elastic

Search. Observe. Protect.

CDM Dashboard II

Your agency's tool for network threat visibility

The Continuous Diagnostics and Mitigation (CDM) Dashboard II is a key component of the federal government's cyber analytics ecosystem, built on the Elastic search platform and delivered in partnership with ECS. The dashboard enables the Department of Homeland Security and federal civilian agencies to ingest and query data at scale for real-time threat identification as part of the CDM DEFEND program.

Delivering faster time to insight

Using petabytes of cyber monitoring data provided by federal agencies, Elastic indexes cyber data into a common schema and enables drill down analytics using Kibana, our easy-to-use visualization tool. With the capacity to index and normalize structured, semi-structured, and unstructured data upon ingest, Elastic makes massive amounts of data immediately available for analysis in the dashboard. Plus, our open architecture facilitates application data integration and interagency sharing in real time. All said, the dashboard enables your agency to gain full insight into network and perimeter components, host and device components, data at rest and in transit, and user behavior – in just seconds.

Enabling data discovery on the fly

Let's say your agency's dashboard is showing anomalous network traffic, now what? With the ability to formulate ad hoc queries about this data on the fly, your security analysts can go to where their intuition and knowledge leads them, and do it quickly. These queries dive deeper into structured, semi-structured, and unstructured data and are great examples of the proactive analysis needed in today's dynamic environment. And since the dashboard is designed for interagency information sharing, identified cyber threats and resolution criteria can be shared across agencies and bureaus in a timely manner. In this way, the dashboard is a true force multiplier in the federal government's cyber analytics ecosystem.

More Agency Resources

ELASTIC SOLUTIONS FOR YOUR AGENCY'S SPECIFIC REQUIREMENTS

Elastic is a search company that maximizes data utility in real time for the federal government. Cabinet-level agencies use our search, observability, and security platform to achieve data-dependent use cases like judicial document discovery, health science analytics, high-performance computing performance monitoring, and homeland security threat hunting. Deployable on GovCloud or on premises, Elastic delivers powerful insight, no matter the mission.

Whether your agency has unmet CDM or other data-dependent requirements, Elastic stands ready to support your agency 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

elastic