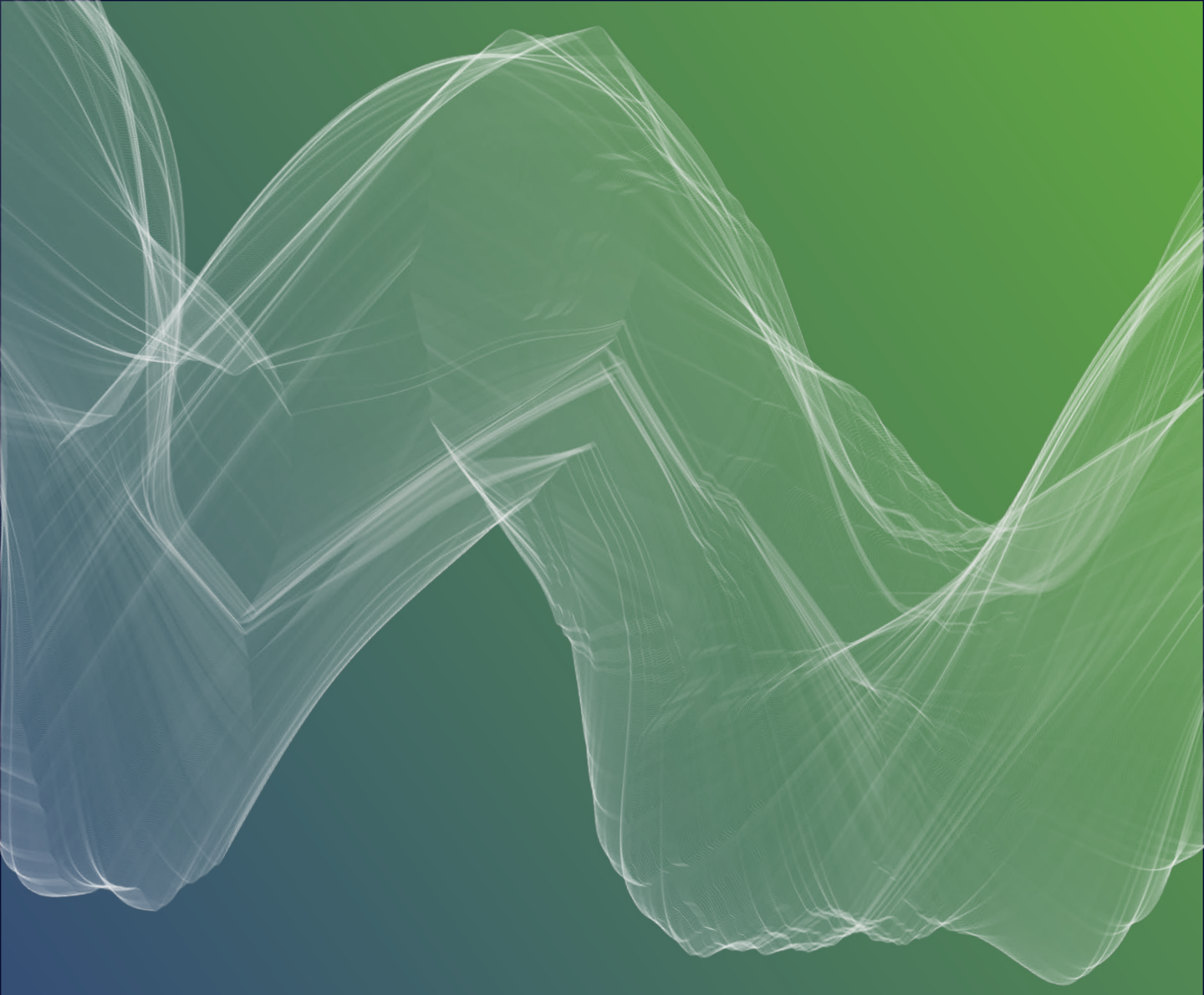


kainos®

Cyber and AI Security Monitoring

Service Definition Document

G-Cloud 15

Status: Definitive
Security Commercial – In Confidence
Version no.1/0

We're Kainos

Formed in 1986, we set about finding the best people to tackle the most difficult digital work. We fostered a culture where people truly care for each other and the world around them.

