR.

We work with the most widely deployed SOAR platforms, and have built a knowledge library of integration mechanisms and workflows.

Our extensive SOC experience equips us with the knowledge to address the day to day challenges experienced in a SOC environment, and how SOAR can help automate some of the most labour-intensive tasks and deliver powerful new capabilities.

Adarma are uniquely positioned to help customers ensure their SOAR program enhances their SOC and Risk, Compliance and Security Management programs.

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 SOAR requirements enquiries@adarma.com

www.adarma.com