G-Cloud 15

Service Definition

Arctic Wolf Managed Risk

NG-IT

Lot 2b Software as a Service (SaaS)

1. Introduction

Company Overview

NG-IT are the UK's leading provider of next generation Private Cloud, Hybrid Cloud and Cyber Security services. We make digital innovation a reality by delivering flexible, always available, highly agile IT services using innovative, next generation technology solutions.

As a multi award winning business, NG-IT is dedicated to meeting the demands of today's business environment. Instead of taking legacy ideas, systems, processes, and technologies, we deliver an exceptional experience around the understanding, design, deployment, and management of next generation data centric and cyber security solutions.

It is critical to stay head of attackers, and our solutions work to identify both new technologies and new and emerging threats. At NG-IT, we understand how important these steps are to ensure that your business is secure against old and new Cyber security threats. This way we can improve your security posture, reduce the risk to your business and keep you where you should be - ahead of the cyber attackers.

NG-IT have deployed over 400 private cloud, hybrid cloud or cyber security solutions including migrating more than 60,000 applications and 32,000 TBs of data. Our professional services capability allows us to provide a full end to end service for our customers, to ensure a seamless working relationship from the initial engagement to the delivery of the chosen solution.

We continually review and assess leading and emerging technology vendors, and our expertise lends us to consider the best options for our customers. We've invested heavily in our people to bring you the very best working relationship and technical consultancy there is to offer.

Social Value

In an increasingly digital and fast-paced world, our Social Value Strategy reflects a deep commitment to people, communities, and the planet. We believe that technology should not only drive innovation but also foster trust, inclusion, and long-term wellbeing. Our legacy is built on a human approach, listening, guiding, and delivering solutions that leave lasting confidence.

Our mission is to be a trusted advisor and supplier of hybrid cloud, security, and data protection services. Our vision is to help businesses prosper through innovative technology, and our values centre on a customer-first culture powered by quality people.

Kickstart Economic Growth

Commitment
We support inclusive economic growth by investing in SMEs and VCSEs, promoting fair pay, and enabling local innovation through ethical procurement.

Initiatives & SMART Objectives

- SME & VCSE Spend Growth: Audit current spend and increase by 15% over 3 years, aligned with local authority targets.
- Fair Payment Code: Ensure 100% of suppliers are paid within agreed terms by Q4 2026.
- Metrics & Monitoring:
- Regular audits
- Supplier satisfaction surveys
- Spend tracking via finance systems

Governance & Ownership

- Led by our Finance Department
- Reviewed annually

Make Britain a Clean Energy Superpower

Commitment

We reduce our environmental footprint and promote sustainable digital practices that support the UK's Net Zero ambitions.

Initiatives & SMART Objectives

- Carbon Reduction Plan: We are currently gathering baseline data on our operational emissions to inform a measurable reduction strategy. Our goal is to identify key areas for improvement and set a science-based emissions reduction target by the end of 2026, with a focus on energy-efficient infrastructure and remote-first working practices
- Net Zero Roadmap: We are currently in the process of gathering baseline data on our carbon emissions across Scope 1, 2, and relevant Scope 3 categories. This data will inform the development of a science-based Net Zero strategy. Our aim is to set a formal Net Zero target by the end of 2026, including plans for verified offsetting of any residual emissions.
- ISO14001 Certification: Maintain certification through annual audits and continuous improvement.

Metrics & Monitoring

- Carbon accounting via Scope 1–3 reporting tools
- Annual sustainability reports
- Internal audits and external verification

Governance & Ownership

- Led by our Operations Manager
- Reported to the Board

Break Down Barriers to Opportunity

Commitment
We foster inclusion through education, skills development, and fair employment practices, empowering underserved groups and future talent.

Initiatives & SMART Objectives

- Digital Skills Outreach: Deliver workshops annually in underserved regions via charity partnerships.
- Careers Advice Programme: Provide virtual careers advice and mentoring to students from diverse backgrounds.
- Volunteering Leave: Provide 2 paid days per employee annually, with 80% uptake by 2026.
- Gender Pay Gap Transparency: Publish annual reports, regardless of company size.

Metrics & Monitoring

- Diversity metrics tracked via HR
- Workshop attendance and feedback forms
- Careers advice session participation and feedback
- Volunteering uptake reports

Governance & Ownership

- Led by Finance and HR and Management
- Supported by Management

Build an NHS Fit for the Future

Commitment
We contribute to a healthier workforce and community through mental health support, wellbeing initiatives, and responsible leadership.

Initiatives & SMART Objectives

- Able Futures Promotion: Increase internal awareness and usage by 30% over 12 months.
- MHFA Training: Train 10% of staff as Mental Health First Aiders by 2026.
- Wellbeing Surveys: Maintain 90% response rate and use feedback to shape quarterly wellbeing actions.

Metrics & Monitoring

- Programme usage analytics
- Training completion rates
- Survey dashboards and action logs

Governance & Ownership

- Led by our Wellbeing Lead and HR Manager
- Reviewed quarterly by the Employee Engagement Committee

This strategy aligns with:

- PPN 06/20: Delivering social value in procurement
- PPN 02/23: Carbon reduction plans and Net Zero
- PPN 09/21: Modern slavery risk assessments
- PPN 03/23: SME-friendly procurement practices

We ensure proportionality to contract size and maintain flexibility to tailor initiatives to specific project needs.

Overview of the G-Cloud Service

NG-IT take great care in selecting our service provider partners. We undertake a rigorous selection process that affords us the confidence to promote and justify Arctic Wolf as our key partner for delivering Fully Managed Cyber Security Services. Arctic Wolf provides essential insights and expertise across all types of environments and infrastructure, making them the ideal partner for our customers to engage and trust as the service provider for this proposed platform. NG-IT partners with Arctic Wolf to deliver managed security operations as a concierge service. Our Security Operations Cloud, built on an Open-XDR framework, spans on-premises, edge, public cloud, and SaaS. Modules include 24x7 threat detection and response, vulnerability management, security awareness training, and digital forensics with incident response.

Throughout this proposal it is our hope to demonstrate our unique approach of focusing on a Cyber Security Outcome that goes beyond and into a true extension of our customer's team, forming a close relationship committed to lowering Cyber Risk across the organisation. To ensure this response is understood correctly, it is prudent to communicate the roles of NG-IT and Arctic Wolf. Arctic Wolf is a 100% Channel Organisation Vendor, which means that procurement would be via NG-IT, a founding member of Arctic Wolf UK Partner program. NG-IT are the channel vendor introducer, billing agent and provider of any complimentary services where applicable. Arctic Wolf directly provides all core Security Operations Centre (SOC) services, Threat Intelligence and guided remediation.

