vorboss

G-Cloud 15 Service Definition

Managed Security Service

Lot 3 Cloud Support

Vorboss Limited is registered in England and Wales at: 10 Exchange Square, London, United Kingdom, EC2A 2BR
Company number: 05678571

vorboss

Contents

vorboss

1. About Vorboss

1.1. Company overview

Vorboss Limited is a London-based telecoms provider building a dedicated, business-only full-fibre network designed to meet the performance and reliability needs of modern organisations. Vorboss delivers 10 Gbit/s connectivity as standard, with bandwidth scalability up to 100 Gbit/s for customers requiring higher capacity to support cloud adoption, data-intensive workloads, multi-site operations, and business-critical services.

Owned by Fern Trading (managed by Octopus Investments), Vorboss works with both enterprise and SME customers, providing secure, scalable connectivity and supporting services that help organisations modernise and simplify their IT and network estates. Alongside fibre connectivity, Vorboss offers UK-wide delivery of managed IT, cybersecurity, and network services through Vorboss Managed Services and related business units. This enables customers to procure connectivity and operational support through a single supplier, with services that can be tailored from standalone components to fully managed solutions.

Vorboss' approach is focused on business outcomes: high-capacity connectivity, operational resilience, and security-led service delivery aligned to customer requirements.

1.2. Value Proposition

Public sector organisations require strong cyber resilience to protect services, data, and users while maintaining continuity of service delivery. Many organisations face increasing exposure to threats such as phishing, credential compromise, ransomware, insider risk and supply chain vulnerabilities. At the same time, security teams are often required to manage growing alert volumes across endpoints, cloud services, SaaS applications and identity platforms, without the internal capacity to provide continuous oversight.

Common challenges include limited in-house security resources, inconsistent monitoring coverage, and reduced visibility of security posture and risk trends. These gaps can lead to delayed detection of malicious activity, inconsistent incident handling, and limited evidence to support governance and compliance expectations.

Vorboss Managed Security Service provides structured security operations and security assurance designed to reduce cyber risk and strengthen operational confidence. The service includes 24/7 monitoring and response options (tier dependent), security event correlation, structured incident triage and escalation, guided investigation and containment actions where applicable, and security reporting to support governance and continual improvement.

The service supports public sector buyers to:

- Reduce risk through proactive oversight and threat detection
- Improve response speed and consistency through structured security incident handling

- Strengthen operational assurance through monitoring, reporting and service review (where applicable)
- Support compliance expectations through improved controls, evidence and security hygiene outcomes
- Deliver measurable outcomes aligned to agreed priorities and service levels

1.3. What the Service Provides

Vorboss provides a Managed Security Service delivered by a UK-based team, including an in-house London-based Security Operations Centre (SOC) for monitoring and response. The service supports public sector buyers by providing consistent security operations processes for continuous monitoring, alert triage, investigation, escalation, and improvement activity. This helps organisations maintain effective security oversight and respond to threats quickly, without needing to build and operate an internal 24/7 SOC function.

The service is designed to support organisations that require improved visibility of cyber risk, faster identification of suspicious activity, and structured response handling aligned to service priorities. Service scope is agreed during onboarding and documented within the Order Form.

The service includes (scope dependent):

- 24/7 security monitoring and alerting (tier dependent)
  Continuous monitoring of security signals and alerts to support early detection of suspicious behaviour and potential threats.
- Threat detection using SIEM/SOAR-aligned tooling and detection content
  Detection capabilities using security monitoring platforms, correlation rules and automated workflows (where applicable) to improve signal quality and reduce time to response.
- Security incident triage, escalation and response coordination
  Structured handling of suspected security incidents, including prioritisation, escalation routes and coordination of response actions with buyer stakeholders.
- Investigation support and guided containment actions (tier dependent)
  Investigation and response support to help confirm impact, identify affected users/systems, and guide containment actions where appropriate.
- Security reporting and service review (where applicable)
  Reporting that supports governance and service oversight, including incident trends, response activity and improvement opportunities over time.
- Optional security assurance services aligned to buyer needs
  Security assurance activities (such as cyber health checks and penetration testing) may be provided as associated services depending on buyer requirements

Overall, Vorboss IT Managed Service enables buyers to maintain consistent IT operations through a scalable support model, improved operational oversight, and service levels aligned to organisational needs.

1.4. Social Value

As part of delivering this service, Vorboss is committed to delivering meaningful social value outcomes aligned to the Public Services (Social Value) Act 2012. We take a long-term, responsible approach to service delivery that prioritises positive impact for people, communities, and customers - through fair work, inclusive employment practices, skills development, and a supportive workplace culture that enables individuals to thrive.

Vorboss is committed to creating and retaining high-quality jobs that are secure, supportive, and built for long-term progression, with a clear focus on widening access for people who may face barriers to entering the industry, such as those from disadvantaged backgrounds. Through our purpose built, in-house Vorboss Academy, we train technicians from scratch and provide a direct route into a high-growth, skills-shortage sector for individuals who may not have traditional entry pathways. Our approach combines ongoing training and mentoring with funded development budgets and structured secondments, giving colleagues meaningful opportunities to build experience, broaden their skills, and progress into more advanced roles over time.

