Security Incident & Event Management

DEV/NULL

Design & Build

Smarter SIEM, Faster Insights, Stronger Defence

Cyber threats are growing in speed, scale, and sophistication, making real-time visibility essential to defending your organization. Our SIEM service centralizes your security data, detects threats as they happen, and accelerates incident response. Powered by Splunk, our service turns complex log data into actionable intelligence while leveraging data tiering to balance performance and cost. The result: optimized visibility, faster detection, and smarter use of your security data.

More detail

Our SIEM Service covers the full lifecycle of your security monitoring capability; from design to deployment and optimisation all aligned with industry best-practices:

- Architecture design and implementation tailored to your organisation's needs.
- Log collection, aggregation, and correlation setup across diverse data sources.
- Use case development and alert tuning to reduce noise and improve detection accuracy.
- Integration with incident response processes and wider security tooling.
- Identifying Automation Opportunities for Security Orchestration, Automation & Response (SOAR).
- Data tiering strategy to balance performance, retention, and cost efficiency.
- Configuration for compliance with frameworks such as ISO 27001, NIST, and PCI DSS.

We'll design, build, and fine-tune a Splunk-powered SIEM that delivers real-time visibility, scalable performance, and actionable security intelligence.

Benefits

This service is particularly beneficial for organisations who want:

- Greater visibility across security logs and events.
- Certainty about the effectiveness of current alerting and correlation rules.
- A low volume of false positives or missed security incidents.
- Better integration between monitoring tools and incident response processes.
- To optimise Splunk performance, data tiering, or architecture.
- To strengthen threat detection, investigation, and response capabilities.

What's included in the Dev/Null service?

Information analysis:

Consultation to understand your environment, logging requirements, business goals, and security priorities. Followed by an in-depth assessment of your current security posture through interview, document review, and tool review.
This phase gathers all relevant data to form a complete picture of your SIEM requirements.

Current state report:

A comprehensive analysis of the information gathered, presenting findings in an easily digestible format. This report includes maturity and capability assessment of people, process, and technology.

Architecture Design:

A detailed document detailing the implementation using industry best practices for SIEM. This includes analysis of tool configuration, processes, risk prioritisation frameworks, and response procedures.

Implementation:

A structured approach to deploying and supporting your Splunk SIEM, including architecture implementation, data onboarding, correlation searches, alerts, dashboards, and tuning use cases for optimal detection.

Maturity Roadmap:

Roadmap guidance covering capability improvements, progress tracking, and continuous refinement to keep your security posture aligned with evolving threats.

Ongoing Support:

Provide knowledge transfer and offer post-delivery support options for continuous improvement and scaling.
Ongoing support covers performance optimization, data management, and continuous enhancements to keep your SIEM aligned with evolving security needs.

Why Dev/Null?

Responsive:

We stay flexible and adapt to your priorities, whether that means shifting focus within a project or responding to an emerging threat to provide the best security for you. Our fast-turnaround, communication, and flexible engagement models keep you moving forward without delays.

Established:

Our team brings deep operational experience developed across a broad range of industries and security domains, backed by proven industry and vendor certifications, and a portfolio of real-world successes. That depth of knowledge lets us solve complex problems with confidence and speed.

Evolving:

Continuous learning is at the core of our culture: we routinely assess, refine, and re-engineer our processes, tools, and skills to stay ahead of the threat landscape. This mindset translates into more effective, efficient, and resilient solutions for you.

Enabling:

Beyond delivering services, we actively coach your staff, sharing best practices, conducting workshops, and providing hands-on training to mature your capability. The result is an empowered internal team that can sustain and expand the gains we deliver.

Sustainable:

We design security architectures and practices that endure, focusing on long-term resilience rather than quick fixes. By embedding best practices, automating controls, and aligning with your business roadmap, we foster a culture of continuous improvement.

Actionable:

Complex cybersecurity concepts are distilled into plain language, ensuring every stakeholder, from executives to engineers, understands the risks, options, and recommended actions. This clarity drives informed decisions and smooth collaboration across your organisation.

Choose Dev/Null

Choosing the right partner for your SIEM Service is crucial. At Dev/Null, we combine cutting-edge methodologies with decades of collective cybersecurity experience to deliver comprehensive assessments tailored to your organization's needs. Our team brings expertise from diverse industries and across all aspects of security operations - from detection and response to cyber threat intelligence and technical operations. We leverage our deep understanding of industry best practices, combined with hands-on operational experience, to provide actionable insights that drive real improvement in your security posture.posture.

Book a conversation with one of our consultants to explore how a SIEM Service can protect you.

info@devnullsecurity.co.uk