vysiion™

AN EXPONENTIAL-E GROUP COMPANY

MANAGED CSOC SERVICES – AlienVault 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

Managed CSOC Services - AlienVault

Service Description

Vysiion Cyber Security Operations Centre Services comprise of all of the Service packages detailed in *The Cyber Security Operations Centre Services Packages* section detailed below and will be provided by Vysiion from its Cyber Security Operations Centre (CSOC).

The Order Form will set out (i) the number of USM virtual sensors to be deployed (ii) the number of days' worth of log the Cloud Unified Security Manager system ("USM System") will collect, store (subject to contracted capacity) and accordingly how many days of log the Customer is able to view at any given time and (iii) the maximum storage capacity for the USM System. The options for (ii) above available are:

- Essentials Option: 15 days of logs will be collected and stored (subject to contracted capacity) by the USM System for viewing
- Standard Option: 30 days of logs will be collected and stored (subject to contracted capacity) by the USM System for viewing
- Premium Option: 90 days of logs will be collected and stored (subject to contracted capacity) by the USM System for viewing.

It is the Customer's responsibility to determine which of the options above and what maximum storage capacity it requires taking into account its IT environment including any requirements mandated by its Compliance department. Vysiion will assist the Customer in deciding which option to select and an appropriate maximum storage capacity but this is conditional on the Customer acknowledging and accepting that Vysiion used information provided by the Customer during due diligence as the basis for calculating the amount of storage required for the Customer's USM System. This included data such as the amount of assets which require monitoring, the number of users and possible applications being used by such users (example EDR's, Office365 accounts, InTunes MDM's etc).

Vysiion makes use of known averages per asset type and user activity. The Customer therefore accepts that any less "mature" environment in terms of application configuration, user abuse or external nefarious activity (DDoS for example) may cause the initial scoping storage requirements to require review and an upgrade.

Notwithstanding that the Customer has pre-selected an option and maximum storage capacity on the Order Form, it is possible for the Customer to exceed the storage limit of that pre-selected option for the following non-exhaustive reasons: misconfiguration, where there is an introduction of non-scoped equipment and/or influx of new users to the environment. In the event that storage limit is exceeded, it may result in the following:

a) The system not storing event data. Event data will not be stored until the beginning of next chosen option (15 days, month or quarter). At the Customer's request, Vysiion may filter some of the additional log sources. However, by doing so, the Customer accepts that this may result in the loss of visibility over its relevant data.

b) The USM System no longer storing events in the searchable data store, but it will continue to generate alarms, run authenticated asset scans and store raw logs associated with events in cold storage (logs collected and stored in the last 365 days). However, by not having immediately searchable and available logs under the

stored events menu, the Customer may be in breach of its own or any other Compliance rules it is required to adhere to. The Customer accepts responsibility for any such breach.

A Statement of Work (SoW) will support each engagement. The SoW contains the timescales for deliverables (such as reports or system outputs and analysis), any target service level for monitoring the Services and the web reporting portals to be used. 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 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.

On boarding and Engagement

Vysiion will collect all the relevant information to create the SoW. Once the Customer has accepted the SoW, the provision of the USM System and the deployment of the scoped USM virtual sensor(s) will begin and be considered complete when the USM System receives its first log. The number of USM virtual sensor(s) deployed in respect of a 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). Additional Charges apply in respect of each additional USM virtual senor to be deployed.

The Service Commencement Date is deemed to have occurred in relation to the CSOC Service once the first log is ingested/collected by the USM System. A NXLog collection tool will need to be deployed on any Microsoft server in order to enable logging and monitoring by the SIEM 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 will not require the agent. The log/syslog information will also be aggregated, correlated and processed by the USM System. Vysiion will also set out in the SoW the agreed list of activities for each Party for the "flags" that are detected.

The Customer will be provided with credentials to have a "read only" view of the USM System. In the event that following on boarding there is a "flag", 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.

Throughout the engagement, the outcome of the initial scan report will be discussed with the Customer so that the Customer has the opportunity to ask questions in relation to that report. If any remedial actions are advised, it is the Customer's responsibility to propose (working with the CSOC) how it wishes to remediate the issues. During the course of the engagement and at a time agreed with the Customer and on no more than 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

Security Incident and Event Monitoring (SIEM)

The SIEM consists of at least one USM virtual sensor. This USM virtual sensor will collect log information from the Customer's monitored assets. This provides a view via a web-based portal of the whole of the Customer's estate within scope of the SoW. The USM virtual sensor can be deployed in public cloud environment, private cloud or using a physical server.