We are deliberate in removing barriers and improving representation for under-represented groups, including women and ethnic minorities, through inclusive recruitment practices such as gender-neutral job adverts, unconscious bias training, and diverse interview panels. Alongside this, we support retention by investing in the everyday success of our people, ensuring they have the stability, development opportunities, and flexibility needed to thrive - helping us build a resilient workforce and deliver consistently high service standards for customers.

2. G-Cloud Service

2.1. Overview

Vorboss Managed Security Service provides structured security operations and security assurance services suitable for public sector environments requiring controlled processes, consistent security outcomes, and operational oversight. The service is designed to strengthen cyber resilience by improving detection capability, supporting structured incident handling, and enabling governance through reporting and service review.

The service supports buyers who require security monitoring and response capability without operating an internal 24/7 SOC function, and provides tiered service options aligned to organisational complexity, risk exposure, and monitoring requirements.

The service supports:

- Continuous monitoring and detection coverage (tier dependent)
  Monitoring is delivered using security event correlation and detection logic to identify

suspicious behaviour and potential threats across supported systems and in-scope data sources.

- Structured security incident triage, escalation and response
  Security incidents and alerts are handled through consistent triage processes, severity-driven prioritisation, and escalation routes aligned to agreed governance requirements.
- Improved visibility through reporting and governance review
  Where included, service reporting supports operational oversight and transparency, helping buyers understand alert volumes, incident trends, recurring risks, and improvement opportunities.
- Flexible monitoring scope aligned to the buyer environment
  The service can be aligned to the buyer's environment, including cloud, identity, endpoint, network and other sources where included and agreed, supporting a scalable approach to coverage.

2.2. Service Components

2.2.1. Managed Detection & Response (MDR) – Security Monitoring and Response

Managed Detection & Response (MDR) provides continuous monitoring and response services designed to identify, investigate, and respond to suspicious activity across the buyer environment. Vorboss delivers MDR using Microsoft Sentinel SIEM, supported by custom detection rules, automated playbooks (where applicable), and a London-based SOC that monitors and responds to threats on a 24/7 basis (tier dependent).

MDR supports buyers by:

- Improving visibility of security events across identity, endpoint and cloud environments
- Correlating alerts and signals to reduce noise and highlight genuine risk
- Supporting structured incident triage, escalation and response coordination
- Reducing time-to-detection and time-to-response through defined workflows and operational processes

Security incidents and suspicious activity are handled through a structured process, including alert review, triage, investigation, escalation to buyer stakeholders, and guided actions for containment and resolution where included within the selected tier.

2.2.2. MDR Service Tier Comparison (Core / Advanced)

Category	Core	Advanced
SIEM platform	Microsoft Sentinel (managed instance)	Microsoft Sentinel (dedicated or shared SIEM instance)
Log sources	Core cloud & identity logs (Entra / Google) + endpoint EDR	Unlimited log sources including firewalls, servers, cloud workloads, custom applications

Log types	Security and audit events	Full coverage (security, operational, endpoint telemetry)
Detection content	Vorboss-curated detection rules	Extended ruleset with custom detections tailored to the environment
Playbooks	Standard automated playbooks	Advanced automated playbooks + custom response paths
Threat intelligence	Included, standard feeds	Enhanced threat intelligence + contextual enrichment
Monitoring	24/7 monitoring from London-based SOC	24/7 monitoring with enhanced correlation and investigation depth
Response	Triage and notification	Full incident response: investigation, containment actions, guided response
Retention	90 days	Fully scalable retention options
Ideal for	SMEs without internal security IT/teams	Organisations with complex systems or regulated environments

Note: Exact scope (log sources, retention, response actions, escalation routes, and reporting cadence) is agreed during onboarding and documented within the Order Form.

2.2.3. Vulnerability & Patch Management (Protect)

Vorboss provides Vulnerability & Patch Management as part of the Managed Security Service to support improved security hygiene and reduce exposure to known vulnerabilities. The service focuses on identifying patch gaps, supporting structured update activity, and improving visibility of device compliance and exceptions over time.

This service is particularly relevant where buyers need to reduce cyber risk associated with outdated operating systems, delayed security updates, unsupported software versions, or inconsistent device patch levels across a distributed workforce.

Vulnerability & Patch Management may include (scope dependent)

- Patch monitoring and compliance oversight
  Monitoring patch status for managed devices and identifying devices that are not meeting agreed patch baselines.
- Automated update and patch deployment (where applicable)
  Supporting automated patching processes for operating systems and key applications where patching is within agreed scope.

- Exception handling and remediation support
  Identifying patch exceptions (e.g., devices offline, failed installs, compatibility constraints) and supporting prioritised remediation activity.
- Prioritisation of security updates
  Supporting prioritisation of patching activity based on risk, severity and operational impact, including high-risk security vulnerabilities where applicable.
- Reporting and service visibility (where applicable)
  Providing visibility of patch posture, patch success/failure trends, and outstanding risks to support governance and continual improvement.

Typical outcomes include:

- Reduced risk from missed patches and outdated systems
  Improved patch coverage helps reduce exposure to known exploits and common attack paths.
- Improved visibility of patch status and exceptions
  Buyers gain clearer insight into patch compliance levels, device posture, and remediation priorities.
- Reduced operational burden for internal teams
  Automated patch workflows and structured monitoring reduce manual effort and improve consistency of delivery.
- Improved baseline cyber hygiene over time
  More consistent patching reduces recurring vulnerabilities and improves overall device health and stability.