The Solution

NG-IT have chosen to propose a suite of services from Arctic Wolf to address the challenges of delivering and maintaining adequate and effective protection from cyber-attack for the organisation, it's IT environment & critical data and the wider user community.

Managed Risk

Managed Risk is continuous Risk and Vulnerability Management delivered by the Concierge Security Team. Many organisations struggle with the complexity of identifying and managing security risks within their environment. Often, even fundamental information like what assets exist, which systems have vulnerabilities, and which systems are not configured properly is hard to obtain. When this information is available it usually overwhelms the security team because existing tools generate too many alerts and lack context. As they struggle with what to do next and how to prioritise, these risks pile up and leave the organisation vulnerable to threats and damaging data breaches. Arctic Wolf Managed Risk enables you to continuously scan your networks, endpoints, public assets, and cloud environments to quantify digital risks. Your security operations experts from the Concierge Security Team works directly with you to discover risks beyond simple vulnerabilities, benchmark the current state of your environment, and implement risk management processes that harden your security posture over time.

Arctic Wolf MR solution (the "Solution" or "Product") enables you to discover, prioritize, and harden your environment against digital risks by contextualizing your attack surface across networks, endpoints, and cloud environments. The Arctic Wolf Concierge Delivery Model ensures that our purpose-built technology, combined with our extraordinarily talented teams, helps you deliver security outcomes for your organization. Included with the Solution, you have access to the Unified Portal (formerly known as the Customer Portal), a real-time, web-based self-service application that enables you to configure and tailor the Solution and provides you with insights to the data, risks, vulnerabilities, and tasks related to your security program. Security touchpoints with your Concierge Security® Team (CST) and your Customer Success Manager (CSM) may be included with MR as

described herein depending on your subscription. These security touchpoints are designed to provide not only a detailed understanding of current security events and threats, but proactive security hardening guidance to improve the security maturity of your security program overall.

MR Activities

Discover

Risk Monitoring

Monitors for vulnerabilities, system misconfigurations, and account takeover exposure across your endpoints, networks, and cloud environments, to the extent licensed and configured.

Risk Prioritization

Security observations are enriched with digital risk information to add greater context, quantify your exposure, and prioritize actions.

Asset Discovery

The solution continuously maps, profiles, and classifies assets on your network to help you understand your attack surface.

Assess

Configuration Benchmarking

Reveal configuration errors and drift over time that are invisible to most vulnerability assessment and management tools.

Risk Scoring

Presents a quantified view of digital risks that exist in your environment weighted based on severity and benchmarked against peers to track the progress of your remediation efforts.

Actionable Reporting

Automated and exportable risk score trends, action lists, executive summary, and risk assessment reports that summarize risk exposure in consumable, shareable formats to help you prioritize actions that harden your environment.

Harden

Guided Remediation

If available with your subscription, the CST provides you with guided personalized risk remediation and validation to assess whether the vulnerability has been successfully remediated, while also enabling you to determine if the vulnerability is still present in your environment.

On-Demand Reporting

Through the Unified Portal you may be able to create and configure dashboard-based reports to showcase the data visualizations important to you. Upon request, the CST may assist with the creation of these reports or generate ad-hoc reports with rich charts and dashboards for meeting compliance needs or provide on-demand executive reporting to support you in gaining the visibility of vulnerabilities and assist with closing gaps.

Strategic Recommendations

If included with your subscription, the CST's goal is to become your trusted security advisor, working with you to make recommendations that harden your security posture over time. Arctic Wolf Labs may be leveraged by your CST during your subscription to provide you with the latest emerging threat intelligence on vulnerabilities with reliable and actionable information.

Arctic Wolf Technology Overview

In addition to the core technologies offered to all Arctic Wolf solutions that are listed here, the below Arctic Wolf Technology Overview sets forth, in general, the Arctic Wolf Technology and the various features and tools that may be included as part of the Solution. The availability and use of any such Arctic Wolf Technology, features, and tools by you is contingent on the specifics of your subscription and reflected in the ordering document (i.e., your Order Form) pertaining to such subscription.

Scanners

Arctic Wolf MR Scanners ("Scanners") and Virtual Scanners ("vScanners") are data collection devices to capture network device identification and vulnerability data associated with your network devices. Scanners and vScanners will be included with your subscription as set forth on your Order Form. Scanners/vScanners are managed, maintained, and updated by Arctic Wolf and include Arctic Wolf's latest vulnerability feeds. For a list of the different Scanners/vScanners, refer to the table below:

Scanner	Description
External Vulnerability Assessment (EVA) Scanner	The EVA scanner is hosted on Arctic Wolf cloud infrastructure. It scans customer-provided, public facing assets such as IP addresses, domains, and cloud accounts (if purchased and configured) by performing port detection (for IPs), DNS scan (for domains), followed by vulnerability scanning on all assets (Account Take Over, Web Application, Vulnerability, and CSPM). The schedule for these scans can be defined within the Unified Portal.
Internal Vulnerability Assessment (IVA) Scanner	The IVA scanner is a physical or virtual appliance deployed in your environment that is managed by Arctic Wolf. The appliance scans your defined targets with host profile and vulnerability scans. The vulnerability scans can be scheduled at times that meet your needs and preferences and may be run monthly, weekly, daily, or continuously. This frequency is configurable on a network-by-network or host-by-host basis. The host profile report enables you to catalogue the assets you have in your environment. The IVA Scanner collects various datapoints using a variety of ever evolving technologies and reports risks found in your environment by running non-credentialed and credentialed
	detections to the extent you elect to configure such detections. Multiple scanners can be deployed to scan distinct parts of your network depending on your environment, size, and preferences.
Account Takeover (ATO) Risk Detection	ATO scanning focuses on known organizational data breach records. The information contains account usernames and passwords. ATO scanning does not focus on the following data sources: • Marketing lists and/or databases — list of employees, which may include their role, title, or department within the organization. • Spam lists — lists of email addresses, corporate, or personal. ATO scanning may include usernames and user passwords for any of your offboarded resources.

The output from the EVA, IVA, and ATO scanning processes will be a comprehensive security risk posture based on an industry standard and recognized Cybersecurity Framework and Arctic Wolf's proprietary algorithm.

