Security Information and Event Management (SIEM)Migration

Minimise risks and maximise rewards with Adarma's expert SIEM migration support

The Challenge

SIEMs must be nourished and maintained Initially used to aggregate security logs, SIEM focus has shifted to proactive threat hunting and automated response and containment alongside Security Orchestration, Automation and Response (SOAR) systems. SIEMs hold a significant amount of business value, but they require substantial maintenance to remain optimised. When they lack important security features or scalability, or if they become too costly, it may be necessary to replace them.

Does This Sound Like You?

- Your current SIEM architecture does not scale to handle the volume of data you need to ingest and analyse.
- You need more advanced analytics to accurately detect threats and reduce false positives.
- Your customers expect real-time situational awareness, but your existing SIEM fails to deliver it.
- Your SIEM struggles to integrate effectively with modern cloud services and IoT devices.
- You are already at full capacity and don't have the internal resources or experience to manage a migration.
- Your SIEM contract is up for renewal, and the projected costs are significantly higher than before.

Adarma's Solution

- Adarma provides experienced security consultants and engineers who specialise in the design, implementation, and optimisation of SIEM solutions. Our experts combine deep technical knowledge with business insight to guide your organisation through secure, efficient, and value-driven SIEM migrations.
- Our consultants bring a comprehensive understanding of programme delivery, risk management, and quality assurance. They work closely with your team to assess current capabilities, identify requirements, and recommend the most appropriate technologies to meet your security and operational objectives.
- We follow a structured delivery framework, built on clearly defined roles and proven methodologies that help maximise value while controlling cost, risk, and timelines. This approach ensures consistency, transparency, and alignment with your strategic goals.
- In addition to SIEM migrations, our projects can also incorporate SOAR platform transitions and case management system migrations, ensuring an integrated and modernised security operations environment.
- Every engagement is tailored to your organisation's unique requirements, with our delivery framework flexibly adapted to suit your specific context and challenges.

SIEM Migration Process Overview

The following table provides an overview of Adarma's SIEM migration process. This is based on our extensive experience in helping customers select and migrate from their legacy system to a new and improved SIEM, enhancing their security posture and cyber defence capabilities.

Step	Name	Description	Outcome
1	Organisational Requirements Gathering	Interview customer stakeholders to identify project planning inputs such as motive for project, critical success criteria timescales, data sources, infrastructure, how the SIEM will be deployed and operated and key detection and response requirements.	Statement of requirements Project brief
2	Tool Selection and Procurement	Shortlist candidate SIEM solutions and evaluate them against customer requirements, focusing on functionality, scalability, integration, customisation, compliance and reporting, product roadmap, innovation, and total cost of ownership.	SIEM platform solution candidates
3	Building Your Business Case	Evaluate key cost drivers, including whether to deploy the solution as SaaS or on-premise, and which pricing model – such as compute-based or consumption-based – best fits your needs. We help you build a project plan and determine how to effectively manage delivery risk.	Business case
4	Discovery	Assess the current SIEM platform(s) to inform the design of the target solution, define the detection content migration strategy, and shape the overall migration plan.	Solution configuration documentation High-level migration plan
5	Design	Document the precise specifications and design details for the new SIEM service.	Target SIEM solution architecture pack Baseline delivery SIEM Migration Plan
6	Build	Use the baseline plans and designs from the previous phase to complete the construction of the SIEM components and processes.	Solution infrastructure and software build SOC processes and integrations
7	Dual Feed Testing & Validation	Run both the legacy and new SIEM platforms in parallel for a period to verify that the new SIEM is properly configured and fully operational before the final cutover.	Dual feeding configuration Technical and process integrations Metrics evidencing SIEM parity
8	Content Migration	Once your new SIEM is successfully ingesting data feeds, the next step is to migrate and fine-tune the detection content.	SIEM Solution content migrated SIEM Solution parity evidenced
9	Cutover From Old to New SIEM Platform	Transition when you are confident of the build, testing, configuration, and parity of your new SIEM service.	SIEM solution switch Legacy SIEM solution archive
10	Monitor Return on Investment	Quantify the cost savings from avoided cyber intrusions, incident response efforts, and business disruption, while also tracking major operational expenses such as licensing, support, and maintenance.	Business report

BENEFITS:

Many organisations report 30–50% cost savings after replacing a legacy SIEM[1]. Cost savings arise through:

Flexible Pricing Models

Modern SIEMs offer usage-based pricing and reduce infrastructure costs, making them more cost-effective.

Lower Storage Costs

Efficient data ingestion and tiered storage can reduce storage expenses by up to 70%.

Tool Consolidation

Integrated features like SOAR, UEBA, and XDR reduce the need for multiple security tools, streamlining operations.

Simplified Compliance

Built-in compliance reporting tools can cut audit preparation time by as much as 80%.

Faster Threat Response

Automation and better analytics improve detection and resolution times – minimising downtime that can cost $9,000 per minute[2].

Success Stories

Adarma has helped organisations across a range of regulated sectors to deter and prevent attacks by minimising their attack surface. Here are some examples:

Global Insurance Leader

Adarma deployed a tailored SIEM and SOC solution to help a leading global insurer secure over 300 business-critical applic-ations. The result was improved threat visibility, faster response times, and tighter alignment with regulatory requirements.

Read the case study

Leading International Airline

We supported a major airline in maturing its security operations through a fully managed SOC service, enhancing threat detection, streamlining incident response, and reducing operational risk in a high-pressure, regulated environment.

Read the case study

Why Customers Choose Adarma

In a crowded cyber security market where quality can be difficult to assess, organisations trust Adarma to deliver their most critical projects with precision and reliability.

Unmatched Expertise

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

Technology Agnostic

We offer truly independent advice, free from vendor bias, so your solution is tailored to your needs.

UK-Based Delivery

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

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.

1 https://tei.forrester.com/go/microsoft/microsoft_sentinel/?lang=en-us

2 https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf

Meet the team

Tim Davis

Security Operations
SIEM Migration Lead

With over 30 years in cybersecurity across operational, architectural, and advisory roles, I take great pride in helping organisations optimise their security operations. If you're exploring SIEM migration or looking to enhance your current setup, I'd be happy to connect.

Connect with Tim on LinkedIn

> **Running efficient security operations is a lot like sailing—it takes experience, focus, and a sense for the changing environment."**

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, insights 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