Note: Supported device types, patching cadence, update windows, and in-scope applications are agreed during onboarding and documented within the Order Form.

2.2.4. Cyber Health Check (Assess and Assure)

The Cyber Health Check is a structured assessment designed to provide buyers with a clear view of their current cybersecurity posture across people, process, and technology. It identifies strengths, gaps, and priority risks, and provides a practical improvement roadmap to support planning, investment decisions, and sequencing of security activity.

This service is intended to support organisations that need improved visibility of cyber maturity, assurance for leadership stakeholders, or evidence to support governance and compliance expectations.

The Cyber Health Check may include (scope dependent):

- Discovery and current-state review
  A review of the existing environment, security tooling, operating model, and high-level risk areas.

- People and process assessment
  Assessment of security roles, responsibilities, operational practices, escalation routes, and how security incidents are handled and managed.
- Technology control review
  Review of key technical security controls such as endpoint protection, identity security, MFA usage, logging and monitoring coverage, patching practices, and email security controls (where relevant).
- Security visibility and monitoring review

Identification of gaps in logging, alerting and monitoring coverage that may impact detection and response outcomes.

- Prioritised improvement roadmap
  A structured set of improvement actions, prioritised by risk and operational impact, supporting staged delivery and realistic implementation sequencing.

Pricing will be in accordance with the Vorboss Rate Card

Typical outcomes include:

- Clear understanding of current cyber posture and key risk areas
- Prioritised recommendations aligned to operational needs and resource constraints
- Improved ability to plan, budget and justify security improvements
- Better readiness for governance, assurance and compliance-driven requirements

Scope, methodology, and deliverables are agreed prior to commencement and documented within the Order Form.

Licensing Requirements (Where Applicable)

Some service components require third-party tooling and licensing (e.g., Microsoft, Proofpoint). Vorboss can supply and manage these licences as part of transition into the managed service or operate using buyer-provided licences where agreed. Final requirements are confirmed during onboarding and documented in the Order Form.

2.3. Service Levels

Operational Service Levels (Indicative)

Service Area	Coverage	P1	P2	P3	P4
MDR – Core	24x7x365	Mean Time to Respond 15 mins	Mean Time to Respond 15mins	Mean Time to Respond 60 mins	Mean time to Respond 60 mins

MDR – Advanced	24x7x365	Mean Time to Respond 15 mins	Mean Time to Respond 15mins	Mean Time to Respond 60 mins	Mean time to Respond 60 mins
Vulnerability & Patch Management	Business hours (as agreed)	Critical plan: 2 business days	High patching: 10 business days	Medium patching: 30 days	N/A

Project Delivery Timeframes (Associated Services – Indicative)

Associated Ser0vice	Delivery Model	Scheduling / Start	Output / Reporting
Cyber Health Check	Project-based	Kick-off scheduled within 10 business days	Draft report within 5 business days of assessment completion; Final report within 10 business days of buyer feedback
Penetration Testing	Project-based	Scope confirmed within 5 business days; Testing start within 15 business days (availability dependent)	Draft report within 5 business days of testing completion; Final report within 10 business days of buyer feedback

2.4. Reporting (where included)

- Monthly service reporting issued within 5 business days after month-end
- Priority incident summary (P1) issued within 2 business days of incident stabilisation
- Reporting format and cadence agreed during onboarding and confirmed in the Order Form

2.5. Associated Services (optional)

In addition to managed monitoring and response, Vorboss offers associated security services to support assurance, improvement planning, and risk reduction activity. These services are delivered as defined project-based engagements and can be used to complement the Managed Security Service or support standalone security assurance requirements.

Associated services may include:

Penetration Testing (Assess and Assure)

Independently delivered testing by accredited specialists to identify exploitable weaknesses and provide actionable remediation guidance. This supports assurance activity and helps buyers demonstrate security posture to stakeholders, auditors, and third parties.

Associated service scope, sequencing and deliverables are agreed prior to commencement and documented within the Order Form.

2.5.1. Cloud and Digital Transformation

Vorboss provides cloud and digital transformation services as to support structured modernisation and controlled change delivery. This associated service is designed for organisations that need to introduce new cloud capabilities, improve the performance or security of existing environments, or complete planned IT change activity with reduced operational risk.

These activities are delivered as defined pieces of work with agreed scope, sequencing and governance, and can be used to support continuous improvement of the buyer's IT and cloud environment alongside the ongoing IT Managed Service.

This may include:

- Microsoft 365 optimisation and hardening
  Configuration improvements to strengthen security, improve reliability, and support consistent operational outcomes across user services.
- Modern workplace solutions
  Enablement and enhancement of cloud-based collaboration and productivity platforms to support hybrid working and consistent user experience.
- M365 optimisation and security hardening
  Implementation of security-led configuration controls to reduce cyber risk, improve baseline protection, and align settings to buyer requirements.
- Teams telephony and licensing management
  Support for planned enablement, configuration and rollout of Teams telephony functionality, alongside licence oversight and operational readiness.
- Cloud and identity management
  Support for cloud identity configuration and management practices, including access control improvements and operational alignment for user access governance.
- Private / hybrid Azure cloud solutions
  Support for Azure-based cloud infrastructure requirements, including hybrid environments where buyers require integration between on-premise and cloud services.

