carahsoft

elastic

Elastic Agentic SOC

Public Sector Threat Brief

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Elastic, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/elasticresources

Join Events & Webinars:
carah.io/elasticevents

Discover Technology Solutions:
carah.io/elastic

Learn About Procurement:
carah.io/elasticcontracts

Connect With Our Team:
Elastic@carahsoft.com
571-590-6810

PUBLIC SECTOR THREAT BRIEF

Defeat threat actors instantly with an autonomous security platform

Threat actors execute devastating cyber attacks in under 30 minutes. Legacy security tools cannot match this operational speed.

State and local technology leaders must modernize defense strategies immediately. The Elasticsearch Platform delivers rapid threat isolation. We empower your lean security team to defend critical public infrastructure.

YOUR CURRENT TOOLS CREATE SEVERE PUBLIC RISK

On average, security operators manage 11 disconnected software consoles. This fragmentation causes 91 percent of serious public sector incidents.

11 CONSOLES

91% INCIDENTS

IS YOUR SECURITY PLATFORM A DEFENSE TOOL OR A DATA TAX?

Traditional legacy vendors thrive on a hidden trap: they force public sector organizations to pay exorbitant fees just to move and ingest log telemetry. Your budget evaporates on basic storage, leaving your lean staff exposed.

We shatter this model: The Elasticsearch Platform deploys autonomous AI analytics across your existing distributed networks. You stop paying for pipeline friction and start blocking lateral movement instantly.

Transform your defense with AI automation

Federated analytics

Threat actors exploit organizational blind spots. Elastic connects distributed municipal networks without requiring expensive data movement.

AI-driven triage

Our engine groups hundreds of distinct telemetry signals into a single timeline automatically. Your team stops chasing false positives.

Automated response

The Elastic AI Assistant for Security generates response playbooks instantly. Your current staff can isolate complex threats immediately.

Open ecosystem

Connect your existing endpoint controls using transparent open integrations. We help public organizations avoid restrictive vendor lock-in cycles.

Dedicated to public sector resilience

State and local governments trust Elastic to protect critical civic operations. We build affordable defense frameworks for resource-constrained public agencies.

Proven results for public sector organizations

100

HOURS SAVED MONTHLY

The Texas A&M University System eliminated manual labor.

The organization deployed Elastic to secure their distributed infrastructure. They successfully saved 100 hours of manual analyst workflow time every month. This reduction allowed their core team to hunt advanced threats proactively.

Eliminate administrative overhead with serverless flexibility and automation

Dynamic infrastructure scaling

The platform updates capacity automatically to handle sudden telemetry spikes smoothly.

Zero backend management

Automated shard configuration optimizes system storage layout. You eliminate database maintenance tasks completely.

Privacy-first architecture

The engine redacts sensitive resident identity details before processing logs. We never train commercial models.

Affordable historical retention

Indexing tiers manage long-term log availability. You maintain records without massive storage fees.

UNLOCK SYSTEMIC OPERATIONAL EFFICIENCY

Accelerate response

Automated triage recovers lost analyst hours instantly. Your operational team focuses on proactive threat hunting.

Consolidate budgets

Unifying security architecture eliminates overlapping licenses. This reduces organizational expenditures significantly.

Magnify skills

The AI assistant guides junior responders through complex investigations. This framework closes urgent talent gaps.

Compare your current operational posture

Critical metric	Legacy environment	The Elasticsearch Platform
Operational visibility	Teams navigate 11 separate consoles slowly.	**One unified analytics environment.**
Threat isolation	Response exceeds the 30-minute danger window.	**AI playbooks contain lateral movement immediately.**
Data sovereignty	Forced log centralization creates huge security risks.	**Cross-cluster search protects local agency data.**
Resource efficiency	Teams waste valuable hours maintaining infrastructure.	**Serverless automation eliminates manual management.**

Stop operating with legacy blind spots.

You cannot fight autonomous threat actors using fractured software tools. Unite your public defense strategy, eliminate tedious administrative workloads, and secure your public infrastructure today.

https://ela.st/state-local-gov