Our reputation for software engineering and problem-solving was quickly established, and our customers started to view us more as their colleagues

We're much bigger now, helping organisations across the globe to navigate change in more ways than ever. But some things never change, like our commitment to our people, delighting our customers, and our technical ability

Some say we're leading a quiet revolution in digital, but if you ask us, we're just doing our bit to make the world a little bit better.

- 3,132 amazing people
- 13 consecutive years of growth
- 40 years of innovation
- £382m revenue (FY2024)
- 13 locations globally
- FTSE 250 listed tech company

Our core expertise

The digital revolution is already happening. We're leading from the front to help our clients **seize every digital opportunity** and be future-ready.

- Cloud
- Business Applications
- Data and AI
- Managed services
- Engineering
- Service and experience design

Workday services and products

- Test
- Deployment
- Audit
- Optimisation
- Shield
- Spark & Grow

Cyber & AI Security Monitoring

Our Cyber and AI Security Monitoring offering ensures customers are provided with real-time monitoring, advanced threat detection, and continuous validation of security controls, across both AI and traditional systems, so they can spot threats, respond quickly, and ensure their defences are always working as intended.

Features

1. **Continuous Monitoring & Telemetry,** live dashboards, alert rules, integration documentation.
2. **Threat/Anomaly Detection Engineering,** detection rule libraries, tuning documentation, coverage maps.
3. **Model Integrity/Drift Monitoring,** monitoring dashboards, drift/integrity alerts, investigation playbooks.
4. **Control Effectiveness Validation,** validation reports, automated test results, improvement recommendations.

Benefits

1. Detect threats early, before they cause operational harm.
2. Respond faster to incidents with clear, actionable intelligence.
3. Reduce risk of undetected breaches and compliance gaps.
4. Gain measurable confidence your security controls are effective.
5. Maintain demonstrated compliance with industry and regulatory standards.
6. Free up security analysts for strategic, higher-value activities.
7. Improve visibility across complex cloud and hybrid environments.
8. Adapt detection rules quickly to new threat types.
9. Protect AI and IT workloads with unified detection.
10. Receive actionable insights for continuous security improvement.

Cyber & AI Security Monitoring

What is Cyber and AI Security Monitoring?

Cyber and AI Security Monitoring is a structured detection engineering and monitoring optimisation service that transforms your existing Microsoft-based security infrastructure into a measurable, auditable, and operationally resilient defence platform. Rather than deploying a SIEM from scratch, we optimise what you already have - Microsoft Sentinel, Defender, Entra ID, and Purview - to deliver real-time visibility, advanced threat detection, and continuous control validation across both AI and traditional systems. The service culminates in a handover to a managed SOC or MDR partner, ensuring your investment in detection engineering is sustained and continuously improved through professional 24/7 operations.

This approach reflects decades of Kainos experience across government, national infrastructure, healthcare, and international organisations. We move you from detection uncertainty and reactive incident response to proactive threat spotting, measurable compliance posture, and confidence that your security controls are working as intended—every day.

Why Detection Engineering Matters for Your Organisation

The cost of a missed breach is immense. Yet many organisations struggle with alert fatigue, false positives, and blind spots where threats go undetected for weeks. Traditional SIEM deployments often fail because they lack contextual tuning, AI-aware rules, or integration with modern cloud and AI workloads. Cyber/AI Security Monitoring solves this by:

- **Engineering detection within your context.** We don't impose generic rules; we map your environment - your data flows, asset criticality, AI models, and threat landscape - then build and tune detection content to reflect your real risk. This includes AI-specific threats such as model drift, adversarial attacks, and unusual ML inference patterns that standard rules miss.
- **Reducing noise whilst improving coverage.** Through alert correlation, and machine learning analytics, we identify the detections that matter and suppress the ones that waste your team's time. This frees security analysts to focus on genuine threats rather than chasing false positives.
- **Proving effectiveness with measurement.** You receive dashboards, KPIs, and coverage maps that show exactly what your detection infrastructure covers, where gaps exist, and how quickly you respond to incidents. This is critical for board reporting, compliance audits, and budget justification.
- **Supporting both traditional and AI workloads.** Whether you're running monolithic applications, microservices, or machine learning models in Azure, AWS, or on-premises, Cyber/AI Security Monitoring provides unified visibility and detection across your hybrid estate. This unified approach is essential in today's multi-cloud, AI-infused world.

Cyber & AI Security Monitoring

How It Works:
We give you the oversight and intelligence to spot threats and control failures, across both AI and traditional systems, before they become business problems.
Build advanced detection rules and analytics to catch both known and emerging threats.
Set up real-time monitoring and alerting for your most important assets.
Continuously test and validate your controls, so you know they're working as intended.

Don't wait for a breach to find out you're exposed, get the visibility and assurance you need, every day, always.

Threat & Anomaly Detection Engineering
Missing advanced threats or subtle attacks?
We build and tune detection rules and analytics, so you catch both known and unknown threats, across AI and conventional environments.
Service: Develops and tunes detection content (rules, analytics, ML models) to identify threats and control failures in both AI and conventional environments.
Outputs: Detection rule library, tuning documentation, detection coverage map.

Continuous Monitoring & Telemetry
Afraid you won't spot an attack until it's too late?
We set up real-time monitoring across your AI and IT systems, so you get instant alerts when something's amiss.
Service: Deploys monitoring solutions for AI and IT systems to provide real-time oversight of security controls and detect anomalies.
Outputs: Monitoring dashboards, alerting rules, telemetry integration documentation.

Control Effectiveness Validation
Unsure if your security controls are actually working?
We continuously test and validate your defences, so you know they're effective, and spot new gaps before attackers do.
Service: Continuously tests and validates that implemented controls (from PROTECT) are working as intended, and identifies emerging gaps.
Outputs: Control validation reports, automated test results, recommendations for improvement.

Model Integrity & Drift Monitoring (AI-specific)
Worried your AI models could be tampered with or degrade over time?
We continuously monitor your AI models for integrity issues, performance drift, and adversarial manipulation—alerting you before small problems become big ones. This ensures your models remain accurate, secure, and trustworthy throughout their lifecycle.
Service: Implements automated monitoring for AI models, tracking behaviour changes, detecting anomalies, and validating model integrity against baseline performance.
Outputs: Model monitoring dashboards, drift and integrity alerts, investigation playbooks, and recommendations for corrective actions.

Cyber & AI Security Monitoring

Why Choose Kainos?

Kainos has delivered detection engineering and monitoring optimisation across complex, high-assurance environments. We bring:

- **Proven expertise in government-grade and regulated sectors.** Our work with UK Central Government (HMCTS platform), national infrastructure (National Highways SOC), health (NHS App), and international organisations (UN's International Organisation for Migration) demonstrates our ability to design detection that scales and meets the strictest security standards.
- **Understanding of co-managed SOC operations.** We don't just build detection and walk away. We understand the realities of 24/7 operations, multi-supplier coordination, and the handover process. Our material reflects active procurement experience and lessons learned from live SOC operations.
- **AI-aware security perspective.** Unlike generic SIEM vendors, we recognise that AI and machine learning introduce new threats and require new detection approaches. Our detection library includes AI-specific content (model drift, inference anomalies, data poisoning signals) that protects your AI initiatives, not just your legacy infrastructure.
- **Measurement-driven approach.** We don't believe in detection-by-assumption. Every detection is tested, every dashboard backed by real telemetry, and every recommendation grounded in data. This rigour earns trust with board members, auditors, and security teams alike.
- **Microsoft ecosystem integration.** We leverage the full power of the Microsoft stack—Sentinel, Defender for Cloud, Entra ID, Purview, Azure Lighthouse—ensuring your detection strategy is unified, efficient, and cost-aware.