Pricing will be in accordance with the Vorboss Rate Card.

2.6. Pricing

Pricing is provided separately and is typically offered as a per-user monthly contract, with a minimum contract term of 12 months for Core and Advanced service tiers.

Please refer to the Vorboss rate card/pricing for detailed pricing information

2.7. Data protection

2.7.1. Informational Assurance

Vorboss follows structured processes to support secure and reliable service delivery, including controls for information security, operational quality, environmental responsibility, and cyber resilience. These processes are designed to support the secure handling of customer information, protect managed devices and user accounts, and ensure that service delivery activities are carried out in a controlled and auditable manner.

Information assurance practices may include:

- Controlled access to systems and administrative functions, aligned to role-based responsibilities
- Secure operational processes for delivering remote support and managing incidents
- Service governance and documentation to support traceability of support activity
- Risk-aware working practices aligned to security and compliance expectations
- Continuous improvement through review of service performance and recurring issues (where applicable)

2.7.2. Accreditations and Certifications

- ISO 9001 – Quality Management Systems, supporting consistent delivery and service improvement
- ISO 14001 – Environmental Management Systems, supporting responsible operational practices
- ISO 22301 – Business Continuity Management Systems
- ISO 27001 – Information Security Management Systems, supporting structured security controls and governance
- ISO 45001 – Occupational health and Safety Management Systems
- Cyber Essentials Plus – Independently tested cyber security controls to help protect against common cyber threats

2.7.3. Data Back-Up and Restoration (Of the service)

Vorboss maintains backup and restoration procedures to support continuity of service delivery and protect the operational data required to deliver the Managed Security Service. This supports recovery of service delivery capability in the event of disruption, including restoration of access to key operational systems and service records.

Backup and recovery controls may cover service delivery components such as:

- Security monitoring and operational tooling configurations (e.g., SIEM/SOAR configuration baselines)
- SOC operational documentation and delivery runbooks
- Service reporting data and supporting service records (where applicable)
- Contact routing and escalation records required for service delivery

Backup frequency, retention and restoration processes are reviewed and maintained as part of ongoing operational management.

Where the buyer's environment includes backup services within scope (for example Microsoft 365 backup via Axcient on applicable tiers), restoration activity may be supported through agreed service processes. Requirements are confirmed during onboarding and documented within the Order Form.

2.7.4. Business Continuity Plan

Vorboss maintains continuity procedures designed to maintain service delivery in the event of disruption and to minimise the impact of unexpected incidents on operational support. These procedures are intended to ensure that IT Managed Service delivery remains available, prioritised appropriately, and coordinated through clear operational processes.

Business continuity procedures include:

- Continuity of SOC and security operations delivery
  Maintaining the ability to monitor alerts, perform triage, initiate investigations, and coordinate response activity.
- Dependencies on monitoring and response tooling
  Identification and management of key dependencies such as SIEM/SOAR platforms, detection workflows, and buyer contact routes required for incident coordination.
- Prioritisation aligned to severity levels
  Applying severity handling to ensure critical or high-risk incidents are managed with appropriate urgency and escalation.
- Operational measures to support service availability
  Defined escalation routes, coverage procedures, internal responsibilities, and coordination processes to sustain delivery during disruption.
- Communication and coordination during disruption
  Supporting updates to buyer stakeholders (where applicable) and tracking incidents through to stabilisation with clear status and outcome confirmation.

- Recovery and stabilisation approach
  Structured recovery processes to restore service delivery capability, validate readiness, and review any follow-on actions required.

A more detailed plan can be provided to buyer on request.

2.7.5. Privacy by Design

- All Vorboss security products are designed with data segregation in mind.
- SIEM systems are deployed within the customer's tenant
- Monitoring platforms are provisioned for each customer and not shared
- All Vorboss staff are UK based and all Vorboss systems which process security data (SOAR, ITSM etc. are EEA/EU/UK based)

2.8. Using the service

Buyers can order Vorboss IT Managed Service through the G-Cloud 15 framework using the standard Call-off Contract process. Ordering is completed using an Order Form to confirm the scope of service, selected tier, user volumes, and any service-specific requirements.

Ordering steps:

Step 1 - Buyer enquiry and requirements confirmation
The buyer contacts Vorboss to outline requirements, including desired service tier, expected user volumes, and any specific operational or compliance requirements.

Step 2 – Scope and service tier agreement
Vorboss confirms the agreed scope of service delivery, including support boundaries and the selected tier (Core / Advanced).

Step 3 – Completion of the G-Cloud Order Form (Call-off Contract)
Vorboss supports the buyer in completing the Order Form, which forms the basis of the Call-off Contract and documents agreed service scope, service levels, onboarding requirements, and reporting expectations (where applicable).

Step 4 – Onboarding and service commencement
Following contract award and confirmation of the Order Form, Vorboss completes onboarding activities and begins service delivery on the agreed start date.

Invoicing:

- Charges are applied in line with the pricing structure agreed within the Order Form and relevant rate card/pricing.
- Invoices are issued on an agreed schedule (typically monthly) and reflect the contracted service tier and user volumes.
- Where applicable, invoicing adjustments for changes in user numbers or scope are managed in accordance with the Order Form and agreed contract terms.

- Buyers receive invoices with sufficient reference information to support internal purchase order and approval processes.

