National Aeronautics and Space Administration

NASA Information System Security:
The Path Forward with Automated Continuous Monitoring

Office of the Chief Information Officer

NASA IT Vision: The NASA IT Organization is the **very best** in government

AUTHENTIC INFORMATION DRIVEN RISK MANAGEMENT

NASA's IT risk management strategy had been ill equipped to effectively respond to risk. The old strategy was to "wait" for the incident to occur and then, if detected, respond (highly reactive) and then repeat

•Response was generally slow and almost always after the incursion has taken place and the data or system is completely compromised

•Mitigation was generally a hastily cobbled together band aide solution that peeled off fairly quickly

•Continuous risk management did not take place so root cause is generally unknown and thus data, information and systems remain at risk of further compromise

The key is to make IT security ***measurably*** better by transforming security into a ***proactive*** and continuous IT security risk management process. This is done by gaining dominance of ***situational awareness***

May 18, 2010 Memorandum*: A Shift in Direction

- Suspension of 3-Year Recertification Requirements
  - » Old processes had proven to be expensive, cumbersome, and ineffective at ensuring system security.
- Provision of ATO Extensions
  - » Authorizing Officials were given an option which avoided needless security expenditures, and emphasized risk management.
- Shift in Security Focus
  - » NASA must move away from sporadic paperwork exercises to effective continuous monitoring.

* http://www.govexec.com/pdfs/051910j1.pdf

The Philosophy:
"What gets measured, gets improved."

What are the things we should really be measuring?

How can we make things consistent across the Agency?

Can we communicate and track our progress?

"I keep six serving men (they taught me all I knew),
their names are what, why, where, when, how, and who."
-Rudyard Kipling

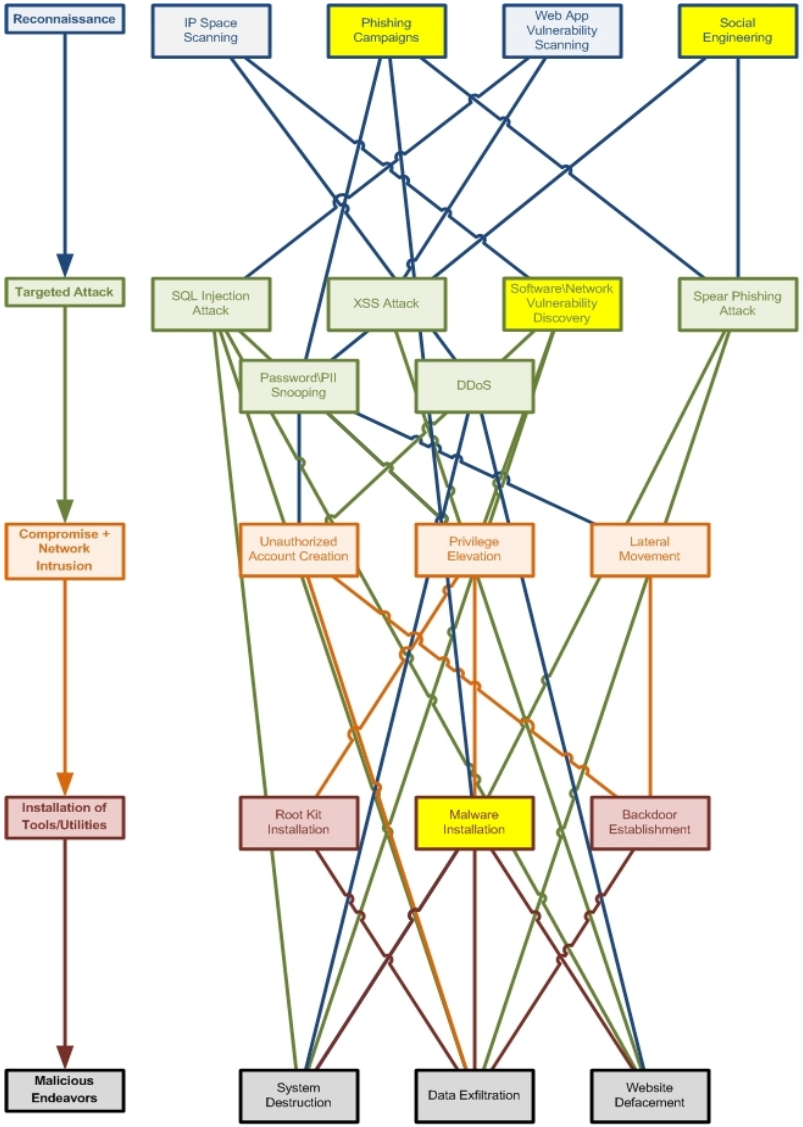
The Plan of Action

- Identify Most Pressing Concerns
  - » Conducting Agency-wide risk assessments.
  - » Analyzing the most frequent and impactful incidents.
  - » Capitalizing on proven industry practices.

- Automate! Automate! Automate!
  - » Where ever possible move the implementation, management, and monitoring of controls to the Agency level using automated tools.

- Develop Risk Score Cards
  - » Consistent, fair security grading for our systems and Centers.