Arctic Wolf Agent

The Arctic Wolf Agent ("Agent") is software installed on endpoints and allows Arctic Wolf to run local system scans to augment your telemetry information collected via the Scanners/vScanners and is used to (a) identify security vulnerability analytics, trends in your network and endpoints, (b) scan for system misconfigurations through the security controls benchmarking function, and (c) perform host-based vulnerability assessment scans. The Agent is managed, maintained, and updated four times daily with the latest vulnerability feeds provided by Arctic Wolf. The Agent is capable of self-updating,

collecting software and asset inventory data, and sends operational metrics and telemetry to the Security Services Team (comprised of the Security Operations Team (SOC) and the CST), if included with your subscription, for analysis and investigation. The Agent can coexist with your existing Endpoint Security vendor, but for the best possible service, visibility, and coverage, we recommend that the Agent be deployed to all devices in your environment alongside Sysmon, if your subscription mix warrants. During the onboarding phase, the Deployment Security Team will assist with the deployment of the Agent at scale within your organization using an appropriate method of deployment such as Microsoft Intune, Microsoft System Centre Configuration Manager (SCCM), Jamf, or group policy.

Arctic Wolf Unified Portal

The Arctic Wolf Unified Portal is the self-service application for Arctic Wolf Products, including MR. The Unified Portal is the single point of access to your CST, if included with your subscription.

You can perform the following tasks related to MR within the Unified Portal:

- Get a consolidated view of EVA, IVA, and Agent scan schedules across all risk sources.
- Manage and create IVA and Agent scan schedules.
- Configure IVA Scanner to manage scanner settings, deny list entries, and authenticated scan credentials

Arctic Wolf MR Workbench

Accessed through the Unified Portal, the Solution includes access to the MR Workbench that provides visibility into the real-time risk landscape on your networks, endpoints, and cloud environments (if purchased and configured). The MR Workbench is a cloud-based portal that is tailored to your organization's priorities to help you make sense of potential vulnerabilities, while also managing and prioritizing patching with the goal of reducing your cyber risk exposure by enabling operational optimization through insights into the prioritization of your information security and technology activities.

For a list of sub-features within MR, refer to the table below.

Feature	Description
Overview of dashboard metrics and health status	Provides visibility into your cybersecurity posture, overall cyber risk score over time, industry comparisons, and asset health.
Management Plan	Lite Gantt chart view where you can create plans, and review progress and deadlines of risk mitigation efforts for risks added into these plans.
Risks	View a catalog of risks with the ability to filter and sift through the list of discovered cyber risks. You can view the following: • Risks and unassigned risks sections • Risk information pane • Risk states

	• Risk statuses • Risk state and status lifecycles • Risks based on an assigned due date • Rescan assets with risks • Active risks • Inactive risks • Mitigated risks • Risks that failed validation • Arctic Wolf Agent vulnerability debug scans You can perform the following tasks: • Assign a user and a due date to a risk • Accept a vulnerability • Edit the state of inactive risks • Edit risks • Unassign a user and a due date from a risk • Download a remediation report • Download risks table data
Assets	View a catalog of assets. You can perform the following tasks: • Assign asset context • Filter assets • View an asset profile • Rescan assets • Review assets • Create an asset tag • Edit assets • Reset sensor details • Remove an asset • Download asset catalog data.
Agent	View risks, assets, and Center for Internet Security (CIS) benchmark data discovered during Agent scans.

External Vulnerabilities Assessment	View a list of configured target groups with risk data discovered during External Vulnerability Assessment (EVA) scans.
Attack Surface Coverage	Provides details about coverage by different scanning technology with target, network capacity, device count, missed, and scheduled targets information.
Scanner configurations	Review operational status of sensors, network, and subnetworks, and a list of hosts enabled for credentialed scanning.
Resources	Provides quick reference links to release notes, and documentation.
Downloads	Provides you with the ability to download a Scanner Virtual Machine image for your virtualization infrastructure.

Arctic Wolf MR Analytics

You can use MR Analytics to view and organize MR and Agent information in your environment. You can view historical data, up to 365 days, to analyze the vulnerability management program. MR Analytics enables you to generate custom dashboards and schedule email delivery to stay updated on changes in your environment. You can use MR Analytics to view raw data tables, refine results to specific subsets of data using filters, aggregate results to answer questions, and combine multiple data views into interactive dashboards.

Cloud Security Posture Management (CSPM)

You may additionally license CSPM for Amazon Web Services (AWS), Microsoft Azure, and any such other cloud and SaaS environments. If included in your subscription, Arctic Wolf will monitor, evaluate, and track your agreed upon cloud configurations and compare such configurations to best practices to identify possible configuration errors in your environment. Any such errors will be displayed within your MR Workbench and a report will be provided to you outlining any additional details.

Services Subscription

The above service is consumed as tiered bundles, each bundle offers increasing levels of technology, service features & assistance. The services proposed will be delivered directly by Arctic Wolf Triage, Concierge and Incident Response personnel and will provide increased levels of cyber defence and response, allowing for improvements in security standardisation, best practice and adhering to recognised cyber security frameworks such as NIST, NCSC Cyber Essentials and ISO27001.

Arctic Wolf will provide a team of assigned security experts that will study and understand the in-place IT and operations methodologies employed by your organisation and find ways to continually optimise cyber security posture specific to the IT environment and security goals. In addition, they will ingest and centralise all security event data into their cloud-native security analytics platform which will enable them to provide 24x7 correlation, analysis and investigation capabilities, whilst leveraging the

in-place technology stack. This allows for unrivalled & broad visibility across all attack surfaces which will maximise effectiveness in preventing and eliminating potential cyber threats.

Your nominated concierge security operations expert works with your in-house teams to provide advice and guidance throughout the service to assess the current state of your environment and identify ways to continually improve cyber posture and reduce risk for the organisation as a whole.

By combining the capacity of the Arctic Wolf ground-breaking Aurora monitoring platform with the capabilities and industry leading skills of Arctic Wolf cyber analysts, response and engineering teams we aim to own the outcome of every critical cyber security event that may present itself to your business.

Principal to our service offering are four specific areas of focus:

- Service & outcome driven approach
- Reduced risk
- Reduced time to value
- Cost efficiency

These can be elaborated on as follows.

Service & outcome driven approach

- Unlimited incident response (incidents and time) with focus on outcome, not contract
- limits.
- Arctic Wolf Triage team own incident response, providing context, threat containment,
- active response and guided remediation.
- Your Concierge team is focused on your strategic security objectives, alignment with
- your chosen security framework and continuous improvement of security posture and
- reduction of cyber risk.

Reduced risk

- Named Concierge Security Team aligned to you to drive Proactive / Strategic security objectives
- 24/7/365 SOC with ~1000 Security Analysts/Engineers/Forensics/Detection Engineers
- Continual platform optimisation, detection rule addition, feature additions included seamlessly in service.
- 400+ R&D team to support “mega events” like Log4JShell.
- ~10,000 customers for crowd sourced threat intelligence – see once and inoculate everyone approach.
- Robust and comprehensive incident planning with defined response times, dedicated incident Director and digital forensics.

