devoteam

elastic

Service Definition Document

Version: 1.0

Date: 29/01/2026

G-Cloud 15

AI-driven tech consulting

Summary

Welcome to Devoteam **3**
- Agile at Scale, Local in Delivery 3
- The Power of Strategic Partnerships 3
- End-to-End Transformation 3

Devoteam Elastic Partnership **4**

Why Elastic? **4**
- Overview 4
- Technical Insight 4
  - Technical Insights: Search AI and RAG Architecture 4
  - Technical Features 5

Why Devoteam? **6**
  - Our Services 6

General Information **8**
- Onboarding and Offboarding 8
- Data Backup and Restore, BCP and Disaster Recovery 8
- Service Levels 9
- Termination 9
- Service Constraints 9

Ordering Process & Contact Details **10**
- Order process 10
- General Enquiries 10

About Devoteam **10**

Welcome to Devoteam

Devoteam is a leading consulting firm focused on digital strategy, tech platforms, cybersecurity, and business transformation. What defines us is Technology, it is our DNA. We believe in technology as a positive force, driving "Creative Tech for Better Change" across the UK Public Sector.

Agile at Scale, Local in Delivery

With over 25 years of experience, Devoteam has reached a level of maturity that allows us to support large-scale government transformations while remaining agile and responsive. We are a "mid-sized" specialist: big enough to offer global reach and massive R&D investment, yet small enough to provide the senior-level attention and flexibility that UK public sector bodies require.

- 11,000+ experts across EMEA.
- Dedicated UK-based consultants, many with high-level security clearances, ensuring compliance with UK data sovereignty and GDS standards.
- We continuously certify our people on the latest technologies to ensure our clients achieve measurable, high-impact results.

The Power of Strategic Partnerships

Devoteam's core belief is that organisations must think and behave like "Tech Players" to thrive. This requires a robust technological foundation built on world-class cloud platforms.

In the UK, we focus on leveraging the research and development power of our primary strategic partners. By mastering these ecosystems, we help our clients scale rapidly and securely.

End-to-End Transformation

Our circular, continuous innovation journey takes you from vision to reality:

- We co-create new digital services and citizen experiences.
- We build and implement these services on secure cloud platforms.
- Through our Cloud Managed Services, we ensure your digital products are always secure, optimised, and evolving with the latest platform features.

By combining the world's leading cloud platforms with our expertise, we provide a powerful end-to-end approach that reduces legacy debt and accelerates the delivery of 21st-century public services.

Devoteam Elastic Partnership

As an **Elastic Elite Partner**, Devoteam combines its extensive EMEA footprint with Elastic's "Search AI" platform to help organisations solve complex data challenges. We specialise in operationalising the **Elastic Stack (ELK)** to deliver real-time observability, enterprise search, and advanced security analytics.

Our partnership focuses on turning massive datasets into actionable intelligence. By leveraging Elastic's vector database capabilities and Devoteam's strategic consultancy, we enable departments to build AI-driven applications that are secure, scalable, and cost-efficient. From migrating legacy logging systems to deploying unified Security Operations Centres (SOC), our certified engineers ensure that Elastic becomes a core pillar of your **Data Intelligence Platform**.

Why Elastic?

Overview

Elastic is the leading **Search AI platform**, empowering organisations to find answers in real-time across massive datasets. By unifying **observability, security, and search** on a single stack, it eliminates data silos. Its scalable architecture provides critical insights, improves system resilience, and secures digital infrastructure while maintaining cost efficiency through advanced data tiering.

Technical Insight

Technical Insights: Search AI and RAG Architecture

Traditional search and analytics tools often fail when handling unstructured data or complex, natural-language queries. Elastic addresses this by evolving from a keyword-based engine into a comprehensive **Search AI platform**. At its core, Elastic utilises a **Vector Database** and **Hybrid Search** capabilities, allowing it to understand the *meaning* behind data, not just the text.

The most significant advancement is the integration of **Retrieval-Augmented Generation (RAG)**. This architecture allows organisations to connect Elastic's real-time data retrieval with Large Language Models (LLMs). When a user asks a question, Elastic retrieves the most relevant, secure, and up-to-date information from your private data estate and provides it to the LLM as context. This ensures that the AI's response is accurate, grounded in your specific policies, and free from the

"hallucinations" common in public AI models. Combined with **Index Lifecycle Management (ILM)** and **Searchable Snapshots**, this architecture provides a high-performance, cost-effective foundation for modern, AI-driven digital services.