The Attack Tree



Attacks tree nodes highlighted in yellow (~) have a high frequency of incidence at NASA; these nodes represent the areas where NASA should focus attention in order to ensure the greatest measurable improvement to the overall Agency security posture.

Related 800-53 Controls

RA-05
Vulnerability Scanning

SANS CAG identifies Vulnerability Scanning as a critical security control, and NASA incident analysis shows that unpatched information systems are a major catalyst to security compromises.

SI-02
Flaw Remidiation

The installation of updates and patches to popular desktop applications and products (e.g., Java and Adobe) could prevent a large number of security compromises which rely on weaknesses in older versions of software.

CM-08
Information System Component Inventory

The ability to quickly identify and rogue information system components (especially software) is dependent on a comprehensive understanding of the Agency's information system inventory.

CM-06
Configuration Settings

Maintaining a consistent baseline for how information systems are configured supports the prevention, identification, and resolution of information system compromises.

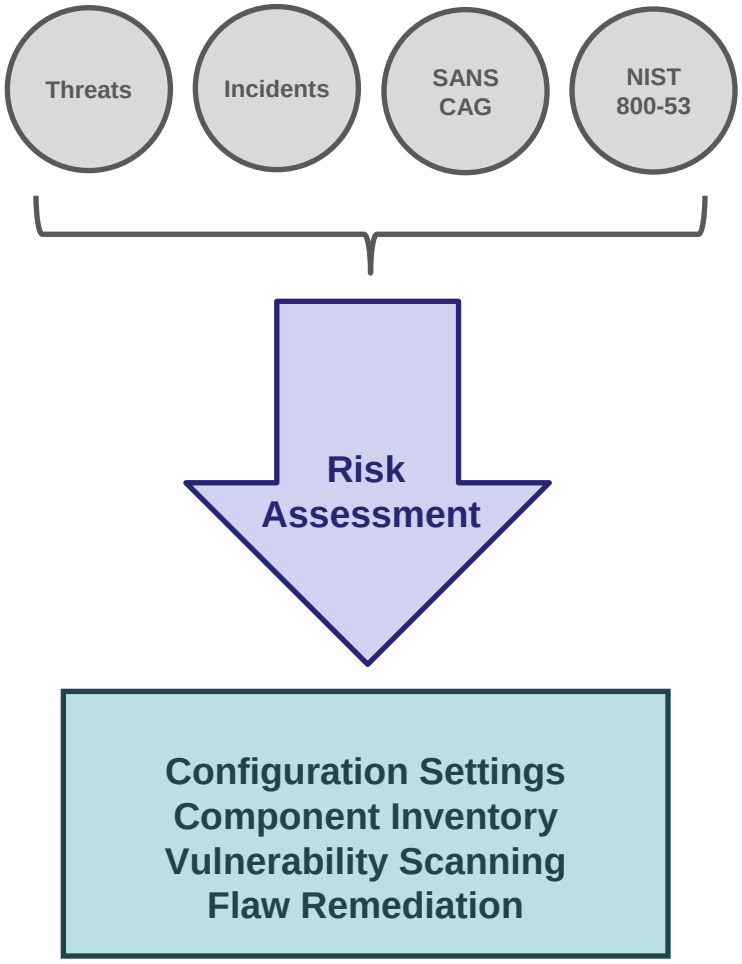
AT-03
Security Training

Well-informed users are a critical, and sometimes last line of defense against common and ever-present phishing, malware, and social engineering attacks.

Identifying the attacker's modus Operandi from end-to-end and Then implementing controls that shunt their capabilities.

From there it's just continuous monitoring of those controls

Security Control Tailoring



Inputs

Vulnerability Data
SOC\CTAP Data
Research from SANS, NIST, and Partners

The threat analysis/risk assessment represents an Agency-wide, all-sources analysis.

