Datasheet

Managed Soc Service

For most businesses, monitoring and responding to cyber-attacks, data breaches and other security threats and incidents is a legal requirement as well as being crucial to business protection and reducing risk.

But developing and running an in-house Security Operations Centre (SOC) to protect your business from security threats can be a challenging and costly undertaking.

We provide a fully managed Security Operations Centre (SOC) capability to help our customers get on with the job of running their businesses, without the overheads associated with building and maintaining their own SOCs.

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.

Delivered out of our secure ISO27001 accredited facilities, our SOC-as-a-service offering provides quick and pain free access to all of the necessary tools, skills and processes to allow our customers to rest easy knowing that a team of trained experts is keeping them safe.

What are the advantages of SOC as a service from Adarma?

Our customers benefit from:

- Complete visibility of threats across their entire monitored domain, highlighted from the background noise of all of their event data. Every event is handled, nothing is ignored
- A day one configuration balancing our industry expertise with a flexible approach focusing on clients key risks.
- Consistent, high quality, context aware and iterative response processes ensuring threats are identified and addressed in a timely manner.
- A flexible service using what we call our "capacity" model where Monitoring & Detection is included with Incident Support, New custom Use Case development and Threat Hunting.
- Compliance with security standards like ISO27001, Cyber Essentials and PCI-DSS.

What challenges are addressed?

- Our customers avoid the lead time and cost barriers associated with setting up a set of SOC tools and processes.
- They do not need to develop their own Security Operations processes from scratch. They have access to a whole library of tried and tested processes as well as the skills and resources required to build additional use cases on their behalf.
- They don't face the challenge of recruiting and retaining cyber security experts to staff their own SOC 24x7.
- Our customers can rest assured that the Adarma SOC capability will scale with their infrastructure and resources as their business changes.

The Adarma Way

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

We believe it's impossible to do what we do successfully without being aware of the context in which security events are happening. Our team seeks to understand the customer environment to improve the quality of response.

We don't see ourselves as just a service provider, we are an extension of our customers. We can only succeed together, so our service is designed to understand and align with our customers' processes and objectives. Our service is not designed with a "one size fits all" mindset. What we do and how we do it is tailored for each customer.

'Out of the Box' provides limited value. Everything we do is customised and tailored to individual client requirements. Where some service providers focus on Out of the Box volumes, we

instead focus on ensuring context is king and that deployed rules provide genuine value and insight

Underpinning our strong and successful relationships with our customers is our commitment to transparency. Everything we do and every decision we take on a customer's behalf is shared with them.

We don't exist to just help tick the 'monitoring' box for the purpose of achieving compliance. We aim to be of real value, and work with customers who want to be ready when attacks happen.

The detail

Our service platform is a scalable SIEM and Workflow toolset that embeds a set of mature incident handling processes to ensure that every single event is handled in a consistent and predictable manner. This is combined with a team of security experts who provide around the clock monitoring and incident handling.

We stand up a dedicated service platform for every customer to ensure proper separation of data and base our service model on an event volume to resource ratio. We scale up accordingly to ensure the quality of what we do for our customers is not impacted by volume.

Our service is constructed around the following core service components -

- Accelerated Onboarding & Use Case Workshop - Our team works with the customer to bring them quickly into the service and establish a baseline set of use cases.
- Setup Event Acquisition – We work with the customer to establish the flow of events from the customer infrastructure into the event handling platform.
- Security monitoring – We monitor and respond to incoming events 24x7.
- The service is cloud based. For our customers this means High Availability Business Continuity options and Service SLAs guaranteed. Along with own dedicated cloud instance, UK or EU data centres and ISO27001 Compliance. Our service is underpinned by Splunk Cloud hosted in AWS.
- Threat Intelligence Framework – everything we do is underpinned by our industry leading threat intelligence framework.
- Proactive Threat Hunting – We seek to understand new threats and encode them into the use cases to improve the level of monitoring provided.
- Use Case Development – our team iteratively refines the use cases for every customer, continually developing the monitoring and response service.
- Incident support – When incidents do occur, we work closely with customer teams to ensure they are able to respond and mitigate effectively.
- Platform support – Throughout the lifetime of the contract we maintain the event management and workflow platform.
- Service Management – We provide our customers with tailored MI, and aim to provide insight into the data we receive, not just to report back on the good and bad.
- We build out a service catalogue for every customer to ensure operating procedures are clearly defined.

Customers have complete visibility of the incident handling workflow tools and the actions we are taking on their behalf.

Throughout the duration of the service, we work with the customer to refine the rules that determine how incidents are flagged to the SOC team. We also improve the incident workflows to minimise customer risk.

We are continually refining the rulesets we use in the light of new threats. Our team of analysts continually identify new threats and implement rules and configurations to address them. This is conducted both in respect of general threat, and those specific to each customer.

The ethos behind our service is to handle the events that matter, and to handle them in a way that minimises any risk to our customers.

Through additional automation capabilities, we are able to minimise the time spent on low value repetative tasks, empowering our SOC analysts to invest time in understanding the customer environment and refining the event handling rules

to ensure that time is only spent on meaningful events, thereby maximising the efficiency of our service.

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 requirements enquiries@adarma.com

www.adarma.com