Ordering Contact Email: supplier@vorboss.com

Availability of Trial Service

Trial services may be offered at Vorboss' discretion depending on scope and buyer requirements.

2.9. On-Boarding, Off-Boarding, Service Migration and Scope

Vorboss supports buyers through a structured onboarding and service mobilisation process to ensure the Managed Security Service can be delivered effectively from the start. Offboarding is managed in a controlled way to support a smooth transition at the end of the contract, or where service scope changes over time. The onboarding and offboarding approach is designed to establish monitoring coverage, confirm service boundaries, agree escalation routes, and enable secure operational delivery aligned to public sector governance requirements.

2.9.1. Onboarding

Onboarding typically includes:

- Kick-off meeting and scope confirmation
  Confirming the selected service tier (MDR Core / MDR Advanced), user volumes (where applicable), in-scope systems and sources, operational priorities, governance contacts, and any service constraints or dependencies.
- SIEM/SOC onboarding approach and monitoring enablement plan (where applicable)
  Agreeing the approach for enabling monitoring coverage, including log source onboarding, alerting requirements, and validation steps to confirm service readiness.
- Agreement of escalation routes, severity definitions and reporting cadence
  Confirming severity handling (P1/P2/P3), escalation contacts, incident notification routes, and reporting expectations (where applicable).
- Asset/source discovery inputs and baseline visibility (where applicable)
  Establishing baseline visibility of in-scope sources (e.g., identity, endpoint, cloud and network) and confirming any required asset/source records or log-source baselining needed to support ongoing monitoring and reporting.
- Access and permissions confirmation (where required)
  Confirming required access approvals and delegated permissions necessary to deliver the service securely, including SOC operational access where applicable.

2.9.2. Service Migration (where applicable)

Where the buyer is transitioning from an existing provider or internal security function, Vorboss can support a controlled migration approach. This may include validating existing monitoring arrangements, confirming in-scope tooling and sources, and establishing continuity of security monitoring and incident handling during transition.

Pricing will be in accordance with the Vorboss Rate Card

2.9.3. Offboarding

Offboarding typically includes:

- Notice of termination in line with contract
  Confirming termination notice in accordance with contractual terms and agreed timelines.
- Exit planning and timeframe agreement
  Working with the buyer to agree an exit approach and timeline, including key dependencies such as SOC access removal, monitoring/tooling offboarding, and stakeholder communications.
- Removal of access following service end date
  Ensuring Vorboss access to buyer systems, security tooling and service routes is removed in a controlled and secure manner following contract end (in line with agreed scope).
- Transition support where required
  Supporting a handover to alternative arrangements where applicable, including knowledge transfer and coordination during the agreed exit period.

2.9.4. Training

Training includes service orientation, engagement routes, and severity understanding to ensure users and stakeholders can work with the Managed Security Service effectively from day one. This supports consistent incident reporting, clear escalation, and smooth coordination during security events.

Training typically covers:

- How to raise a security incident or concern
  How to contact Vorboss, what information to provide, and how to report suspicious activity or confirmed incidents through the agreed routes.
- Understanding incident severity (P1/P2/P3)
  How severity levels are applied, how prioritisation impacts response handling, and what buyers should expect depending on incident type and impact.
- SOC engagement and escalation routes
  Introduction to escalation paths, key service contacts, and how communication is managed during a live incident (including stakeholder updates where applicable).
- Basic security response expectations
  High-level guidance on likely early actions during an incident (e.g., isolating a device, resetting credentials, confirming affected users/systems), aligned to buyer governance and approval routes.
- Operational reporting and governance (where included)
  Overview of how reporting is delivered, what is included (e.g., incident trends and key actions), and how service reviews support continual improvement.

Additional training can be provided depending on scope and buyer requirements, including tailored sessions for admin users or key stakeholders. Training approach and delivery method

can be agreed during onboarding and documented within the Order Form. Pricing will be in accordance with the Vorboss Rate Card

Pricing will be in accordance with the Vorboss Rate Card

2.10. Implementation Plan

A detailed implementation plan can be provided to the buyer on request, however, a High-Level Plan (indicative) may include the following:

Milestone	Phase	Objective	Typical Activities (High-Level)
1	Service Kick-off & Scope Confirmation	Confirm service scope and mobilisation requirements	Confirm selected tier (MDR Core / MDR Advanced), user volumes (where applicable), in-scope systems and log sources, incident severity approach (P1/P2/P3), escalation routes, governance contacts, reporting expectations (where applicable), and any operational constraints.
2	Access & Tooling Enablement	Establish secure service access and enable delivery tooling	Confirm required administrative access and permissions, configure SOC contact routes, validate secure access methods, and enable monitoring tooling (SIEM/SOAR) required to deliver the service.
3	Source Discovery & Monitoring Baseline (where applicable)	Establish visibility of the security monitoring scope	Identify and confirm in-scope data sources (e.g., identity, endpoint, cloud services, network/security systems), establish baseline coverage, validate log ingestion and normalisation (where applicable), and confirm any required monitoring/asset records.