Outcomes You Can Expect

- **Reduced mean time to detect (MTTD).** From weeks or months to hours or minutes, through early threat spotting and actionable alerting.
- **Lower operational burden on your security team.** Alert fatigue drops; analysts focus on high-confidence incidents; time-to-respond improves.
- **Auditable compliance posture.** Dashboards prove control effectiveness to auditors, regulators, and internal stakeholders. You can demonstrate continuous monitoring and rapid response capabilities.
- **Confidence in your defence posture.** By validating controls through exercises and measurement, you move from guessing to knowing that your defences work.
- **Smooth transition to managed operations.** Your handover to a SOC or MDR partner is clean, well-documented, and supported by Kainos' expertise and runbooks.

Where we are

The Americas

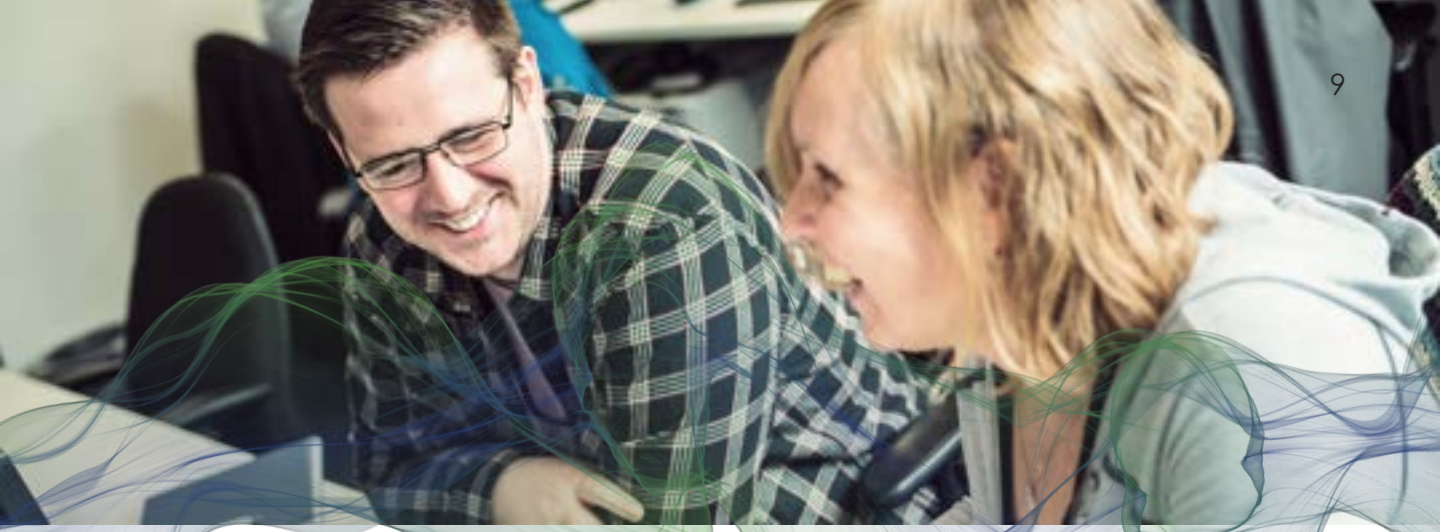
Buenos Aires
Indianapolis
Nova Scotia
Toronto

UK and Ireland

London
Birmingham
Belfast
Derry
Dublin

Central Europe

Gdansk
Helsinki
Paris
Wommelgem



What makes us stand out

- Our people
- True collaboration
- Innovation
- Digital know-how
- Common goals
- Trust

Digital Services

We are **engineers**, specialists. We **overcome big challenges** for our clients, through delivery of **intelligent** digital services that use the best in **talent and technology**.