Reduced time to value

- Cloud native Security Operations Cloud platform detects threats immediately and replaces need for in-house SIEM tool and the effort to implement, configure, detection rule writing, threat intelligence addition & curation, and runbook writing.
- Onboard and live within 30 to 60 days. Implementation project managed by Arctic Wolf and aligned Professional Services team.
- Tuned and customised response actions to your precise needs by your Concierge team.

Cost efficiency

- Unlimited access to aligned Concierge Team, not constrained by contractual hours or maximum number of incidents/requests.
- Achieve world class SOC platform and service at ~20% the cost of DIY SIEM / SOC build out.
- Virtually extend your organisation security and/or IT operations team through named Concierge Team and Triage teams.
- 99.9% true positive tickets – remove practically all the noise generated by security tools and time spent investigating alerts. Allow your organisation to focus only on verified and actionable security events.
- Unlimited security log data ingestion – broad visibility with no trade-off between visibility and cost, thereby delivering predictable pricing for you.
- No need to rip and replace existing security tools – Vendor neutral approach with integration into existing tools from day one.

Associated Services

NG-IT can provide Professional Services to install and configure the proposed solution. Data migration services are available if required

2. Data Protection

Information Assurance

- Cyber Essentials Plus
- We are certified under the Cyber Plus scheme, demonstrating our commitment to protecting against common cyber threats across our remote working environment.
- ISO 9001 – Quality Management
- This certification ensures our virtual service delivery is consistent, customer-focused, and continuously improving.
- ISO 14001 – Environmental Management
- Reflects our commitment to sustainability through digital-first operations, reduced travel, and energy-efficient cloud-based tools
- Information Management Process:
- Secure Cloud Platforms: All internal and client communications are conducted via encrypted cloud-based systems with strict access controls.
- Remote Access Security: Employees use multi-factor authentication, VPNs, and endpoint protection to securely access company resources.
- Data Handling Policies: We comply with GDPR and the Data Protection Act 2018, ensuring lawful and transparent data processing.
- Incident Response: We maintain documented procedures for breach detection, escalation, and resolution, aligned with industry best practices.
- Supplier Vetting: All third-party vendors are assessed for compliance with security, ethical, and sustainability standards

Data Back-Up and Restoration

NG-IT Limited recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory, and regulatory obligations, to ensure the protection of personal information and to enable the effective operation and management of the organisation.

To guarantee that, we have a Data Backup Policy that applies to all staff within the Company with a purpose of safeguarding information belonging to us, any third parties and clients. We do not hold business critical data within a traditional on-premises network or managed data centre, all line of business application data and unstructured file data is located within cloud storage, owned and managed by the relevant application vendor the data is specific to.

This business systems technology model allows for continuous replication of data from production cloud platform to secondary storage or an alternative cloud platform, effectively providing always available, fully comprehensive, granular backup with quick restore capabilities.

Backup Model

- Full backups of all data are performed weekly. Full backups are retained for 3 months before being overwritten.
- Backups are stored in secure locations. A limited number of authorised personnel have
- Backup of data held within Database Systems have data backup routines which ensures database integrity is retained

NG-IT adopts the best security practices by defining security controls applicable to the entire organisation. Additional security measures identified through risk analysis, legal, regulatory, and/or contractual concerns, and/or specific standards -shall be addressed accordingly. Security controls and best practices are be considered and implemented as appropriate to the risk level

Business continuity statement/plan

Business continuity is not simply a matter of contingency, it is a core component of delivering consistent, reliable service in a competitive and fast-evolving industry. As an IT reseller/security and service provider operating with a fully remote workforce and reliant on only on cloud-based systems with no corporate network, NG-IT Ltd recognises the importance of being prepared for unforeseen disruptions, whether technical, operational, or external.

We have a Business Continuity Plan that outlines measures to ensure that our operations remain stable and responsive during periods of disruption. It defines the procedures, responsibilities, and safeguards that enable us to continue supporting our clients, maintain supplier relationships, and uphold our professional standards. The plan reflects our commitment to resilience and readiness, and will be reviewed regularly to ensure it remains aligned with our business needs and the expectations of those we serve

This Business Continuity Plan sets out the procedures and responsibilities required to ensure the continued operation of NG-IT Ltd in the event of a disruption. It applies to all employees and covers both the reselling of IT services, hardware and software distribution. The plan is designed to safeguard client relationships, maintain service delivery, and protect the company's reputation.

The key aims of this plan are to:

- Ensure continuity of service provision to clients.
- Minimise delays in hardware fulfilment and vendor coordination.
- Maintain secure and effective communication with customers and suppliers.
- Uphold contractual obligations and regulatory compliance.

The following functions are considered critical to the business and must be maintained during any disruption:

- Vendor liaison and procurement
- Order processing and fulfilment
- Customer support and issue resolution
- Financial operations including invoicing and payments
- Internal communication and collaboration

All our staff members have defined roles in the event of a disruption. The Managing Director is responsible for overseeing the implementation and maintenance of this plan. The Operations Manager and Finance Manager manages supplier relationships and hardware sourcing. The Technical Director and Cyber Lead ensure access to systems and data security. The Account Managers handles customer communications, and the Finance Officer ensures continuity of financial operations

All our business systems are cloud-based and configured for daily automated backups. Access is controlled via multi-factor authentication and role-based permissions. A centralised password manager is used across the organisation. Security audits are conducted quarterly to ensure compliance with data protection regulations and best practice.

Internal communications during a disruption will be conducted via internal messages and email, with SMS or telephone used for urgent alerts. External communications with clients and suppliers will be managed via email and telephone.

In the event of a disruption, recovery procedures will be activated immediately. Alternative suppliers may be engaged to maintain service continuity. Clients will be informed of any delays or changes to service provision. Staff availability will be managed through cross-training and flexible working arrangements. Any cybersecurity incidents will be addressed by isolating affected systems, restoring data from backups, and notifying relevant stakeholders.

This plan will be tested annually through structured exercises. Supplier performance and supply chain reliability will be reviewed in line with our ISO management system. Contact lists and standard operating procedures will be updated accordingly. Following any real disruption, a post-incident review will be conducted to identify areas for improvement.

Privacy by Design

We are committed to embedding privacy into every aspect of our service delivery. As an IT reseller, we do not process personal data directly through proprietary platforms, but we ensure that all technologies we recommend, resell, or support meet GDPR standards and respect user privacy from the outset.

