Managed Security Operations Centre (SOC)

Better Security Outcomes, Delivered Together

The Challenge

Running a 24/7 SOC has become one of the most demanding and high-stakes challenges in cybersecurity. CISOs are under pressure to deliver around-the-clock threat detection, investigation and response amid rising attack volumes, growing regulatory demands, and an industry-wide shortage of cybersecurity expertise.

For many organisations, building and sustaining an in-house SOC is no longer viable. The result? Gaps in coverage, analyst burnout, and difficulty translating security activity into business value.

Does This Sound Like You?

- You're overwhelmed by threat data and alert noise, but still missing what matters.
- You don't have the in-house skills or capacity to keep pace with threat detection demands.
- Your current service feels opaque and you're left questioning the value it delivers.
- You're stuck with a reactive service, long change cycles, and limited coverage and you're unsure how well it defends against emerging threats.
- Hidden costs mean you're not getting the value you were promised.
- It's difficult to demonstrate how your team is reducing risk to the business.
- Your current provider is underdelivering, and you need a partner you can trust.

Why Act Now?

Boards expect measurable outcomes. Regulators demand accountability. Customers won't tolerate breaches. With threats evolving rapidly and compliance frameworks like DORA and the UK Cyber Security & Resilience Bill tightening, proactive threat management is no longer optional. The time to modernise your SOC is now.

Adarma's Solution

- Adarma delivers a co-managed SOC service built around your business needs, combining deep operational expertise with proven processes to help you detect, investigate, and respond to threats more effectively.
- We act as an extension of your internal team, providing UK-based analysts, engineers, and consultants who work shoulder-to-shoulder with you to elevate your security maturity.
- We are technology independent and operate across your preferred platform, whether that's Splunk, Microsoft Sentinel, or Google SecOps. Our service fits your environment, not the other way around.
- At the heart of our Managed SOC is a proactive, intelligence-led approach. While we leverage advanced automation and orchestration through our Socket platform, it's our expert threat hunters, detection engineers, and incident responders who ensure we stay ahead of emerging threats.

Our service includes:

- 24/7 Threat Monitoring, Triage & Response
- Intelligence-Led Threat Hunting & Detection Engineering
- Incident Investigation, Escalation & Collaborative Response
- Continuous Coverage Expansion, Tuning and Quality Assurance
- Weekly Technical Sessions & Monthly Strategic Reviews
- Designated Service Delivery Manager, Offering Personalised Management of Relationships, Performance, Risks and Issues

Managed SOC Service Overview

Here's a more detailed view of the objectives, tasks, and activities that lead to a comprehensive threat detection, investigation and response framework designed to quickly and effectively identify and contain threats while proactively improving your security posture.

	Build and Deploy		Detect and Respond		Manage and Optimise		
Objective	**Provide a functional and efficient platform within Adarma service**	**Ensure detection coverage against key threats**	**Detect and contain threats**	**Pro-actively find advanced threats**	**Improve security posture**	**Ensure successful service and provide security advice**	**Outcome** Comprehensive detection and response to quickly and effectively identify and contain threats while proactively improving your security posture.
Task	Build platform and onboard to service	Deploy detection content	Detect and respond to threats 24/7	Hunt for threats	Expand and enhance detection coverage	Service delivery management	
Activities	• Plan project configure access • Design service & technical architecture • Configure platform and build Ingestion layer • Certify service as fully functional • Onboard key assets/data sources	• Identify key threats and TTP's • Agree and align use cases & rules • Deploy and test rules • Agree and deign playbooks and response processes • Implement automation	• Monitor, triage and prioritise alerts • Investigate threats and escalate suspected incidents • Enact agreed response actions to contain threats	• Research new threats and ingest intelligence • Manual, hypothesis-directed and intelligence-lead threat hunting • Automated hourly IoC threat hunts	• Continuously tune detection content • Identify detection gaps • Prioritise and onboard additional data sources • Deploy further detection content based on gaps and intelligence • Continously review and improve playbooks & response processes	• High-touch service with regular touchpoints • Multiple named individuals aligned to ensure understanding and familiarity • Quarterly strategic threat reporting • Monthly threat briefings. Monthly service reviews • Quarterly business reviews	
			Incident Response - Enact to co-ordinate, response contain and help remediate if required and in scope				

Powered by Socket™

You retain full strategic oversight and control—we bring the operational firepower, platform expertise, and proactive mindset needed to reduce your risk and build long-term resilience.

BENEFITS:

Open, Extensible Technology
Bring your own SIEM, EDR, SOAR and ticketing tools. Our modular connectors and open APIs avoid costly rip-and-replace projects. You can also port workloads to our security operations platform, Socket, reducing costs.

Faster Detection & Response
Significant reduction in the mean time to detect and respond (MTTD/MTTR).

Wide Detection Coverage
Coverage spans cloud, on-prem, SaaS, OT and endpoint using >1,000 behavioural and ML-driven rules.

Transparent Partnership
Access to live case notes, coverage visualisation, and real-time SOC metrics via the Socket Portal.

Portability & Control
Your detection content is yours to keep, and we support migrations across platforms.

Operational Maturity
Embedded detection engineers, regular planning sessions and threat-informed improvements.

Success Stories

Leading Airline
We helped a global airline mature their security operations through a co-managed SOC model—increasing threat coverage and accelerating response.

Read the case study

Top 5 UK Retail Bank
Our managed SOC service enabled real-time threat visibility and measurable improvements in security posture.

Read the case study

Luxury Goods Retailer
Delivered an award-winning SOC service that drastically reduced incident impact and improved executive reporting.

Read the case study

Why Customers Choose Adarma

UK-Based Expertise
Delivered on-shore, embedded with your teams, aligned to UK and EU regulations.

Platform Independent
We work across Splunk, Microsoft Sentinel, Google SecOps, and more.

Outcome-Focused
Every engagement includes jointly defined KPIs (MTTD, MTTR, and business risk reduction), and we report on them weekly.

Trusted by UK Enterprise
Delivering continuous security improvement for UK's most valuable and complex businesses.

Meet the team

Chris Chalmers

Head of Security Operations

With over a decade of experience in SOC architecture, implementation, and optimisation, Chris leads the day-to-day delivery of Adarma's Managed SOC Service.

Connect with Chris on LinkedIn

> **"Adarma's agility and high-context approach to detection and response set us apart from the rest of the market."**

Who We Are

Adarma is a trusted partner in security consulting and co-managed security operations. We work as an extension of your team to help simplify operations, build resilience, and deliver measurable outcomes.

We specialise in 24/7 threat detection, investigation and response, security consulting, and engineering support for large, complex organisations in high-risk sectors. Our platform, Socket, enhances automation, insight, and orchestration – empowering teams to act faster and more decisively.

Technology-independent and customer-led, we integrate with platforms like Microsoft, Splunk, CrowdStrike, and Google SecOps to maximise the return on your security investments. Together, we build stronger business resilience and deliver measurable security outcomes that matter.

Ready to Accelerate Your Security Outcomes?

Book a strategy session with one of our solution consultants and receive a complimentary Threat Landscape Report tailored to your industry.

Book a consultation