ADARMA

SOC Management & Resourcing

The ability to detect and respond to cyber-attacks, data breaches and other security related incidents is a critical part of building the safe operating environment every business needs to succeed. However, few organisations are either equipped or skilled in the field of cyber security and cyber incident response to offer their organisation an adequate and acceptable level of defence.

Our next generation SOC Management and Resourcing services are flexibly designed for organisations of all sizes with a wide range of SOC delivery models available. Adarma firmly believe that cyber security provision demands an element of customisation and therefore our services are tailored accordingly to each individual customers requirements.

Our team of highly skilled cyber security experts not only help our customers improve security maturity but also allow the redistribution of precious existing cyber resources to be developed and utilised in advanced cyber techniques such as threat modelling and or threat hunting. Adarma offer a variety of SOC delivery models, each underpinned by our own internally developed and matured SOC Delivery framework.

At Adarma, we run SOC capabilities for clients across finance, retail and many other industries - analysing, monitoring and responding to threats for some of the world's largest companies.

Why not focus on your core business goals, and rely on us to do what we do best, help you be completely prepared for all cyber incidents?

What are the advantages of SOC Management from Adarma?

SOC capability, from the customers own operating locations, staffed and run by our experts embedded within the customer's team. This provides customers with the following benefits;

We allow our customers to step away from the day to day operational challenges of running a SOC, and gain the assurance that those challenges are being dealt with by a specialist SOC provider with considerable pedigree, scale and experience.

We build a close and meaningful operating partnership with all of our customers. We believe a collaborative and transparent approach to the way security monitoring is delivered forms part of the organisation's broader security strategy and ensures the services we deliver meet every customer's unique needs.

We deliver consistent, high quality, context aware response processes ensuring threats are identified and addressed in a timely manner. The insight gained from each incident analysis is replayed into operating procedures and system configurations to ensure the SOC capability continuously improves and evolves with every new incident. Our ambition and goal is to continuously improve our clients cyber maturity with our ultimate goal being to reduce both Mean-Time to Detection (MTTD) and Mean-Time to Respond (MTTR).

We provide a security monitoring capability which helps organisations achieve compliance with a variety of security standards like ISO27001, Cyber Essentials+ and PCI-DSS, all of which require effective monitoring and incident response procedures.

What challenges are addressed?

Organisations can face many challenges building and maintaining an effective SOC capability. Some of the most common ones we see are;

Under performance of an in-house SOC due to SOC management lacking in specialism, scale or experience.

Ineffectiveness of a current SOC outsourcing or MSS partner due to overly generic 'Standard' service and monitoring capabilities which address the simplistic low hanging fruit, but fail to address complex and targeted threats.

Organisations often struggle with the recruitment and retention of suitably qualified people to run and staff a SOC function, with the churn resulting in gaps in delivery and increasing recruitment overheads.

Organisations generally want a SOC function that runs in accordance with industry best practice and

is staffed by industry experts with the broadest possible perspective on threat and risk, but struggle as their own teams have a single organization experience which creates cyber blind spots relative to the wider picture.

Perhaps worst of all, some organisations have suffered a repeating pattern of failures in monitoring, detection and response capabilities, resulting in security and data breaches which have impacted their Confidentiality, Integrity and Availability.

The Adarma way

For most of us at Adarma, Security Operations Centres are like a second home.

Whether it's our own SOC, or SOCs we operate on behalf our our customers, the same core values drive everything we do.

We don't see ourselves as just a service provider, we are an extension of our customers in-house team. We can only succeed together, so our service is designed to understand and align with our customers' processes and objectives.

'Out of the Box' provides limited value. Everything we do is customised and tailored to individual client requirements. Where some service providers focus on a standardised baseline, we instead focus on ensuring context is king and that deployed rules provide genuine and immediate value and insight.

We believe a breadth of experiences prepares our team in the best way possible for every eventuality. Our SOC teams are both extensively trained and experienced in a range of SOC and security operating environments.

We believe SOC resourcing needs to be flexible. Attacker behavior can be unpredictable and inconsistent, SOC resourcing should be capable of flexing to meet those needs.

We don't exist to just help tick the 'monitoring' box for the purpose of achieving compliance; if that's all you want to achieve, we are not the SOC service provider for you. We aim to be of real value, and work with customers who want to be ready when incidents happen.

The detail

A SOC is an ecosystem that consists of people, process and technology comprising of a group of people with different skills and experiences, supported by a set of processes and technology infrastructure.

We are uniquely positioned to provide people and services at all levels, with the relevant technology skills and process experience to fit comfortably into any SOC environment.

Our modular approach means we are able to provide everything from a complete SOC service to providing specific individuals with particular skill sets to augment an existing SOC team.

Common across all approaches is a set of core beliefs that security matters, and that professionalism, diligence and accuracy will lead to reduced risk.

Over the years, our customers have come to us to help them deliver the SOC function within their organisation. No two requests are the same, so our response is always tailored to client need.

We've helped our customers with everything from a simple need to provide additional analyst cover during periods of increased workload all the way to the implementation and ongoing management and delivery of a new SOC environment for global financial institutuons.

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

- 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 processes to support their strategic plan

- Implementation and Deployment – to implement the technologies and procedures required to build an effective SOC

There are a number of interconnected functions within a SOC environment, which combine harmoniously to deliver a complete SOC function. We provide our customers with advanced capabilities in the following areas;

- **SOC Management.** No SOC performs well without an experienced management function with access to the relevant data and analytics to lead the SOC team.
- **Monitoring Capability.** A team of analysts focussed on reviewing incoming events and threat intelligence.
- **Incident Response.** A dedicated team of incident responders able to investigate, mitigate and remediate as demanded by each specific incident.
- **Threat Hunting Capability.** Creating time to go and proactively look for the threats designed to evade monitoring platforms and gives defenders another way to close the gaps attackers seek to exploit.
- **SOC Technology Platform Design & Implementation.** The capability to successfully plan and deploy SIEM, SOAR and Workflow platforms that form the basis of SOC infrastructure
- **SOC Technology Platform Maintenance and Management.** A team to ensure SIEM, SOAR and other technology platforms continue to function properly.
- **SOC Process Definition.** The effectiveness and efficiency of a SOC function is heavily influenced by the processes it follows. We help customers develop processes
- **Vulnerability Management.** A function to detect, track, prioritise and respond to vulnerabilities within the organisation.

Every customer is different, not every organization will need all of the capabilities listed above, every SOC function is designed to meet the target organisation's specific needs and integrate with existing operations and teams.

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 350 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 Management & Resourcing requirements enquiries@adarma.com

www.adarma.com