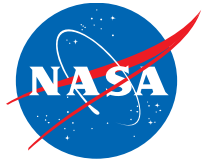


Continuous Diagnostics & Mitigation (CDM)

Willie D. Crenshaw, Jr

NASA CDM Program Executive

What is CDM?

- The **Continuous Diagnostics and Mitigation** (CDM) program is a Federal IT Security program in which the Department of Homeland Security (DHS) provides Departments and Agencies with IT Security tools to support Information System Continuous Monitoring (ISCM) and feed the Federal CDM Dashboard

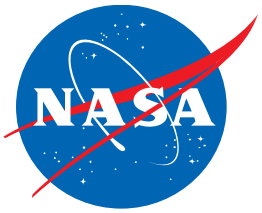
- CDM Program affects all Federal Departments/Agencies

- All NASA Centers/Missions are in scope

- Data collected from CDM Sensors will feed the Federal Dashboard –will provide a more complete cyber posture of all Federal Departments/Agencies

- CDM is tasked with replacing and/or enhancing IT Security tools and sensors – goal is to ***consolidate, standardize and centralize*** IT Security tools

CDM Objectives/Capabilities



Overarching CDM Program Objectives

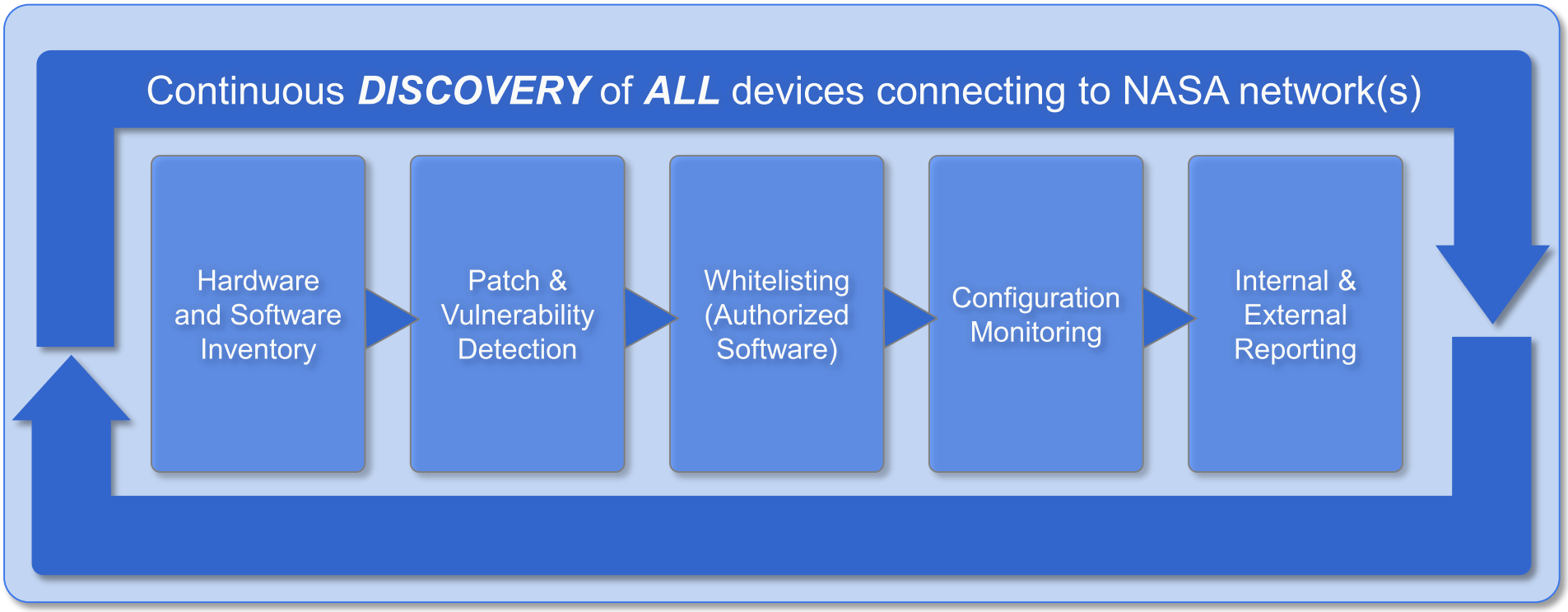
– Fix most critical problems first

– Strengthen federal networks against attack

Updated CDM Phases and Capabilities

- Phase 1 (What is on the Network?)- **In progress (being implemented at NASA)**
- Phase 2 (Who is on the Network?) –
- BOUND (Protecting the boundaries)- *added to accelerate some phase 3 activities per Congress*
- Phase 3 (What is happening on the Network?)
- Phase 4 (Protecting the data on the Network?)

CDM Lifecycle



The CDM Program will increase Information Security ***Continuous*** Monitoring for NASA

Advantages -
What benefits do we get out of CDM?

- IT Security Tools paid for by DHS
- Increase over current capabilities –

  Passive network discovery – will help us identify WHAT is connected to our networks

  Additional Operating Systems support for patch/vulnerability management

  Whitelisting – prevent unwanted (malicious) software from running on our machines

- Consolidated tools – cost savings and efficiencies by retiring duplicative tools
- Standardized tools – cost savings and efficiencies by retiring duplicative capabilities
- Centralized tools – efficiency gains by removing the need to configure/manage/maintain the same tools at each Center
- Increased AUTOMATION in tool integration
- Automation for FISMA reporting (future)
- Decreased time in reporting on vulnerabilities/configuration settings

INCREASED IT SECURITY POSTURE!!!

Better Management of Risk

- New capabilities provide increased visibility and will enable the agency to know its true risk posture.
- Provides the department and agencies with more accurate information that will allow for better management of risk.
- Allows for prioritization for risk.

Its about Team

For the CDM team to be successful you must have:

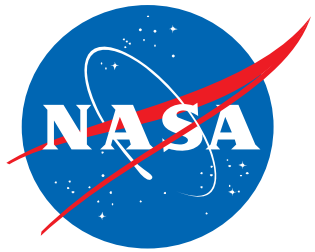
- The support of leadership
- Members that understand the mission and the goal
- A good game plan
- A well executed game plan

A team that is dedicated, working together to achieve a common goal will be successful

How to achieve success?

- Understand the challenges we face
- Be flexible in our application and implementation of the tools and capabilities.
- We must be resilient
- Be forward thinking

Questions


NASA

Slide Master