Microsoft Defender XDR Security Service

G-Cloud Service Definition

1 Jisc Cloud Security Services

Jisc can help you optimise the security of your cloud infrastructure through the provision of our professionals' services designed to offer expertise, skills, security industry knowledge and experience.

Our Cloud Security Services can be procured as stand-alone engagements or as part of the following series:

- **Microsoft Defender XDR Security Services** (this one) – **see the summary section below**
- **Cloud Professional Services - Security Reviews**, provides specialist security technical consultancy to review and benchmark an organisation cloud-based infrastructure against the security industries standards e.g. NCSC, CIS, and we also apply our own Jisc's security expertise benchmarks. Jisc has a broad range of practical experience in the cloud security domain. We draw on this experience to offer organisations skilled, flexible and pragmatic resources to meet short-term business challenges and/or to contribute to, or lead, longer-term projects or cloud-centred IT transformation programmes. The Cloud Professional Services - Security Reviews are applicable to the following cloud infrastructures:
    - Microsoft 365
    - Google Workspaces
    - Microsoft Azure
    - AWS
    - GCP
- **Microsoft Sentinel Security Services.** This service provides specialist security technical consultancy to deploy new Microsoft Sentinel instances or review existing Microsoft Sentinel instances. Our Cloud Security team will provide expertise and guidance when implementing Sentinel if customers are new to Sentinel. We will assist with on boarding & configuration. If your organisation already uses Sentinel, we can provide a service where we will review your current Microsoft Sentinel deployment, offer recommendations and best practises to take your Sentinel to its optimal configuration, so that it can reach its operational potential.
- **Cloud Professional Services** Jisc's cloud Professional Services provide specialist technical consultancy to organisations using or planning to use cloud-based IT service delivery models. Jisc has a broad range of practical experience in relation to managing many aspects of cloud service design, migration and operation. We draw on this experience to offer organisations skilled, flexible and pragmatic resources to meet short-term business challenges and/or to contribute to, or lead, longer-term projects or cloud-centred IT transformation programmes.
- **Cloud Architectural Services** – The Jisc Cloud Architectural Service will support you in designing services to run effectively on public cloud infrastructure. These may be redesigns of existing (legacy) services that currently run on physical or virtualised infrastructure, or new services that will be developed specifically for AWS or Azure. It may also be determined that a hybrid (cloud and on-premises) or multi-cloud solution is the most appropriate approach. For projects that already include cloud architecture, the service pragmatically reviews and assess your current public cloud estate and associated operational processes against your business objectives from the perspectives of operations, security, reliability, performance, and cost optimisation. It then makes architectural and operational recommendations with respect to cost-benefit, best practices, processes, implementation approaches and timescales.

We can also assist you, if necessary, in gaining the government accreditation required to operate a service in accordance with its associated information assurance requirements or to meet a compliance regime, e.g., PSN.

Jisc has worked extensively with several leading UK government third sector and education organisations to assess, design, plan and implement significant cloud-centric, IT transformation projects. These have supported business change, cost reductions, improved productivity and new channels for focused service delivery or revenue generation.

1 Summary

Jisc's Microsoft Defender XDR Security Services, provides specialist security technical consultancy to deploy new Microsoft Defender XDR instances or review existing Microsoft Defender XDR instances. Our Cloud Security team will provide expertise and guidance when implementing Defender if customers are new to Defender. We will assist with on boarding & configuration. If your organisation already uses Defender, we can provide a service where we will review and offer remediation to take your Defender to its optimal configuration, so that it can reach its operational potential.

Jisc's Microsoft Defender XDR Security Service will help you with:

- Design, Pilot, Train
- Help organisations understand Microsoft Defender
- Help organisations deploy Microsoft Defender
- AV migrations
- Ensure endpoint security is in-line with best practices.
- Enable service consolidation
- Facilitate cost optimisation
- Result in Improved security posture/baselines

1.1 Functional Overview

Jisc provides the following roles using appropriately qualified and experienced staff. These roles are available for leading public cloud vendors such as Microsoft and AWS. As well as offering staff for set pieces of work or projects, resource can be booked on an ad-hoc basis with no minimum or maximum requirements in terms of timescales.

- Project Manager
- Cloud Solution Architect
- Security Consultant
- Technical Specialist
- Network Consultant

As an established Cloud Managed Service Provider, Jisc has a broad range of practical experience managing many aspects of cloud service design, migration and operation.

