elastic
government solutions

The Data Foundation for AI-Driven Cyber Operations

How Elastic enables the Department of the Air Force to detect, investigate, and respond at machine speed.

elastic government solutions

The Modern SOC Is Drowning in Data

Volume and complexity are outpacing analyst capacity at the exact moment Air Force cyber threats are accelerating.

4,484

alerts per analyst per week

Vectra AI, 2026

63%

of alerts go uninvestigated

Prophet Security, 2026

183 days

avg. time to identify a breach

IBM 2026

20k+

DoW cyber workforce gap

Federal News Network, 2026

The answer isn't more analysts, it's smarter tools that surface what matters, automatically.

elastic
government solutions

Elastic Security: Built for Federal Scale

One platform. Petabyte-scale data. AI-native from the ground up.

SIEM

Search-Powered SIEM

Ingest, normalize, and correlate data from 700+ sources at petabyte scale. Built on Elasticsearch, the engine behind the world's most demanding search workloads.

AI

AI-Powered Detection

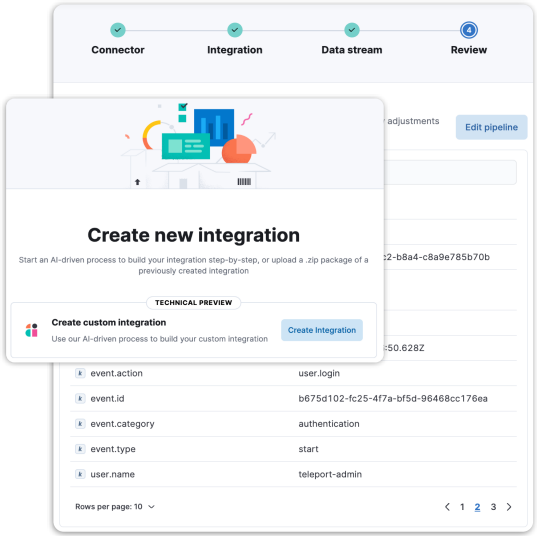
ML-driven anomaly detection, behavioral analytics, and MITRE ATT&CK-mapped rules that surface real threats, not just more alerts, with context analysts can act on.

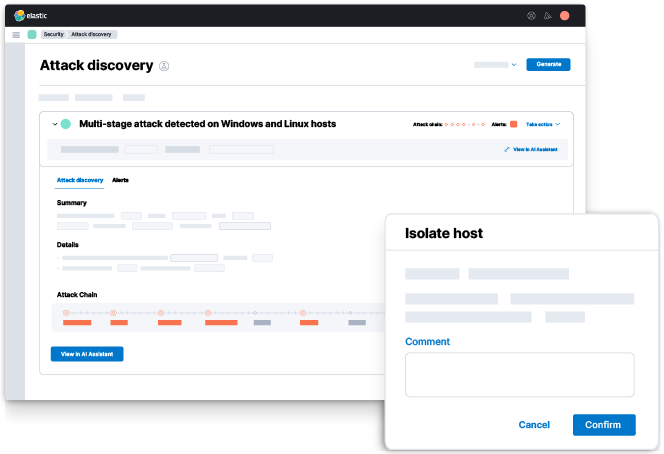
EDR

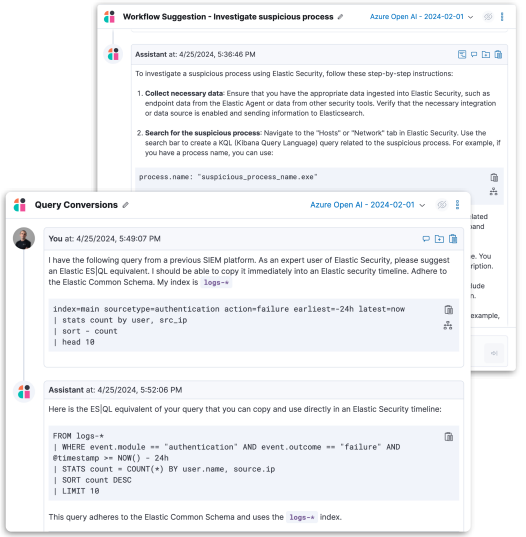
Integrated Response

Elastic's built-in interactive response console lets analysts remotely isolate hosts, kill processes, run commands, and pull forensic artifacts, turning a detection into a contained incident in seconds, with a full audit trail.

