ADARMA

Security Information & Event Management (SIEM) Assessment

DATASHEET

Your Roadmap to Increase the Performance and Value of Your SIEM

The growing array of security tools and the evolving scale of infrastructure are leading to a rapid increase in telemetry and data across your organisation. Paired with the shifting threat landscape and compliance requirements, your SIEM and associated data, detection content, and workflows may no longer deliver their promised value and/or have become prohibitively expensive.

The Adarma SIEM Assessment can help. Our experts conduct a thorough evaluation of your situation, establishing objective measures of effectiveness and value. It includes technical analysis, process evaluation, documentation review, and recommendations for alternative strategies and adjustments to maximise ROI.

The SIEM assessment starts with understanding your operational context, identifying your business-critical assets and crucially who may threaten them and how. With this context we can effectively assess critical aspects of your SIEM performance:

- Telemetry and context collection
- Telemetry and context collection
- Integration of threat intelligence sources
- Data ingestion, normalisation and storage
- Data strategy analysis of cost vs security value
- Performance, development, and tuning of detection content
- Alert triage, automation and alert enrichment
- Response automation and actions
- Escalation and incident response integration and workflows

WHY CHOOSE AN ADARMA SIEM ASSESSMENT?

- With a proven track record in establishing and managing SOCs for highly targeted organisations across various industries in the UK, we have earned the status of a trusted advisor to our FTSE 350 customers.
- Leveraging our in-depth understanding of risk, threats, and capabilities across SOC tooling, data pipelining, staff, and workflows, Adarma eliminates silos and offers comprehensive programmatic improvements to support your SIEM selection.
- Our practical assessments deliver outputs that are relevant, actionable, and focused on risk reduction and resilience. We enhance SOC performance and maximise the value of your technology investment.

Through our longstanding Elite Technology Partnerships with leading security technology vendors, you gain access to impartial advice, accurate scoping, and engineering expertise, ensuring confidence in our ability to deliver on recommendations.

- We offer a comprehensive portfolio of supporting services tailored to all aspects of your SOC, ranging from operating model design and process design to innovative data management and SOC engineering services. Whether you require a fully managed service or specific assistance, we help you achieve your desired SOC maturity.

Why Does My Organisation Need a SIEM Assessment?

With tightening budgets, rising security costs and increasingly complex threats, a SIEM assessment can help if:

- Your SIEM data costs are increasing exponentially.
- You are unsure if your SIEM complies with recent regulation changes.
- Your analysts are overwhelmed by incoming alerts and CVEs.
- You have no clear upgrade path to the latest technology.
- You need an objective measure of your SIEM's current capabilities, and its value compared to costs.
- You are encountering more security incidents and vulnerabilities.
- You need to boost productivity and efficiency without expanding your headcount or budget.

We are Adarma

We are Adarma, independent leaders in detection and response services. We specialise in designing, building, and managing cybersecurity operations that deliver a measurable reduction in business risk. We are on a mission to make cyber resilience a reality for organisations around the world. Our team of passionate cyber defenders work hand in hand with our customers to mitigate risk and maximise the value of their cybersecurity investments.

Powered by Socket, Adarma's Security Operations Platform and optimised to our customers' individual needs, we deliver an integrated set of services that improve your security posture including best in class Managed Detection and Response services.

We operate with transparency and visibility across today's hybrid-SOC environments to ensure our customers are protected as they innovate, transform, and grow their businesses. Adarma delivers the cybersecurity outcomes you need to make a remarkable difference.

KEY BENEFITS OF A SIEM ASSESSMENT:

- Evaluate the capability and performance of your SIEM to align with your mission, meet objectives, and deliver value within your allotted budget.
- Understand your performance metrics such as Mean Time to Detect (MTTD) and Mean Time to Response (MTTR), benchmarked against industry standards and peer performance.
- Get an objective evaluation of alternative approaches, including innovative data pipelining and storage options to better suit your needs.
- Clear validation of your detection content, coverage and your ability to develop new content.
- Document evidence to support your strategy development and decision-making with deliverables including a realistic step-by-step action plan and ongoing support to achieve your desired future operational state.

Engage with Adarma Assessments

To learn more about our SIEM Assessment or to discuss how we can address your specific requirements, we welcome you to connect with an Adarma Client Director or email hello@adarma.com. Visit adarma.com/cybersecurity-advisory-assessments/ for additional information.