Splunk SIEM Foundation
Design & Build

DEV/NULL

Establishing a solid, scalable foundation for your Splunk investment

Modern security environments are fast-moving, diverse, and increasingly targeted, making unified visibility essential for effective threat detection and response. Our SIEM Foundation service brings together your critical data sources into a central Splunk-powered platform, delivering clarity across your entire landscape. By aligning data onboarding, architecture, and detection foundations to best practices, we help you identify threats sooner, streamline investigations, and strengthen your overall posture. The result: faster insights, improved operational readiness, and a more resilient ecosystem.

More detail

Our SIEM Onboarding Service supports the full lifecycle of establishing and maturing your Splunk security monitoring capabilities from designing and implementing reliable data ingestion pipelines to aligning detections, dashboards, and correlation searches with industry best practices. We focus on ensuring your SIEM ecosystem is accurate, efficient, and actionable, enabling consistent, high-quality visibility across your security data sources:

- SIEM Assessment to baseline existing security logging, data quality, and visibility gaps.
- Best-practice Architecture Design or Review to ensure a scalable, resilient Splunk SIEM foundation.
- Identify bottlenecks, improve search performance, and tune system configurations for high-volume or complex deployments.
- Data onboarding & normalisation assistance to standardise log formats, enhance CIM alignment, and ensure clean, high-value telemetry data.
- Development or configuration of dashboards to support threat monitoring, investigations, and operational reporting.
- Application development, installation and configuration to meet functional requirements.
- Integration with Incident Response workflows, including alert routing, prioritisation, and escalation paths within SOC processes, ITOps use cases or case management tools.
- Alert optimisation to improve signal-to-noise ratio and reduce false positives.
- Compliance alignment with frameworks such as ISO 27001, NIST, PCI DSS, and organisation-specific security policies.
- Empower internal teams through structured workshops, documentation, and coaching to operate and innovate the SIEM independently.

Dev/Null will help design and configure 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.
- Certainty about the reliability, completeness, or usefulness of existing security logging and data sources.
- Minimal manual effort in investigating incidents with consistent data and quality log sources.
- To optimise data onboarding, normalisation, and correlation capabilities for clearer and more actionable data insights.
- To improve threat detection, accelerate investigation and response, and establish a consistent, scalable SIEM foundation.

What's included in the Dev/Null service?

Assess:

An in-depth assessment of your current capabilities through interview, document review, and tool review. This phase gathers all relevant data to form a complete picture of your SIEM requirements.

Architect:

Comprehensive design documentation presenting findings, decisions, and solution designs in a clear, consumable format, ensuring the SIEM architecture aligns with your operational readiness and future-state security objectives.

Deploy:

Deploying the SIEM environment with supporting infrastructure and enabling core functionality as defined.

Onboard:

Onboarding and validating agreed data sources, ensuring data quality, CIM alignment, and foundational detection coverage.

Enable:

Delivering operational dashboards and structured guidance to strengthen confidence and capability in SIEM workflows.

Support:

Providing short-term operational support, assisting with tuning, troubleshooting, and optimisation as the SIEM begins to mature.

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. Install, configure, and validate Splunk Enterprise Security (ES), including post-install hardening and version alignment.
2. Validate data source readiness for ES, including CIM compliance, data model compatibility, and ES-required fields.
3. Configure ES-specific components such as notable events, investigations, and adaptive response actions.
4. Review and tune out-of-the-box correlation searches to align with customer risk appetite and priority use cases.
5. Configure findings and intermediate findings (Risk-Based Alerting) where applicable.
6. Enable and optimise ES dashboards, data model acceleration, and investigative views.
7. Align ES workflows with SOC processes, including triage, escalation, and case handling.
8. Optional integration with Splunk SOAR for automated response workflows.
9. SOAR Onboarding / Development (Separate Service)
10. Data tiering strategy support. (Separate Service)

Splunk Observability Cloud

1. Configure Splunk Observability Cloud tenant.
2. Configure Observability Cloud capabilities in scope (Infrastructure Monitoring, APM, Log Observer, RUM, Synthetic Monitoring).
3. Standardise telemetry naming, tagging, and enrichment to ensure consistent signal correlation.
4. Build key service, application, and infrastructure dashboards aligned to operational workflows.

Optimise telemetry volume, cardinality, and retention to balance visibility and cost

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 Foundation service can protect you.

info@devnullsecurity.co.uk