Seconds to Insight: The Next-gen CDM Dashboard

Bringing Scalability, Extensibility, and Performance Benefits to Federal Agencies

Federal agencies faced 31,107 cybersecurity incidents in fiscal year 2018, down 12 percent from the 35,277 incidents that agencies reported in FY 2017, according to the most recent data from the Office of Management and Budget. While the number of incidents declined, the magnitude of cybersecurity risks – coupled with the growing number of devices that U.S. government agencies use for daily operations – demands responsive, scalable, and fast monitoring and mitigation. Visibility into the full spectrum of cyber risk could help bring down those top-line numbers even further.

The Continuous Diagnostics and Mitigation (CDM) program, managed by the U.S. Department of Homeland Security, provides DHS and Federal civilian agencies with capabilities and tools to identify cybersecurity risks, prioritize risks based on impact, and mitigate the most significant problems first.

CDM tools increase agencies' cybersecurity posture by ingesting, analyzing, and visualizing data that provides insight into asset management, identity and access management, network security, and data protection management. The CDM program has moved through its first two capability areas, formerly called phases, with a focus on what and who is on Federal agency networks. Now, the latter stages of the program provide services collectively known as Dynamic and Evolving Federal Enterprise Network Defense, or DEFEND, to expand Federal agency expertise on network management and protection strategies.

The CDM Dashboard Moves to Its Second Iteration

CDM goals in DEFEND are to provide capabilities for dynamic monitoring of security controls for network and perimeter components, host and device components, data at rest and in transit, and user behavior. In today's ever-changing threat environment, meeting these goals requires an advanced cyber analytics solution that can handle tens of petabytes of structured and unstructured data.

Cyber monitoring tools – used by the 23 civilian CFO Act agencies and dozens of smaller agencies covered under the CDM program – each feed data up to a government-wide, Federal CDM Dashboard. The dashboard receives, aggregates, and displays information from CDM tools at the agency and Federal levels for agency cyber situational awareness and governmentwide insight into risk exposure.

elastic

The sheer volume of data from the agencies' tools and sensors presented a considerable challenge for DHS, which oversees the CDM Dashboard. The agency has noted that the previous iteration of the dashboard had difficulties scaling to meet the need.

So, DHS in May 2019 selected ECS Federal, which is partnering with Elastic, to implement a new cyber analytics ecosystem, the CDM Dashboard II. The second iteration of the dashboard will migrate agencies to a more manageable and efficient solution for continuous monitoring and mitigation of cyber threats and vulnerabilities, expanding visibility into network activity and providing new analytics capabilities.

With a simplified technical architecture, the new dashboard will draw on Elastic tools including Elasticsearch, a distributed, open-source search and analytics engine, and Kibana, an open-source analytics and visualization platform designed to work with Elasticsearch.

Dashboard Capabilities Improve and Expand

The new dashboard will provide numerous capabilities to Federal agencies, including:

- Aggregation and visualization of cyber threats and vulnerabilities across systems
- Faster ingest, enhanced connectivity between applications, and simplified information sharing for better cyber threat awareness and response
- Evolving situational awareness for threat-based defense and reduced time to insight, from weeks to seconds

ECS chose Elastic for the increased scalability, extensibility, and performance that it can offer Federal agencies in a modern platform. ECS' partnership with Elastic is designed to overcome the limitations of the previous dashboard, which included sluggish data ingest and time to insight, lack of search capability, and challenges with data quality.

The new dashboard will be able to quickly ingest massive amounts of data from Federal agencies, overcoming a huge challenge with the current dashboard – agencies could not get the full volume of their data into the dashboard, which limited visibility into network assets and activity. It will ingest data into a common schema, enabling analytics sharing across bureaus and agencies.

In addition, Elastic technology will enable integration with other systems, consolidating activity at the integration layer where agencies have been collecting data from tools and sensors – instead, sending that data directly to the dashboard for even faster time to insight.

The dashboard will also enable removal of stale data. In the current dashboard, agencies cannot remove old data associated with their hardware assets. In the new dashboard, logic will remove data that has not been updated in 72 hours, under the assumption that those assets are no longer present. As a result, agencies will have near real-time insight into assets on their networks.

