

CDM: Situational Awareness for Risk Identification and Prioritization

Enhancing Security Through Effective Risk Awareness Strategies



Agenda

- 01 Speaker Bio
- 02 CDM In the Beginning
- 03 The Early Days
- 04 Legacy CDM Solution
- 05 Breaches Prompt Change
- 06 BODs Put CDM in the Spotlight
- 07 Evolution of CDM “as-a-Service” Model
- 08 SIEM as a Service (SIEMaaS)
- 09 AI Integration
- 10 Priority Risks Dashboard Demo
- 11 Q&A



01 Speaker Bio: Conrad Jalali



Conrad Jalali

- Seasoned technology leader with 30 years of experience driving innovation across federal agencies
- Joined the Continuous Diagnostics and Mitigation (CDM) Program in 2017
- Managed multiple initiatives to enhance CISA's situational awareness of the cyber risk posture of the federal government
- Background in project management, software development, and database design
- Currently serves as CDM Dashboard Service Owner and Enterprise Asset Governance Section Chief (acting)



02 CDM In the Beginning

The CDM Program serves approximately 100 Federal Civilian Executive Branch (FCEB) agencies, providing operational insight and risk identification for unclassified, FISMA-reportable assets.

Every FCEB agency except the Department of War and the IC participate.

The CDM Program was established in 2012.

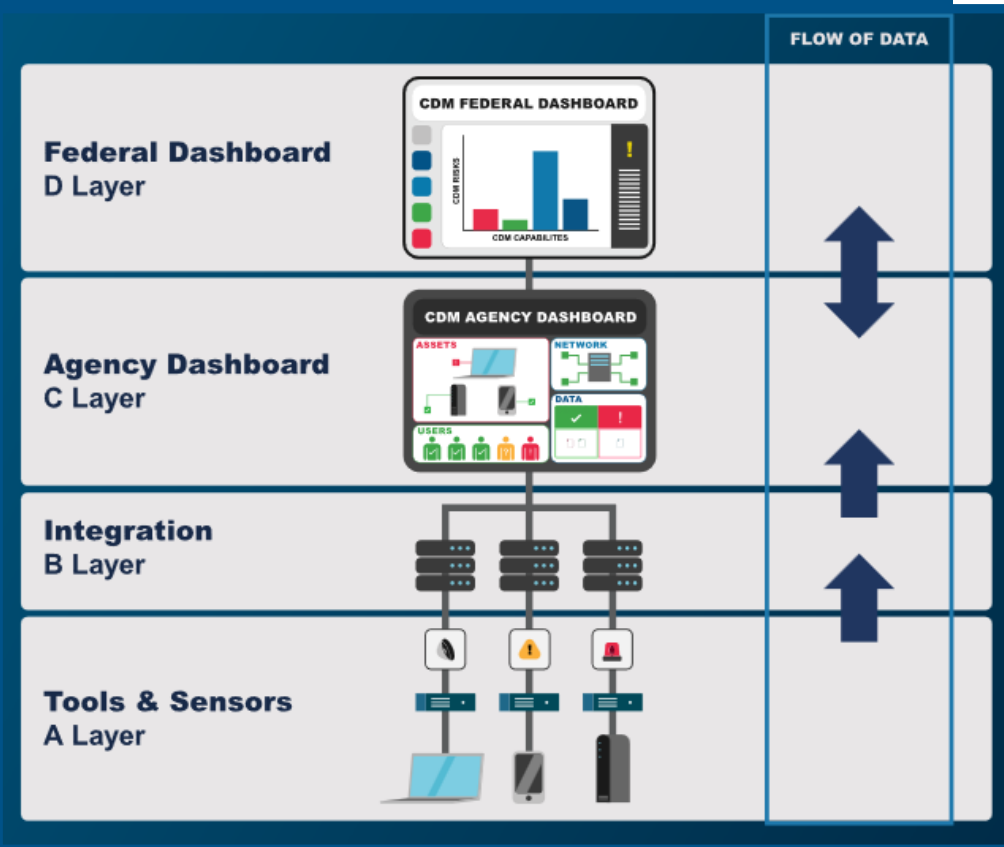
We started with a delivery order to buy cybersecurity tools for agencies.

Although we obtained deep discounts, agencies struggled to find the infrastructure and engineering resources needed to use the tools effectively.

We had to find a way to help agencies implement capabilities.



03 The Early Days



The CDM Program spun-up new contracts to deploy tools and deliver a system of agency dashboards that provide operational awareness of cyber risk by synthesizing tool data to form a picture of the agencies' assets, and their software, vulnerabilities, and misconfigurations.

