

Splunk consultancy, implementation and support

G-Cloud 15

Contents

Splunk	3
Service overview	4
Features and benefits	5
Features	5
Benefits	6
Business continuity and disaster recovery plans	6
Onboarding and offboarding	6
Onboarding	6
Offboarding	7
Ways of working	7
Training.....	7
Quality assurance and performance testing	8
Security services.....	8
Ongoing support	9
SLA Incident Response.....	10
Hosting managed services	10
Service constraints	11
Ordering and invoicing	11
Pricing	11
Industry standards	11
Contact details	12

Splunk

CDS provides the full range of services needed to define, build, assure and deploy secure cloud platforms, creating robust cloud computing architectures on which applications can run, providing end-users with the ability to leverage the power of cloud resources.

Our expert cloud architecture capability provides services including:

- Cloud security and monitoring services
- Cloudflare
- Cyber and information assurance consultancy
- Data architecture, analysis, and consultancy
- Secure by design technical consultancy
- Secure infrastructure and monitoring design
- Splunk.

We work with client stakeholders to capture and prioritise business requirements and constraints, hosting needs, service levels and maintenance implications. Our cloud architects implement secure-by-design infrastructures with risk-proportionate controls, to support reliable, scalable cloud provision that ultimately delivers improved services to end-users whilst minimising administrative and labour overhead for our customers.

CDS has both wide and deep experience of enabling organisations to move to the cloud, with a proven methodology that includes discovery and consultancy as well as implementation and migration. This methodology starts with discovery and requirements gathering, using business analysis to understand the role of legacy systems and technologies that need to remain on-premise, vs applications that are natively cloud-based.

We then make recommendations for the appropriate cloud hosting provider and architectures, with a formal integration and implementation plan that ensures seamless and timely migration with an extremely high level of availability.

In addition, as a partner to Cloudflare, CDS' work in cloud hosting and migration is secure by design. Cloudflare now handles 10% of the world's internet traffic, with 10 trillion requests flowing across the platform from 2.5 billion users.

CDS is experienced in architecting, managing, and implementing scalable cloud services on a range of platforms.

- UK Policing Single Online Home on Microsoft Azure: a secure, high-availability, scalable platform, active-active across two data centres, leveraging Terraform, PowerShell and Chef

- Social Work England on Microsoft Azure, including microservices-based using Azure AD, Storage Queues, Functions, Logic-Apps, Redis Cache and MySQL Service, solution to migrate and transform large volumes of data
- Rail Delivery Group: content management and delivery solution on Amazon Web Services (AWS) for National Rail Enquiries, capable of handling daily peaks of up to 10 million users.

Service overview

CDS provides Splunk consulting, implementation, and support services to help customers turn data into action at scale across cyber security and IT operations, risk management and compliance, business intelligence and analytics teams, to ensure their organisations are secure, resilient and innovative.

Splunk offers an open, extensible data platform that supports shared data across any environment so that all teams in an organisation can get end-to-end visibility, with context, for every interaction and business process.

The CDS cloud strategy, architecture and security teams have significant experience deploying Splunk. Cloud transformation, business resilience and digital customer experience solutions have been implemented across a broad range of high-profile public and private sector clients focused on driving resilience, improving security and unlocking innovation across their organisations.

Our advisory, professional, and support services allow customers to offload and optimise their Splunk solutions and focus on their core business. Services include:

- **Strategy and design:** including discovery, exploring customer organisational and operational landscapes to build architecture and security recommendations with service design that champions end user, stakeholder and experience needs
- **Cloud migration services:** supporting customers to migrate workloads to the cloud to gain greater scale and efficiency while reducing downtime
- **Application modernisation:** advisory services to re-architect and build cloud-native applications to unlock faster innovation and deliver exceptional customer experiences
- **IT modernisation:** supporting customers to maintain high uptime in IT service delivery while improving operational efficiency and streamlining manual, noisy IT workflows with integrated solutions for alerting, triage, investigation and response
- **Advanced threat detection:** implementation services to detect network and host activity that might indicate an advanced threat. Customers can collect, index, correlate and analyse all data and monitor activity patterns
- **Inside threat detection:** implementation services to help customers automatically observe anomalous behavior to minimise risk by detecting potential threats that use legitimate credentials, permissions and endpoints
- **Incident investigation and forensics:** using security analytics to help analyse and confirm high-priority incidents across data sets and cross-reference and correlate relationships with other entities
- **DevOps:** advisory services to support customers to achieve end-to-end visibility of their data to instantly understand and optimise modern infrastructure and applications
- **SOC automation and orchestration:** support services to automate and orchestrate, enabling greater security operation centre productivity and faster threat response.