NHS
Ministry of Defence
Department for Environment Food & Rural Affairs
Department for Transport
UK Health Security Agency
Home Office
Driver & Vehicle Standards Agency
Ministry of Justice
HM Revenue & Customs
Foreign & Commonwealth Office

55 million UK citizens

positively impacted by services we've delivered

892 customers

13 locations

And growing

99% of customers

rate our service as good, great or excellent

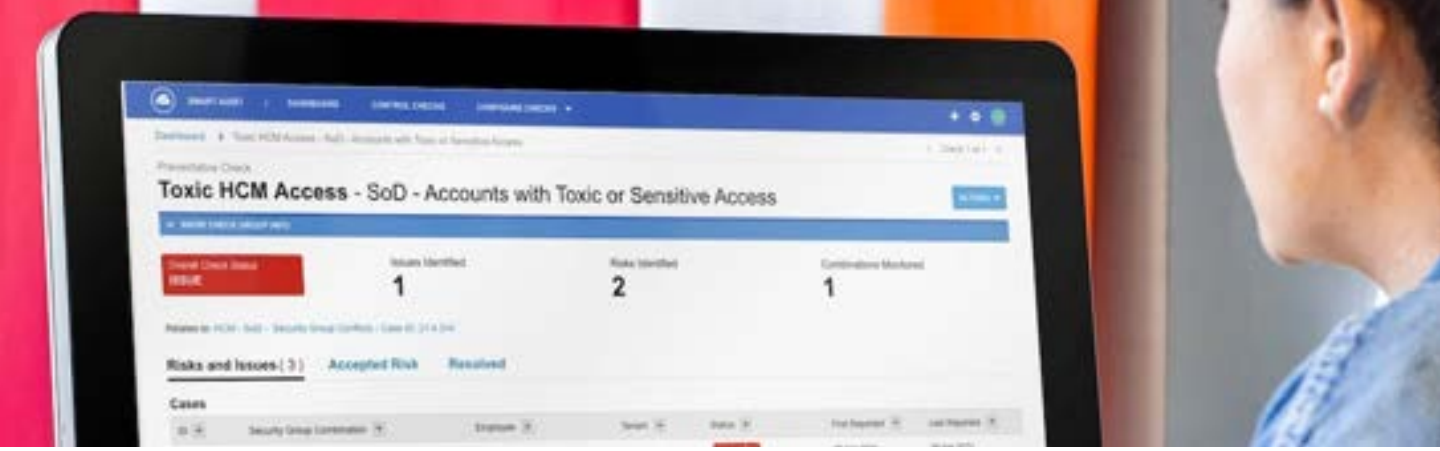
Key partners

Working closely with Microsoft and AWS to deliver results

Award-winning

90+ industry awards

kainos®



Workday

Kainos is a Workday **phase one prime status partner** in all European, North American and Asia Pacific markets. We have worked with many public and private sector customers of various sizes and scale in over **40 countries worldwide**.

aggreko | KION GROUP | Magellan HEALTH | St. Luke's Health | The National Archives

Crown Commercial Service | Department for Education | NETFLIX | UKRI Innovate UK | Nasdaq

Partner Since 2011

We are the only certified Workday Services, Technology and Extend partner globally.

Workday Services

Full range provider from pre-deployment consulting, implementation and support.

650+ Customers

We have deployed to over 650 customers and are a proud Workday customer also, using HCM, Financials, Recruitment, Planning and PSA to run our business.

Workday Public Sector

We have worked with many UK Public Sector customers with their initial deployment, post-deployment support and adoption of new modules.

Kainos Smart

Our product is deployed to 500+ customers globally saving them 1000s of testing hours.

900+ Consultants

Hold over 2,700+ Workday certifications covering all areas of the platform.

