IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

DATA PROTECTION MANAGEMENT – How is Data Protected?

DEFEND TODAY, SECURE TOMORROW

The Cybersecurity and Infrastructure Security Agency (CISA) Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security postures by delivering better visibility and awareness of their networks and defending against cyber adversaries. The CDM Program ultimately reduces the threat surface and improves federal cybersecurity response through four capability areas: Asset Management, Identity and Access Management, Network Security Management, and Data Protection Management.

OVERVIEW OF DATA PROTECTION MANAGEMENT

The Data Protection Management (DPM) capability provides additional protections to the most critical mission data and systems on federal civilian networks. While the other CDM capabilities provide broader protections across federal networks, the DPM capability has a targeted focus on those networks and systems containing highly sensitive data. Protecting sensitive data requires security and privacy protections at rest, in use, and in transit to ensure the integrity, availability, and confidentiality of data and data assets. The CDM Program employs the DPM capability to help agencies and industry partners strengthen data protections to include identifying sensitive data, classifying data assets based on severity and impact, supporting timely response procedures to notify stakeholders of data breaches or spillage, and more. DPM helps agencies protect sensitive data through five capabilities: data discovery/classification (DATA_DISCOV), data protection (DATA_PROT), data loss prevention (DATA_DLP), data breach/spillage mitigation (DATA_SPIL), and information rights management (DATA _IRM).

BENEFITS OF DATA PROTECTION MANAGEMENT

The DPM capability helps agencies and industry partners strengthen data protections to include identifying sensitive data, classifying data assets based on severity and impact, supporting timely response procedures to notify stakeholders of data breaches or spillage, and provides agencies with the tools necessary to protect sensitive and private data in their networks. These tools allow agencies to ensure sensitive data is properly secured and stored by: (1) identifying sensitive data assets; (2) classifying the severity and impact of such assets; (3) identifying authorized roles, users, and policies for retention of private data; (4) collecting and reporting on data asset compromise; (5) developing timely response procedures to notify stakeholders of data breaches or data spillage and how to effectively recover from an attack; and (6) implementing standard cryptographic controls and mechanisms, such as FIPS-140-2 or data obfuscation.

DATA PROTECTION MANAGEMENT CAPABILITIES

The CDM Program leverages commercial-off-the-shelf tools to provide the following five DPM capability offerings:

Data Discovery/Classification

DATA_DISCOV is the collection and reporting of information that provides consistent identification of data assets across the agency environment for processing, storing, and transmitting data. Functions include automated data discovery, which allows tools to scan targeted databases to identify sensitive data (e.g., usernames and addresses).

Data Protection

DATA_PROT offers two methods for protecting sensitive data: 1) the application of cryptographic technology which protects confidentiality by translating sensitive data into another form that can only be accessed with the proper decryption key; and 2) using data masking or obfuscation methods that are programmed to replace sensitive data with substitute data that is generated based on a set of rules. Both methods increase agency protection from malicious interception or exfiltration of data stemming from internal or external sources.

Data Loss Prevention

DATA_DLP techniques minimize the loss of data by providing consistent protection to block unauthorized exfiltration of sensitive data and include exfiltration alerts and prevention, role-based data protection, and enhanced protections for sensitive information. DATA_DLP allows an agency to limit or prevent data exfiltration from data assets or other key infrastructure components.

Data Breach/Spillage Mitigation

DATA_SPIL provides techniques for response and recovery from a data breach or spillage. It uses specialized tools to identify specific points of failure that caused the data breach, quantify sensitive data lost or exfiltrated from a data spillage, calculate a mean time to recovery of standard operations, and develop new or enhance existing data security and privacy controls to prevent future data breaches.

Information Rights Management

DATA_IRM provides controls for access relating to enterprise information (e.g., documents, files) and uses tools that employ cryptographic controls for encrypting sensitive data, a granular control system for least-privilege access, and identification mechanisms for authenticating users.

CURRENT STATE OF CDM DATA PROTECTION MANAGEMENT DEPLOYMENT

The CDM Program has a DPM pilot underway with one large agency and a select number of high-value asset systems making sure that the appropriate data protections for those systems are in place for the most critical data. Funding dependent, the program is planning to initiate additional agency pilots over the next two years.

For more information on DPM capabilities and/or the CDM Program, please contact the CDM Program Management Office at CDM@cisa.dhs.gov.