ADARMA

SOC Consulting

Building a SOC capability requires an organisation to develop an effective set of SOC processes, build a technology platform that can handle all of the incoming data, and assemble a team of people with all of the necessary experience.

Building a new or significantly transformed SOC is not something businesses do very often. Given the infrequent nature of the activity, the complexity of the task, and the impact associated with getting it wrong, the support of an experienced specialist in all aspects of Security Operations can bring many benefits.

At Adarma, we have built SOC capabilities for a range of clients with differing needs. We have successfully built SOC capabilities from the ground up, transformed existing SOC capabilities and engaged on a short-term basis to help customers with specific needs.

We believe any organization looking to build or improve their SOC maturity will benefit significantly from our expertise.

What are the advantages of SOC Consulting from Adarma?

Working with Adarma means customers are able to tap into our SOC toolkit. Built from years of experience and continually being developed with contributions from our most experienced managing consultants, the toolkit codifies our best practices. The SOC toolkit contains more than a hundred tried and tested methodologies for various aspects of SOC development, meaning we deliver all of our services within a consistent and proven framework.

At Adarma we are a true SOC specialist. We have experience of building SOCs, delivering significant improvement programs, providing operation management, and delivering a fully or co-managed SOC from customer or Adarma premises.

We have helped customers build SOC and security monitoring capabilities in industries from retail to banking and have experience in some of the highest threat environments.

We have developed a modular approach which allows customers to engage with us to solve a specific problem, or allow us to guide them through a comprehensive SOC program;

- Assessment and Direction – to understand where the customer is today, and what they aim to achieve.
- Strategy – to help customers develop a strategic plan to achieve their aims.
- Architecture and Design – to help customers architect the tools and design the processes to support their strategic plan along with the people considerations.
- Implementation and enhancement – to implement the technologies and processes required to build an effective SOC.
- Operate and Manage – to develop an operating model and ongoing support and management capability.

What challenges are addressed?

When it comes to cyber security monitoring, and the effectiveness of the SOC, the stakes are high. The consequences of failing to provide effective threat detection can vary from short term operational impacts to long term financial and legal implications. Ensuring the SOC has effective tools, processes and people and are able to address the full range of dynamic threats is vital to ensuring the cyber resilience of any business.

Many organisations simply can't retain the specialist skills and experience necessary to build or transform a SOC . Those organisations that do retain cyber security skills and experience often find these resources are consumed with the daily operational challenges of defending their organisations. Refocusing these resources on transformation projects may present a risk to their organisations critical defence capabilities.

Whilst every organisation is a cyber target some are higher profile targets than others due to the neture of their business. This threat profile is not static and can change rapidly in response to geo-political, economic or other factors.

Adarma partner with customers to solve these challenges by applying our proven toolkits and methodologies with experienced consultants.

The Adarma way

We are passionate about taking a methodological approach to our SOC Consulting engagements. This means our consultants work in a consistent and proven manner on every project. When working at scale, this allows us to use larger teams of more specialist resources for each task. Each member of the team is able to bring their specific expertise to bear whilst working within a structured framework. The practical manifestation of this is the SOC toolkit. We expand and improve our methodologies as various aspects of the SOC discipline evolve, and will continue to do so, helping all of our customers stay ahead of the game.

We believe it's vital to work within the culture of the organisations we help and aim to be an extension of the customer's team.

The detail

We guide our customers through a number of different activities based on their needs.

Every SOC is a composite of People, Process and Technology. Some projects will inevitably focus in on one of these areas, whilst others will cut across all of them.

People – An effective SOC needs well-trained people, with clearly defined roles and responsibilities. Retention of staff is key and this needs clear personal development paths and continual learning and training.

Processes – A robust process framework is a critical component of any SOC. Consistency of action is crucial to effective response, and during times of high stress, processes provide a set of guard rails to guide the whole team through the most complex and challenging cyber incidents.

Technology – Technology platforms, like SIEM, SOAR and Workflow tools are critical components of any SOC. Understanding the strengths and weaknesses of each tool and developing a clear vision of tool development and integration is essential for cost effective operational efficiency and stability.

ECS SOC Consultancy engagements include the following types of engagements:

- Assessment and Direction - A thorough review of current capabilities allows organisations to identify their current strengths and areas for improvement.

  We produce a Gap Analysis for our customers to help them understand where their biggest opportunities are, and where it's likely they are currently carrying the biggest risks.

- Strategy - Our strategy engagements help customers to build a long-term approach to their SOC. We deliver an agreed roadmap that provides the ability to cleary plan future enhancements.
- Architecture and Design - We help our customers develop and agreed an overall service architecture and from these create High and Low Level Designs which de-risk the actual implementation and leverage our best practices gained through years of experience.
- Implementation and Enhancement - We provide technical subject matter experts to execute the project, and ultimately produce Test plans, Build Documentation, Handover documentation, Service Operating Procedures and Maintenance Procedures.
- SOC Toolkit - Guiding us on every step of this journey with our customers is our SOC toolkit. Containing hundreds of proprietary artefacts covering all aspects of SOC planning, design, implementation and operation, it brings structure and consistency to our projects.

  The toolkit contains everything from questionnaires allowing us to assess current capabilities, to implementation templates for specific technology solutions.

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 SOC and Threat Management requirements enquiries@adarma.com

www.adarma.com