vysiion™

AN EXPONENTIAL-E GROUP COMPANY

MICROSOFT SENTINEL CSOC SERVICE – 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

Microsoft Sentinel CSOC Service

Service Description

Vysiion Microsoft Sentinel Cyber Security Operations Centre Services (Microsoft Sentinel CSOC Service/s) comprises of the Service packages detailed in the 'The Cyber Security Operations Centre Services Packages' section below and will be provided by Vysiion from its Cyber Security Operations Centre (CSOC).
The Security Information and Event Management (SIEM) used for this Service is Microsoft Sentinel. The Order Form will set out the number of committed security incidents per instance covered by the Charges for that instance on the Order Form. Any incidents beyond the committed number of security incidents set out in the Order Form will be at additional charge to the Customer and be invoiced monthly in arrears in accordance with the then current Rate Card (available upon request from sales@vysiion.co.uk).
A Statement of Work (SoW) will support each engagement. The SoW contains the timescales for deliverables (such as reports or system outputs and analysis), and any target service level for monitoring the Services. Once signed by both Parties, the SoW is deemed to form part of the Contract. The definition of Contract in the General Terms shall therefore be considered amended accordingly. In the provision of all Microsoft Sentinel CSOC Services, Vysiion acts as a consultant providing advice to the Customer in relation to the security of its estate. Vysiion will not be liable for any failure to meet any target service levels where such failure arises as a direct or indirect result of changes which the Customer may implement. Changes made by the Customer are made at the Customer's sole risk. It is the Customer's responsibility to qualify the impact of any potential change and to satisfy itself that the change is required, actionable and supportable for the security of its estate.
Microsoft Sentinel licensing is not part of this Service. The Customer must bring the Microsoft Sentinel Licensing. This can be purchased through Vysiion or another Microsoft Cloud Service Provider.

On boarding and Engagement

Vysiion will collect all the relevant information to create the SoW for each Microsoft Sentinel instance (an instance is the deployment by Vysiion of the Customer's Microsoft Sentinel licensing connected to an Azure Log Analytics workspace, each instance would require a separate workspace). Once the Customer has accepted the SoW, the provision of Microsoft Sentinel CSOC Service will begin and it will be considered complete when the Microsoft Sentinel instance receives its first log. The number of Microsoft Sentinel instances and associated components deployed in respect of the Customer will depend on the number of assets to be monitored and the quantity of zones (i.e. whether the Customer's servers are located in more than one location namely; Azure, AWS and at data centres). The number of Microsoft Sentinel instances to be deployed will be set out on the Order Form.
As per above, the Service Commencement Date is deemed to have occurred in relation to the Microsoft Sentinel CSOC Service once the first log is ingested/collected by the Microsoft Sentinel instance. Where servers are included in the scope (as detailed within the SoW), a Windows Agent will need to be deployed on any Microsoft server, in order to enable SIEM

logging and monitoring, by the Customer unless Vysiion is managing that Microsoft server as part of a Flex Manage Service. Devices such as firewalls that generate syslog, as well as other solutions that might provide an API integration, may require additional servers to facilitate log collection. Vysiion will also set out in the SoW the agreed list of activities for each Party for the alerts that are detected. The Customer will be provided with credentials to have a read-only view of the Microsoft Sentinel instance on the Azure portal. In the event that following on boarding there is an alert, CSOC will respond to the Customer as agreed in the SoW, subject always to the severity of the incident monitored. The Parties will also discuss on a weekly basis during the on-boarding stage, at a time agreed between the Parties, the output logs and the variations which occur in the logs. CSOC will refine and tune these output logs throughout the on boarding stage. During the course of the engagement and at a time agreed with the Customer and no more than on a quarterly basis, a CSOC engineer will have a telephone discussion with the technical contact of the Customer to discuss the technical operation of the Service. If during the engagement, a monitored asset which forms part of another service which Vysiion is providing to the Customer has a fault, CSOC will notify the Customer and the relevant Vysiion support team who will then liaise with the Customer as set out in the applicable Service Document for the affected Vysiion service.