1.2 Non-functional Overview

The service provides:

- On-shore UK staff resource
- Staff Curriculum Vitae, detailing relevant skills, experience, references and availability for interview.
- A customer contact point for service requests, change requests and escalations.
- Committed service levels for responses to customer requests and service deliverables.

1.3 Information Assurance

In delivering Jisc's Microsoft Defender XDR Security Services to designated customer security requirements, Jisc staff will comply with customer security policies and procedures. Jisc staff will work with the customer to gain any

required security clearance. Any Jisc provided infrastructure, software and network connectivity will be used in line with customer security requirements and processes.

1.4 Jisc Data Storage and Processing Locations

Jisc will store and process any service-related data to information assurance requirements and procedures. All data will remain in the European Economic Area unless agreed otherwise. For example, customers may prefer to use a cloud provider's UK region.

2 Service Description

Jisc's Microsoft Defender XDR Security Services provides skilled and experienced technical, project and/or business specialists for an agreed duration and day rate depending on the nature and length of the resourcing engagement.

2.1 Jisc Cloud Professional Service Roles

Jisc has wide-ranging experience with cloud services, ranging from assessing cloud cost-benefit, to designing integrated cloud solutions, implementing cloud migration projects and operating integrated cloud services.

Jisc has successfully managed a range of cloud migration projects including large and complex cloud-centred IT transformation projects. Often our team manage all project streams holistically across technical, service and commercial phases.

Jisc can provide the following roles in support of customer business requirements as well as on an as and when basis.

2.1.1 Cloud Technical Consultant

Jisc Technical Specialists have in-depth knowledge of a broad range of cloud-related server, virtualisation, storage, database, application and system integration technologies. Much of this experience has been gained with respect to migrating and consolidating IT services within a new cloud service delivery model. Key areas of expertise include:

- IT Build and Integration Services: technically implementing designs in relation to server, virtualisation, storage and cloud solutions, software and application configurations including database, business intelligence and CMS systems.
- IT Migration Services: Jisc specialists can support or implement the technical migration of 'as is' customer IT service functionality to a new agreed IT technical environment and contractual arrangement.
- IT Consolidation Services: to support or implement a range of technology and/or IT operational approaches to rationalise IT systems and services. This may include:
    - Infrastructure consolidation: the utilisation of virtualisation approaches to rationalise physical servers and improve resilience, scalability and agility.
    - Storage consolidation: the discovery, rationalisation and centralisation of legacy data stores, to establish storage as a flexible, resilient enterprise resource.
    - Database consolidation: the utilisation of common database platforms to rationalise disparate databases and underpinning database servers.
    - Application consolidation: establishing flexible platforms which permit mixed and/or multiple application workloads from within the same server or on a common shared platform.
- IT Modernisation Services: the implementation of technology updates or refreshes, including software platforms and applications, to gain benefits in terms of new system features, efficiencies, supportability and on-going sustainability.

System and Service Integration: assessing designated systems, applications and related 3rd party services; and using appropriate integration tools, code, methods and services to form a consistent end-to-end IT solution.

2.1.2 Project Manager

Jisc Project Managers use well-defined project management approaches such as Agile DSDM, Scrum and PRINCE2 to pragmatically deliver prioritised products in the shortest possible timescales. In addition to this we have defined an approach to larger projects and programmes of work (such as migrations) that encompasses both the flexibility of Agile with a gated, structured approach of other methodologies; this blended approach ensures successful delivery of projects on time and on budget.

Our Project Managers have sound technical competency and draw on other Jisc IT skills and knowledge as appropriate to support IT service project specialisms such as workload migration and consolidation planning. They have excellent communication, leadership and motivational skills to ensure effective project control and the management of risk and cost in liaison with customer stakeholders.

2.1.3 Cloud Solution Architect

Jisc provides solution architecture, infrastructure design and hands-on deployment services via experienced AWS and Azure Solution Architects who operate within the customer project management framework producing deliverables such as requirements specifications, high-level designs (HLD), low-level designs (LLD), infrastructure as code (IaC) artefacts and development and test plans as required.

Our AWS Azure and Solution Architects and Cloud Consultants are familiar with working on bespoke solution design activities, being attached to cloud migration projects as a technical authority and/or being allocated on a long-term basis to complex solution lifecycle or roadmap management.

2.1.4 Cyber Security Consultant and Cloud Security Engineer

Jisc provides security consultancy services with respect to:

- Cloud security/compliance consultancy
- Penetration testing
- Secure network solutions including secure access WAN solutions, encryption and IPsec VPN services
- Vulnerability assessment services
- Firewall management consultancy services
- Web Application Firewall (WAF) consultancy
- Distributed Denial of Service (DDoS) consultancy and protection
- Security event, alerting and correlation consultancy
- Infrastructure/Active Directory (AD) consultancy
- Endpoint/Security solutions (AV IPS ATP)

Jisc's qualified security specialists have worked with public sector and government customers for over a decade and work closely with independent CHECK and CLAS consultants.

