Trusted Cyber Technologies

THALES

Continuous Diagnostics and Mitigation: Data Protection & Assurance

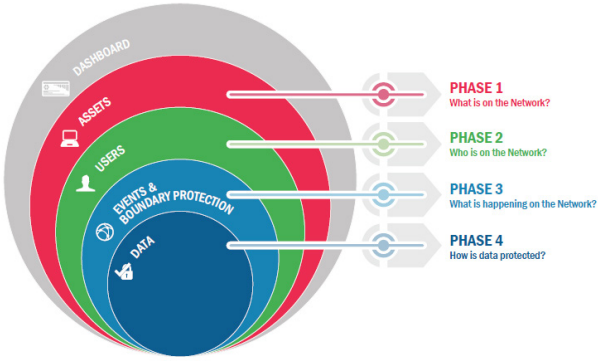
White Paper

Overview

The Continuous Diagnostics and Mitigation (CDM) program was established by Congress mandating the Department of Homeland Security (DHS) to establish a program to advance the state of government's cyber security infrastructure for unclassified networks. The program focuses on providing tools and services that automatically detect and report on flaws, vulnerabilities and the overall state of a network's security stance. It creates a framework for continuous monitoring of cyber security risks and allows for those risks to be prioritized to enable the efficient deployment of the most critical mitigations first. It enables continuous improvement through an awareness approach to information security. This CDM architecture embraces NIST's Cyber Security Framework by creating the infrastructure and process to actively manage and continuously improve department and agency information systems infrastructure.

The risks and threats facing government systems are continuously evolving and are increasing in aggressiveness. The key elements of the CDM program include purchasing vehicles for the acquisition of qualified tools and capabilities; agency level dashboards that identify, analyze and address vulnerabilities; and a federal dashboard that collects tactical data enabling strategic decisions making.

Acknowledging that cyber security is a monumental task, CDM has taken a structured approach by defining four phases that enable agencies to fold in different aspects of cyber security over time. The program begins with dashboards at both the federal and the agency/department level. The program then deploys sensors throughout the network infrastructure that address different strategic questions associated with network security.



Source: Department of Homeland Security
https://www.dhs.gov/cdm

Asset Management: What is on the network?

Sensors are deployed to detect and report on the hardware and software assets installed within the network. This includes collecting each asset's security configuration. This enables an initial vulnerability management program to identify which assets in the network are affected by known vulnerabilities and prioritize their mitigation. Knowing what is on the network is the first step to enabling active management of the security risks to the network. (HWAM, SWAM, CSM, & VUL)

Identity and Access Management: Who is on the network?

This phase shifts to focusing on the management and control of accounts, user access and managed privileges. This includes the determination of trust for the people granted access; credential and authentication management; and security-related behavior training. Acquiring this information enables the realization of a least privilege approach by eliminating unnecessary privileges based on an individual's role and level of trust. This phase provides confidence in knowing who is on the network, another key requirement for network control. (TRUST, CRED, BEHAVE)

Network Security Management: What is happening on the network?

DEFEND builds on the previous efforts phases by addressing event management, boundary protections and the security lifecycle. This includes planning for physical access controls, preparing for protection of data at rest and in motion; and managing the cryptographic infrastructures required by cryptographic controls. Another key aspect of this phase is developing the capabilities to respond to security incidents and generating and capturing audit data. Finally, this phase addresses product assurance by ensuring products and systems have security built in during the design and development phase. (MNGEVT, OMI, BOUND, & SCRM)

Data Protection Management: How is data protected?

Arguably the most critical, and ultimately the goal of CDM, is monitoring and mitigating how data is protected. DEFEND achieves this by implementing new technologies that monitor and secure data across the network. First, data is identified and classified so that agencies can pinpoint protection requirements. Understanding where data is, what structure it is in, and classifying its sensitivity defines protection requirements. Once this is known, data protection tools can be deployed to protect data in a prioritized and managed manner. (DISC, PROT, DLP, & IRM)

CDM Realized

With the rollout of CDM DEFEND, the program is finally achieving all of its goals by addressing all aspects of information system governance. Deploying the phase 4 data protection tools on top of the previous capabilities realizes a holistic approach to network security, enabling the Department of Homeland Security's stated goal:

> "CDM capabilities support the overall CDM Program goal to identify cyber security risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cyber security personnel to mitigate the most significant problems first." [1]

However, completing Data Protection is just the beginning as CDM finally becomes a fully capable system for continuously monitoring and improving each agency's infrastructure. Once fully realized, the four CDM phases transition into four questions that CDM continuously re-evaluates. As new threats arise, or new data is added to a network, CDM enables continuous improvements to be identified and deployed on an ongoing basis.

Thales Trusted Cyber Technologies and CDM

Thales Trusted Cyber Technologies (TCT) offers encryption and key management solutions that deliver the same level of security whether deployed in enterprise, tactical or cloud environments. Our solutions enable agencies to meet their CDM requirements while investing in a solution that provides robust security, a growing ecosystem, and the scalability needed to build a trusted framework for the future. Our solutions have a U.S. supply chain, can be deployed in any environment and easily integrate into an existing cyber security infrastructure. Thales TCT's encryption and key management solutions have received CDM Approved Product List (CDM APL) approval to address CDM requirements.