- Privacy by Design: We assess privacy risks during the initial selection and onboarding of any suppliers. This includes reviewing data handling practices, encryption standards, and access controls before recommending solutions to clients.
- Supplier Vetting: All vendors we work with are evaluated for GDPR compliance, including their use of data processors, sub-processors, and data residency policies.
- Minimal Data Handling: We store minimal personal data (e.g., names and email addresses) solely for communication and support purposes. This data is handled securely, in line with GDPR principles, and is never used for profiling, marketing, or shared with third parties without consent.

3. Using the service

Ordering and Invoicing

To order services from our organisation, you can simply send an email to gcloud@ng-it.co.uk to discuss your requirements in more detail and initiate the process. We recommend including key information in your email such as your organisation name, a brief description of the services needed, preferred start date, expected outcomes, and any relevant procurement references. Once we have reviewed your request, we will assist you in completing the Order Form, which formalises the agreement under the framework and becomes the Call-off Contract. This includes support with service scope, pricing, and terms to ensure everything aligns with your expectations. Our fees are invoiced monthly in arrears, and payment terms are 30 days net from the date of invoice receipt.

Availability of Trial Service

At the present, complimentary trial of the Arctic Wolf Managed Risk Solution cannot be offered, as the nature of the Service involves fully managed security operations that cannot be replicated in a short period and standalone trial environment. As an option to the trial and upon request, we can offer a product demo and a Proof of Concept (POC). The POC will give you a good view of the Product capabilities and how the service aligns within your environment, allowing an applied assessment, and the demo can provide an overview of core functionalities.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

Once the Managed Service Contract is signed and we have the confirmation of your order, the onboarding process begins, and a designated team is assigned within the Service Provider to coordinate all aspects of your contract and provide a smooth onboarding process. As the IT Reseller, NG-IT will assign a dedicated Service Delivery Coordinator, that will look after your contract and lease periodically with the Service Provider during the whole lifetime of your service. At this point, your dedicated Service Delivery Coordinator will make sure that the Service Provider will follow the steps outlined in their onboarding process

As a starting point, you will receive a Welcome Email from the Service Provider and an invitation to schedule a kick off call. This servers as a formal starting point and you will be introduced to the team that will work with you during the implementation period. During the kick off call, it is expected that the Service Provider walks through the initial scope of the service, get a mutual understanding of what is included and outline next steps.

- The effort required to onboard to the service is minimal, but there are a few activities below that are required by the customer IT team:
- Attend the Onboarding and Technical Kick Off calls (1 hour each)
- Add required information in Customer Portal (30 mins)
- Connect the MDR Network Sensor (30 mins in firewall site)
- Download and deploy Managed Risk internal scanner (30 mins)
- Deploy Arctic Wolf agent (typically automated through software deployment tool like SCCM)
- Configure syslog sources to forward to network sensors (30 mins)
- Attend handover call to Concierge team (1 hour)

There are four phases that the Solution covers to ensure it can be leveraged to effectively discover, prioritize, act, and report on your cybersecurity risks.

Phase 1 - Deployment phase

The Deployment Security Team (DST) will work with you to deploy the Arctic Wolf platform, integrate critical data points, and build an understanding of your network.

Installation and Integration

DST starts with the essential task of identifying assets in your environment and defining your attack surface across network, perimeter, host, and accounts. Arctic Wolf configures and validates the environment, and makes reports available for the internal, external, and agent-based scanners, as well as CSPM (if purchased).

Phase 2 - Configuration phase

Throughout the deployment phase, DST will continue to gain a clear understanding of and visibility into your attack surface by establishing asset context and a vulnerability baseline.

Concierge Kick-Off

If applicable to your subscription, Concierge kick-off is when your CST will begin the proactive MR security process. The CST contextualizes your attack surface with definition and identification of your internal IT practices and requirements, including asset criticalities, policies, procedures, patching cycles, and your service level objectives (SLOs), enabling you to prepare your environment to end cyber risk. Once this information has been collected, the CST assesses and provides you with your documented risk priorities within your environment.

Identity and Coverage Resolution

CST delivers your overall vulnerability management program context, providing insight on your current device and network coverage, as well as identity issues within your environment. CST will provide recommendations to fix any identified coverage issues and ensure coverage of your desired attack surface is covered by the Solution.

Define and Configure Asset Context

The Arctic Wolf platform provides an initial critical asset list. This list is reviewed with you to identify any gaps. We then recommend asset criticalities, workflow, and organization tagging to make your environment more contextualized.

Threat Landscape and Prioritization Review

The Solution provides you with tailored risk prioritization according to asset and risk context on your overall attack surface so you can begin patch management.

Phase 3 - Active Cycle

The Active Cycle phase centers on vulnerabilities and is a steady state and continuous cycle. The goal of the Active Cycle is to ensure proper coverage of your environment, provide surface information that will aid the prioritization of risks, provide consultation to you as you harden your environment (if included with your subscription), and ensure your risk mitigation efforts are successful. The goal is accomplished through the following four sub-phases that are continuously cycled through:

Discover
Identify differences between the initial or previous asset baseline to understand your attack surface.

Assess
Obtain risk metrics and prioritized list of risks and their descriptions through the MR Workbench and/or Unified Portal to gain a clear understanding of prioritization of risks and to support assignment to an appropriate mitigation team.

Harden

With CST's support, if included, resolve prioritized risks and manage and mitigate overall cyber risk, ensuring you benchmark against configuration best practices and continually harden your security posture.

Validation

Review progress made towards overall cyber risk mitigation by rescanning such risks to ensure efforts were successful.

Phase 4 - Decommissioning phase

Decommissioning is the process of removing MR from your organisation's environment and your organization's data from the Arctic Wolf environment.

Please have in mind that this is not a static process and the steps and timeframes may vary according to the environment sizing and complexity. A detailed implementation plan can be provided to the buyer on request.

Training

As a reseller, we provide buyers with access to the service provider's comprehensive training and onboarding resources. These include online help documentation, knowledge bases, and guided assistance to support orientation with the new service. Introductory onboarding sessions are available to ensure buyers understand h
ow to configure, monitor, and manage the cyber security platform effectively. Where required, we facilitate access to the provider's customer success team for tailored onboarding support. Our role is to ensure buyers are connected to the appropriate resources and that any queries are escalated promptly to the service provider for resolution.

To guarantee a seamless and smooth environment transition and data migration, the Service Provider will provide support and guidance as part of the Service onboarding. You will receive all the instructions to help you migrating and setting up your Service. Service Provider will provide training around the Arctic Wolf systems, either via training materials or walk-throughs, to ensure that you have all necessary information to navigate through Arctic Wolf with confidence. You will also have access to Webinars and Education Sessions, and an extensive learning content library available on the customer portal.