2.1.5 Technical Specialist

Jisc Technical Specialists have in-depth knowledge of a broad range of cloud-related server, virtualisation, storage, database, application and system integration technologies. Much of this experience has been gained with respect to migrating and consolidating IT services within a new cloud service delivery model. Key areas of expertise include:

- IT Build and Integration Services: technically implementing designs in relation to server, virtualisation, storage and cloud solutions, software and application configurations including database, business intelligence and CMS systems.
- IT Migration Services: Jisc specialists can support or implement the technical migration of 'as is' customer IT service functionality to a new agreed IT technical environment and contractual arrangement.
- IT Consolidation Services: to support or implement a range of technology and/or IT operational approaches to rationalise IT systems and services. This may include:

    - Infrastructure consolidation: the utilisation of virtualisation approaches to rationalise physical servers and improve resilience, scalability and agility.
    - Storage consolidation: the discovery, rationalisation and centralisation of legacy data stores, to establish storage as a flexible, resilient enterprise resource.
    - Database consolidation: the utilisation of common database platforms to rationalise disparate databases and underpinning database servers.
    - Application consolidation: establishing flexible platforms which permit mixed and/or multiple application workloads from within the same server or on a common shared platform.
- IT Modernisation Services: the implementation of technology updates or refreshes, including software platforms and applications, to gain benefits in terms of new system features, efficiencies, supportability and on-going sustainability.
- System and Service Integration: assessing designated systems, applications and related 3rd party services; and using appropriate integration tools, code, methods and services to form a consistent end-to-end IT solution.

2.1.8 Network Consultant

Jisc's Network Consultants play a key role in cloud network design and delivery. Our consultants are a well-established team and have extensive experience in delivering high profile network services to diverse markets. The network designs are tailored to provide the optimum end-to-end solution for the customer's specific requirements.

Jisc's network design consultancy key areas of expertise include:

- Public and private cloud networking and security
- Azure ExpressRoute, AWS Direct Connect and Google Cloud Interconnect
- WANs, LANs & VPN technologies, including public or private MPLS.
- IP transit and Internet services
- Next generation firewalls, IPS and DDoS services
- Enterprise and service provider network design, including PSN.
- Global system load balancing and application firewalls
- Network rationalisation and modernisation.

2.2 Cloud Professional Services On-boarding

Jisc Cloud Professional Services on-boarding is centred on quickly embedding Jisc staff into the customer environment, working practices and culture to expedite their contribution and value. It includes the following:

- Customer selection of a named Jisc staff resource following CV review and interview
- Customer specification of duration and any on-premises requirements, including travel and subsistence payments
- Customer specification of desired outputs and deliverables, ideally in the form of a Work Package definition. Specification of governance processes and acceptance criteria
- Customer specification of customer locations, line manager, key processes and security, logistical requirements
- Jisc will provide a staff laptop, mobile phone and evidence of required security clearance (if appropriate)
- Customer induction of Jisc staff into customer organisation practices and facilitation of logistical requirements (security passes, network and email access) as necessary

- Establishment of service and change request and escalation processes.
- Establishment of monthly invoicing and payment procedures

2.3 Cloud Professional Services Off-boarding

Jisc Cloud Professional Services will terminate either on completion of the agreed resourcing duration period or if the customer or Jisc terminates the contract in line with the relevant Jisc terms and conditions.

On service termination, Jisc will commence a service off-boarding process, including:

- The return of any customer equipment including security passes, phones and computer equipment
- The supply to the customer, on request, of any relevant customer software, data or documentation held by Jisc.
- The purging of any customer backups, data, logs or documentation held on Jisc server, storage, media or other infrastructure, within 10 working days of service termination.

2.4 Service Management

Jisc Cloud Professional Services will be resourced and managed in a clear and systematic manner with appropriate channels for communication and change in place.

2.4.1 Hours of Service

Cloud Professional Services are provided during the core business hours of 9am to 5pm, Monday to Friday excluding national holidays and booked Jisc annual leave.

Jisc will endeavour to be flexible to customer priorities and business cycles and may agree specific tasks outside of core business hours based on a service request.

2.4.2 Customer Contact and Escalation

Jisc will provide a telephone and email service desk for customers during core business hours in order to facilitate the logging of service requests and change requests.