Agency Dashboards sent summarized data up to a Federal Dashboard, which informed CISA about the FCEB asset inventory and its risk posture.

04 Legacy CDM Solution

- 1 In the early days, we had six different contracts with four different System Integrators (SIs), serving 100 agencies.
- 2 Each agency had their own CDM Dashboard that was supported by our SIs.
- 3 The legacy integration layer (aka, Layer B) was incredibly complex, often consisting of Splunk and custom technical add-ons that the SIs constantly updated.
- 4 The system worked but there were significant challenges:
 - High level of labor and infrastructure resources were needed to support all agencies and their variations.
 - It took a long time between device scans to data being visible in the Dashboard, due to multiple steps in the process of collection, normalization, enrichment, and ingest.



05 Breaches Prompt Change

The SolarWinds incident in December 2020 led to EO 14028 in May 2021.

The EO made significant changes for the CDM Program, including:



AGENCIES WERE REQUIRED TO GRANT CISA ACCESS TO OBJECT LEVEL DATA

Sharing object level data allowed us to use Elastic Cross-Cluster Search in the Federal Dashboard, to query the billions of records in Agency Dashboards and retrieve detailed results in seconds.

Previously, CISA had limited visibility, through daily, summary data.



CISA WAS DIRECTED TO DEPLOY ENDPOINT DETECTION AND RESPONSE (EDR) CAPABILITIES

EDR prompted agencies to adopt cloud-based Software as a Service (SaaS).

EDR showed that complex security tools are far easier to implement when agencies are relieved from the burden of provisioning and supporting infrastructure.





06 BODs put CDM in the Spotlight

CISA Directives

CDM's Directives Dashboards give agencies ways to find devices with missing patches or outdated scans.

<https://www.cisa.gov/directives>

CISA issues Binding Operational Directives (BODs) and Emergency Directives (EDs), which compel federal agencies to take specific actions to reduce risk.

BOD 22-01 Reducing the Significant Risk of Known Exploited Vulnerabilities (KEVs)

- CISA implemented the KEV catalog and the CDM Dashboard flagged KEVs for prioritized remediation.
- Agencies now patch KEVs faster than other vulnerabilities.

BOD 23-01 Improving Asset Visibility and Vulnerability Detection on Federal Networks

Agencies must:

- Scan all IP-addressable devices every seven days.
- Complete vulnerability scans every 14 days.
- Execute credentialed scans.

BOD 26-04 Prioritizing Security Updates Based on Risk

- Using [Stakeholder Specific Vulnerability Categorization \(SSVC\)](#) and internet-facing criteria add nuance to prioritize VULN remediation.
- Providing remediation target dates based on VULN and device details will maximize risk reduction and focus agency vulnerability teams on the worst problems.

07 Evolution of CDM “as-a-Service” Model

BETSIE

The central pillar of CDM Program modernization is the **Baseline Extraction and Transformation Security Information Environment (BETSIE)**, a modernized **Layer B**, consisting of a **commercial off-the-shelf (COTS) Cyber Asset Attack Surface Management (CAASM)** tool and a **singular CDM Data Pipeline**.

- This model reduces the number of variations of the we support, while allowing us to deploy enhancements at a rapid pace.
- CAASM vendors build connectors for hundreds of cybersecurity tools.

DBaaS

Every participating agency now uses our **Dashboard as a Service (DBaaS)**.

DBaaS uses Elastic Cloud Hosted (ECH), which reduces our operations and maintenance tasks, allowing us to focus on delivering the CDM Dashboard rather than patching Elastic.



08 SIEM as a Service (SIEMaaS)

- The CDM Program provides a comprehensive Security Information and Event Management (SIEM) system at no cost to agencies.
- SIEMaaS complies with [M-26-14 Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats](#).
- SIEMaaS puts invaluable data in the hands of CISA analysts while relieving a substantial resource burden from agencies.
- CISA's Threat Hunting team serves as a collaborative agent, helping agencies detect advanced cyber actors.
- **SIEMaaS is open for business, and we are accepting new customers!**



09 AI Integration



1. The CDM Program will incorporate AI with SIEMaaS to sift through massive amounts of security data, spot hidden anomalies, reduce false positives, and speed up incident response.
2. AI will also be integrated into the CDM Dashboard, adding features like chat-based queries, providing insights into data, prioritized risk scores, and trend visualizations for Agency Dashboard users and CISA analysts.



10 Priority Risks Dashboard Demo





Q&A



For more information:
<https://www.cisa.gov/cdm>

Questions?
Conrad Jalali
conrad.jalali@cisa.dhs.gov