Secure Operations vs Security Operations

Adopting Continuous Diagnostics and Mitigation (CDM) in the Health Care Industry To More Effectively Manage Cyber Security Risk

Healthcare has

- HIPAA
- HITECH
- HITRUST…

So Why Should We Care?

Moving beyond HIPAA

HIPAA Compliance Doesn't Manage Operational Cyber Security Risk

HIPAA compliance alone will not account for all the considerations in modern healthcare cybersecurity risk management. A compliance-centric and healthcare-specific approach can be limiting for a variety of reasons such as:

Every technology in a modern healthcare enterprise network is becoming healthcare-neutral.

Healthcare leaders need to consider the broader computing environment.

Healthcare organizations need to look far beyond healthcare-specific cybersecurity tools and start to adopt security technologies and practices from other industries.

By adopting a broader perspective healthcare organizations can go beyond the typical compliance and assessment activities associated with HIPAA-centric initiatives.

Compliant Insecurity

Compliance-centric cybersecurity initiatives fall short because they do not include the continuous diagnostic and risk management-based mitigation elements that are crucial to maintaining an effective security program.

Security Operations

The implementation and management of tools and processes
To collect information about and monitor the computing environment, Information stores, and applications for vulnerabilities and malicious activity.

Secure Operations

The use of securely engineered/configured, operated, and maintained computing environments that continually protect Information, remain properly patched/supported/configured, and retain secure connectivity by architecting, building, operating, continuously monitoring, and then mitigating risk-based
Vulnerabilities.

Basic Premise of Secure Operations:

You cannot secure what you do not (risk) manage.

You cannot (risk) manage what you cannot see.

You cannot see what you don't continually look for. (monitor)

Therefore…

How Do We?

Continually monitor and inventory all assets (including hardware, software and data) on the network, as well as how they are connected?

Based on the above, continually scan for secure configurations, architecture, and connections,
As well as,
Types of access to these assets and by whom/from where?

And manage vulnerabilities, based on risk, for all of the above?

Continuous Diagnostics and Mitigation (CDM)

The CDM program is a dynamic approach to implementing automated, risk based cybersecurity that will better assure the security of sensitive data and the provision of essential functions while protecting sensitive information.

