elastic | The Search AI Company

AI-driven security analytics

How Elastic Security aligns with the UK's AI framework

Responsible AI innovation

Artificial intelligence (AI) plays a crucial role in enhancing cybersecurity capabilities. Analysts and incident responders can—and will—gain a significant advantage by leveraging AI & generative AI to speed up threat detection, investigation, and response. Even UK regulators are promoting the use of "safe AI" through a principles-based framework to provide flexibility, collaboration, and responsible innovation.

5 core principles underpinning the UK government's AI regulation framework[1]

Safety, security & robustness

AI systems must be safe, secure against attacks or misuse, & robust enough to operate reliably in their entire life cycle.

Appropriate transparency & explainability

The basis & rationale for AI systems decisions should be transparent & explainable to those impacted by the decisions.

Fairness

AI systems should be developed & used in an equitable way, avoiding bias that leads to unfair discrimination or market outcomes.

Accountability & governance

There must be clear accountability & governance processes governing AI system development & use across the entire lifecycle.

Contestability & redress

Where appropriate, users & impacted third parties should be able to contest harmful AI outcomes or decisions.

[1] UK Government Policy: AI regulation: a pro-innovation approach

Introducing AI-driven security analytics

Elastic Security is the first and only AI-driven security analytics solution, replacing the traditional SIEM, that can empower analysts with limitless visibility, generative AI, and advanced analytics. It is poised to meet the challenges of the modern security team, the forthcoming UK AI regulation, and the existing EU AI Act. Why?

Secure, open, & flexible

1. **Distributed architecture:** Elastic's distributed data mesh architecture empowers teams with secure, governed access to stop damage and loss quickly
2. **Real-time visibility:** AI features of Elastic Security asses data representing the entire attack surface
3. **Privacy-first:** Anonymize and redact confidential information by default and as needed with field and document-level control
4. **LLM-agnostic:** Safely surface hyper-relevant knowledge and ground responses in proprietary data with retrieval augmented generation (RAG) and your chosen LLM.
5. **Open Security:** With Open Security, Elastic is committed to doing its work out in the open to ensure that customers are protected by the collective brainpower of everyone
6. **Elastic support:** Elastic is committed to offering guidance and assistance to customers protecting their network with the use of LLMs via access controls, cryptography, and Elastic Security Labs LLM Safety Assessment.

The AI advantage

Many Security Operations Centers (SOCs) have 1000s of alerts to sift through daily, and much of this work is dull, time-intensive, and error-prone. Elastic Security removes the need for such manual effort with AI Assistant and Attack Discovery.

AI Assistant

Make every user a power user

Empower every SOC analyst with Elastic AI Assistant. Streamline triage, investigation, and response while automating routine tasks for admins to boost team efficiency.

Attack Discovery

Prioritize attacks, not alerts

Triage hundreds of alerts into the few that matter with Attack Discovery. Assess alerts holistically rather than as one-off events to quickly understand the most impactful attacks and take immediate follow-up actions.

Validated by the best

Elastic named a Leader in The Forrester Wave™: Security Analytics Platforms

Bolt Booking.com Cranfield University SITECORE orange Emirates NBD mimecast

Accelerate the SOC with AI-driven security analytics, powered by the Elastic Search AI platform. Detect sooner, investigate faster, and respond before threats have a chance.