elastic

Search. Observe. Protect.

CDM and beyond

Tools for today's hyper-digital world

Delivering faster time to insight with CDM Dashboard II

As a trusted solution provider on **GSA's Continuous Diagnostics and Mitigation (CDM) Tools SIN Approved Product List**, Elastic helps move insight to action for the Department of Homeland Security and federal civilian agencies with the CDM Dashboard II. The dashboard is a key component of the federal government's cyber analytics ecosystem, built on the Elastic search platform and delivered in partnership with ECS. Using the dashboard, agencies are enabled to ingest and query data at scale for real-time threat identification.

Event logging and endpoint security for Executive Order compliance

Beyond the CDM Dashboard II, the Elastic search platform can be utilized to meet or exceed requirements set forth in the **Executive Order on Improving the Nation's Cybersecurity (EO 14028)**. Portions of EO 14028 emphasize a belief we have at Elastic: While you observe, why not protect? Below are the pertinent sections related to event logging and endpoint security, and how we can help your customers comply with EO 14028, all on a single platform:

DEPLOYMENT OF AN ENDPOINT DETECTION AND RESPONSE (EDR) INITIATIVE

Section 7 of EO 14028 calls for Federal Civilian Executive Branch agencies to deploy Endpoint Detection and Response (EDR) capabilities to support early and proactive detection of cyber incidents, active cyber hunting, containment and remediation, and incident response. At Elastic, our **Limitless XDR solution** combines endpoint security with SIEM, empowering security teams with defense in depth. This means that security teams can proactively threat hunt, contain threats with one-click quarantining, and query older data in frozen tier storage for deeper investigations.

COLLECTION AND MAINTENANCE OF EVENT LOGS ON FEDERAL INFORMATION SYSTEMS

Section 8 of EO 14028, and the follow-on memorandum entitled Improving the **Federal Government's Investigative and Remediation Capabilities,** calls for agencies and their IT service providers to collect and maintain network and system logs on Federal Information Systems, and provide them, upon request and consistent with applicable law, to DHS, the FBI, or other Federal agencies for cyber risks or incidents. At Elastic, our **event logging tools** give users better insight into networks and systems and alert on anomalous activity.

Your go-to for search, observability, and security

ELASTIC SOLUTIONS FOR YOUR FEDERAL CUSTOMER'S REQUIREMENTS

Elastic is a search company that maximizes data utility in real time. Systems integrators and resellers partner with us on use cases that drive on-contract growth and new business. Whether your customers need website search, event logging, or threat hunting, our search platform aligns with their documented data strategies and delivers powerful insight no matter the mission.

We want to be your go-to partner for search, observability, and security opportunities. Elastic staff, including cleared personnel, are available for RFI/RFP consult, solution architecture, and co-selling. Our cloud-based platform is FedRAMP authorized and ready to grow with customer data. Elastic Cloud is also available on AWS, Azure, or Google Cloud. We help end users gain more power and performance from data no matter where they are in their cloud journey.

Whether your customer has unmet CDM, EO 14028, or other requirements, Elastic stands ready to support your program team with trusted search, observability, and security solutions. See why federal customers turn to Elastic for use cases related to:

Enterprise Search

Enterprise systems and networks

Public-facing websites and applications

Document e-Discovery

Big data environments

Audits / investigations

Observability

Critical infrastructure monitoring

Cloud migration

DevSecOps

Microservices

Data visualization

Unified Agent management

Security

Endpoint Detection and Response (EDR)

Security Information and Event Management (SIEM)

Fly away kits for threat hunting

Real-time situational awareness dashboards

Security Operations Center (SOC) as a service

For more information, contact us at federal@elastic.co
or visit elastic.co/industries/public-sector/civilian