Technical Features

Unified Observability (Logs, Metrics, APM): Elastic provides a single pane of glass for monitoring your entire digital estate. By correlating logs, infrastructure metrics, and Application Performance Monitoring (APM) traces, teams can detect performance bottlenecks and system failures in real-time, significantly reducing Mean Time to Resolution (MTTR).

Generative AI & Vector Search (ELSER): Elastic's specialised vector database and Elastic Learned Sparse EncodeR (ELSER) allow for semantic search capabilities. This means the system understands the *intent* and *context* behind a query, rather than just matching keywords, which is foundational for building Retrieval-Augmented Generation (RAG) applications.

Cross-Cluster Search and Replication (CCS/CCR): Designed for geo-distributed environments, this feature allows users to search and replicate data across different Elastic clusters, regions, or even cloud providers (AWS, Azure, GCP) from a single interface, ensuring data high availability and disaster recovery.

Advanced SIEM & Security Analytics: Elastic Security provides an integrated SIEM (Security Information and Event Management) with pre-built detection rules and ML-driven threat hunting. It allows security teams to ingest petabytes of data for long-term forensic analysis while maintaining real-time threat detection across the network.

Index Lifecycle Management (ILM) & Data Tiering: Elastic optimises storage costs by automatically moving data between "Hot," "Warm," "Cold," and "Frozen" tiers based on age and frequency of access. The "Frozen" tier allows users to search data directly from low-cost object storage (like S3 or Azure Blob) without needing to re-hydrate it.

Kibana Lens & Advanced Visualisation: Kibana offers a drag-and-drop interface (Lens) that allows even non-technical users to build sophisticated dashboards. It supports geo-spatial mapping, time-series analysis, and complex data relations, making it easier to communicate insights to executive stakeholders.

Machine Learning & Anomaly Detection: Unsupervised machine learning features automatically learn the "normal" behavior of your data (e.g., typical server CPU usage or login patterns). When data deviates from this baseline, Elastic triggers alerts, allowing teams to catch issues before they impact end-users.

Fleet & Elastic Agent: Management of data collection is simplified through Fleet, a centralised management console. A single Elastic Agent is deployed to all hosts,

which can be remotely configured to collect logs, metrics, and security signals, eliminating the need to manage multiple individual "Beats."

Searchable Snapshots: This breakthrough technology allows Elastic to treat snapshots stored in low-cost cloud storage as live, searchable indices. This enables organisations to keep years of data online and searchable for compliance or historical analysis without the high cost of SSD-backed storage.

Open API and Extensive Integration Library: Elastic provides a robust REST API and hundreds of pre-built integrations for common technologies (Microsoft 365, Okta, ServiceNow, Kubernetes). This ensures that Elastic can easily ingest data from, and export insights to, any other tool in your technology stack.

Why Devoteam?

Choosing Devoteam for your Elastic journey ensures you aren't just deploying a search engine, but building a unified **Search AI and Observability foundation**. As an **Elastic Elite Partner**, we provide the specialised architectural knowledge required to scale the Elastic Stack (ELK) across complex enterprise environments.

Elite Partner Expertise

Devoteam holds the highest level of partnership with Elastic. This means our consultants have direct access to Elastic's engineering teams and product roadmaps, ensuring your implementation follows "Gold Standard" architecture.

- **Certified Architects:** Our team consists of Elastic-certified engineers with deep experience in large-scale cluster management.
- **Proven Blueprints:** We use standardised deployment frameworks to accelerate your time-to-value, avoiding the common pitfalls of self-managed ELK clusters.

Our Services

Search AI & Generative AI Integration

We help you move beyond traditional keyword search to build modern, AI-driven experiences.

- **Vector Search & RAG:** Implementing Retrieval-Augmented Generation (RAG) to provide secure, private context to Large Language Models (LLMs).

- **Semantic Search:** Utilising ELSER (Elastic Learned Sparse EncodeR) so your search tools understand user intent and meaning.
- **Private AI:** Ensuring your data stays within your sovereign cloud boundaries while powering advanced AI features.