The contact telephone number of a Jisc Account Manager will also be provided for customer requests and for escalations.

2.4.3 Service Levels

Service requests and change requests:

- A service request is a customer request for non-standard working, for instance out of core business hours, typically in support of a business priority or business cycle requirement.
- A change request is a customer request for an extension to an existing resourcing engagement or the addition or modification of a resourcing engagement.

Jisc will respond to a customer service request or change request within 2 working days.

2.5 Service Pricing and Invoicing

- Cloud Professional Services resourcing is invoiced monthly in arrears using a day rate from our SFIA rate card.

2.6 Service Credits

Service credits are not issued with respect to Jisc Cloud Professional Services.

2.7 Service Constraints

Jisc Cloud Professional Services have the following limitations and exclusions:

- The service is provided during core business hours (9am to 5pm, Monday to Friday, excluding national holidays)
- A customer service request may be made to change core business hours, in support of priority requirements. Jisc will respond to requests within 2 working days.
- The service does not include travel and subsistence costs.

2.8 Customer Responsibilities

The customer has the following responsibilities in relation to the service:

- The customer will provide appropriate induction and logistical support for contracted Jisc Professional Services staff (including security passes, email and network access, computer equipment) as appropriate.
- The customer will provide appropriate line management and governance over work tasks, and promptly notify the nominated Jisc Resource Manager should any issues arise.
- The customer will provide Jisc with access to – and participation of customer business and technical stakeholders for Jisc to conduct the discovery work in accordance with mutually agreed timelines.
- The customer will provide relevant questionnaire responses, documentation, staff time and stakeholder contacts in relation to the consultancy services offered.

3 Associated Services

Jisc is a trusted technology advisor and ally of the education, public and third sectors. We provide best-in-class technology advice, engineering and support and work as part of your team to transfer knowledge at every step. As a not-for-profit membership organisation, we are an allied technology partner, and we reinvest our profits back into the communities we earn them in.

We see public cloud technology as a key enabler of a digital revolution in the sectors we serve. Our technical consultants, architects, engineers and support staff are the best at what they do and are dedicated to delivering the best service possible whilst also transferring their knowledge and skills to our members and customers.

Together, our services provide a full suite to support your use of public cloud services from start to finish. They can be taken in sequence to support your entire cloud journey or selected as needed to enhance just those parts of your programme where you need support.

3.2 Cloud Professional Services

- Cloud web application firewall (WAF). A cloud-based service that makes your websites safer, faster and more reliable. The service protects web properties, including websites and applications, regardless of their hosting platform. The platform guards against DDoS attacks that threaten the availability of web services and protects against data breaches that result from malicious cyber-attacks and vulnerability exploits.
- Microsoft Sentinel Security Services – provides specialist security technical consultancy to deploy new Microsoft Sentinel instances or review existing Microsoft Sentinel instances. Our Cloud Security team will provide expertise and guidance when implementing Sentinel if customers are new to Sentinel. We will assist with on boarding & configuration. If your organisation already uses Sentinel, we can provide a service where we will review and offer remediation to take your Sentinel to its optimal configuration, so that it can reach its operational potential.
- Cloud Architectural Services – we provide advice on optimisation, cost control, performance enhancements, security improvements and service resilience. We develop high-level and low-level designs

based on a ‘well architected’ theme for new or re-architected uses of public cloud and we deploy and test them to your chosen platform using infrastructure as code.

3.3 Cloud Resell & Support

- Cloud Managed Services:
    - Managed AWS – we resell AWS and provide the day-to-day management and support for your AWS deployments.
    - Managed Azure – we resell Microsoft Azure and provide the day-to-day management and support for your Azure deployments.
- Managed Microsoft 365 – we resell Microsoft 365, help to optimise your use of Microsoft licencing, maintain a secure environment and ensure that you always have access to Microsoft Premier Support when you need it.

3.4 Connectivity & Security

- Janet Cloud Connect – we provide high-capacity, resilient and secure access to AWS, Microsoft and Google via the Janet Network
- Govroam – we provide public sector staff with seamless access to roaming connectivity at participating sites across the UK.
- Cloud Web Application Firewall (WAF) – we provide DDoS mitigation and Web Application Firewall (WAF) protection for your public-facing websites.

At every step of every engagement, we aim to transfer our knowledge and skills to you because, by doing so, we will have a greater impact on society and become trusted and long-term allies. Our ultimate intention with all our services is to empower education, public and third sector organisations to become digitally independent.