Security Engineering

Optimised Security Operations, Engineered for You

The Challenge

Security operations are only as strong as the foundations they're built on. But for many organisations, those foundations – platforms, detections, integrations – are fragmented, inconsistent, and underperforming.

With environments evolving rapidly and skilled engineering resources scarce, many teams struggle to:

- Keep detection content relevant to their threat landscape
- Balance automation with analyst insight
- Optimise SIEM, SOAR, and EDR tools to deliver consistent value
- Efficiently collect, transform and route security data to the right tools
- Demonstrate impact and value to stakeholders

Why Act Now?

Security engineering inefficiencies compound over time—leading to alert fatigue, missed threats, and rising costs. Meanwhile, regulators are increasing enforcement: in 2025, a major UK NHS provider was fined £3 million for insufficient controls following a ransomware attack.

A mature, well-engineered SOC can mean the difference between early containment and costly disruption.

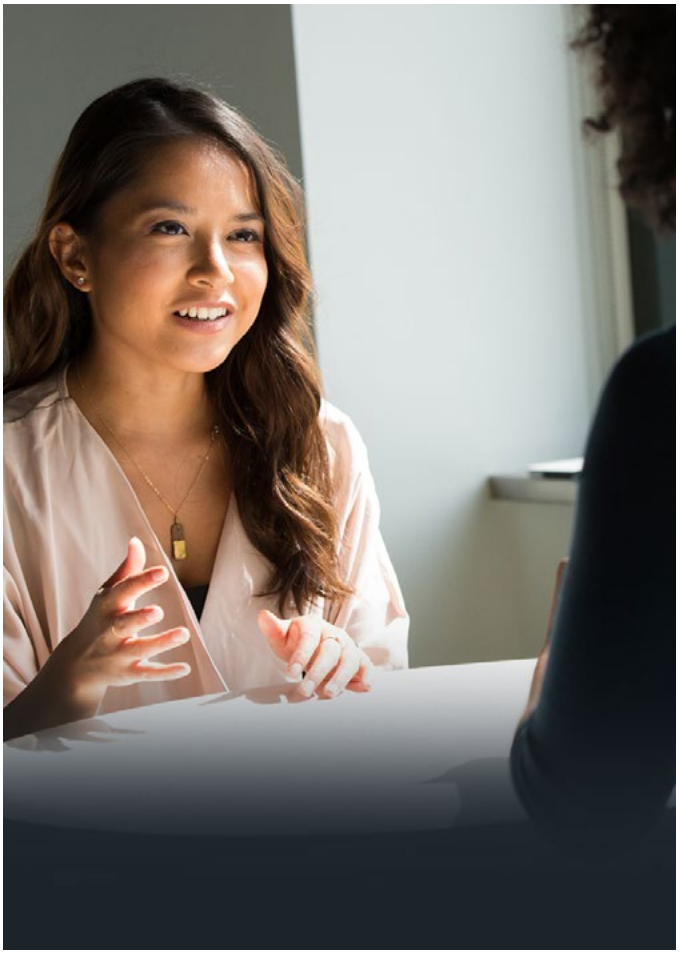
Adarma's Solution

Adarma's Security Engineering services focus on two core areas: **Security Platform Engineering and Detection Engineering.**

We help you design, deploy, and optimise your SOC technology stack and detection content – ensuring everything works together to reduce risk and improve efficiency.

- **SIEM, SOAR, and EDR platform installation and optimisation**
- **Detection content development, tuning, and QA**
- **Security data pipeline engineering and log source integration and deployment**
- **Custom parser, playbook, and automation development**
- **Assessment and enhancement of detection coverage**

All engagements are grounded in best practice frameworks like MITRE ATT&CK, and supported by certifications.



BENEFITS:

Consolidation
Modern security tooling offers the ability to replace multiple point products with a single, unified platform—streamlining operations, reducing licensing costs, and improving coverage.

Faster Threat Detection & Response
Through fine-tuned detection logic, engineered SOAR playbooks, and efficient data pipelines, our engineering accelerates threat identification and incident resolution—reducing mean time to detect (MTTD) and mean time to respond (MTTR).

Operational Efficiency
Our services help analysts focus on high-impact activities by reducing alert fatigue and manual overhead. We optimise dashboards, automate triage, and ensure your SOC runs lean and effectively.

Improved Security Maturity
Our engineers work to build long-term capability within your SOC, from content engineering through to architectural design—helping reduce dependence on manual processes and build resilience against evolving threats.

Risk Reduction
With broader visibility and improved detection coverage, we help you spot and contain threats earlier, reducing dwell time and limiting potential impact to the business.

Strategic Value
Security engineering helps bridge the gap between technical implementation and business outcomes. We provide data-backed insights to support board-level reporting and investment decisions.

Success Stories

Global Insurance Leader

Optimised detection content and SIEM platform performance across 300+ applications.

Read the case study

Leading UK Bank

Enhanced Splunk performance and coverage through platform remediation and advanced engineering support.

Read the case study

Top Global Cosmetics Retailer

Delivered post-divestment SOC transformation, including EDR tuning, SOAR integration, and custom detection engineering.

Read the case study

Global Technology Provider

Successful migration to Splunk Cloud and improved detection performance and reduced alert fatigue across SOC teams.

Read the case study

Why Customers Choose Adarma

Engineering Depth

We have made significant investments in technical training, making us one of the most highly certified providers of leading security technologies in the UK.

UK-Based Delivery

All our services are delivered on-shore, ensuring alignment with local compliance requirements and providing easy access to our expert teams.

Technology Independent

We offer truly independent advice, free from vendor bias, so your solution is tailored to your needs—not ours.

Proven Track Record

We are a trusted partner to large, complex organisations, including many of the FTSE 350 across regulated sectors, delivering consistent results in complicated environments.

Meet the team

Laks Ganesan

Security Engineering Specialist

Laks brings deep experience in SIEM optimisation, transformation projects, and managed detection response. He specialises in aligning engineering effort to business risk.

> **“Our role is to make sure your security investments are delivering their full potential—from detection content to platform performance.”**

Connect with Laks on LinkedIn

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 Optimise Your Security Operations?

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

Book a consultation