vysiion™

AN EXPONENTIAL-E GROUP COMPANY

OT SOC WITH THREAT DETECTION, VULNERABILITY MANAGEMENT AND REMEDIATION – Service Definition

RM1557.15 G-Cloud 15: Lot 3 – Cloud Support

ISO 9001 QUALITY MANAGEMENT

ISO 27001 INFORMATION SECURITY MANAGEMENT

ISO 14001 ENVIRONMENTAL MANAGEMENT

ISO 45001 HEALTH & SAFETY MANAGEMENT

HM Government G-Cloud

Crown Commercial Service Supplier

Constructionline Gold Member Verified Member

Cyber Essentials Certified Plus

SafeContractor Approved

Audited RISQS

Achilles UVDB Verified

Contents

Service

Service Type

Lot 3: Cloud Support

Service Name

OT SOC with Threat Detection, Vulnerability Management and Remediation

Service Description

Vysiion provides a managed service for Operational Technology (OT) risk management covering vulnerability assessment, threat detection, and coordinated remediation.

We use sector-leading platforms, such as Dragos, for continuous OT asset discovery and network mapping, identifying all ICS/SCADA, DCS, and PLC assets across client networks.

Vulnerabilities are detected through automated scanning, correlation with global threat intelligence and advisories, and in-depth analysis by accredited OT cyber security specialists.

The service covers continuous monitoring for known and emerging cyber threats, including malware, unauthorised device activity, lateral movement, and protocol anomalies unique to OT.

When a threat or vulnerability is identified, our analysts deliver clear, prioritised reports outlining impact, risk ranking, and remedial actions, tailored for industrial environments.

Vysiion supports remediation, working with client teams or technical contacts to review, advise, and manage the safe application of patches, configuration changes, or network segmentation, respecting operational constraints and industry safety standards.

All detection and mitigation activities align with industry frameworks, including IEC 62443, NIST 800-82, and NCSC guidance, supporting sector and regulatory compliance.

We produce service and incident reports for operational and management teams, track remediation progress, and hold regular review meetings to update on threat trends, vulnerabilities, and compliance status.

Service Features and Benefits

Key Features

- Automated asset inventory and network mapping
- Vulnerability and threat detection with real-time alerts
- Prioritised remediation action plans with OT-specific guidance
- Direct support and consultancy from OT cyber security specialists
- Compliance-aligned service processes and reporting
- Scheduled review meetings and ongoing risk tracking.

Key Benefits

The service reduces risk, increases visibility, and strengthens resilience for OT asset owners in regulated and safety-critical environments.

Service Constraints

Does your service have any constraints that buyers should know about?

- **Role-Based Access Controls**: Access to both internal and customer-managed systems is restricted based on the principle of "need-to-know". Strong controls, including multi-factor authentication, are enforced to ensure security
- **SLA Variability**: Service Level Agreements (SLAs) vary depending on the types of assets or platforms supported and their criticality. Response times for issues are categorised by priority levels (e.g., P1 for critical services down, P2 for major degradation, etc.)
- **Customer Governance Framework**: For customer-managed systems, security events are addressed under the customer's governance framework and contractual terms. Vysiion acts as a supporting service provider, adhering to the agreed procedures for escalation and notification
- **Data Privacy and Security**: All data is encrypted using AES-256 at rest and TLS 1.3 in transit. Access is strictly controlled and audited. Vysiion follows ISO27001, ISO9001, and Cyber Essentials Plus, ensuring compliance and data protection
- **Vulnerability Management**: Patching and vulnerability management are governed by ITIL-aligned processes. Critical updates are applied within agreed maintenance windows following formal risk assessments and change approvals
- **Physical and Logical Separation**: For hosting environments, strict separation of client environments is maintained, with optional secure integrations. Physical security measures include biometric access and multi-layered monitoring.

Supplier Type

Vysiion will be carrying out the main delivery of services, with support from our Vulnerability and IDS.

Service Levels

For incidents logged to the CSOC by the Customer, the priority can be set by the Customer acting reasonably in line with the below definitions, when logging the incident, via either email or telephone.

Severity Level	Description
S1	A critical business service is non-operational impacting the Customer organisation, multiple users or multiple sites; or severe functional error or degradation of service affecting production, demanding immediate attention. Business risk is high, with immediate financial, legal or reputational impact.
S2	The Customer is experiencing failure or performance degradation that severely impairs operation of a critical business service; or the Customer or service has been affected, although a workaround may exist; or application functionality is lost; or significant number of users or major site is affected. Business risk is high.
S3	The Customer is experiencing a problem that causes moderate business impact. The impact is limited to a user or a small site; or incident has moderate, not widespread impact; or the Customer or IT service may not have been affected. Business risk is low.
S4	Standard service request (e.g. User Guidance); or updating documentation. Low or Minor localised impact.

User Support

Vysiion understands the necessity of ensuring the uptime and availability of your cloud services. For complete peace of mind, Vysiion's Support Desk provides a fully managed 24/7/365 Cloud Connectivity Monitoring service for all your cloud services. We provide bespoke levels of support packages to suit your business needs.