Data Visualization and Analytics Capabilities Advance Agency Awareness

By indexing data upon ingest, Elastic makes data immediately available for analysis, unlike alternative approaches that index data only when requested, adding significant delays to the threat identification process. Further, Elastic leverages all data for analysis – structured (log files), semi-structured (packet capture or PCAP), and unstructured (full text). Because Elastic can manage petabyte-sized datasets efficiently, accommodating agency requirements to retain massive data troves, query results can be delivered in seconds, rather than minutes or hours.

In addition, the new dashboard will present data visualizations in real time. Agency users will be able to click on a visualization and drill down to see the underlying data. This transparency will improve trust in the data and in resulting cyber risk scores. In contrast, the current dashboard displays are static; underlying data is not accessible.

Open Data Integration Enables Data Ingest and Exchange

Agencies use a variety of tools, from next-generation to legacy. In order to facilitate a CDM ecosystem that can incorporate a variety of technologies, all ecosystem members must have a means of exchanging information. Elastic's open-source solutions work with leading and legacy tools, facilitating data integration in real time.

With an extremely open architecture leveraging RESTful application programming interfaces, Elastic components can be used independently or as a full stack depending on each user's specific requirements. Data and processing can easily be shared with other big data platforms using connectors.

Iterative Development Brings New Capabilities at Each Phase

The new dashboard will roll out in quarterly phases, with new capabilities in each phase informed by user feedback. This iterative development emphasizes value-based delivery and reduces rework. The first release, the minimum viable product (MVP) – focused on baseline capabilities – will roll out in April 2020 to CDM DEFEND integrators. ECS will help integrators get the dashboard set up in their labs, assign integration logic, and work with representative datasets in their lab environment.

Then, DHS will deploy the dashboard in a pilot program at five agencies. Preparations between integrators and agencies will begin in mid-April, with the goal of rolling out in early June.

In partnership with Elastic, ECS is developing an installer application for integrators that will facilitate deployment of the dashboard in a few hours, compared to a day and a half with the previous dashboard. Ultimately, more than 100 instances of the dashboard will be deployed across the Federal government, so simplifying deployment is an important part of the rollout.

MVP Agency Dashboard Features

Object-level Hardware Asset Management
Configuration Settings Management
Vulnerability Management
Software Asset Management
Identity and Access Management
Agency Dashboard Container Hierarchy
Risk Scoring
Ongoing Assessment Metrics Visualization

After the pilot deployments at five agencies, DHS will pivot to the governmentwide Federal dashboard, which is targeted for deployment in November. The Federal dashboard provides an integrated view of networks governmentwide, ensuring that when a cyber attack or heightened vulnerability is identified on one agency network, that information can be communicated rapidly to all other agencies.

elastic

Agencies Gain AWARE Scoring Visibility, Threat-hunting Capability

The CDM program's Agency-Wide Adaptive Risk Enumeration (AWARE) algorithm scores, which are designed to enable Federal agencies to track their relative security status, will be available in the first release of the dashboard. Because of challenges with latency in data feeds with the current dashboard, agencies didn't always trust their scoring. With the new dashboard's faster ingest and greater ability to house data, latency issues will be resolved, and data quality will improve greatly. Ultimately, the goal is for agencies to have better awareness of how their scores are generated.

In the second release, AWARE scoring will include trending, so agencies can track their scores over time. Subsequent releases could introduce the ability to look backward in time at network data. This new capability would enable threat hunting, in which agencies could drill into past data for signs of vulnerability or exploitation. Analysts would be able to go where the data – coupled with their intuition and knowledge – led them, generating ad hoc queries quickly and getting immediate results.

Advancing Federal Cybersecurity With Dashboard II

The new CDM Dashboard delivers significant improvements designed to help agencies achieve near real-time cyber insights and enable faster mitigation of critical vulnerabilities. Its iterative development – leveraging essential agency feedback – will continue to bring new capabilities that significantly enhance agencies' cyber posture. Together, the CDM program, Federal agencies, ECS, and Elastic will further the nation's cyber defenses through the CDM ecosystem.

elastic