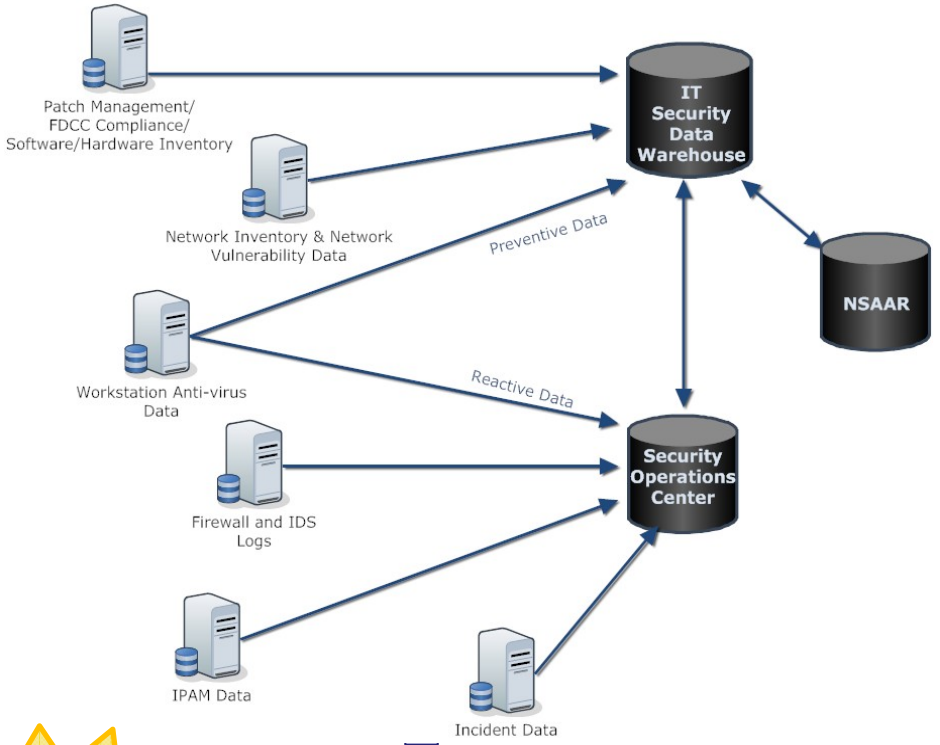
Outputs

The set of security controls which would best address NASA's most critical and pressing security needs.

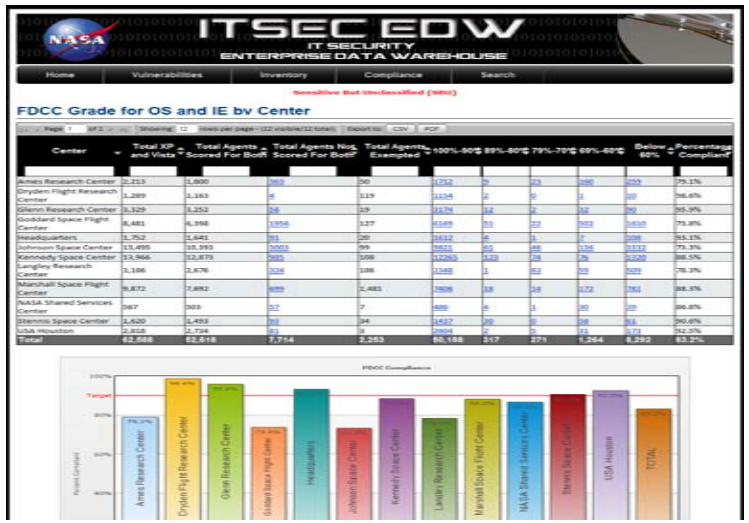
Automated Continuous Monitoring: Tools and Reference Architecture

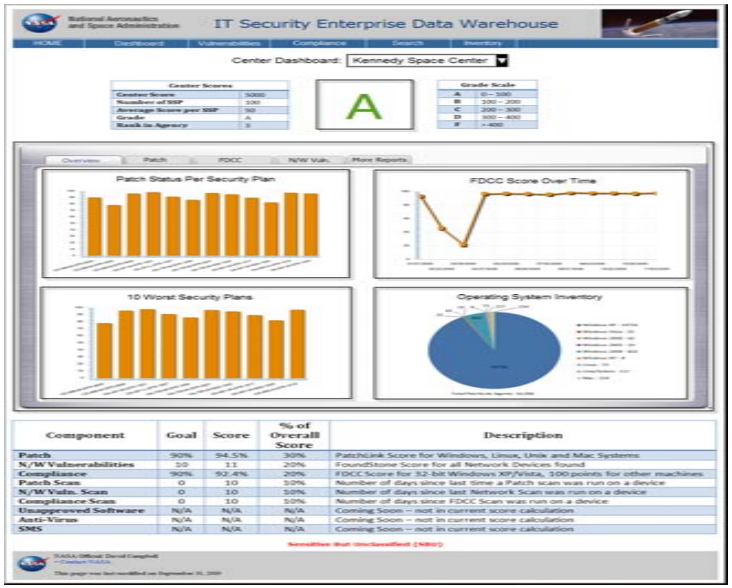
For Example:

- P Address Management (IPAM) for inventory management.
- Active Directory Group Policy Objects (AD-GPO) for configuration management.
- Vulnerability Management (VM) which augments and supports inventory management.
- Patch Management (PM) is useful for software management, Operating System inventory, and custom builds.
- Antivirus (AV) logs can also provide really good information on malware vectors into the environment.



Risk Score Cards: Measuring Performance





Grades and Ranks
Summaries empower executives

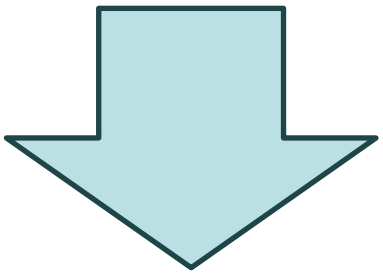
Drill Down Data

Metric Information
Details empower technical managers

Ongoing Authorizations

- Enabled by readily accessible score cards.
- Based on near real-time insight into security posture.
- Saves time, money, and resources over arbitrarily periodic traditional C&A methodologies.

Ultimate expression of…



True Situational Awareness and Authentic Risk Management

The key to all of this, and our primary goal is to make IT security **measurably better** by transforming security into a **well-informed**, **proactive** and **ongoing** risk management process.