4	Detection & Response Configuration	Enable operational detection and incident handling workflows	Apply agreed detection content and alerting rules, enable automated playbooks (where included), confirm triage processes, validate escalation paths, and agree incident handling and communications approach.
5	Service Go-Live	Start 24/7 operational security delivery	Activate continuous monitoring, begin alert triage and incident handling aligned to agreed service levels, confirm operational handover and key stakeholder communications, and validate service readiness.
6	Stabilisation & Early Life Support	Embed service delivery and optimise early performance	Review early alert volumes and incident trends, tune false positives/noise (where applicable), validate reporting outputs, confirm recurring risks and quick wins, and agree initial improvement actions with the buyer.

2.11. Service Management

Vorboss delivers the Managed Security Service using structured service management processes aligned to the principles of the NIST Cybersecurity Framework (CSF). This supports consistent security operations delivery, clear incident prioritisation and escalation, improved visibility of security posture, and an approach to continual improvement. NIST alignment supports buyers by ensuring the service operates through defined, repeatable processes that provide governance, traceability, and oversight of security activity.

In addition, Vorboss provides operational reporting (where applicable) to support service governance and transparency. Reporting helps buyers understand alert volumes, incident trends, security posture improvements, and areas for risk reduction over time.

Key NIST-aligned practices include:

- Identify – establishing visibility of in-scope environments, users, assets and monitoring coverage
- Protect – supporting preventative controls such as vulnerability management and patching activity (where included)
- Detect – continuous monitoring, alert triage and detection rule coverage (tier dependent)

- Respond – structured incident handling, escalation and response coordination aligned to severity and governance requirements
- Recover – supporting recovery coordination and post-incident review activity (where applicable)
- Reporting and Governance (where applicable) – providing security reporting to support oversight, including alert volumes, severity breakdown, incident trends, key actions taken, and improvement opportunities
- Continual Improvement – using reporting and lessons learned to improve security outcomes and reduce recurring issues over time

2.12. Outage and Maintenance Management

Vorboss supports continuity of the Managed Security Service through structured monitoring operations, operational resilience measures, and planned communications where required. This is designed to ensure security monitoring and incident response capability remains available and effective, including during periods of service disruption or planned maintenance activity.

Unplanned security-impacting events (such as suspected compromise, loss of monitoring visibility, or critical security tooling interruption) are captured through structured incident handling. Incidents are formally logged, prioritised appropriately (P1/P2/P3), escalated through agreed routes, and managed through to stabilisation. Where applicable, incident records support service visibility by capturing key information such as operational impact, affected sources, response actions taken, and time to restore monitoring and security oversight.

Planned maintenance activities and service changes (where applicable) are managed in a controlled manner to reduce operational risk. This includes scheduling maintenance windows where required, communicating expected impact to relevant stakeholders, validating monitoring and alerting functionality following changes, and ensuring service delivery returns to a steady operational state.

Where recurring issues are identified (for example repeat alert patterns, repeated visibility gaps, or recurring control weaknesses), Vorboss uses trend analysis and reporting (where applicable) to support continual service improvement and reduce the likelihood of repeated disruption over time.

2.13. Financial Recompense Model

Service credits may be available depending on contract terms and documented within the Order Form.

2.14. Customer Responsibilities

To help the Managed Security Service operate effectively, the customer plays an important role in ensuring scope information is accurate, escalation routes are clear, and approvals can be provided when required. Clear responsibilities help security events be investigated faster, reduce delays caused by missing access or unclear ownership, and support effective coordination during time-sensitive incidents.

Customers are expected to:

- Maintain accurate scope and contact information
  Provide and maintain up-to-date details on key contacts, escalation stakeholders, and in-scope systems, services and user groups (including changes that may affect monitoring coverage or incident handling).
- Use agreed incident engagement routes
  Ensure suspected security incidents, urgent concerns and relevant requests are raised through the agreed contact routes so they can be logged, prioritised and tracked appropriately.
- Provide operational and escalation decision-makers
  Nominate suitable operational contacts (and escalation contacts where required) to support incident coordination, approvals, and timely decision-making during security events.
- Approve access and permissions where required
  Provide timely approvals for administrative access, delegated permissions, or security actions required to deliver monitoring and support incident investigation and response in a controlled manner.
- Support onboarding and offboarding activity (where applicable)
  Communicate changes that may affect security risk and monitoring scope, such as onboarding/offboarding of users, high-risk role changes, and access removal requirements.
- Communicate business-critical services and priorities
  Inform Vorboss of critical services, operational constraints, or time-sensitive periods that may affect incident prioritisation, escalation handling, or response expectations.
- Support third-party coordination where applicable
  Where incident response requires third-party suppliers (e.g. managed application providers, connectivity providers, or cloud vendors), support coordination where contractual ownership sits with the buyer.
- Maintain internal governance and decision-making
  Retain ownership of organisational policies and risk decisions, including approvals for security-related changes or containment actions that may affect service availability or user access.
- Support security and compliance requirements
  Where relevant, ensure compliance expectations, internal control requirements, and

reporting obligations are communicated so service delivery can align to governance needs.

- Engage in service review and continual improvement (where applicable)
  Participate in agreed review cycles to discuss service performance, recurring risks, incident trends and improvement actions, ensuring the service remains aligned to evolving requirements.

2.15. Technical Requirements and Client-Side Requirements

Vorboss delivers the Managed Security Service through security monitoring, threat detection and incident response processes supported by SIEM/SOAR tooling (where applicable), log source onboarding, and agreed governance/reporting arrangements. To enable secure and effective service delivery, buyers must ensure that in-scope systems, connectivity, and access arrangements meet baseline requirements. Any additional organisation-specific requirements are confirmed during onboarding and documented within the Order Form.

