Defence DataSec

SERVICE DEFINITION

G-CLOUD 14

- Data Consultancy
- Security Consultancy
- Cryptography and GeoSpatial

1. INTRODUCTION

COMPANY OVERVIEW

Defence DataSec is an innovative Data and security solution provider helping the organisation align their information system and protect business data by providing expert-level solutions in line with industrial tried and tested best practices.

Defence DataSec enables organisations to protect digital and analogue information which provides coverage for cryptography, mobile computing, as well as infrastructure and networks containing private, financial, and corporate information. Cybersecurity, on the other hand, protects both raw and meaningful data, but only from internet-based threats.

The main objectives of Defence DataSec are typically related to ensuring confidentiality, integrity, and availability of company information. We involve in the implementation of various types of security, including application security, infrastructure security, cryptography, incident response, vulnerability management, and disaster recovery.

WHAT THE SERVICE PROVIDES

Defence DataSec provides the following services:

CYBER SECURITY:

- NCSC Cyber Assessment Framework (CAF)
- CIS Critical Security Controls
- Cyber Essentials
- Cloud Security Alliance Matrix
- Cyber Security Audit
- Cloud Security Posture Assessment for AWS, Microsoft Azure & 365

CLOUD SERVICES:

- AWS Cloud Services
- Google Cloud Services
- Azure Cloud Services
- Oracle Cloud Services
- SAP Cloud Services
- Cloud Cost Optimisation Services
- SalesForce Cloud Services
- ServiceNow Cloud Services
- Workday Cloud Services
- Nutanix Cloud Services

SECURITY ARCHITECTURE:

- Provide an independent validation and review of proposed security architectures.
- Understand and map to industry-standard methodologies e.g SABSA, TOGAF.
- Design and implement Identity and Access Management solutions.
- Deliver Network and Infrastructure designs
- Deliver Application designs using an agile approach.

- Design and deliver big data and analytics solutions.
- Technical Design Authority (TDA)
- Deliver SOC and SIEM Solutions.
- Deliver Gateway and boundary architectures. (PSN etc.)
- Deliver PCI-DSS compliant solutions.
- Deliver Cryptographic and Cryptographic key management solutions.
- Deliver Link 16 Electronic Crypt Key Solutions.

MANAGED SECURITY:

- Managed Detection and Response
- Security Operations Centre (SOC)
- Security Information & Event Management (SIEM)
- Cyber Threat Intelligence
- Vulnerability Management Services
- Digital Forensics & Incident Response (DFIR)

TESTING:

- Web Application Testing
- Infrastructure Penetration Testing
- Mobile Penetration Tests
- Wireless Penetration Testing
- Social Engineering Testing
- Phishing Assessments
- Open-Source Intelligence (OSINT)
- Red Team Assessment
- Cloud Security Assessments

DATA MANAGEMENT/PRIVACY

- Data Maturity Assessment Framework
- Data Consolidation
- Data Extraction Service
- Data Privacy Management Framework
- Data Privacy Assessments & Audits
- Data Privacy Consultancy
- GDPR Readiness
- Data Consultancy / Scientists

SECURE CLOUD TRANSFORMATION

- AWS Well-Architected Security Review/deployment
- Azure Well-Architected Security Review/deployment
- Cloud Advisory on Data Security and Strategy Services
- Security aspects of Cloud API Infrastructure Development
- Security aspects of Cloud Consultancy, Professional Services and Software Support
- Security aspects of Cloud Discovery and Design

- Security aspects of Cloud Provisioning and Migration Services
- Security aspects of Cloud Security and Professional Services
- Security aspects of Office365 Consultancy and Professional Services
-

2. Data Protection

Information Assurance

Cyber essentials/Cyber essentials Plus

GDPR compliant

PCI – DSS compliant

ISO27001 compliant

ICO compliant

Data Back-Up, Data Restoration and Disaster Recovery

In the event of DEFENCE DATASEC be required Data backup, Data restoration and disaster recovery and to hold any personal information are done using industry best practices and tools. We do so under our own GDPR regulations, and it is secure within our own server environment and included in our Data Classification Policy. We have been accredited by Cyber Essentials PLUS, only users within DEFENCE DATASEC who have a need to access this information in the performance of their duties do so.

