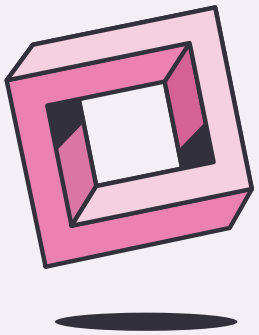
tines

elastic



Elastic Security and Tines

A modern approach to security operations for Federal agencies

The challenges facing Federal agency stakeholders today are relentless. Not only are they responsible for defending their organizations, they are also tasked with complying with new and in-depth mandates spanning zero-trust, logging, and most recently, artificial intelligence.

- More alerts than ever
- Little to no integration between point solutions
- Obsolete or limited SOPs for responding to known threats
- Forced ad-hoc and manual approaches to fill the gaps which slows response and increases risk of missing signals

M-21-31, compounded with ever-increasing stakeholders and systems, makes it critical for federal SOCs to adapt faster to achieve EL3 maturity. Modern SIEM and SOAR solutions, such as Elastic Security and Tines, provide the adaptability required to meet these growing demands without breaking your budget.

WHAT IS ELASTIC SECURITY?

AI-powered SIEM and security analytics solution for the modern SOC.

WHAT IS TINES SOAR?

Vendor-agnostic security automation, orchestration, and response platform.

tines

elastic

Why now

CHALLENGE	SOLUTION
Limitations in cyber event information sharing M-21-31 called for agencies to share logging data with one another, "as needed and appropriate, to accelerate incident response efforts." Traditionally, sharing data outside an agency heightened risk for already-sensitive data, as well as potential costs and time required to copy data or move it to a central source.	**Breadth of information sharing** By leveraging Elastic Security and Tines, agencies gain the ability to share pertinent information swiftly to promptly address alerts. This helps SOC staff swiftly respond to actionable alerts by providing them with relevant context, enabling immediate action. Such flexibility not only supports fast responses but also minimizes redundant data storage requirements.
Lack of staff and high turnover SOC teams face high turnover and stagnant or shrinking headcounts, all while being required to tackle overwhelming numbers of threats and alerts. Knowing which signals to focus on and when is critical to team and individual success.	**Efficient, effective teams** The Tines workflows enabled by the wealth of data in Elastic Security facilitates automation of crucial tasks. This includes processes such as data integration, alert prioritization, automated remediation, and generating reports, among others.
Event logging technical challenges Many organizations are challenged with the high costs involved in managing and storing large quantities of disparate logging data.	**Depth of integration** With Elastic Security and Tines, organizations can effectively align with the objectives outlined in M-21-31. Through this integration, security teams can significantly reduce mean time to respond and false-positive rates, while enhancing their overall agility and impact.

The smarter way to approach SIEM + SOAR

elastic — **Intelligence & Data**
Real-time cyber threat detection, prevention, and remediation.

\+

tines — **Automation & Integration**
Smart, secure workflow platform for security teams.

SIEM

INGEST EVERYTHING
- Data Extraction
- Transformation
- Loading/Indexing

STORE, SEARCH & ANALYZE
- Intelligent data storage
- Modify runtime fields
- ML analysis

WORKFLOW AUTOMATION

ENRICHMENT
- Threat enrichment
- Search Elastic datasets

REMEDIATION
- Vulnerability mgmt
- Cloud remediation
- Infrastructure mgmt

COMMUNICATION
- Chat Ops
- Build reports

YOUR TECH STACK

YOUR WORKFLOWS

SIEM

VISUALIZE & EXPLORE
- Real-time federated search
- Exploration & correlation
- Visualization

tines

elastic

Why Elastic Security + Tines SOAR together

CAPABILITY

Detect, investigate, and respond at cloud speed and scale

BENEFIT

Scale security operations efforts

- 30s process time per request, reduced from 10-20 minutes with Tines at Applied Systems
- 95% reduction in severe incidents with Elastic Security at Mimecast

CAPABILITY

Enrich alerts with relevant context to investigate alerts faster

BENEFIT

Reduce time to detect and remediate

- 55% decrease in vulnerabilities with Tines at BCM One
- 99% reduction in incident response time with Elastic Security at Texas A&M

CAPABILITY

Automated triage processes lead to greater consistency

BENEFIT

Makes it easier for teams to be compliant and work faster

- Consistency and auditability saved tons of human hours with Tines at PathAI
- 50% increase in SOC efficiency with Elastic Security at Proficio

CAPABILITY

A distributed approach allows you to share data outside your agency without moving it

BENEFIT

Retain control of your data in its original secure location

- Ability to extract greater value from products that were less flexible when it comes to integrations with Tines at Crossbeam
- Elastic Security enables detection of threatsacross clusters and regions in 20ms at Opsys

CAPABILITY

Unify workflow integrations for ease of implementation and updates

BENEFIT

Reduce toil on analysts

- ~2,100 hours saved per quarter with Tines at Upwork
- 75% reduction in maintenance with Elastic Security at Bolt

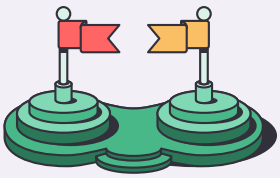
CAPABILITY

Drag-and-drop visualizations allow everyone on your team to access information in real-time

BENEFIT

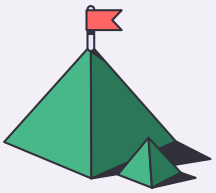
Reduce burden on threat analysts with specialized knowledge or access

- 50% of an analyst's time saved working on each case with Tines at Sophos
- Slashed analysis time at a Fortune 1000 technology retailer with Elastic



tines

elastic



Better together

Tines + Elastic to deliver regular reports at Oak Ridge National Laboratory

CHALLENGE

The ORNL team uses Elastic Security for SIEM.

During their evaluation of SOAR tools, they found that the integrations offered by other vendors varied in quality and consistency.

SOLUTION

The seamless integration between Tines and Elastic was a massive operational win.

As the team went through implementation, it resurfaced a long-deferred initiative: improving reporting.

IMPACT

The ability to automate reporting saves the Defensive Cyber Operations Group at least two hours a week.

For the first time, the team sends scheduled reports internally on a weekly basis and up to leaders on a monthly cadence.

> "We make all the API calls in Tines, where it's cleaned up, then push this data from the API calls to Elastic. In Elastic, we create any visualization we want out of them...
>
> That's putting Elastic and Tines to work and extracting insights we always wanted but could never get to."
>
> —Pete Wood, Lead Engineer

OAK RIDGE National Laboratory

SIEM + SOAR USE CASES

Alert Handling, Response and Triage, Issue Tracking, Enrichment, User Interaction, Remediation, Continuity, Procedure, Organization-wide Reporting, Curating and Combining Information across Databases, Vulnerability Management, Cyber Threat Intelligence, Endpoint Detection and Response, Firewall Rule Management, Forensics, Digital Investigations, Incident Response

INDUSTRY LEADERS

Elastic

Leader in The Forrester Wave™ Security Analytics Platforms Q4 2022

Tines

2023 Deloitte Fast 50 November 2023
Nasdaq Redpoint InfraRed 100 August 2023
Gartner Peer Reviews (4.8/5 stars)
G2 High-performance Fall 2023

Get started

Accelerate M-21-31 compliance

Learn more about how Elastic Security and Tines can provide integrated, cost-effective support for M-21-31 compliance, including log storage, management, and comprehensive system integration and monitoring. **Visit tines.com/book-a-demo**