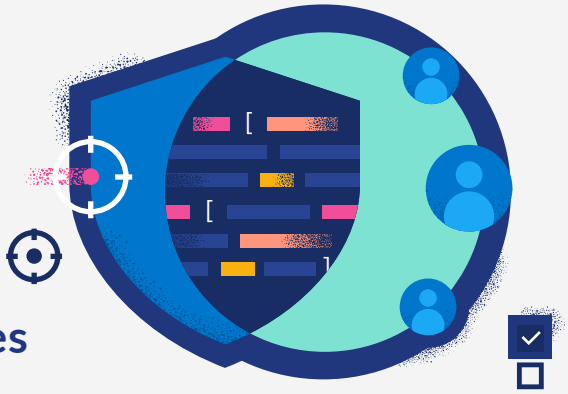
UNIFIED SECURITY OPERATIONS

TECH SPOTLIGHT SERIES
INNOVATION IN GOVERNMENT®

ABOUT
With Elastic Security, agencies can unify and streamline data from both off-the-shelf and custom-built systems to monitor logs from a single source of truth.

Streamlining SIEM Infrastructure:

How Elastic Transforms Cybersecurity Operations for Federal Civilian Agencies



TECHNICAL SUMMARY

A major Federal Civilian agency has successfully leveraged Elastic's Search AI Platform to modernize its Security Information and Event Management (SIEM) infrastructure and achieve critical compliance milestones, including completion of Executive Level 1 (EL1) requirements. Working in partnership with TVAR Solutions for professional services support, this agency has transformed its cybersecurity operations by creating comprehensive dashboards that meet Risk Management Framework (RMF) and Office of Management and Budget (OMB) M-21-31 compliance standards.

The Elastic platform serves as the foundation for unified security operations, enabling petabyte-scale data analysis across multiple environments while providing rapid onboarding capabilities for custom data sources. Through expert-guided detection rules curated by Elastic Security Labs and embedded generative AI (GenAI) capabilities, the platform accelerates security workflows and assists analysts of all skill levels in real-time threat detection, triage, investigation and response processes.

THE CHALLENGE

This agency confronted multiple complex requirements that demanded a comprehensive approach to security information and event management. Compliance with OMB M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities," required significant upgrades to logging and monitoring capabilities across the agency's diverse IT infrastructure.

The agency needed to achieve EL1 compliance standards, which mandate that the most critical data sources and assets be properly logged and monitored. This requirement created substantial pressure to modernize aging SIEM infrastructure while maintaining operational continuity. Traditional security approaches were insufficient for addressing the rapid growth of new technologies, including AI integration, and the rising sophistication of threats specifically targeting the transportation sector.

Recent cyberattacks on transit networks in major cities worldwide highlighted the urgent need for future-proof defenses against ransomware, Distributed Denial-of-Service (DDoS) attacks and other emerging threats. This agency required a solution that could eliminate blind spots across its infrastructure, strengthen defenses through customizable detection capabilities and provide the scalability necessary to protect one of the nation's most critical sectors. Managing disparate security tools and data sources created operational inefficiencies and left potential vulnerabilities in the agency's defense posture.

RESOURCES

U.S. Public Transit Agency Customer Story
carah.io/elastic-customer-story

Elastic Public Sector Summit
carah.io/elastic-public-sector-summit

GSA and Elastic Blog
carah.io/elastic-gsa-agreement

Elastic Cloud Hosted FedRAMP® Blog
carah.io/elastic-cloud-fedramp

elastic | TVAR SOLUTIONS | carahsoft.

Streamlining SIEM Infrastructure: How Elastic Transforms Cybersecurity Operations for Federal Civilian Agencies

Recent cyberattacks on transit networks in major cities worldwide highlighted the urgent need for future-proof defenses against ransomware, Distributed Denial-of-Service (DDoS) attacks and other emerging threats. This agency required a solution that could eliminate blind spots across its infrastructure, strengthen defenses through customizable detection capabilities and provide the scalability necessary to protect one of the nation's most critical sectors. Managing disparate security tools and data sources created operational inefficiencies and left potential vulnerabilities in the agency's defense posture.

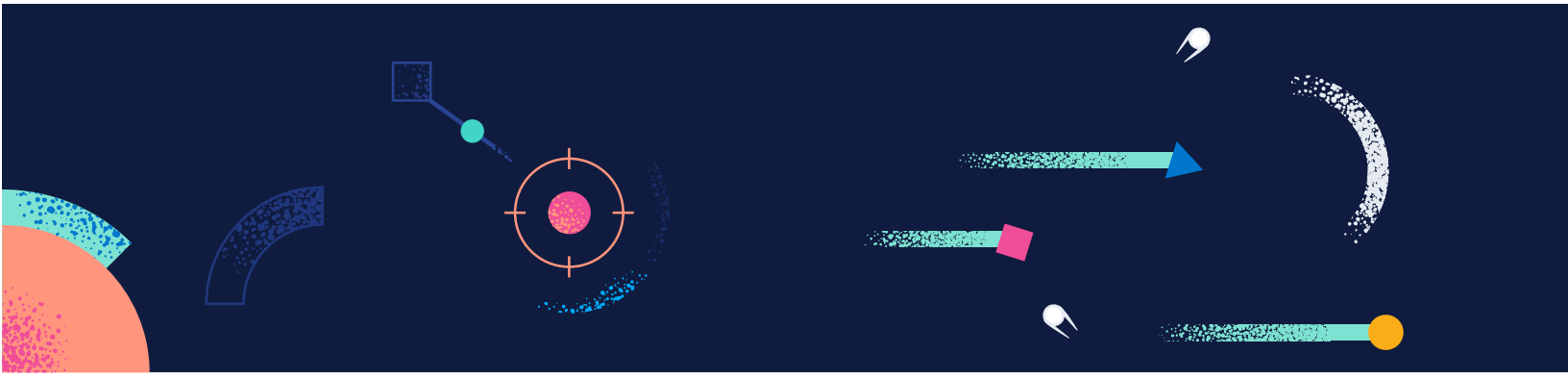
THE SOLUTION

The agency's Office of the Chief Information Officer (CIO) Cybersecurity Division selected Elastic's Search Platform as their comprehensive solution to meet OMB M-21-31 requirements while achieving EL1 compliance standards. TVAR's professional services team played a crucial role in this implementation, providing specialized expertise for onboarding additional data sources and optimizing the existing Elastic ingest pipeline.

Elastic Security now serves as the agency's primary SIEM platform, aggregating data from multiple sources into a single, unified repository. The platform's petabyte-scale data analysis capabilities enable comprehensive visibility across continents and clouds, while rapid onboarding features allow for quick integration of custom data sources. Years of archived data remain readily accessible for deep investigations, eliminating previous limitations in historical analysis and forensic capabilities.

The implementation includes sophisticated dashboard creation and maintenance capabilities specifically designed to meet compliance standards. Machine learning (ML) capabilities enable agencies to create custom models without requiring dedicated data science teams, while embedded GenAI assists analysts throughout security operations, significantly improving productivity across all skill levels.

Through the partnership with Elastic and TVAR, the agency has successfully completed EL1 requirements while establishing a robust foundation for ongoing cybersecurity operations. The platform's automated workflows reduce manual tasks and eliminate the need for subject matter experts on each specific system, making security operations more efficient and scalable, making security operations more efficient and scalable for civilian agencies.



CONTACT US Elastic@carahsoft.com • (571) 590-6810 • www.carahsoft.com/elastic

elastic | TVAR SOLUTIONS | carahsoft.