Typical technical and client-side requirements include:

Monitoring Sources and Environment (In Scope as Agreed)

- In-scope environments suitable for monitoring, such as:
  - Cloud platforms and SaaS services (e.g., Microsoft 365)
  - Identity platforms (e.g., Microsoft Entra ID / Google)
  - Endpoint protection telemetry (EDR/XDR where used)
  - Network/security systems (firewalls and other sources where included)
- Supported systems configured to generate relevant audit and security events (where applicable)
- Source ownership and responsibility understood for escalation and remediation actions

Connectivity and Data Ingestion Enablement

- Reliable internet/network connectivity to support log forwarding, monitoring feeds, and secure SOC engagement
- Network routes available to support onboarding of monitoring sources (where applicable)
- Ability to support secure communications between Vorboss delivery systems and buyer environments (as required)

Access, Permissions and Approvals

- Appropriate permissions granted to enable monitoring setup, troubleshooting and incident investigation activity (where agreed)
- Administrative access or delegated permissions where required to onboard log sources, validate telemetry, and support response actions (tier/scope dependent)
- Timely customer approvals for actions that require elevated access, containment activity, or policy enforcement

Endpoint and Security Tooling Requirements (Where Applicable)

Where included within the agreed tier, buyers must support the enablement and operation of:

- Endpoint security telemetry sources (e.g., Defender / MDR/XDR tooling)
- Vulnerability and patch management capability (where included)
- Email security controls (where included)
- Required device onboarding workflows and deployment permissions (where applicable)

Identity and Account Requirements

- Access to identity platforms (where required and agreed) to support investigation of authentication, access anomalies, and account risk events
- Ability to confirm and apply identity security controls such as MFA and access policies (customer-owned, where required)
- User/account details provided where required for incident coordination and response actions

Third-Party Dependencies (Where Applicable)

- Where the buyer uses third-party suppliers (e.g. hosted applications, network/security providers, cloud service providers), coordination or access may be required to support end-to-end investigation and resolution
- Buyer support may be needed to engage third parties where contractual ownership sits with the buyer

Information Provided During Onboarding

To support smooth mobilisation, buyers may be required to provide:

- Key stakeholder and escalation contacts
- Confirmation of in-scope systems and monitoring sources
- Operational priorities and service constraints
- Required access approvals and delegated permissions
- Any restrictions or policies that affect monitoring scope, log retention, or response actions

2.16. Outcomes and Deliverables

Vorboss Managed Security Service is designed to provide practical operational outcomes that support cyber resilience, service continuity, and consistent security oversight. Deliverables focus on strengthening detection and response capability, improving visibility of security risk, and reducing the impact of cyber threats through structured processes, tier-aligned monitoring coverage, and repeatable security operations.

Deliverables and outcomes typically include:

Security Operations Delivery

- Security monitoring and alert handling through a managed service model
  Security events and alerts are monitored, reviewed, and handled through structured processes to support consistent triage and response coordination.
- Consistent security incident management
  Incidents are logged, tracked, and managed through defined workflows, supporting clear prioritisation and auditability of actions taken.
- Priority-based handling for high-impact security events
  Security incidents are handled against agreed service levels (P1/P2/P3), ensuring urgency is aligned to business impact and risk exposure.

Improved Detection and Response Outcomes (Tier Dependent)

- Faster identification of suspicious activity
  Continuous monitoring (tier dependent) supports early detection of threats such as credential misuse, suspicious access activity, or endpoint compromise.
- Structured incident escalation and response coordination
  Escalation routes and stakeholder communications support timely decision-making and controlled response activity during incidents.
- Improved consistency of response actions
  Defined operational processes support repeatable handling of incidents and reduce reliance on ad-hoc decision-making.

Vulnerability Reduction and Security Hygiene (Where Included)

- Improved patch and vulnerability management outcomes
  Where included, vulnerability and patch management supports reduced exposure to known vulnerabilities and improved baseline cyber hygiene.
- Better visibility of exceptions and recurring weaknesses
  Identifying recurring issues and exception trends supports planning and prioritisation of remediation activity over time.

Security Visibility, Reporting and Governance

- Operational reporting and performance visibility (where applicable)
  Buyers may receive reporting to support oversight of security activity, alert trends, and service performance against agreed service levels.
- Improved auditability and traceability of security actions
  Security events and incident handling are recorded in a controlled way to support transparency, review, and governance needs.
- Support for continual improvement
  Trend analysis and service review (where applicable) support improvement planning and ongoing strengthening of security outcomes.

Assurance and Confidence (Associated Services)

- Support for assurance activities and improvement planning
  Optional cyber health checks and penetration testing can be delivered as associated services to provide assurance, highlight gaps, and support prioritised improvement roadmaps.

2.17. Development Life Cycle

This service is delivered as an operational managed security service rather than bespoke software development. Improvements are delivered through continual improvement practices and controlled change (where applicable).

2.18. After-sales Account Management

Following service go-live, Vorboss provides ongoing account management to support operational governance and continual improvement of the Managed Security Service. This includes structured service reviews and a Customer Service Improvement Plan (CSIP)-aligned approach to monitoring performance, identifying recurring security themes, and agreeing prioritised improvement actions with the buyer.