Our Cloud Connectivity Monitoring Service enables you to extend your existing IT services without increasing your headcount, removing the significant expense of customers setting up their own internal Support Desk provision.

- **Alert**: our Support Desk utilises the most advanced event detection to proactively monitor our customers' infrastructures 24/7/365, raising alerts when pre-defined thresholds are met. The Support Desk's monitoring and alerting systems are configured to each customer's requirements. Alerts will either be passed directly to the customer's service team or integrated with our own service management tool, triggering the ITIL aligned Event and Incident Management processes as appropriate
- **Inform:** our Support Desk team provides customers with information on Capacity and Performance, as well as access to the Vysiion online portal. Here, customers can retrieve real time monitoring data, ticket status updates and allows them to track the progress of any Incidents online
- **Resolve:** when an Incident arises, the Support Desk team resolves or escalates to the relevant Vysiion/customer Resolver groups or third-party suppliers. In all cases, the Vysiion team will manage the Incident until it has been resolved to the customer's satisfaction, and the ticket closed.

The Vysiion Support Desk provides the focal point for proactive and reactive network activities 24/7/365 including monitoring, performance tuning, software distribution and updating, router and domain name management, and coordination with affiliated networks.

Connecting to your infrastructure securely and seamlessly, our Support Desk uses industry leading monitoring tools to provide detailed metrics and visibility.

Support Methods

Vysiion provides multiple contact methods from its 24/7/365 Service Desk, ensuring accessibility and efficient support for its customers. These methods include:

- **Email**: Customers can report incidents or raise support requests by emailing *servicedesk@vysiion.co.uk*. This ensures a clear and traceable communication route for managing support needs
- **Phone**: A dedicated support telephone line is available 24/7, allowing customers to speak directly with Vysiion experts. This ensures immediate response for critical issues
- **Support Portal (Ticketing System):** Vysiion utilises an ITIL-aligned Service Management Platform, ServiceNow, branded as the Service Centre, accessible through an online portal. Customers can log incidents, submit service requests, and monitor ticket progression. The Service Centre is configured to align with specific service levels and KPIs, ensuring efficient workflows and consistent communication
- **Onsite Support:** Vysiion provides robust onsite support through its Smart Hands solution, delivering 24/7/365 assistance via SC-cleared engineers. These engineers handle a range of activities such as remote IT infrastructure management, equipment troubleshooting, installation services, and maintenance tasks. With formal Service Level Agreements (SLAs) tailored to individual requirements, we ensure rapid response times, including the ability to be onsite within 15 minutes. This ensures efficient and secure operations for organisations across high-compliance sectors.

Support Levels

Vysiion provides multiple levels of support tailored to meet specific customer requirements. These levels include:

- **Standard Support**: Covers basic operational support such as incident management, proactive monitoring, and maintenance activities during defined working hours, typically 08:00–18:00 on weekdays
- **Enhanced Support**: Includes 24/7 support for incident resolution, proactive monitoring, and escalations to ensure critical systems remain operational
- **Customised Support**: Tailored packages designed in collaboration with customers to meet unique business needs, including managed services, system administration, and application support.

Cost of Support Levels

The cost of support services varies based on the level selected:

- **Standard Support**: Included in the base service agreement if within predefined thresholds. Any additional requests are charged per the agreed rate card
- **Enhanced Support**: Fees are typically based on 24/7 availability and include time-related charges for on-site support, along with travel and subsistence costs
- **Customised Support**: Bespoke pricing based on the scope of requirements, based on a per unit per day for consultancy and tailored support.

Technical Account Manager or Cloud Support Engineer

- Vysiion provides **dedicated Account Managers** such as a Service Delivery Manager (SDM) and Sales Account Manager. The SDM ensures service reviews, reporting, and escalations are handled effectively, while the Sales Account Manager oversees additional service discussions
- **Cloud Support Engineers** are available as part of enhanced operational support packages. Their responsibilities include managing Microsoft public cloud environments, monitoring, troubleshooting, and maintaining security configurations.

Security Clearance

Vysiion's employees are screened to the Baseline Personnel Security Standard (BPSS) as a minimum, with many holding Non-Police Personnel Vetting (NPPV) Level 3 or Security Check (SC), and a subset holding Developed Vetting (DV). Vetting is conducted by Warwickshire Police under NPPV procedures and includes identity verification, BPSS checks, internal records checks, security questionnaires, criminal record checks, credit reference checks, and security service checks.

Our pre-employment screening covers the core control areas specified in BS7858:2019 by performing identity verification, criminal record checks, credit checks, and security service checks through the NPPV process, and we retain auditable records of screening and approvals within our ISO 27001 Information Security Management System. All staff undergo BPSS/NSV screening prior to employment, with additional clearances granted based on role and access to customer data and assets. All operational staff are vetted and cleared to work in high-security environments, enabling on-site delivery for Defence, Blue Light, and CNI customers.

We operate at scale with an Operations team of around 80 people; 26 are responsible for Secure Operations and Support and all hold security clearances. This provides assured 24/7/365 service coverage in restricted environments and an auditable trail for starters, movers, and leavers to manage access across systems and locations.

Why Vysiion?

