

# Enhanced Managed Security Operations Centre (SOC) Powered by Splunk Enterprise Security (ES)

**Stronger Detection. Smarter Response. Seamless Collaboration.**

## Modernise Your SOC with Mission Control-Enabled Automation and Insight

Adarma's Enhanced Managed SOC (MSOC) is built to maximise the value of your investment in Splunk Enterprise Security. Now optimised for ES8 our service enables deeper integration with Mission Control to streamline investigations, improve analyst efficiency, and accelerate threat response.

Whether you're looking to upgrade from ES 7.x or migrate from an underperforming SIEM, Adarma's enhanced service offers a clear path to stronger outcomes and greater control.

## Does This Sound Like You?

- You want to upgrade to Splunk ES 8.x but don't have the capacity or confidence to do it alone.
- Your team is overwhelmed by alerts and lacks visibility into what really matters.
- Your current SIEM feels inflexible and disconnected from your response workflows.
- You're unsure how well your current setup protects you against emerging threats.
- You need a trusted partner to help you modernise without disruption.



## Why Upgrade to Adarma's Enhanced Managed SOC?

### For Current Splunk ES 7.x Users:

- Seamless upgrade path from ES 7.x to ES 8.x
- Access to new automation, correlation, and enrichment features via Mission Control
- Continued integration with Adarma's Socket platform and service tooling
- Future-ready support for Splunk SOAR on-prem integrations
- Ability to deploy Splunk's Enterprise Security Content Updates (ESCU) via Adarma Socket Automate, with further ability to tune and optimise content to specific customer requirements

### For Those Switching Providers:

- Immediate uplift in visibility, collaboration, and response speed
- Transparent, co-managed operations with bi-directional case management
- UK-based analysts, engineers, and delivery managers who embed into your workflows
- Proven migration playbooks to accelerate onboarding and reduce risk

# Adarma's Solution

**Our Enhanced Managed SOC service is purpose-built to help organisations harness the full capabilities of Splunk ES8 and Mission Control.**

We provide end-to-end integration, continuous tuning, and bi-directional case management that seamlessly links your environment with our UK-based SOC.

We act as an extension of your internal team – helping you detect, investigate, and respond to threats more effectively while accelerating your platform maturity.



## What's new in the Enhanced MSOC Service

- **Upgrade Path from ES 7.x**  
We provide a clear migration roadmap, helping you move from Splunk ES 7.x to 8.x without disruption.
- **Bi-Directional API Integration**  
Incidents flow seamlessly between Adarma's Socket Automate and Splunk's Analyst Queue via Findings, with full enrichment and context maintained.
- **Mission Control Enrichment**  
Leveraging the latest response templates, searches and saved views, our analysts receive actionable context, ensuring high-confidence investigations.
- **Future-Ready Architecture**  
Designed to support on-prem SOAR and later ES 8.x feature releases.

## Our Enhanced MSOC Service Includes:



24/7 Threat Monitoring,  
Triage & Response



Bi-Directional Workflow Integration  
with Splunk Mission Control



Intelligence-Led Threat Hunting  
& Detection Engineering



Weekly Technical Sessions  
& Monthly Strategic Reviews









Incident Investigation, Escalation  
& Collaborative Response



Continuous QA, Use Case Tuning  
& Content Development

You retain full strategic control, while we deliver the operational firepower, deep platform expertise, and proactive mindset needed to reduce risk and build long-term resilience.

## BENEFITS AT-A-GLANCE

Capability	Benefit
 <b>Mission Control Integration</b>	Reduced alert fatigue and faster triage
 <b>Bi-Directional API Workflows</b>	Seamless incident handling with enhanced enrichment
 <b>Real-Time Findings &amp; Enrichment</b>	More context for faster, more confident decisions
 <b>Automation &amp; Playbooks</b>	Faster containment and repeatable actions
 <b>Scalable &amp; Flexible</b>	Easily support Splunk SOAR and future ES releases
 <b>Enhanced Analyst Productivity</b>	Unified workflows for improved SOC efficiency

## Meet the team



### Lakshamanan Ganesan

Security Engineering Specialist

With over a decade of experience in SOC architecture, implementation, and optimisation, Laks heads up our technical Splunk practice and has been instrumental in developing Adarma's Enhanced Managed SOC service, Powered by Splunk.

 [Connect with Laks on LinkedIn](#)



Splunk ES8 represents a step change in how security teams can investigate and respond to threats. By integrating with Mission Control, we've built a co-managed SOC experience that's more responsive, more collaborative, and more effective. Our enhanced service helps customers reduce complexity, accelerate response times, and extract full value from their Splunk investment."

## 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 Elevate Your SOC?

Book a strategy session to discuss your ES 8.x roadmap or SIEM migration and receive a tailored Threat Landscape Report for your sector.

[Book a consultation](#)