Data-At-Rest Encryption:

Whether it's in the cloud or on premises, encrypting files or individual data objects, Thales TCT's data-at-rest encryption solutions offer a single managed solution for protecting data-at-rest, eliminating critical threats to data.

Data-in-Motion:
Thales TCT's physical and virtual high speed encryption solutions offer powerful tools to securely connect information systems across untrusted networks. These high-performance communication devices tie distributed assets together with a high-assurance cryptographic barrier.

Cryptographic Key Management
From PKI to TLS server keys to digital signatures to authentication systems, Thales TCT's cryptographic key management solutions, which include hardware security modules and enterprise key managers, bring trust and assurance to all cryptographic deployments. Large volumes of encrypted data yield copious amounts of cryptographic keys which need to be managed, stored, and secured efficiently. If these keys are compromised, attackers can gain access to encrypted information. Complete security depends on cryptographic key management. Thales TCT's cryptographic key management solutions enable agencies to centrally, efficiently, and securely manage and store cryptographic keys and policies—across the key management lifecycle and throughout the enterprise.

Thales TCT delivers a comprehensive set of technologies to address the CDM requirements for government agencies. In addition to delivering key solutions that implement critical boundary protections for data-at-rest and data-in-motion, Thales TCT's also offers high assurance protection to many other security controls by delivering leading cryptographic key management solutions.

Addressing CDM Questions

The phases of CDM represent a staged rollout of key questions that need to be addressed in an infrastructure governance system. Phase 4 has begun and that means the last question (How is data protected?) is now being addressed by CDM. As phase 4 completes, the questions remain central to the ongoing governance. Each question gets continuously re-evaluated to identify improvements and corrective actions required to keep ahead of the ever-changing threat landscape. Thales TCT can address requirements in each of these functional areas.

What is on the Network?
All Thales TCT network-addressable products are fully compatible with tools and capabilities deployed to address the management and control of devices on the network. Active scanning technology can interrogate Thales' hardware security modules (Luna HSMs), data-at-res encryption and key management (Data Security Platform), and High Speed Encryptors to detect and report on the services they offer the network.

All Thales TCT network appliances have administration interfaces that allow the querying of configuration. This enables automated sensing of their actual state without human intervention. All software products use standard installers ensuring they are visible in each operating system's standard installation configuration – making it easy to detect and monitor all software on devices.

Deploying Thales TCT products and solutions while addressing data protection requirements fit seamlessly into an existing CDM infrastructure.

Who is on the Network?
Managing who is on the network requires controlling accounts and privileges, determining the trust of people granted access, issuing credentials and authenticating users, and finally deploying security-related training. Thales TCT's HSMs deliver assurance to the credential issuance and authentication systems addressing the need to strongly control who is on the network. As threats arise that require strengthening the assurance of your authentication and access control systems, Thales TCT solutions are the industry standard for assurance. Not only will they deliver the assurance required, they'll reduce total cost of ownership by reducing the number of mitigating controls that would otherwise be required.

What is Happening on the Network?
Managing the ongoing activities of the network require detailed event tracking and consolidation techniques. All Thales TCT products come ready to support this capability by including detailed audit log services that are ready to integrate with a CDM architecture. Each product also includes standard network monitoring services that allow your CDM dashboards to monitor key security events in real time.

Another key factor in this capability is contingency planning, the ability to restore and reconstitute a system and the capability to apply additional safeguards to prevent future compromise. Data Security Platform, Luna HSMs and the High-Speed Encryptors all offer redundancy and disaster recovery features that ensure systems remain active or can be rebuilt quickly when necessary – all without ever risking control over the protected keys.

Monitoring what is happening on the network includes protecting the network boundaries. This includes the use of devices such as firewalls that sit at the boundary and regulate network traffic. It also includes the use of encryption to create and enforce physical and logical boundaries. Thales TCT's High Speed Encryptors create and enforce network boundaries by encapsulating network traffic whenever it travels across untrusted infrastructure. It implements policy that defines authorized endpoints and controls and cryptographically encapsulates traffic between these end points. Finally, Thales TCT's cryptographic key management products deliver the assurance and key management required to implement effective cryptographic boundaries.

As agencies advance through the CDM phases, cryptographic controls become more critical with a broader impact. Almost all cryptographic controls ultimately rely on the high-grade protection of a few high-value cryptographic keys. If these keys are lost, the protection enabled by it typically becomes transparently porous. This means that the attacker can use the compromised key to silently bypass the control, leaving no evidence of their presence. This makes it critical to control the cryptographic keys used for a security control. Thales TCT's Luna HSMs provides the assurance necessary for a wide range of cryptographic solutions including:

- Certificate authorities for public key infrastructures and authentication solutions
- TLS server private key protection
- Document, code and email signing and encryption solutions

Luna Network HSM is the best in class HSM for U.S. Federal Government use. It offers unparalleled root of trust assurance. If a cryptographic control does not have an HSM protecting its keys, the control may not be achieving its goals.