The Cyber Security Operations Centre Services Packages

a) Security Incident and Event Monitoring (SIEM)

The SIEM consists of at least one Microsoft Sentinel instance. This instance will collect log information from the Customer's monitored assets. This provides a view via the Azure portal of the Customer's assets within scope of the SoW. The Microsoft Sentinel instance is deployed in the Customer's Microsoft Azure public cloud environment. Azure resources are not part of this Service. The Customer must bring the required Azure resources. This can be purchased through Vysiion or another Microsoft Cloud Service Provider.
The Customer acknowledges and accepts that any failure on its part to allow for the installation of Microsoft Sentinel instance and the required alerting and monitoring components for the integration with Vysiion systems will result in none of its assets being monitored by Vysiion.

b) Threat Detection

Vysiion will alert and monitor the Customer's estate for triggered threats. This is a service consisting of a deployed Microsoft Sentinel instance and the proactive monitoring of the Customer's estate, as defined in the SoW, on a 24x7x365 basis. The result of the monitoring consists of ServiceNow cases, available on the dashboard, flagged with the respective severity level (S1-S4). CSOC will provide the Customer with further intelligence via ServiceNow case about the incident in order to support remediation.

Service Features and Benefits

Key Features

- 24/7/365 in-house UK-based Cyber Security Operations Centre (CSOC) staffed by certified security analysts, engineers, architects, and consultants.
- Integration with Microsoft Sentinel for Security Incident and Event Monitoring (SIEM).
- Aggregates, monitors, and analyses logs and telemetry from Azure, on-premises, and third-party sources.
- Proactive threat detection and real-time incident response, triaged and actioned by the CSOC team.

- Automated ticketing and case management using ServiceNow, with incidents flagged according to severity and tracked on a dashboard.
- Use of custom analytics rules, playbooks, and integration of threat intelligence tools to enhance detection and automate response.
- Access via Azure Lighthouse with role-based access control, enforcing the principle of least privilege.
- Regular review and tuning of analytics rules for evolving protection needs.
- Change management support for notifications or addition of new monitored devices, following structured procedures and agreed Service Level Agreements (SLA).
- Compliance processes aligned with industry standards such as NIST Cybersecurity Framework, NCSC guidelines, PCI-DSS, ISO 27001, and Cyber Essentials Plus.
- Reporting and customer access provided via the Azure portal and dashboards.

Key Benefits

- Rapid incident response and resolution from a single point of contact, reducing dwell time and minimising impact of cyber threats.
- Continuous, real-time protection and monitoring ensure early threat detection and mitigation.
- Holistic view and correlation of signals across endpoints, identities, and workloads, providing integrated threat intelligence and improved security posture.
- Fully managed and automated processes reduce the burden on internal IT teams, who can view incident status and reporting in real time.
- Ongoing optimisation of defence through regular rule review and compliance enforcement.
- Policy-driven, automated response enables swift isolation and remediation of threats, including automated containment and rollback for ransomware events.
- Operated entirely in-house, ensuring service quality and direct accountability without reliance on outsourced security functions.
- Helps customers maintain and demonstrate compliance with regulatory and industry standards.
- Scalable service supporting assets of varying size, geography, and manufacturer.
- Supports integration with both Microsoft and non-Microsoft assets already in operation.

The service combines continuous monitoring, automated and manual threat management, and compliance-driven processes to protect and manage risk across mixed and complex estates.

Service Constraints

- *Customer-provided Licensing*: The customer must supply Microsoft Sentinel licences. These are not included in the service and must be purchased directly, either through Exponential-e or another Microsoft Cloud Service Provider.
- *Scope and Limits Defined by Order Form*: The number of committed security incidents covered is specified in the Order Form. Incidents over this limit incur extra charges, invoiced monthly in arrears.

- *Statement of Work (SoW)*: Each engagement is governed by an SoW detailing deliverable timescales, monitoring targets, and defined activities for each party. The SoW becomes part of the contract once signed.
- *Consultancy Role and Liability*: Exponential-e acts as a consultant and provides advice. It is not responsible for missed service targets caused directly or indirectly by customer-initiated changes. These changes are at the customer's sole risk.
- *Service Commencement*: Service is considered to have started when the first log is ingested by the Sentinel instance.

Supplier Type

Vysiion will be carrying out all services through Vysiion resource. No services will be sub-contracted.

Service Levels

Exponential-e will use reasonable endeavours to notify the Customer of an alarm raised by the Customer asset within 60 minutes of receiving such alarm.

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**