



Turning complexity into clarity through end-to-end observability.

Modern digital environments are complex, dynamic, and data-rich, making real-time visibility essential to maintaining performance and reliability. Our Observability Service unifies metrics, logs, and traces to deliver deep insight across your entire technology stack. Powered by Splunk, it transforms data into actionable intelligence, helping you detect issues faster, optimise performance, and enhance user experience. The result: proactive monitoring, faster resolution, and a more resilient digital ecosystem.

More detail

Our Observability Service supports the full lifecycle of your monitoring and analytics capabilities; from designing and implementing new data pipelines and dashboards to optimizing alerting, instrumentation, and correlation workflows. We focus on ensuring your observability ecosystem is efficient, actionable, and aligned with industry best practices so you can achieve reliable, repeatable insights across metrics, logs, and traces:

- Observability Readiness to baseline review of existing logging, metrics and tracing capabilities.
- Architecture design in line with best practice to establish a reliable flow of logs, metrics, and traces.
- Telemetry collection configuration assistance to standardise log formats and metric naming conventions.
- Building or configuring key dashboards for Infrastructure, Application & Service monitoring.
- Assistance in integrating Observability data to Incident Management workflows with alert routing and escalation paths.
- Optimising Telemetry to reduce noise and unnecessary logging. Ensuring retention policies are adhered to.
- Alignment with compliance frameworks such as ISO 27001, NIST, and PCI DSS.

Dev/Null will help design and configure a Splunk-based Observability foundation that improves visibility across your systems, supports more informed troubleshooting, and gradually strengthens the effectiveness of your operational monitoring.

Benefits

This service is particularly beneficial for organisations who want:

- Better visibility into system performance, application behaviour, or infrastructure health.
- Certainty about the reliability, accuracy, or usefulness of existing dashboards, alerts, or monitoring configurations.
- Minimal manual effort in troubleshooting incidents or investigating performance issues.
- Meaningful integration between telemetry sources, monitoring tools, and operational workflows.
- To optimize existing observability practices for clarity, efficiency, and actionable insights.
- To improve detection, accelerate problem resolution, and gain more consistent operational awareness.

What's included in the Dev/Null service?



Information analysis:

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 Automation 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.



Identification & Definition:

Collaboratively define priority observability use cases to guide a practical implementation plan. Define key metrics, logging standards, and tracing practices.



Develop and Design:

Develop high-level architecture and design documentation for the telemetry pipeline for review and alignment.
Design dashboards and alerts that provide meaningful insights for teams.



Implementation & Configuration:

Set up or refine telemetry pipelines, integrate data sources, configure dashboards and alerts, and ensure data flows reliably to monitoring platforms.
Build and tune initial dashboards, alerts, and basic telemetry workflows to support meaningful visibility and reduce noise



Maturity Roadmap:

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



Knowledge Transfer:

Provide knowledge transfer and offer optional post-delivery support to help teams adopt the tools effectively and continue maturing observability over time.



Ongoing Support:

Ongoing support covers playbook optimization, workflow refinement, and continuous enhancements to keep your SOAR automation effective, efficient, and aligned with evolving security operations.

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 Observability services is crucial. At Dev/Null, we combine practical methodologies with deep operational experience to help organizations gain meaningful visibility into their systems and applications. Our team brings expertise from diverse industries and across infrastructure, applications, and operational workflows. We leverage our understanding of observability best practices, paired with hands-on experience, to provide actionable insights that improve troubleshooting, performance monitoring, and overall operational awareness.

Book a conversation with one of our consultants to explore how an Observability services can protect you.

info@devnullsecurity.co.uk