Splunk SOAR Managed Services

Ongoing administration, optimisation and assurance of security orchestration and automation capabilities

Splunk SOAR Managed Service provides ongoing operational management, maintenance, and assurance for Splunk SOAR environments. The service ensures security orchestration, automation, and response capabilities remain reliable, effective, and aligned to operational and security objectives, enabling organisations to respond to incidents consistently and at speed.

Service Overview

Delivered by Splunk-certified specialists, this managed service provides business-as-usual operation and continuous improvement of Splunk SOAR. The service focuses on maintaining automation reliability, improving playbook effectiveness, and ensuring Splunk SOAR continues to support efficient and repeatable security operations.

Service Scope

- Ongoing administration and operation of Splunk SOAR
- Monitoring and maintenance of SOAR platform health and availability
- Playbook lifecycle management and controlled updates
- Maintenance and tuning of automation workflows
- Integration oversight with security tools and data sources
- Incident queue and case management support
- Error handling, troubleshooting, and recovery for automation failures
- Platform-level incident investigation related to SOAR behaviour
- Operational documentation and knowledge transfer

What the Service Delivers

- Stable and well-governed Splunk SOAR environments
- Reliable execution of security automation and response workflows
- Reduced manual effort and improved response consistency
- Improved confidence in automated incident handling
- Sustained operational value from SOAR automation over time

How the Service Is Used

This service is typically used by organisations operating Splunk SOAR that require ongoing operational ownership and assurance but do not wish to retain specialist SOAR expertise in-house. It may also be used to supplement internal security teams during periods of increased incident volume, automation expansion, or organisational change.

Delivery & Commercial Model

- Delivered as an ongoing managed service
- Scalable based on number of playbooks, integrations, and incident volumes
- Delivered by SFIA v8-aligned Splunk specialists
- Clear operational boundaries and responsibilities
- Suitable for G-Cloud Lot 3 (Cloud Support) procurements