As part of our service we include, as standard, the Concierge delivered Security Journey. The security journey is unique to you and tailored to achieve your security objectives, for example: cybersecurity compliance, secure cloud adoption, improved security posture. The journey can be delivered at a cadence that supports your team and your CST owns scheduling meetings and driving the outcome at a pace suitable for your organisation. Your CST team will prepare and own the delivery of each Security Journey session - SPIDR (Security Posture in depth Review).

We encourage customers to attend these sessions to understand the recommendations your CST outlines to improve your security posture and reduce your cyber risk. Each security journey session typically lasts an hour.

You will also count with 24x7 support team, that can be contact via email, phone or ticket and will be available not only to assist you with incidents and technical related issues but answering any questions you may have on how to use the Service Provider features.

Service Management

We take an integrated approach when it comes to the management of Services as we understand that an effective service delivery relies on a balanced integration of expert personnel, mature ITIL v4 aligned processes and technology. From a workforce perspective, our team possess both technical and behavioural competencies required. This includes not only the commercial knowledge of our products and solutions, but technical proficiency to build the service architecture, relying on a Team of experienced Solution Architects that holds the accreditations necessary to support the delivery of our Services.

In alignment with the technical team, we have a Service Delivery process in place that maps out the level of Service that is expected and provide operational consistency and governance throughout the delivery of the Service. This includes a Team of dedicated Coordinator that hold ITIL v4 Certification and is assigned to reinforce a customer-centred approach and guarantee that all aspects of your contract are being provided accurately. This process guidelines are outlined based on ITIL Framework, which set the basis for all the procedures followed to guarantee the delivery of IT Services that meet customer's needs.

This process counts with clear escalation paths, service level agreements and communication protocols to safeguard service continuity and accountability. We also count with a well-structured continuous improvement procedure, including post incident review with the customer and the Service Provider, and trend analysis that will help us to identify and tackle any systemic issue and enhance our client experience and satisfaction. These processes help us to set the standards of what we do as the IT Reseller but also direct what we expect from the Service Provider Partner.

Service Constraints

The Service Provider do not count with a published Uptime Guarantee as the solutions include outside factors that are outside their control including use of hosting providers. They also ingest data from 3rd party sources which could be delayed due to items outside of Arctic Wolf control and result in an inability to notify/detect threats for a given telemetry source. It is also important to say that Arctic Wolf has architected its solution for high availability aligned to the six pillars of the AWS Well Architected Framework, including replication in AWS availability zones for recovery purposes. While Arctic Wolf does not publicly publish uptime numbers, the percentage of uptime measures the functional availability of Arctic Wolf products and services, specifically how many logs they successfully ingest within their platform. Their typical uptime SLO is at least 99.75%.
Rest assured that, as your IT Reseller, we will make sure that the Service Provider will notify you of any outages with a portion of its solution and provide a recovery time estimate.

Service Levels

Arctic Wolf monitor and manage the technology components required to deliver 24/7 MDR SOC service. This includes upgrades, uptime, status monitoring, etc. As well as monitoring their own infrastructure we also monitor the feeds / agents / sensors etc. from our customers environments that are ingested into their environment. Should there be an issue with any of the customers components, the Service Provider will engage with them to resolve based on the defined escalation paths in the system. Arctic Wolf staffs all its worldwide SOCs on a 24/7 basis, services for UK customers would be provided by their EMEA SOC's based in Germany and Ireland.

Incident Response Time
Arctic Wolf's current Service Level Objective for emergencies is 30 minutes. However, this is 30 minutes to receive an alert, triage an alert (providing information such as what, where, when, why and how and remediation actions) and provide a ticket to our customers. Caution should be exercised when measuring metrics in isolation with mean time to ticket or mean time to respond (e.g. MTTD and MTTR). If the alert is serious enough the triage engineer will have already acted in the form of host containment, session closure or user disabling as per the agreed engagement action with the customers prior agreed requirements. As a standard practice, Arctic Wolf provides response time SLOs which are incorporated into the contracts.
Standard response time SLOs are as follows:

- Emergency escalated via phone to Arctic Wolf's Security Services (inbound notice) - Arctic Wolf will respond within five (5) minutes
- Escalation of any Emergency (outbound notice) - Thirty (30) minutes of Arctic Wolf's discovery
- Acknowledgement of any schedule request submitted by Customer to security@arcticwolf.com One (1) hour from receipt of request
- Notification and escalation of any Security Incidents (outbound notice) - Two (2) hours of Arctic Wolf's discovery

What defines an emergency is jointly agreed between Arctic Wolf and the customer.
Emergencies - Following transition from the deployment team to the Core Support Team (CST), Customer and the CST will agree on and document which Security Incidents will be defined as an "Emergency". Emergencies will typically include the discovery of ransomware and other alerts that could cause degradation/outage to Customer's infrastructure security. Arctic Wolf will escalate Emergencies to Customer within thirty (30) minutes of Arctic Wolf's discovery of the Emergency.

As mentioned, NG-IT as your IT Reseller, throughout its Service Delivery Process and according to the ITIL v4 Framework guidelines, will make sure that the Service Levels will be followed by the Service Provider according to what has been agreed on the Service Agreement signed by all parties. As part of this, you will be able to count with a dedicated NG-IT Service Delivery Coordinator that will conduct period checks to all support tickets that you might have opened with the Service Provider and action on whatever is required to guarantee the effective delivery of the service.

Outage and Maintenance Management

Service Provider will monitor and manage the technology components required to deliver 24/7 Service. This includes upgrades, uptime/status monitoring, etc. As well as monitoring their own infrastructure we also monitor the feeds / agents / sensors etc. from our customers environments that are ingested into their environment. The Provider, to the extent possible, will notify the Customer about scheduled or emergency maintenance through the Provider's Account Management Application and portal. The Provider, to the extent possible, will notify the Customer about scheduled or emergency maintenance through the Provider's Account Management Application. The Provider will constantly update the Account Management Application information to advise the Customer when a maintenance is completed.

NG-IT as your IT Reseller, throughout its Service Delivery Process and according to the ITIL v4 Framework guidelines, will make sure that the Service Levels will be followed by the Service Provider according to what has been agreed on the Service Agreement signed by all parties. As part of this, you will be able to count with a dedicated NG-IT Service Delivery Coordinator that will conduct period checks to the Service Provider state and promptly address any outages and request ad-hoc service if applicable. Root Cause Analysis and Service Improvement Plans will also be requested whenever is appropriate.