Elastic AI Capabilities







ACCELERATE DATA ONBOARDING

Automatic Import

- Create custom data integrations in minutes, not days
- Extend visibility beyond Elastic's 400+ prebuilt data integrations
- Reduce the cost, complexity, and stress of SIEM migration

AUTOMATE TRIAGE

Attack Discovery

- Prioritize attacks, not alerts
- Assess alerts holistically, rather than as one-off events
- Get guidance on what to do next, ask follow-up questions, and take action

AUGMENT EXPERTISE

AI Agent

- Make every user a power user
- Guide analysts through triage, investigation, and response
- Help admins with routine tasks
- Automate and orchestrate tasks

elastic
government solutions

AI is only as good as the data behind it.

The quality, speed, and context of your security data determines the quality of every AI decision, in the SOC and beyond.

elastic
government solutions

Unified Data at Scale

Logs, metrics, and traces from 700+ sources normalized automatically via ECS.

Real-Time Enrichment

Entity analytics and threat context applied at ingest, not hours after the fact.

ML at the Source

Anomaly detection and behavioral models run inside the data pipeline itself.

Open & Extensible

Standard APIs and schemas that feed any downstream AI or automation platform.

elastic
government solutions

Elastic + Tines: Detect. Automate. Respond.

Two platforms. One mission: giving Air Force cyber operators a decisive advantage.



Elastic Security

DATA & DETECTION FOUNDATION

- → Ingest & normalize at petabyte scale
- → ML-based threat detection & enrichment
- → Alert triage & case management
- → Open APIs for downstream automation

Enriched
alerts & data

→



Tines

SOAR & AUTOMATION ENGINE

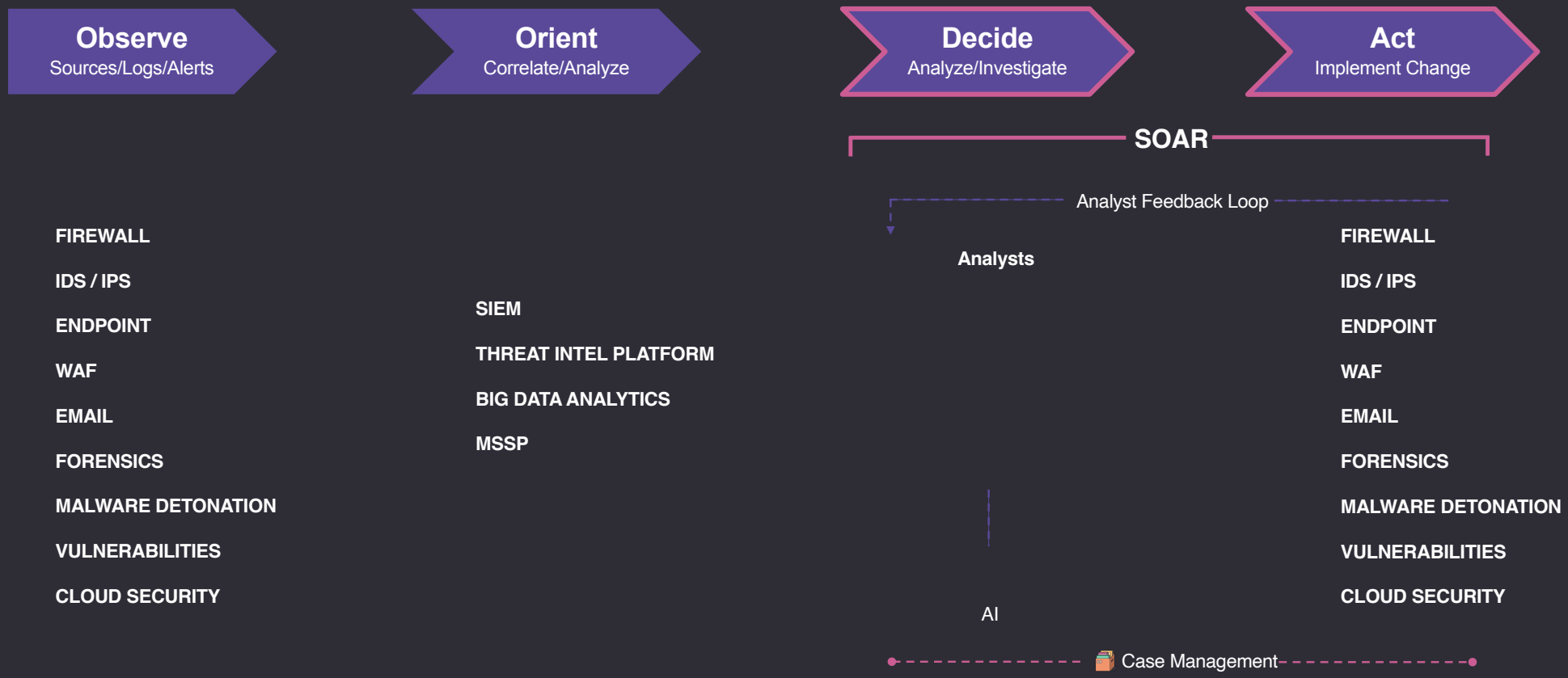
- → No-code/low-code SOAR workflows
- → AI-driven playbook execution
- → Human-in-the-loop decision gates
- → Automated containment & response