Features and benefits

Features

- Advisory services covering discovery, assessment and use-case definition
- Implementation, configuration, on-boarding and ongoing support services
- Ingests and indexes data from any source
- Powerful search, analytics and data visualisation capabilities
- Access to a wide variety of apps, add-ons and data sources
- Security cleared Splunk consultants
- Access and audit controls
- Automation and orchestration
- Security information and event management - SIEM Platform
- Information assurance and security analysis services

Benefits

- Optimise Splunk deployment and investment
- Identify opportunities and risks in current operations
- Minimise risk through detection of internal and external cyber threats
- Greater scale and efficiency whilst reducing downtime
- Improved productivity and faster threat response
- Flexible support services and options
- Agile DevOps processes
- Access to qualified, security-cleared strategy, architecture and security teams
- Improved innovation through access to data and insights
- Improved customer and end user experiences both internal and external.

Business continuity and disaster recovery plans

CDS is committed to minimising and managing its exposure to disruption to the business and the services provided to our customers. This encompasses robust systems and processes necessary to maintain continuity of service and operations.

CDS maintains a comprehensive Business Continuity and Disaster Recovery (BCDR) plan, certified to **ISO 23001**, that defines clear roles, responsibilities, processes, and procedures for assessing and responding to disruptions to ensure continuity during disruptions. **Our plan is tested annually with lessons learned incorporated into plan improvements.**

Our Business Continuity Management System (BCMS) is underpinned by regular business impact assessments and threat and risk analyses, and annual tests to ensure all contingencies remain effective, current, and fit for purpose.

Onboarding and offboarding

Onboarding

CDS provides a tailored onboarding pathway, based on clients' individual requirements.

Onboarding is a collaborative process, through which we fully understand our clients' short-, medium- and long-term goals, and plan our service accordingly, to deliver best value and appropriate resourcing, governance, communication and planning.

Our multi-disciplinary agile teams will work with project stakeholders to understand the client and project needs and requirements.

We will define and capture ways of working, including definitions of 'ready' and 'done', and identify acceptance criteria for each sprint, underpinned by modern test practices and OKRs.

Offboarding

Upon starting the engagement, CDS will provide an exit plan for client approval. This will cover matters such as knowledge transfer and documentation, roll-off schedules, data and asset transfer, intellectual property and removal of access / permissions and return of devices / equipment.

Ownership of data contained in any solution belongs to and rests with the client; as the service is decommissioned, raw data will be transferred to the client. CDS is certified to ISO 27001 for data security and will always adhere to these standards – including data removal and destruction.

Ways of working

At CDS we apply agile principles across our projects, primarily using the SCRUM Agile methodology. We operate multi-disciplinary squads that combine domain expertise with technical excellence, delivering value early and iteratively through two-week sprints. Our approach is underpinned by the following core practices:

- **Daily standups:** A team call for 15 minutes each morning to track progress, surface blockers and ensure sprint goals are achieved.
- **Sprint planning:** Held at the start of each sprint to prioritise the work, align on objectives and ensure the team is fully prepared.
- **Sprint review:** At the end of the sprint, the team demonstrate to all stakeholders the deliverables achieved and present the sprint goal for the next sprint.
- **Sprint retrospective:** For each sprint the team will review what went well, identify areas of improvement and embed lessons learned to drive continuous improvement.

Additionally, we have an Agile mindset and culture at CDS, in which we apply:

- **User-centred design and customer-focus:** Through collaboration and partnership working we deliver outcomes that meet user needs.
- **Adaptability and flexibility:** Short feedback loops enable us to respond quickly to change, with teams empowered to pivot as required.
- **Continuous learning:** Retrospectives encourage open, honest feedback to continually improve ways of working and delivery effectiveness.
- **Partnership and teamwork:** We create a one-team culture with our clients and their supplier partners, working collectively towards shared project goals.

Training

As well as continual 'on the job' knowledge transfer to upskill client teams, CDS can provide formal, comprehensive training for administrators and users prior to handover and go live designed to support successful change management, ensure smooth implementation and embed solutions that are integral to business operations.

Our training also builds internal technical capability, empowering teams to become self-sufficient and reduce the long-term cost of change.

In most cases, we adopt a 'train-the-trainer' model, delivered through a blend of on-site and remote sessions. This is supported by comprehensive training materials and easy-to-follow digital end-user guides, written for non-technical audiences and compliant with WCAG 2.2 accessibility guidelines.

Quality assurance and performance testing

CDS applies rigorous testing as part of our Quality Assurance process (ISO9001) to ensure we maintain quality across our deliverables and that outcomes are fit for purpose and fulfil functional and performance requirements.

Our testing capability is led by ISTQB (International Software Testing Qualifications Board) qualified testing experts with all the skills and expertise to quality assure AI, technology & cloud services.

We use a flexible, agile testing approach utilising tools and techniques tailored to each client's context to ensure solutions meet business objectives and success criteria.