Financial Recompense Model for not Meeting Service Levels

While us, as your IT Reseller and the Service Provider, aim to meet all proposed Service Levels, there may be occasions where performance falls short of circumstances outside of our direct control as outlined in the Service Constraints and Outage and Maintenance Management sessions of this document. The SLAs is an important way of measuring service quality rather than to trigger financial compensation, therefore, there is no financial credit available or refund.

In case of a failure from Service Provider on achieving the agreed SLAs, as your IT Reseller we will focus on addressing the issue with Arctic Wolf and providing you with clear answers and, when applicable, formal root cause analysis. We will also work collaboratively to ensure that a Service Improvement Plan is put in place and, if necessary, apply any change to prevent the failure from happening again in the future.

We are confident that this approach helps us maintain a strong and transparent partnership with our clients and service partner, keeping the service reliable, issues visible and improvement actions transparent.

4. Provision of the service

Customer Responsibilities

To deliver the best service and guarantee efficiency on the Service implementation and consistent service delivery, we operate under a shared-responsibility model, where all parties contribute and work in partnership during the lifetime of your contract. As our client, for service delivery effectiveness, we kindly ask your collaboration on:

- Providing the most accurate information during all phases of the Service Delivery
- Promptly notifying us of any significant business and technical changes that may affect the Service performance
- Providing timey responses to the Service Provider queries, incident responses and approval requests
- Adhering to agreed change-management processes, including approvals, lead times and risk assessments
- Submitting requests using approved channels
- Participating in Services Reviews
- Honouring contractual payment terms

Customer must identify the administrative users for its account which may include Customer's and its Affiliates' authorized (email authorization sufficient) third party service providers and agents ("Administrators"). Each Administrator will receive an administrator ID and password and will need to register with Arctic Wolf.

Customer is responsible for registering and updating its Administrators, or notifying Arctic Wolf, as applicable, about changes to Administrators, including but not limited to termination, change of authority, and the addition of Administrators. Customer acknowledges and agrees that Administrators will be able to view all Solutions Data and other traffic and activities that occur on Customer's network and that Customer is responsible for all activities that occur under Administrator accounts. Administrator IDs are granted to individual, named persons and cannot be shared or used by more than one Administrator but may be reassigned from time-to-time to new Administrators. Notwithstanding anything contrary herein, Customer understands and agrees that transmission of Solutions Data to Arctic Wolf may be impacted by in-country technical issues and requirements. Arctic Wolf will provide reasonable assistance to Customer in such instances but is not liable if the Solutions Data cannot be transmitted outside of such country.

Customer is responsible for implementing appropriate internal procedures and oversight to the extent it utilizes the configuration of workflows and processes, including but not limited to containment actions, and similar functionalities in conjunction with the Services. Arctic Wolf may recommend Customer, depending on the scope of the deployment, implement software and services to enable features of the Solutions or to permit increased visibility into Customer's environment.

Customer is responsible for making such determinations in its discretion and Arctic Wolf has no liability for Customer's decisions related thereto. Customer acknowledges that any changes Customer makes to its code, infrastructure, or configuration of the Solutions after initial deployment may cause the Solutions to cease working or function improperly or could prevent Arctic Wolf from delivering the

Solutions and Arctic Wolf will have no responsibility for the impact of any such Customer changes. Customer understands that depending on the Solution deployed, a Solution may consume additional CPU and memory in Customer's environment while running in production.

Public Entity Customers

If Customer is a public entity, Customer acknowledges and agrees this Agreement is the sole set of terms governing the delivery of the Solutions to Customer and for the avoidance of doubt, terms related to acceptance related to any services or work product shall not apply. The terms of any request for proposal(s), request for information, invitation to qualify, purchasing agreement or cooperative contract, or similar agreement Customer is using to purchase the Solutions (as defined below) from an Authorized Partner do not apply to Arctic Wolf. Further, Customer understands, and hereby consents, that Solutions Data may be accessed and processed by Arctic Wolf and its non-US Affiliates and their non-US citizen employees and Arctic Wolf's authorized third-party service providers in the United States, Europe, or other locations around the world. Notwithstanding anything contrary in any other agreement or purchasing contract, Customer understands and agrees that during the Subscription Term, Arctic Wolf will maintain security controls and processes no less restrictive than those set forth in its SOC 2 Type II report and ISO 27001 certification.

Customer is responsible for determining if Arctic Wolf's controls and processes comply with Customer's data handling and security policies. Customer represents that in purchasing the Solutions, (i) Customer is not relying on Arctic Wolf for performance of a federal prime contract or subcontract and (ii) Customer is not receiving federal funds to purchase the Solutions. If Customer does intend to rely on Arctic Wolf Solutions to fulfil its obligations under a federal prime contract or subcontract or utilize federal funds to purchase the Solutions, Customer agrees to provide Arctic Wolf advance written notice of that intention, and Arctic Wolf shall have the option to terminate this Agreement. Arctic Wolf Technology is a "commercial item", "commercial computer software" and "commercial computer software documentation," pursuant to DFARS Section 227.7202 and FAR Sections 12.211-12.212, as applicable. All Arctic Wolf Technology is and was developed solely at private expense and the use of Arctic Wolf Technology by the United States Government are governed solely by this Agreement and are prohibited except to the extent expressly permitted by this Agreement.

Detailed Service Terms and Conditions, including the Contractual Customer Responsibilities will be addressed in the Service Agreement.

Technical Requirements and Client-Side Requirements

To determine the details about the exact technical and client-side requirements to deliver the service, it is essential that we have a full understanding of your current environment, operational needs and challenges you may be facing. This initial assessment will help us to guarantee the correct application of the Arctic Wolf Managed Risk solution. Therefore, many of the technical requirements and client-side requirements will be discussed prior to an order being placed, but also during the onboarding and implementation stages, where all parties will work together to refine connectivity, security, access and workloads considerations. All requirements discussed prior to the order being placed shall be documented in the Order form and agreed between the parties. We consider that this approach ensures that the technical prerequisites are mapped out accurately and are aligned to the customer needs and expectations.

To ensure that full value of the Solution is received, each party's roles and responsibilities are defined in the table below.