Vysiion provides integrated turnkey solutions, delivering critical infrastructure and comprehensive managed services into a broad range of sectors including central government, utilities, defence, and the emergency services.

Our customers have come to rely on us for the delivery of Critical National Infrastructure (CPNI) and business systems alike ranging from WAN and Operational Networks, Fibre and Cabling in the field and datacentre, to Cloud, Managed Services and consultancy for IT networks and Infrastructure for the delivery of key applications and compute environments.

Having built a reputation in delivering and supporting critical infrastructure (communications and IT), over the past 30 years, through a combination of organic and acquisitive growth, Vysiion has built on this foundation and undergone a period of accelerated growth. This culminated in Vysiion becoming an 'Exponential-e Group Company' following the acquisition of all Vysiion shareholding in February 2020.

Vysiion and the Exponential-e group have a combined annual turnover of c.£200m, employing 850+ staff, and are recognised as one of the fastest growing private companies in the UK. We are a Customer First organisation, committed to the delivery of customer service excellence, demonstrated by 99% of customers renewing annually and a sector leading NPS score of 88.

The Group provides customers with a variety of IT managed services, leveraging Exponential-e's core network infrastructure to provide a backbone of network connectivity services, with additional/standalone Cloud, Communications, Infrastructure, Security & Managed Services. By leveraging group resources and expertise, Vysiion ensures its clients receive best-in-class service.

Proven Expertise

Vysiion is a trusted provider of cloud solutions with proven expertise in delivering tailored, secure, and scalable cloud deployments across a wide range of sectors including central and local government, utilities, defence, and emergency services. Our solutions are designed to meet the unique requirements of enterprise-level organisations, providing the foundation for seamless digital transformation and operational efficiency.

Vysiion offers a full suite of cloud services, including Public Cloud, Private Cloud, and Hybrid Cloud solutions. These services are designed to optimise performance, scalability, and security, ensuring organisations can transition their workloads to the cloud with confidence. Our team works closely with clients to design bespoke solutions tailored to their goals, compliance requirements, and existing infrastructure.

Vysiion specialises in designing and managing cloud environments for sectors with complex requirements, including CNI, Defence, and Central Government. Our solutions provide isolated development environments optimised for testing, development, and production, ensuring security and compliance are always maintained.

Experience

Vysiion's combination of industry expertise, robust methodology, and strong vendor partnerships makes us the ideal choice for organisations seeking reliable and efficient cloud services. Our cloud solutions are designed to maximise cost savings and scalability. By utilising intelligent automation, we deliver faster deployments and ensure organisations can scale resources up or down based on changing demands, reducing operational overheads and improving efficiency.

A range of G-Cloud services and complementary capabilities are available from Vysiion. These can be procured alongside this service to support an organisation's transition towards more commodity-based ICT.

Partnerships with Leading Providers

We have established strategic partnerships with key vendors such as Microsoft Azure, AWS, VMware, Cisco, and Ark Data Centres. These partnerships allow us to leverage cutting-edge technologies to deliver robust cloud environments that meet the stringent compliance and security standards required for enterprise applications.

Robust Security and Accreditation

Vysiion demonstrates robust capabilities in delivering secure cloud solutions, ensuring compliance and accreditation with industry-recognised standards. Our cloud solutions are built on stringent security frameworks, including ISO 27001, Cyber Essentials, Cyber Essentials Plus, and ISA/IEC 62443 certifications. These certifications confirm Vysiion's commitment to maintaining high standards in information security management systems and mitigating vulnerabilities in critical infrastructure design and operation. Vysiion also adheres to the NCSC's Cyber Assessment Framework (CAF) and Secure by Design principles, ensuring the comprehensive protection of customer infrastructures from cyber threats and unauthorised access.

We integrate security as a fundamental aspect during the design phase of business applications. A 'Secure by Design' approach ensures infrastructure and assets are protected from initial concept through ongoing operations, validated against applicable regulatory frameworks. This includes proactive measures informed by the latest threat intelligence to mitigate risks across IT and OT environments. Access controls such as multi-factor authentication and role-based permissions further enhance the security of internal systems used in pre-sale, design, delivery, and support processes.

Vysiion employs security-cleared engineers and operates a UK-based Cyber Security Operations Centre (CSOC) that provides 24/7 real-time security monitoring and alerting services. This approach ensures organisational cyber resilience and minimises risks associated with cybercrime. Additionally, Vysiion engages CREST-approved third-party vendors for penetration testing to validate the security of IT infrastructures.

Hosting solutions are delivered through Tier 3+ Data Centres, offering high levels of physical and cyber security. These data centres are equipped with multi-layered security measures, biometric access controls, and environmental monitoring systems, ensuring compliance with Cabinet Office and NCSC standards.

Our Accreditations

We support the security and compliance standards of the Public Sector by embedding our compliance certifications into our Business Management Systems. These include:

- ✓ **ISO9001 -** Quality Management
- ✓ **ISO2000 -** IT Service Management
- ✓ **ISO27001 -** Information Security
- ✓ **ISO14001 -** Environmental Management
- ✓ **ISO45001 -** Health & Safety Management
- ✓ **Cyber Essentials Plus**