# Splunk SOAR Assurance

## Governance & Assurance

DEV/NULL

Assured automation for confident response

Security automation only delivers value when it is operating as intended. The Splunk SOAR Assurance service is a structured health check designed to assess the current state of your SOAR platform and how effectively it supports incident response. Through targeted review of playbooks, integrations, automation performance, and operational workflows, we identify gaps, inefficiencies, and risks that limit automation effectiveness. By benchmarking your environment against Splunk and industry best practices, we provide clear insight into what is working, what is not, and where optimisation or remediation is required. The outcome is a practical, prioritised view of your SOAR health and a roadmap to improve reliability, efficiency, and response outcomes.

## More detail

Our SOAR Assurance service evaluates the full lifecycle of your Splunk SOAR environment, from playbook design and automation efficiency to integration reliability, alert handling, and operational workflows. We focus on ensuring your SOAR ecosystem is effective, optimised, and actionable, providing consistent, high-quality orchestration across your incident response processes and aligning your environment with industry and Splunk best practices:

- Evaluate your current automation, playbooks, and orchestration workflows to identify gaps, inefficiencies, and opportunities for improvement.
- Ensure a scalable, resilient SOAR platform, design and validate integrations with SIEM, IT systems, and case management tools.
- Assess any existing playbooks for effectiveness, efficiency, and alignment with operational best practices.
- Review alert handling, incident routing, prioritisation, and escalation processes to optimise SOC efficiency.
- Evaluate dashboards and reporting to ensure actionable insights, visibility, and operational oversight.
- Identify opportunities to improve workflow efficiency, reduce manual effort, and increase accuracy in automated responses.

Dev/Null will provide a clear review and actionable roadmap for your Splunk SOAR environment, optimising playbooks, enhancing automated response, and establishing a scalable foundation for long-term operational efficiency.

## Benefits

This service is particularly beneficial for organisations who want:

- Deeper visibility into end-to-end incident handling, with clear automation, playbook execution, or clean hand-offs between SOAR and downstream tools.
- Certainty around the reliability and effectiveness of existing playbooks, integrations, and automated actions.
- Minimal analyst effort and fast response times using automation and quality response workflows.
- To optimise alert ingestion, enrichment, and response workflows to maximise SOAR value across SIEM and ES detections.
- To reduce MTTR, improve response consistency, and establish a scalable automation framework that supports long-term security maturity.

## What's included in the Dev/Null service?

### Assess:

Run focused workshops and configuration reviews to evaluate Splunk SOAR automation maturity, playbook usage, and integration effectiveness across the response ecosystem.

### Analyse:

Assess the architecture, integrations, performance, and security posture of your Splunk SOAR environment against Splunk-recommended best practices.

### Validate:

Validate playbooks, integrations, automation logic, alerts, and response workflows to identify gaps, inefficiencies, and risks impacting SOAR effectiveness.

### Optimise:

Identify opportunities to optimise playbook execution, automation triggers, enrichment workflows, and integration usage to improve response speed, reliability, and signal quality.

### Recommend:

Deliver a prioritised roadmap outlining immediate improvements, medium-term enhancements, and long-term initiatives to strengthen SOAR automation and operational maturity.

### Support:

Provide short-term advisory support to assist teams with any issues, questions, or challenges that arise after the engagement, ensuring recommendations are effectively implemented.

## Service Enhancements

While Splunk SOAR can operate as a standalone platform, it is often deployed as part of a broader Threat Detection, Investigation, and Response (TDIR) ecosystem. If your organisation also leverages Splunk Core, Enterprise Security, or Observability Cloud, this SOAR Assurance service can be extended with additional, focussed services to provide full visibility, coverage, and optimisation across the entire TDIR capability.

### Splunk SIEM Assurance

The SIEM Assurance Service provides a comprehensive review of your Splunk deployment, covering Splunk Core, Enterprise Security, and Splunk Observability Cloud. It evaluates platform health, data quality, and operational effectiveness, identifying gaps and optimisation opportunities to strengthen visibility, performance, and overall security posture.

### Splunk Mission Control

If Splunk SOAR is leveraged for Case Management in Splunk Mission Control and the full SIEM Assurance service is not required, this service can include additional assurance focused on the interactions between SOAR and Mission Control.

## 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 SOAR Assurance engagement is essential to gaining an accurate, objective view of how your automation is performing. At Dev/Null, we apply structured assessment methodologies backed by extensive real-world experience reviewing and validating Splunk SOAR environments in production. Our team brings deep understanding of incident response operations, automation patterns, and platform behaviour, enabling us to identify risks, inefficiencies, and improvement opportunities with precision. By benchmarking your environment against Splunk-aligned best practices, we provide clear, actionable insight to help you strengthen automation reliability, improve response confidence, and make informed decisions about next steps.

Book a conversation with one of our consultants to explore how a Splunk SOAR Assurance service can help you.

info@devnullsecurity.co.uk