Splunk Solutions, Licensing, and Managed Services from 2T Security

Service description

2T Security is a UK-based cyber security and cloud consultancy recognised as both a Splunk Manage Associate Partner and a Splunk Sell Associate Partner. We enable public sector organisations to maximise the value of their data through Splunk's analytics and security ecosystem—spanning solution design, licensing, implementation, optimisation, and managed operations.

With deep experience in security monitoring, data engineering, and automation, we help government clients build resilient and compliant Splunk environments that strengthen threat detection, improve operational insight, and meet UK public sector digital and assurance standards.

Capabilities

As certified Splunk partners across both Sell and Manage designations, we deliver full lifecycle services that combine technical expertise, governance assurance, and ongoing operational support. These services include:

- Splunk Solution Supply and Licensing: As a Sell Associate Partner, we can supply Splunk licences and assist clients in selecting appropriate editions, capacity tiers, and scaling models that align with operational and budgetary goals.
- Architecture and Implementation: Design and deployment of secure and scalable Splunk environments across on-premises, hybrid, and cloud infrastructures (including Splunk Cloud Platform).
- Integration and Data Onboarding: Secure integration with enterprise data sources, cloud applications, and security telemetry systems (e.g., Corelight, Suricata, NDR, and threat intelligence feeds).
- Security Analytics and Operations: Creation of high-value correlation searches, dashboards, and detections to enhance SOC capabilities and accelerate incident response.
- Managed Splunk Operations: As a Splunk Manage Associate Partner, we provide ongoing service management, performance tuning, alert optimisation, upgrades, and data retention strategy support.
- Training and Knowledge Transfer: Hands-on enablement for security analysts, operations engineers, and system administrators to promote self-sufficiency and long-term sustainability.

Service benefits

Our Splunk partnership status and consulting experience deliver measurable value for government clients:

- End-to-End Service Offering: Combined licence supply, implementation, and management through a single trusted provider.
- Enhanced Operational Capability: Unified data visibility across security, IT, and operational domains, through Splunk's analytics platform.
- Faster Time to Value: Pre-defined implementation templates and configuration accelerators reduce deployment complexity and timeframes.

- Assured Security and Compliance: Continuous alignment with NCSC, ISO 27001, and UK public sector governance standards.
- Optimised Service Costs: Efficient index management, data tiering, and licence utilisation ensure maximum performance-to-value ratio.

Engagement Process

Our structured approach ensures transparency, repeatability, and compliance with government delivery standards:

- Discovery and Requirement Analysis: Understand customer objectives, use cases, and existing environment baselines.
- Solution Design and Licensing Advisory: Define architecture, capacity planning, and licensing strategy to support business and technical goals.
- Deployment and Integration: Implement and configure Splunk components with security, compliance, and performance validation.
- Managed Operations: Provide managed service oversight, including continual monitoring, optimisation, and patch assurance.
- Knowledge Transfer and Service Handover: Deliver training, detailed documentation, and service transition to customer teams.

Onboarding and Offboarding

Onboarding: We deliver a secure and collaborative onboarding process to ensure minimal disruption and full compliance with client governance frameworks.

- Kick-Off and Planning: Define objectives, roles, communication methods, and timescales.
- Security and Access Control: Verify consultant clearances, manage credentials, and establish secure access paths under customer control.
- Environment Readiness: Conduct platform assessments and define the architecture plan for build and integration.
- Service Initiation: Formalise milestones, deliverables, and reporting mechanisms aligned to project governance.

Offboarding: At contract conclusion or transition to internal management, we ensure a complete, secure, and auditable disengagement.

- Knowledge and Asset Handover: Provide configuration documentation, runbooks, and operational guidelines.
- Data Protection and Sanitisation: Return or securely erase customer data in compliance with GDPR and retention policies.
- Access Decommissioning: Revoke all accounts, keys, and credentials with audit confirmation.
- Optional Transitional Support: Provide short-term assistance to enable smooth service ownership transfer.

Security, data protection and compliance

Security and compliance are at the core of all Splunk services we deliver. Our methodologies and frameworks align with UK Government assurance expectations and industry best practice:

- Data Protection and Sovereignty: All engagement activities comply with UK GDPR and the Data Protection Act 2018. Government data remains within approved UK boundaries under full customer ownership.
- Access Control and Governance: Strict access control and auditing standards are applied, including MFA, RBAC, and full engagement audit trails.
- Assured Operations: Our consultants hold appropriate level clearances where required and are experienced operating in sensitive environments.