Up next: Navid Wlotzka, Tines — Security Automation Reimagined: SOAR Evolution and AI-Powered SecOps

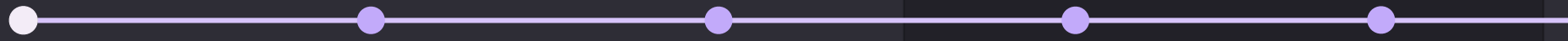


SOAR for Security Operations

Faster & intelligent execution through the loop yields improved response times



A Brief History…
from code warriors to flow architects



SOAR TRANSFORMATION

pre-2010	2010-2015	2015-2018	2018-Present	Beyond
EARLY DAYS: MANUAL PROCESSES AND BASIC SCRIPTING	**FIRST WAVE:** BASIC INTEGRATIONS AND CUSTOM SCRIPTS	**SOAR EMERGENCE:** FIRST-GENERATION PLATFORMS	**MODERN SOAR EVOLUTION:** NEXT-GENERATION PLATFORMS	**AI DRIVEN AUTOMATION:** SOAR & BEYOND

No-Code/Low-Code Approaches

Fully Integrated AI Capabilities

API-First Architectures

Emphasis on UX and Time-to-Value

© Tines · Private and Confidential

The Tines **intelligent workflow** difference

Beyond our fastest time to value across SOAR, Enterprise Workflow Automation, and NCAB.

Intelligent workflows

The secure, reliable integration layer that connects teams, tools, and data.

Vendor agnostic

Secure integration across your stack including LLMs, MCPs, and internal tools.

Born in security

Governance, guardrails, and monitoring across every surface of the workflow.

Ease of adoption

Meets builders where they are with no code, low code, and natural language options

© **Tines** · Private and Confidential

A new **foundation** for work

AI that delivers

Integration



Connect across your systems and processes

Automation



From rules-based deterministic to fully agentic; eliminate muckwork

Interaction



Apply AI where it delivers value, leverage your people for the rest

© **Tines** · Private and Confidential

Support for **every type of workflow**, including automated and agentic

Best for: Volume; mission-critical; predictability; compliance; provisioning; triage and routing; explainability

Best for: Strategy; judgement calls; communication; risk assessment; context-based decisions



Best for: Flexibility; ambiguity; simplicity; quick review and escalation; logical next steps and advice; taking safe actions

© **Tines** · Private and Confidential

Tines Values

Top 5 things to know about Tines for Federal

1

Automate in Seconds…

- 500+ OOTB integrations
- cURL to Tines
- 1000+ prebuilt automations

2

Fully Integrated AI Capabilities - BYO AI

- AI Agents (Agentic)
- MCP Server
- Workbench
- Workbench Stories

3

AI + Traditional = Intelligent Automation Workflows

- API First Architecture
- Automation Fabric
- Time-to-Value

4

Self-Hosted (On-Premise)

- 3-5 Docker Containers (Core)
- K8s, Open Shift, AWS Fargate, etc.
- Highly Scalable

5

Self-Hosted Release Cycles

- Feature Parity
- Nightly Release Cycle
- No Customer Left Behind

© Tines · Private and Confidential

Demo

Thanks for your time.
Any questions?

Upcoming Elastic + Tines Webinar – **Automating ATO & RME**

Registration Link



Navid Wlotzka
Principal Solutions Engineer - Public Sector
nwlotzka@tines.io

© Tines · Private and Confidential