Splunk SIEM Assurance

Operate & Evolve

DEV/NULL

Clarity, confidence, and optimisation for your Splunk SIEM.

Modern security environments are fast-moving, diverse, and constantly targeted, making a healthy SIEM essential for effective threat detection and response. Our Splunk SIEM Assurance Service provides a comprehensive evaluation of your platform, spanning data quality, architecture, detections, and operational processes to reveal gaps, inefficiencies, and optimisation opportunities. By benchmarking your environment against Splunk best practices, we help strengthen visibility, streamline investigations, and improve overall security posture. The result: clearer insights, faster response, and a more resilient SIEM foundation.

More detail

Our SIEM Assurance evaluates the full lifecycle of your Splunk security monitoring capabilities, from data quality and ingestion reliability to detection coverage, dashboard effectiveness, and operational workflows. We focus on ensuring your SIEM ecosystem is accurate, efficient, and actionable, providing consistent high-quality visibility across your security data sources and aligning your environment with industry and Splunk best practices:

- SIEM Readiness Assessment to baseline existing security logging, data quality, and visibility gaps.
- Best-practice Architecture Review to ensure a scalable, resilient Splunk SIEM foundation.
- Data onboarding & normalisation review to ensure standardised log formats, CIM alignment, ensuring clean, high-value telemetry data.
- Review of dashboards supporting threat monitoring, investigations, operational reporting and more.
- Review of integrations with Incident Response workflows, including alert routing, prioritisation, and escalation paths within SOC processes, ITOps use cases or case management tools.
- Alert Optimisation Review to offer advice on improving signal-to-noise ratio and reduce false positives.

Dev/Null will provide a clear review and roadmap for a Splunk-based SIEM foundation that strengthens visibility, accelerates response, and provides a scalable platform for long-term maturity.

Benefits

This service is particularly beneficial for organisations who want:

- Deeper visibility into security events, user activity, or critical system logs across the environment, including gaps that reduce the effectiveness of Enterprise Security detections or Observability insights.
- Certainty about the reliability, completeness, or usefulness of existing security logging, metrics, or telemetry feeding Splunk Core, Enterprise Security, or Observability Cloud.
- Minimal manual effort in investigating incidents with consistent data, quality log sources, connected signals across logs, metrics, and traces.
- To optimise data onboarding, normalisation, correlation, and telemetry pipelines to deliver clearer, more actionable insights across SIEM, ES content, and Observability use cases.
- To improve threat detection, accelerate investigation and response, and strengthen service and platform visibility through a consistent, scalable Splunk foundation that supports both Enterprise Security and Observability Cloud.

What's included in the Dev/Null service?

Discovery:

Perform targeted workshops and configuration reviews to understand current SIEM capabilities, maturity, and usage across Splunk Core and any premium apps in use.

Analyse:

Review architecture, data quality, performance, and security controls against Splunk best practices, including Enterprise Security, SOAR, and Observability touchpoints where applicable.

Validate:

Validate data onboarding, CIM alignment, detection logic, dashboards, alerts, and workflows to identify gaps, inefficiencies, and risks impacting SIEM effectiveness.

Optimise:

Identify optimisation opportunities across searches, detections, alerting, retention, ingest strategy, ES features, SOAR automation triggers, and Observability signal usage to improve efficiency and reduce noise.

Recommend:

Produce a clear, prioritised set of recommendations and improvement options covering quick wins, medium-term enhancements, and longer-term maturity initiatives across the Splunk platform.

Support:

Provide guided playback, clarification sessions, and optional short-term advisory support to help teams interpret findings, plan remediation, and confidently take next steps.

Service Enhancements

Dev/Null provide service enhancements that can be customised to enhance the scope and impact of your engagement with the presence of Splunk Premium Applications.

Below are additional activities performed on top of the standard service, based on the choice of Premium Application. The below will be in addition or in parallel to the main service activities:

Splunk Enterprise Security

1. Review correlation searches to assess detection logic, thresholds, scheduling, performance, and alignment with security use cases and organisational risk appetite.
2. Evaluate the configuration and usage of findings and intermediate findings (formerly Risk-Based Alerting), including risk scoring, aggregation, and effectiveness in prioritising high-risk activity.
3. Assess ES dashboards, investigations views, and analyst workflows to ensure they provide actionable insight and support efficient triage and investigation processes.
4. Analyse ES content coverage against recognised frameworks (such as MITRE ATT&CK where applicable) to identify gaps, overlaps, and opportunities to strengthen detection maturity.
5. Review Mission Control Case Management processes and usage (if applicable).
6. SOAR Assurance / Foundation (Separate Service)
7. Data tiering strategy support. (Separate Service)

Splunk Observability Cloud

1. Assess coverage of metrics, logs, and traces across critical services, applications, and user journeys, identifying visibility gaps and blind spots.
2. Review telemetry pipelines, collectors, and data flows to ensure reliable, scalable signal ingestion and processing.
3. Evaluate adoption, configuration, and effective use of Splunk Observability Cloud capabilities, including Infrastructure Monitoring, APM, Log Observer, RUM, and Synthetic Monitoring.
4. Review metric cardinality, tagging standards, trace sampling strategies, and log volume to improve signal quality and control observability spend.
5. Assess metric resolution, trace and log retention, and signal granularity to ensure alignment with troubleshooting needs and cost objectives.
6. Review dashboards, service maps, and dependency views to ensure effective service-level visibility and root-cause analysis.
7. Review integration with CI/CD pipelines, deployment markers, and change events to improve incident context and root-cause identification.
8. Assess observability maturity across instrumentation, alerting strategy, service ownership, and governance, and provide a prioritised improvement roadmap.

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 deployment is essential to establishing a strong, scalable data foundation. At Dev/Null, we combine proven methodologies with deep real-world big data experience to help organisations achieve meaningful visibility across their environments. Our team brings expansive expertise spanning multiple disciplines. We apply industry-aligned best practices and hands-on implementation knowledge to deliver a SIEM that provides clear, reliable, and actionable security insight, strengthening detection, accelerating investigations, and elevating overall security maturity.

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

info@devnullsecurity.co.uk