Security Orchestration, Automation & Response

DEV/NULL

Design & Build

Faster Response, Smarter Security

Cyber threats are growing in speed, scale, and sophistication, making rapid response essential to defending your organization. Our SOAR service automates and orchestrates security workflows, accelerates incident response, and reduces manual effort. Powered by Splunk, it turns alerts into coordinated actions, streamlining operations while optimizing efficiency and impact. The result: faster response, smarter workflows, and stronger security outcomes.

More detail

Our SOAR Service covers the full lifecycle of your security automation capability, from designing and building new playbooks to optimizing and refining existing workflows, all aligned with industry best practices to ensure trusted, efficient, and repeatable automated response:

- Architecture design and implementation tailored to your organization's automation and orchestration needs.
- Integration with incident response processes and broader security tooling.
- Development, optimization, and tuning of automated playbooks for trusted, repeatable actions.
- Identifying and implementing opportunities for SOAR.
- Workflow optimization to reduce manual effort and improve operational efficiency.
- Alignment with compliance frameworks such as ISO 27001, NIST, and PCI DSS.

We will design, build, and optimize a Splunk-powered SOAR solution that automates trusted workflows, accelerates incident response, and maximizes the efficiency and impact of your security operations.

Benefits

This service is particularly beneficial for organisations who want:

- Better automation or orchestration across security workflows.
- Certainty about the reliability or effectiveness of existing playbooks.
- Minimal manual effort in responding to alerts or repetitive security tasks.
- Good integration between tools, workflows, and incident response processes.
- To optimise existing automation for efficiency, accuracy, and scalability.
- To accelerate incident response and improve the consistency and impact of security operations.

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.

Playbook Design:

A detailed design document outlining playbook implementation based on SOAR best practices. It includes analysis of tool integrations, process workflows, risk-based prioritisation, and automated response procedures to ensure reliable, repeatable, and effective security actions

Implementation:

A structured approach to deploying and supporting your Splunk SOAR. Includes architecture implementation, integration configuration and development in-line with industry and vendor best practices for on-prem or cloud-based environments. Deploy and fine-tune playbooks and workflows for optimal automation.

Maturity Roadmap:

Provide knowledge transfer and offer post-delivery support options for continuous improvement and scaling.
Roadmap guidance covering capability improvements, progress tracking, and continuous refinement to keep your security posture aligned with evolving threats.

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.

Who to choose

Choosing the right partner for a SOAR build 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.

Book a conversation with one of our consultants to explore how a building a SOAR function can protect you.

info@devnullsecurity.co.uk