Activity	Arctic Wolf	Customer
Deployment		
Install Scanners/vScanners		X
Scanner/vScanner configuration recommendations	X	
Configure Scanners/vScanners		X
Provide credentials for internal vulnerability scanning		X
Provide IP and domain targets for external vulnerability scanning		X
Provide domain targets for Account Takeover (ATO) scanning		X
Create a defined outbound security rule from your scanner IP address to all necessary Scanner IP addresses		X
Discover and deduplicate assets	X	
Assign asset criticality and tag assets	X	
Verify assigned asset criticality and tags		X
Configuration of owned network or host devices		X
Ongoing		
Enumerate vulnerabilities	X	
Patch systems showing vulnerabilities		X
Platform prioritized risks	X	
Remediation and mitigation of the risks		X
Verification of remediation activities	X	
Monitoring and alerting	X	
If ATO targets are configured, alert on high and critical severity breaches	X	
Metrics and reporting	X	
Update and maintain scanners	X	
Troubleshoot scanning MR technologies for issues and coverage	X	

After-sales Account Management

As the IT Reseller, we are not only committed to offering the best solution but also to build strong relationships with our clients, working with you closely, not only during the initial phase of the project but also after the Service is delivered and implemented. This is pivotal to us, as a Company, to work with you on a full end to end service and make sure your expectations regarding the Service are meet during the whole lifetime of your service. Unlike some specialist integrators, we are not just about selling a product, we are more interested in providing the right solution and we are committed to our customer's satisfaction.

As part of your service, you will have a designated Account Manager that will work closely with you on period reviews of our environment and will guarantee that you are being offered the most suitable solution/ service. You will also count with a Service Delivery Team that will liaise with you and the Service Provider on a regular basis, addressing all aspects of your service delivery and serving as your advocate to all your related service matters.

The Service Provider will also schedule Quarterly Business Reviews (QBRs) with your CST team and your Customer Success Manager. The purpose of these sessions is to review the last 3 months of service and your cyber risk status, review your security objectives, and share roadmap and service updates. The QBRs typically last an hour.

Termination Process

The Service Agreement shall be in effect for the Subscription Term, to be specified in the Order Form. Unless otherwise set forth on the Order Form, the Subscription Term for the Solutions, in its entirety, will automatically renew at the end of the initial Subscription Term for the same period of time as the initial Subscription Term, but in no event more than a twelve (12) month term, and subject to the then-current terms and price at the time of renewal; provided however, if either party would like to opt out of automatic renewal of the Subscription of the Solutions or reduce Subscription scope, then such party must notify the other party no less than sixty (60) days prior to the expiration of the then-current Subscription Term.

As a subscription Solution, Arctic Wolf does not allow for termination for convenience. Arctic Wolf relies on committed subscription terms, in part, to manage our dedicated CST resource model. Either party may terminate this Agreement for cause if the other party commits a material breach of this Agreement, provided that such terminating party has given the other party ten (10) days advance notice to try and remediate the breach. Upon termination, Customer agrees to cease all use of the Arctic Wolf Technology, installed or otherwise, and permanently erase or destroy all copies of any Arctic Wolf Technology, including all Content and virtual Equipment, that are in its possession or under its control and promptly remove and return all physical Equipment to Arctic Wolf. Except as otherwise required by law, Arctic Wolf will remove, delete, or otherwise destroy all copies of Confidential Information in its possession upon the earlier of (i) the return of the Equipment, if applicable, to Arctic Wolf, or (ii) one hundred-twenty (120) days following termination. Notwithstanding anything contrary in the Agreement, should Customer fail to return any Equipment within ninety (90) days following discontinuation of use of the Equipment or termination or expiration of the Agreement, Customer will be liable for the replacement cost of the Equipment, which shall be due and owing upon receipt of the invoice from Arctic Wolf or the Authorized Partner, and Customer shall be liable for any breach of the Confidential Information and Arctic Wolf Technology contained within the unreturned Equipment. Sections 6 through 13, 14, and 15 will survive the non-renewal or termination of the Agreement.

5. Our experience

Case Study

Security Operations Service for a Large UK Education Organisation

Overview

A major UK education institution with over 35,000 users—a mix of students, academic staff, and administrative teams—faced escalating security risks across a highly distributed, multi-site environment. With critical teaching, research, and operational services at stake, the organisation required a modern security operations service that could deliver full visibility, integrate with existing technologies, and operate within tight public-sector budget constraints.

Challenges

- **Complex, multi-site estate:** The organisation operated multiple campuses and satellite locations, each with differing levels of maturity and legacy infrastructure.
- **Highly sensitive data:** Research outputs, student records, financial information, and regulated datasets demanded robust protection and rapid incident response.
- **Limited visibility:** Fragmented tooling and inconsistent logging meant the internal team lacked a unified view of threats across endpoints, networks, cloud services, and identity systems.
- **Public-sector budget pressures:** The institution needed a predictable, fixed-cost model that avoided unexpected overages or consumption-based volatility.
- **Operational noise:** High volumes of low-value alerts were overwhelming internal IT teams, reducing their ability to focus on genuine threats.
- **Varied service needs:** Different departments and services required different response times and coverage windows, from 24/7 monitoring for critical systems to business-hours support for administrative services.

Solution

The organisation partnered with NG-IT to select a specialist Security Operations provider to deploy a **fully managed SOC service** built around the following capabilities:

- **Unified visibility:** Integration with existing endpoint, network, and cloud security tools created a single, correlated view of activity across the entire environment.
- **Technology-agnostic approach:** The service was designed to work with the institution's current investments—including EDR, email protection, networking equipment, cloud and identity platforms—avoiding costly rip-and-replace programmes.
- **Predictable pricing:** A fixed annual subscription model aligned with public-sector budgeting cycles, ensuring transparency and long-term affordability.
- **Noise reduction:** Automated and human triage enrichment filtered out false positives, ensuring that only genuine, high-fidelity security alerts were escalated to IT teams.

- **Customisable service levels:** Tailored SLAs allowed the organisation to match response times and operating hours to the criticality of each system or service, optimising service delivery & resources without compromising protection.
- **Multi-site coverage:** The SOC provided consistent monitoring and response across all campuses, regardless of local infrastructure differences.

Conclusion

- **Reduction in alert noise**, enabling internal teams to focus on strategic security improvements rather than reactive firefighting.
- **An outcome focussed service**, by incorporating environment specifics and context with an enhanced level of detection logic and alert efficacy the team were able to concentrate their efforts more effectively.
- **Full estate visibility** across multiple campuses and inclusive of on-premises & cloud, environments, significantly improving threat detection and response times.
- **Improved compliance posture** for data protection and alignment with regulatory requirements.
- **Cost predictability** that aligned with public-sector financial planning and avoided unexpected operational expenditure.
- **Enhanced resilience** across critical teaching, research, and administrative services through tailored SLAs and 24/7 monitoring where required.
- **Stronger security culture** as internal teams gained confidence in the clarity, accuracy, and relevance of escalated alerts.

Clients

Contact Details

For any questions regarding this offer, please send an email to ***gcloud@ng-it.co.uk*** and we will respond as quickly as possible to assist with your request.