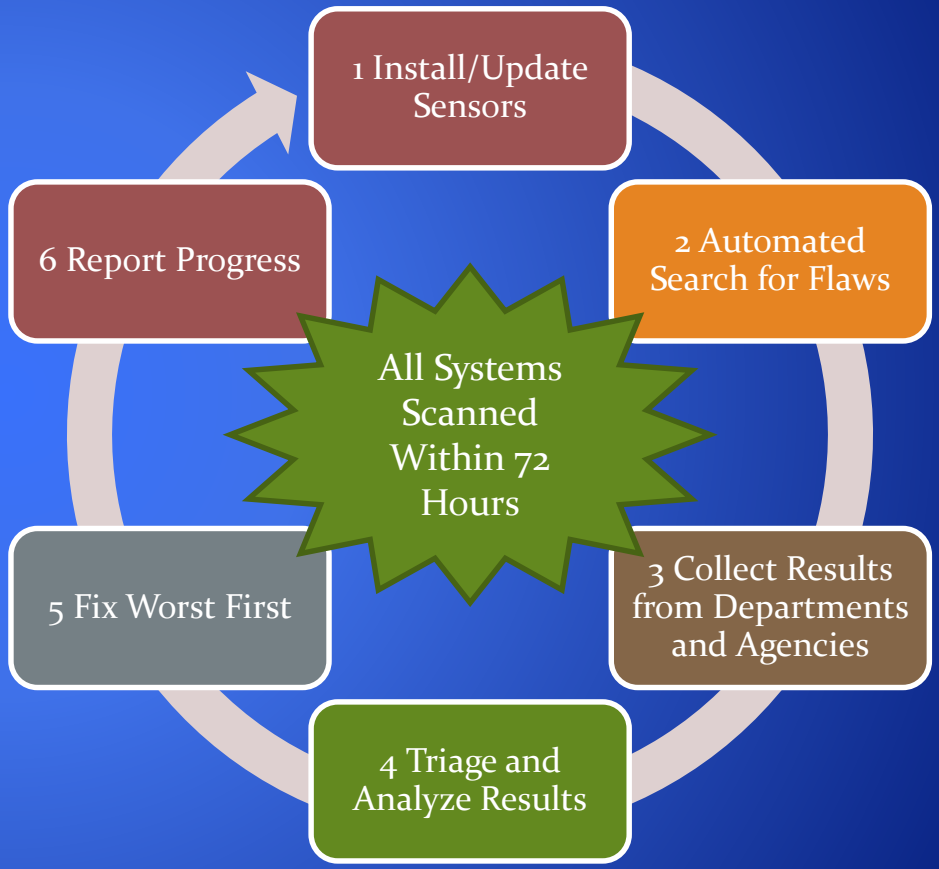
What CDM Does

Enables network administrators to know the state of their respective networks at any given time

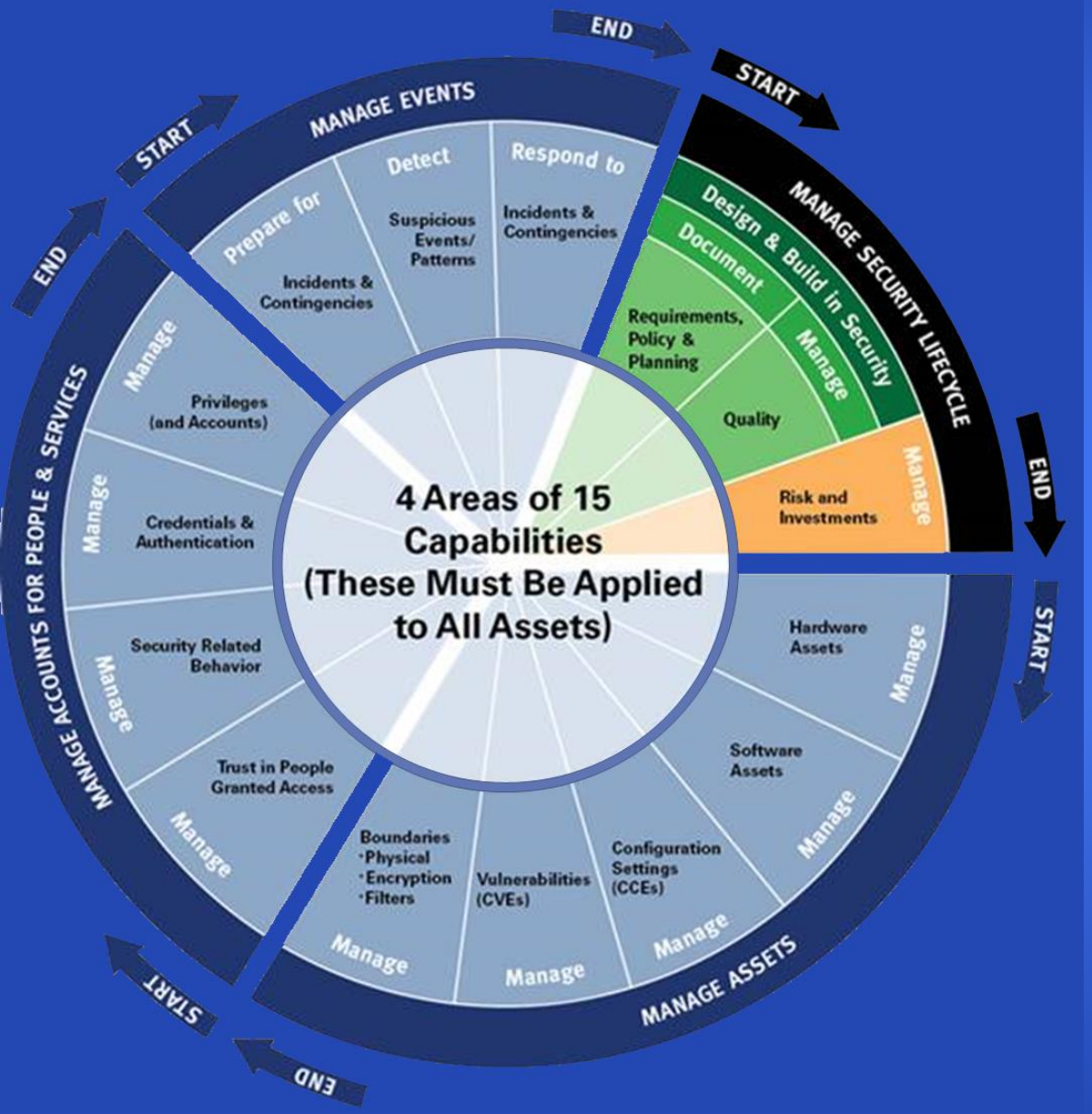
Informs on the relative risks of threats