For public cloud deployments, the Customer shall be responsible for the installation of the SIEM in their instance.

For private cloud deployments, the responsibility for the installation shall be on the entity responsible for management of the cloud platform.

For physical server deployments, Vysiion will provide a pre-configured server, the responsibility for plugging and providing connectivity to such server will be the Customer's responsibility (and/or any 3rd party employed by the Customer to manage its infrastructure).

The Customer acknowledges and accepts that any failure: (a) on its part to install the SIEM (b) on the part of the entity responsible for managing the private cloud deployment to install the SIEM; and/or (c) on its part or any third party employed by it to plug in the pre-configured server and provide connectivity to such server will result in none of its assets being monitored by Vysiion.

Threat Detection

Vysiion will alert and monitor the Customer's estate for triggered threats. This is a service consisting of a deployed USM sensor 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 a web-accessed dashboard, which highlights alerts on a red, orange and green (RAG) priority basis. CSOC will provide the Customer with further intelligence via email-ticket about the incident in order to support remediation.

Internal Vulnerability Monitoring

Vysiion will provide vulnerability scans of the Customer's estate, as defined in the SoW. This Service consists of a deployed USM virtual sensor and the proactive testing of the Customer's monitored estate on a once per month basis. The result of the monitoring and testing consists of a web-accessed dashboard with a report on the testing schedule, which is highlighted on a red, amber and green (RAG) priority basis. CSOC will assist the Customer or third party responsible for the management of the estate in establishing the remediation action to take in all cases.

Monitored Compliance

This offers a managed platform that monitors the status of the Customer's estate compliance based on the Customer's elected compliance standard controls and any detected events and threats on a 24x7 x365 basis. The alert will notify the Customer of industry best practice to follow in order to maintain the security of their estate to their elected compliance standard. The Customer will also be notified as part of this package of actions to undertake in order to protect against the particular threat or incident that has been detected. Vysiion will use its reasonable endeavours to provide the Customer with a monthly report and a supporting call to explain any technical issues in greater detail. The Customer will also be supplied with credentials to enable the Customer to log in to a web-based portal in order to obtain further information on the status of its estate compliance.

CSOC Service Demarcation Point (SDP)

The Customer will be responsible for the hosting of a USM virtual sensor at its Site(s) or datacentre space and the required network configuration to ensure that the USM System can communicate with the managed platform.

The SDP is the supplied USM System. This will be the point up to which Vysiion has responsibility.

Change Management

Changes requested will be limited to a change of priority notification or change of monitored devices and will only be carried out during Normal Business Hours. In the case that a new device type is introduced to the CSOC Service, the CSOC won't be required to ensure that any agreed SLA of alerts, stated in the SoW, are met until a pre-agreed tuning period is completed, during this time the Customer will regress to a Staging period instead of a Live status. Staging period being the period during which Vysiion will monitor the SIEM to understand what changes, if any, is required to the CSOC Service before handover. The Customer is not entitled to any Service Credits for any failure by Vysiion to meet the Service Level Agreement during the Staging period.

Access and Reporting

The USM System enables read-only access to the SIEM so that the Customer can obtain further information on a particular incident. The reports obtained following a vulnerability scan shall be shared with Customer via an agreed method.

Service Features and Benefits

Key Features

- 24/7 x 365 monitoring
- Reporting
- Case management
- Threat detection and response
- Playbooks
- Behavioural Monitoring
- SaaS based Model

Key Benefits

- Continuous monitoring enables businesses to respond to threats as and when they are identified
- Giving the customer full visibility of their reports as well as analytical information to give a clear indication of their threat levels
- Linking alarms, events, notes, and other files to their responses, to have a complete view for investigating and managing security incidents
- This provides visibility into attacks that may not trigger traditional prevention rules, whilst reducing costs that will be used in having a dedicated endpoint solution
- Allows to accelerate threat detection and incident response process by streamlining and automating common or alarmspecific workflows.
- Uses machine learning to observe specific types of behaviours over a period of time to determine a baseline and then identify suspicious behaviour and potentially compromised systems.
- This allows the business to save money as there is a lower TCO, and IT teams no longer must focus on updates and maintenance.

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

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.

Target Availability

Service	Target Availability
Cyber Security Operations Centre Services - Customer Portal	99.9%

Service Credits

		Service Credit*
Measure	>0.1 below Target	10%

The Service Credit is applied as a percentage of the Monthly Charge for the CSOC Service where the Customer portal is not available.

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**