How is Data Protected?
Protecting data is CDM's ultimate goal. Encryption is paramount for data protection and Thales TCT's solutions perform the necessary encryption while providing the high assurance key management required by government agencies.

As an organization classifies data, sensitive data will undoubtedly be found everywhere and in every form. Thales TCT's data protection solutions allow a common platform no matter what structure, format or location the data is found. Thales TCT's enterprise-ready data protection solutions offer:

- Data-in-motion and at-rest protection
- Comprehensive encryption for data in databases, files, media, virtual environments, and applications
- Centralized encryption and key management validated to FIPS 140-2
- Cloud-ready security for private, hybrid, public and multi-cloud deployments
- Transparent performance

The Data Security Platform provides the foundation for a full suite of data-at-rest data protection solutions. Often, the media used to store data is the forgotten network boundary. Thales TCT's data-at-rest encryption solutions take control of this boundary by enabling the encryption of all forms of data stored on media. Thales TCT's data-at-rest encryption solutions do the work of encrypting data while Data Security Manager manages the cryptographic keys. As data is identified and classified during CDM phase 4 activities, Thales TCT data protection is ready to secure it with enterprise-grade data encryption.

It is not always feasible to identify and encrypt sensitive data as it is being distributed across internally controlled assets. Since an organization's assets are typically distributed, Thales TCT's High Speed Encryptors are ready to protect data in motion. The high-performance of Thales TCT's High Speed Encryptors enable the encryption of all traffic on the links, so there is no need to worry if data is being missclassified.

Thales TCT Advantages

The CDM program is a complex security system that addresses a complex security problem for agencies. Realizing a government-wide program that automates the governance of information systems using an architecture that fosters a continuous improvement approach that is both cost efficient and highly responsible is a major accomplishment. With unsurpassed credentials and experience with encryption and key management technologies, Thales TCT is the obvious choice as the foundation of an organization's cryptographic controls. Here are some key reasons to choose Thales TCT for a CDM program:

Compliance

Thales TCT solutions have their cryptographic module validated to FIPS 140-2. In fact, the Luna HSM family is one of the most highly credentialed modules in the FIPS 140-2 validation program.

Integration

Thales TCT solutions include management interfaces that support integration with CDM solutions. Multiple management options are available, including SNMP, scriptable administration interfaces and human driven interfaces. These interfaces support the CDM requirements around collecting encryption policy for the creation of automated security verification.

Simplicity

The breadth of Thales TCT's data protection solution enables a single solution to be used for all an organization's data protection requirements. This reduces the management burden for the agency, optimizing operational costs. Similarly, the Luna HSM family is one of the most widely integrated HSMs on the market. Using the same HSM as the root of trust for all your cryptographic controls further optimizes operational costs.

Contingency Ready

The ability to restore and reconstitute a system quickly after incidents is a critical CDM requirement. Data Security Platform, Luna Network HSM and the High-Speed Encryptors all offer redundancy and disaster recovery features that keep systems operating and enable rebuilding systems quickly in the event a disaster recovery program must be activated.

Audit Ready

The collection and management of audit data from network assets is another critical CDM requirement. Again, Thales TCT products come ready to support this requirement by including detailed audit log services that are ready to integrate with your CDM solution. Not only does this allow the integration of the product as an asset in the CDM infrastructure, it also enables collecting configuration information on data protection policies.

Trusted Supply Chain

The CDM program encourages addressing the full life-cycle of the systems it is built on. Thales TCT follows a secure development life cycle that actively minimizes the probability of vulnerabilities within the solutions. Equally importantly, Thales TCT operates in the U.S. and is focused on developing mission critical solutions for U.S. government agencies. Thales TCT develops, manufactures, sells and supports all core products in the U.S.

ROI

Failing to deploy proper key management controls in an infrastructure can lead to massive unplanned costs down the road. If the integrity of a key is questioned it could lead to redeploying an entire system or compromising the integrity of all the information protected by the key. This could easily double the cost of rolling out the solution. Integrating Thales TCT cryptographic key management solutions on day one minimizes the risk of key compromise, by leveraging the best in class key management solutions.

Conclusion

As agencies work through the CDM phases, technical solutions are deployed or enhanced as they address CDM requirements. Many of these solutions require cryptography and Thales TCT plays a central role in delivering the cryptographic tools for boundary protection, access control, and the key management that is required to allow the cryptographic solution to achieve the CDM goals and objectives.

As phase 4 proceeds, government organizations are focused on delivering effective data protection systems and integrating them into the continuous monitoring framework created by CDM. After phase 4 the CDM program will finally be a fully operational system involving continuous monitoring and improvement on a department or agency's overall information security posture. Thales TCT is ready to help agencies reach their CDM data protection objectives.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

[1]Department of Homeland Security CDM Program https://www.dhs.gov/cdm

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com