We adopt an automation-first approach, embedding high-quality automated checks into robust CI/CD pipelines to ensure quality is treated as a first-class citizen throughout the deployment process.

Our testing services include:

- Test strategy
- Test planning
- Automated test frameworks
- Testing, defect management and reporting
- Support of customer UAT
- Security (perimeter/application) testing / DevSecOps
- Performance and stress testing.

Security services

CDS holds certifications to international standards - Cyber Essentials Plus and ISO27001 Information Security, encompassing physical security, personnel security, storage, electronic data handling and secure destruction.

We embed 'secure-by-design' principles in our standard service design approach, aligned with security best practises and in addition we provide expert security consultancy.

CDS works closely with National Cyber Security Centre CHECK-accredited providers to conduct IT Health Checks (ITHC)/penetration testing in line with best practice.

CDS staff are BPSS cleared as a minimum. We can deploy SC, NPPV cleared teams and staff with DV clearance, if required.

Ongoing support

Our service model is designed to provide comprehensive, proactive support that operates to **ISO20000:2018 Service Management and ITIL best practices**, covering the full-service management lifecycle.

We deliver a fully managed service that encompasses application support, platform maintenance, incident management, problem management, change management, supplier management, and out-of-hours support for major incidents. This approach ensures that business-critical systems remain operational and performant whilst maximising customer value through continuous service improvement.

All CDS Service Delivery team are ITIL-certified.

We offer three service levels (Bronze, Silver and Gold) each providing:

- Online Service Desk Portal available 24x7 for logging and tracking incidents and requests.
- Telephone support via a dedicated helpline available from 9am to 5pm Monday – Friday (excluding English Bank Holidays).
- Highly skilled service desk team who manage and resolve incidents and requests in accordance with the agreed SLA.
- Ongoing maintenance including application of security patches.
- Structured change management to ensure updates are properly assessed, approved and implemented.
- Monthly performance report to provide visibility of service levels and operational metrics.

Support and maintenance contracts stipulate a minimum level of support provision per month, appropriate to the size and complexity of the service, aligned to the preferred service support tier. Additional time is chargeable at the day rates listed on the rate card.

SLA Incident Response

Service	Bronze	Silver	Gold
Incident response			
P1 - To be called in	15 minutes	15 minutes	15 minutes
P2	1 hour	1 hour	1 hour
P3	1 hour	1 hour	1 hour
P4	4 hours	4 hours	1 hour
P5	1 working day	1 working day	1 hour
P6	1 working day	1 working day	1 hour
Target incident resolution - core hours			
P1	8 hours	6 hours	4 hours
P2	15 hours	11 hours	8 hours
P3	5 working days	3 working days	1 working day
P4	7 working days	5 working days	3 working days
P5	N/A	14 working days	10 working days
P6	N/A	N/A	N/A
Major Incident Report	N/A	10 working days	5 working days

Hosting managed services

CDS provides a range of consultancy and management services for design, implementation and management of application infrastructure, including:

- Technical architecture and implementation
- Infrastructure management and maintenance including:
 - Critical security patches
 - OS (operating system) patches: testing and deployment

- Application and platform availability
- Anti-virus & Malware updates
- Obsolescence management
- Proactive monitoring and alerting of Infrastructure & solution performance and function.

Service constraints

Attainable service levels will be dependent upon the service performance of cloud suppliers within the service chain. Maintenance windows may apply, and clients should refer to the SLA for the specific service in use.

Ordering and invoicing

We recommend contacting CDS before placing an order via G Cloud 15, to confirm and agree scope, scale, SLAs, KPIs, outcomes, etc. We will be pleased to support clients to define statements of work that reflect their requirements.

Invoices are issued monthly in arrears, with payment terms of 30 days.

Pricing

Timescales and costs vary, depending on several factors; we recommend a preliminary review to provide a firm cost.

Please refer to our pricing document and rate card.

Industry standards

CDS delivers all its services to internationally recognised standards. CDS is accredited to the following standards:

- ISO 9001 Quality Management System.
- ISO 27001 Information Security Management.
- ISO 20000 IT Service Management and IASME certified.
- ISO 14001 Environmental Management.
- BSI 1008 Electronic Information.
- ISO 22301 Security and Resilience (Business Continuity).
- ISO 45001 Health and Safety Management.
- ISO 10008 Evidential Weight and Legal Admissibility of Electronic Information.
- ISO 50001 Energy Management Standard.
- Cyber Essentials Plus.
- IASME certified.
- ITIL compliant service desk.
- PlanetMark Sustainability.

We comply with the Data Protection Act 2018 and UK GDPR regulations.

Contact details

Matt Johnson,
Head of Public Sector
CDS, Yorkshire House, Greek Street, Leeds, LS1 5SH
Email: bidteam@cds.co.uk
Telephone: 07939 866831
Website: www.cds.co.uk