Makes it possible for system personnel to identify and mitigate flaws at near-network speed.

Provides a consistent set of continuous diagnostic solutions to enhance the organization's ability to identify and mitigate the impact of emerging cyber threats



How CDM does it

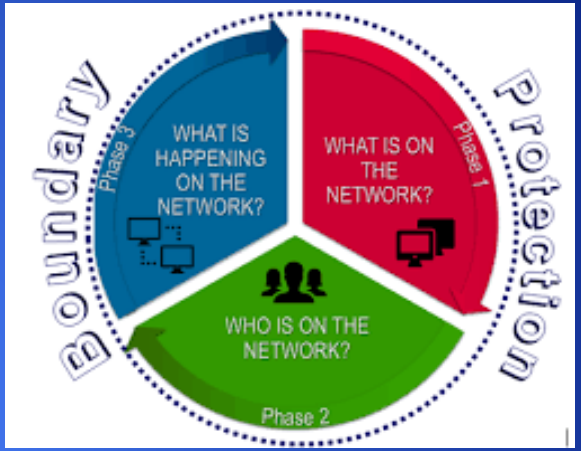


CDM Phases of Implementation

PHASE 1:
Endpoint Integrity
HWAM – Hardware Asset Management
SWAM – Software Asset Management
CSM – Configuration Settings Management
VUL – Vulnerability Management

PHASE 2:
Least Privilege and Infrastructure Integrity
TRUST –Access Control Management (Trust in People Granted Access)
BEHAVE – Security-Related Behavior Management
CRED – Credentials and Authentication Management
PRIV – Privileges

PHASE 3:
Boundary Protection and Event Management for Managing the Security Lifecycle
Plan for Events
Respond to Events
Generic Audit/Monitoring
Document Requirements, Policy, etc.
Quality Management
Risk Management
Boundary Protection – Network, Physical, Virtual



The DHS also has created a Continuous Diagnostic & Mitigation Product Catalog (**http://www.gsa.gov/portal/getMediaData?mediaId=199735**) that lists tools that can be used for the implementation of Phases 1 and 2.

In the future, adopting a CDM approach will facilitate:

Machine learning, artificial intelligence (AI), big data analytics and other advanced methods—including statistical models and adaptive rules to sort through gigantic volumes of data—are being refined to help identify the trace evidence of malware and other intrusions.

Automated responses—leveraging more advanced techniques for security orchestration, incident investigation, containment and remediation—will help reduce post-breach dwell times and damage costs.

Deceptive technologies, including honeypots and undercover surveillance, will increasingly be used to detect or deflect malicious attacks.

Context-based analytics will be deployed to detect anomalies in user and network behavior and to counter adversaries who seek to circumvent traditional known and signature-based security methods.

In the future, adopting a CDM approach will facilitate: (cont)

Purpose-built simulation environments with isolated networks are now being used to run the world's most dangerous malware and to recreate actual attacks without allowing those malicious codes to spread.

Segregation and containers are being refined to separate the security execution environment from the larger operating system, thus preventing OS attacks from compromising the security protections.

New computing architectures are replacing traditional RAM- and disk-based storage with faster, nonvolatile memories. This allows security teams to process larger data volumes, find patterns faster and create new defensive techniques.

Employment of robust identity-protection mechanisms. This will entail risk-based authentication and access, leveraging tools such as policy-driven adaptive authentication across multiple data points.