Ongoing account management supports:

- Regular service performance reviews
  Review of service activity including alert volumes, incident handling performance, and service level metrics (where applicable) to ensure the service continues to meet operational requirements and buyer expectations.
- Recurring security issue and trend analysis (threat and control focused review)
  Identification of recurring incident types, repeat alert patterns, visibility gaps, and common risk themes to support targeted improvements and preventative actions over time.
- CSIP-style improvement actions
  Agreed improvement actions documented and tracked through to completion, focusing on service stabilisation, detection quality improvements (e.g. tuning), and operational effectiveness of monitoring and response.
- Change, maintenance and service impact review (where applicable)
  Review of planned changes, maintenance activity, and any monitoring impact to ensure service continuity is maintained and lessons learned are captured (for example, changes affecting log sources, alerting behaviour, or security tooling coverage).
- Scope and tier alignment over time
  Regular validation that monitoring scope, service tier (MDR Core / MDR Advanced), log source coverage, retention expectations, and response requirements remain aligned to evolving buyer priorities and risk exposure.

- Service governance and stakeholder engagement
  Clear buyer points of contact, escalation routes, and governance processes to support communication, decision-making, and coordinated response during priority security incidents.

2.19. Termination Process

Termination is managed in line with Contract terms:

- Per-user contract basis
- Minimum Initial Period: 12 months (Core/Advanced)
- Early termination terms in accordance with terms of the Contract

2.20. Our Experience

Case Study: Maintaining Information Security and Compliance for Cyted Health

Cyted Health Ltd is a data-driven diagnostics company specialising in gastrointestinal oncology, digital pathology, AI-driven biomarker discovery and laboratory services. As a medical and diagnostics technology firm, maintaining stringent data security and regulatory compliance is critical to its operations and trust.

The Challenge Cyted required expert, ongoing support to manage its Information Security Management System (ISMS), ensure continued compliance with ISO/IEC 27001 standards, and effectively manage its Governance, Risk, and Compliance (GRC) program.

Vorboss, (formerly Optimity) Managed Security Solution Vorboss (Optimity) provides comprehensive managed security services to Cyted, structured around a phased approach to ensure both initial compliance and continuous security maturity.

Phase 1: Information Security Roadmap & Governance

Vorboss (Optimity) established a robust ISMS framework to ensure compliance with ISO 27001. This phase focused on foundational governance and policy setting:

- ISMS & ISO 27001 Management: Defining and adopting minimum security policies, including the information security policy, security policy development, and managing the policy audit and review cycle.
- Security Organisation & Governance (GRC): Establishing security roles, implementing risk governance, and managing partner security agreements.
- Security Audit & Remediation: Performing Gap Analysis against the ISO 27001:2022 standard, conducting a retrospective review of the infrastructure, and performing internal audits (such as the Clause 9 Performance Evaluation, Clause 4 Context of the organisation, and A.15 Supplier relationships).
- People & Awareness: Managing HR-related security aspects, including the security awareness programme and staff awareness.

Phase 2: Ongoing Remediation and Maintenance (Continuous GRC)

Following this roadmap, Vorboss (Optimity) provides ongoing managed security services focused on maintaining the security posture and ensuring continuous compliance:

- Infrastructure & Endpoint Security: Maintaining device management, asset inventory, patching, and EDR solutions.
- Identity & Access Management: Managing directory services, authentication to devices, and authorisation to data.
- Data Protection: Overseeing policies, encryption deployment, and auditing related to sensitive data.

- Operational Security: Managing change control, secure infrastructure/delivery, and security logs.
- Impact and Results Vorboss (Optimity) partnership successfully supported Cyted in its GRC and ISO 27001 compliance efforts:
- Sustained Certification: The scope of Vorboss (Optimity) ISMS work covers the entirety of Cyted Ltd's operations, including its data-driven diagnostics, digital pathology, and laboratory services.
- Effective ISMS Operation: Continuous internal audits were conducted by Vorboss (Optimity) (David Osen) across critical clauses such as Performance Evaluation, Context of the organisation, and Supplier relationships, helping to monitor and continually improve the ISMS.
- Clear Security Accountability (GRC): Utilisation of the RACI framework ensures clear roles for security tasks, defining who is Responsible, Accountable, Consulted, and Informed.
- Secure Supplier Relationships: Processes for managing suppliers that affect information security are managed through systematic change control and review, ensuring third-party risk is controlled as required by ISO 27001 A.15

"As a rapidly expanding biotech company we identified the need to bring on an IT support partner in a quick turnaround. Vorboss (Optimity) was adaptable and able to provide support services with little notice, filling identified gaps and onboarding at speed. Once onboard , Vorboss (Optimity) conducted a detailed analysis of our organisational systems with a highly pragmatic approach and understanding of our requirements as a business.

Over the past couple of years Vorboss (Optimity) has become a trusted IT management partner helping us work towards cyber compliance in a heavily regulated sector. They have embedded themselves into our business well and provide an extremely personable approach with the team; this has enabled them to tackle complex obstacles dealing with legacy systems as well as tailoring their systems to support our unique operational needs."

Head of People, Cyted

2.21. Contact details

For G-Cloud enquiries:

Toby Morgan-Grenville
Head of Public Sector
E: supplier@vorboss.com
T: +44 (0) 73 5037 1723