65 million

citizens positively impacted by services **built by Kainos** for the UK Government

Every driver & every car on the road
Every piece of work to fix roads
Every court case & every prisoner
Every home helped with help-to-buy
Every passport & renewal application
Every COVID test sent out
Every COVID test result
Every user of the NHS App

Every voter registered
Every company opened & closed
Every UK civil servant trained
Every piece of produce grown in the UK
Every thing imported & exported to the EU
Every benefit fraud prevented
Every body's pension details

kainos®

Our Social Values and commitment to HM Government strategy

Education & Capability Building

We empower people through technical and behavioral learning programs, academies, and outreach projects, fostering skills development and inspiring future technology leaders across communities and organisations.

Social Responsibility

Tackling workforce inequality and ensuring equal access to technical and vocational education, through our Academies, Camps and Earn as you Learn schemes.

Innovation & Future Readiness

Driving continuous improvement through technology

Health, Wellbeing & Accessibility

We support colleagues' physical, emotional, and career wellbeing through initiatives, guidance, and inclusive design, ensuring equal access, experiences, and compliance for all users with diverse needs.

Climate Action & Sustainability

With a comprehensive sustainability strategy underway, we will be a Carbon Net Zero company by 2030.

Equality, Diversity & Inclusion

Maximising service experience for citizens and civil servants by delivering projects with diverse teams, underpinned by our BAME, LGBTQIA+ and female communities.

The Code of Ethics

We are guided by our 6 ethical principles.

Wellbeing
We protect the wellbeing of our staff, customers and communities.

Equality
We improve access and inclusion and minimise bias.

Transparency
Our decisions are traceable and accountable.

Integrity
We hold ourselves and others to ethical standards.

Environment
We act responsibly towards the Earth and its resources.

Initiative
We take initiative to deliver social value and positive impacts.

BCDR and Exit Plan

Business Continuity and Disaster Recovery (BCDR)

A Business Continuity Plan can be provided if required. This shall set out the arrangements to be invoked in the event of an actual or perceived threat to business continuity, to ensure continued operation of the system and continuity of the services provided by Kainos pursuant to the Prime Agreement and shall include: the alternative processes, options and responsibilities that may be adopted in the event of a failure or disruption to the system and/or services provided by Kainos pursuant to the Prime Agreement; and the steps to be taken by Kainos upon resumption of the system and services provided by Kainos pursuant to the Prime Agreement in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

Exit Plan

An Exit Plan can be provided if required to detail the steps that would be carried out to ensure smooth transition of Kainos services to a new supplier. The steps outlined in the Exit Plan will help mitigate against any disruption to the service during the transition period. It is assumed that any new supplier will themselves have a procedure they wish to follow during the transition period, and as such the steps in this Exit Plan will serve as a checklist for the new supplier to ensure all key areas of the transition have been covered. The Exit Plan will therefore be subject to refinement should it be exercised.

Commercial Statement

Confidentiality and copyright

Trademarks

Caveats

Kainos has used all reasonable endeavours to ensure that the contents of this document are accurate but is not responsible for any errors or omissions.

All information provided prior to execution of a contract is provided 'as is' and 'subject to contract' without warranty of any kind.

This document does not constitute an offer from Kainos. In the event that the parties elect to work together, they will only be contractually bound to each other upon signature of a contract.

Corporate information

"Kainos" is the trading name of the Kainos group of companies, further information on which can be found here: https://www.kainos.com/corporate-information/.

Kainos Software Limited/ Kainos WorkSmart Limited, will be the contracting entity under this tender / for the provision of the service and may be assisted from time to time by other Kainos group companies.

Freedom of information

Kainos considers that the following information provided in this document is exempt from disclosure under the Freedom of Information Act 2000 (FOI):

The CVs of staff qualify under the "Personal Information Exemption (s.40)" of the Freedom of Information Act and are exempt from disclosure under the Data Protection Act 1998. The Period for which this information should be confidential is the lifetime of the Data Subject.

Rate and pricing information is confidential and commercially sensitive and covered by the 'Commercial Interests' exemption (s.43) of the FOI, as the release of this information is likely to prejudice the commercial interests of Kainos and is likely to adversely affect its (and the Customer's) future negotiating position. The period that this information should be confidential for should be 5 years.