Privacy by Design

All new DEFENCE DATASEC projects will go through PIA (Privacy Impact Assessment) and every PIA is completed within the official template document. All Projects completed by DEFENCE DATASEC also adhere to TOGAF (The Open Group Architecture Framework) An enterprise architecture methodology for business to ensure all risks are identified and mitigated.

Training

DEFENCE DATASEC can provide knowledge transfer at all stages of the cloud transition process. By working closely with your in-house technical teams, we'll help ensure they are equipped with the necessary skills via our tried-and-trusted combination of shadowing our experts during implementation and formal knowledge transfer and training sessions. A training approach will be agreed upon during the planning phase and may include any or all of the below with an additional charge – however, knowledge transfer for the project delivered by Defence DataSec is free of charge: -

- Train the trainer
- Classroom-based sessions for super users
- Online guided training
- Pre-recorded show and tell videos
- Inbuilt system guides and help tips
- Knowledge base
- Knowledge transfer of the HLDs (High Level Design),
- Knowledge transfer of the LLD (Low-Level Design),

- Knowledge transfer of the Infrastructure and Network Diagrams.

Service Management

DEFENCE DATASEC on-boards the systems to be supported by DEFENCE DATASEC managed services. The system is assessed for management needs and the appropriate policies and procedures are adopted from the ISO27001 compliant process library. A customer support representative is assigned to the customer and service management commences.

A typical managed service includes -

- 9.00 am to 5.00 pm (UK time), Monday to Friday coverage system support
- Helpdesk support for incident management and resolution
- Managed backup and recovery service
- Managed disaster recovery service
- Quarterly patching of operating system and application
- Named account manager
- Audit and compliance support and annual system optimization review

Service Levels

Defence DataSec provide support for the customer requirement. Typically, this will be remote support for systems hosted in the Cloud.

Priority 1 Support - for production system outages, 9.00 am to 5.00 pm (UK time), Monday to Friday coverage and 1-hour response

Priority 2 Support - for non-urgent production system incidents, 9.00 am to 5.00 pm (UK time), Monday to Friday coverage and 3-hour response

Priority 3 Support for non-production support incidents, 9.00 am to 5.00 pm (UK time), Monday to Friday coverage and 3-hour response

All customers are allocated an account manager

Financial Recompense Model for not Meeting Service Levels

Can agree a financial recompense model based on the customer requirements

3. PROVISION OF THE SERVICE

CUSTOMER RESPONSIBILITIES

- Submit Business Requirement
- Submit Technical Requirements Functional and Non-Functional
- Attend meetings and design workshops
- Attends service/Technical review meetings
- Provides service level requirements on an agreed basis with the Service Level Manager
- Negotiates, defines, agrees and communicates service levels agreements within the organisation

TECHNICAL REQUIREMENTS AND CLIENT-SIDE REQUIREMENTS

- Ensures escalation procedures are practiced if agreed service levels are about to be breached
- Ensures that all escalations are appropriately recorded. All of our projects have an extensive site survey carried out before the project commences. Bandwidth requirements and client requirements are set out in the method statement, which is discussed and distributed with the customer before any work is undertaken.

TERMINATION PROCESS

The Buyer can terminate a contract at any point with 30 days' notice (the amount of notice time can be agreed at the call-off stage). If the Buyer decides to terminate the contract, the Buyer should send a termination notice in writing to assigned DEFENCE DATASEC project manager via email to kick-off the termination process. DEFENCE DATASEC will respond to this email within 24-48 hours.

We can discuss with the Buyer to set a timeline to use up their final support time and offboarding process that needs to be adhered to as part of the termination process. We would provide High Level Documents (HLD) and Low-Level Documents (LLD) produced at the time of termination which will enable Buyers to transfer to another supplier subject to the contract being fulfilled.

All property, data and information held in connection with the Framework or Call Off Contract will either be returned or destroyed as per "DEFENCE DATASEC Secure Disposal Policy.'

Defence DataSec

+44 777 2 866727

info@defencedatasec.co.uk

Address: Office 267,
Spaces The Porter Building,
1 Brunel Wy, Slough SL1 1FQ,
United Kingdom