Unified Observability & ServiceOps

We eliminate operational silos by consolidating logs, metrics, and traces into a single "Source of Truth."

- **Full-Stack Visibility:** Real-time monitoring across multi-cloud and hybrid infrastructures.
- **AIOps & Anomaly Detection:** Using Elastic's machine learning to automatically detect performance issues before they impact users.
- **Tool Consolidation:** Replacing fragmented monitoring tools (Splunk, Datadog, New Relic) with a unified Elastic instance to reduce licensing costs.

Elastic Security (SIEM & EDR)

We deploy Elastic as a modern Security Operations Center (SOC) foundation.

- **Threat Hunting:** Leveraging pre-built detection rules and ML models to identify sophisticated cyber threats.
- **Security Analytics:** Centralising security logs for long-term forensic investigation and compliance auditing.
- **Endpoint Protection:** Integrating Elastic Defend to prevent, detect, and respond to threats directly on the host.

Architectural Excellence & FinOps

We ensure your Elastic environment is performant and cost-effective.

- **Data Tiering Strategy:** Implementing "Hot-Warm-Cold-Frozen" architectures to store petabytes of data affordably.
- **Searchable Snapshots:** Enabling real-time queries on data stored in low-cost object storage (S3/Azure Blob).
- **Cloud & Hybrid Deployments:** Expert management of Elastic Cloud (SaaS) or self-managed deployments on Kubernetes/EKS.

General Information

Onboarding and Offboarding

Every Devoteam assignment requires close collaboration with our clients and their suppliers. Our people build strong relationships; quickly orienting themselves with each Stakeholder's perspective, understanding their current and future needs as well as the desired state, the work underway and any current challenges, whilst facilitating consensus across the groups. We appoint one of our senior leaders to direct engagements and actively participate in senior-level workshops

It would be our aim to have continuously transferred knowledge throughout each engagement. However, at project closure, our Engagement Lead would also:

- Ensure that all defined Products have been delivered
- Any work in progress is documented and passed to an agreed client stakeholder.
- Run lessons learnt exercises relating to our delivery with key stakeholders and share the results.

Data Backup and Restore, BCP and Disaster Recovery

We are a professional services company and we deliver within our client's physical or virtual environment, we, therefore, adopt and follow our client's DR/BCP policies. Our engagements do not require us to remove data from our client's environments.

We operate hybrid and flexible working so agree with our clients where it would be best to locate the joint project team and we frequently have a mix of home working, on client site and at Devoteam offices. In addition, all Devoteam employees and associates use standardised laptops, operating systems and adhere to strict procedures and anti-virus measures to protect both Devoteam and client information at all times.

Devoteam maintains an office in central London for management and administration purposes, this is a serviced office, we rely on and adhere to services provided by that Serviced Office and their backup procedures. Should the office become inoperable for any reason our policy is to instruct central office personnel to work at home, where they are able to undertake their roles using their portable laptops until the event has been resolved. All Devoteam software is Cloud-based and so has a high degree of resilience and backup is provided as part of the licensing arrangements.

Service Levels

We would agree on a set of Service Levels that are appropriate for the type of engagement, covering, for example, Response and Resolution times. These services, depending on the scope and complexity of the delivery can take the form of

- Dedicated resources, from a single resource to a team of many.
- Remote and/or onsite delivery.

Full details of a Service Level Agreement, including consequences for failure to meet Service Levels, will be mutually agreed upon between both parties where appropriate.

Termination

Termination will be agreed upon on a project by project basis in alignment with G Cloud Terms and Conditions.

Service Constraints

Our services typically do not have any constraints.

Ordering Process & Contact Details

Order process

To place an order or request assistance please contact:

John Lacey

Managing Director

UKGovTenders@devoteam.com

0207 288 2800

General Enquiries

uk.info@devoteam.com

UKGovTenders@devoteam.com

0207 288 2800

About Devoteam

Devoteam is a tech consulting firm specialised in cloud, cybersecurity, data, and sustainability. Tech Native for over 25 years, Devoteam guides businesses through sustainable digital transformation to unlock their full potential.

With over 11,000 employees in more than 25 countries across Europe, the Middle East, and Africa, Devoteam is committed to putting technology at the service of people. To realise this vision, we partner with the top cloud platforms in the world, Microsoft Azure, Google Cloud, and AWS.