Headquarters U.S. Air Force

Integrity - Service - Excellence

A4 Cybersecurity Transformation

Mr. Charles Wade
A4PA

Nov 2018

U.S. AIR FORCE

Purpose

- Provide the Strategy for Cybersecurity Transformation
- Discussion Content:
  - Context
  - Problem Statement
  - Vision
  - Strategic Framework
  - Future State – Vulnerability Based Risk Management
  - Assessment & Mitigation Key Steps
- 10 Year Action Plan

Context

The Air Force operates in an *increasingly complex, highly digitized, cyber contested environment.* Information is as critical of an asset as jet fuel or ammunition. From IT systems to Operating Technology (OT), to “stand alone” devices, information permeates Basing & Logistics technology and processes. The Air Force is *highly reliant on these technologies and the information they contain to execute our mission.*

Our reliance on information creates *asymmetric threats* that do not require our adversaries to be peer or near-peer in order to significantly disrupt operations.

Current Status of Risk Management

- “Compliance-Based” Risk Management
  - Shaped by DIACAP paradigm - checklist
  - Compliance with standards vs. finding vulnerabilities
  - Limited testing to simulate malicious attacker
  - Standards do not reflect current threat environment
  - Program Managers don’t understand or respond to vulnerabilities for maximum risk reduction
- Interconnectedness of IT systems and information magnifies the vulnerabilities and increases the risks
- Lack comprehensive understanding of all vulnerabilities

Current Status of Risk Management (cont)

- Program Management security testing
  - Acquisition KPPs -- Cost/Schedule/Performance
    - Security “bolted on” at the end rather than engineered up front
  - Cybersecurity personnel are often funded by or through the program office – may not possess needed independence
  - PMs cannot test systems once in production environment
  - Automated vulnerability test configurations may provide a “Green Light” when vulnerabilities actually exist
- Basing & Logistics culture that:
  - Does not understand or appreciate the risks
  - Does not understand the individual’s role in identifying, detecting, reporting, and mitigating risks

Vision

By 2029, the Basing & Logistics enterprise with have processes and culture where:

(1) **Cyber Ready Vigilant Logisticians are the norm**

(2) **Limited resources are leveraged judiciously**

(3) **Continuous monitoring with symmetric and asymmetric testing is the normal process to secure information**

(4) **Vulnerability discovery and remediation are the drivers for risk management**

(5) **Continuity of operations across the Basing & Logistics enterprise is assured for critical IT**

U.S. AIR FORCE

Strategic Goals

Pillar 1: Risk Identification

Goal 1: Assess evolving cybersecurity risks

Pillar 2: Vulnerability Reduction

Goal 2: Protect Critical Information Systems

Goal 3: Protect Critical Operational Technology

Pillar 3: Continually Monitor IT

Goal 4: Detect vulnerabilities and harden on the fly

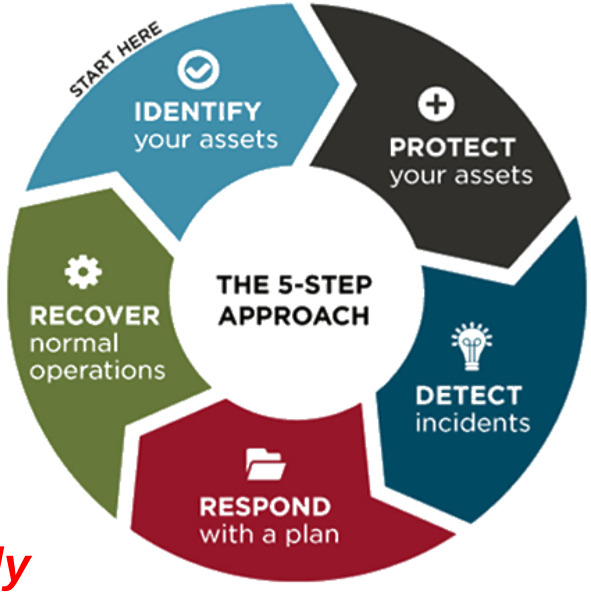
Pillar 4: Consequence Mitigation

Goal 5: Respond Effectively

Pillar 5: Enable Cybersecurity Outcomes

Goal 6: Strengthen Security and Reliability of the Cyber Ecosystem

Goal 7: Improve Cybersecurity Activities



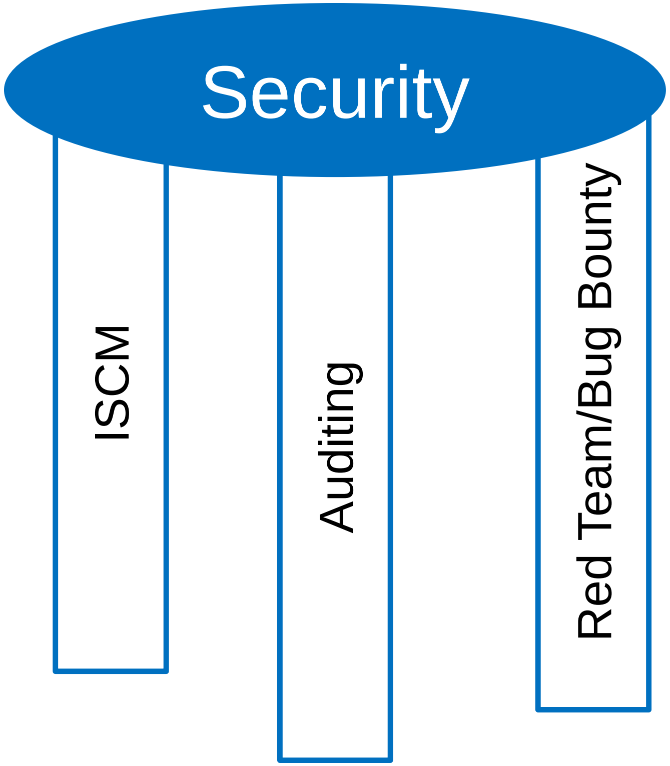
Vulnerability Management

Know that you know what you know

Pillar 3: Continually Monitor IT

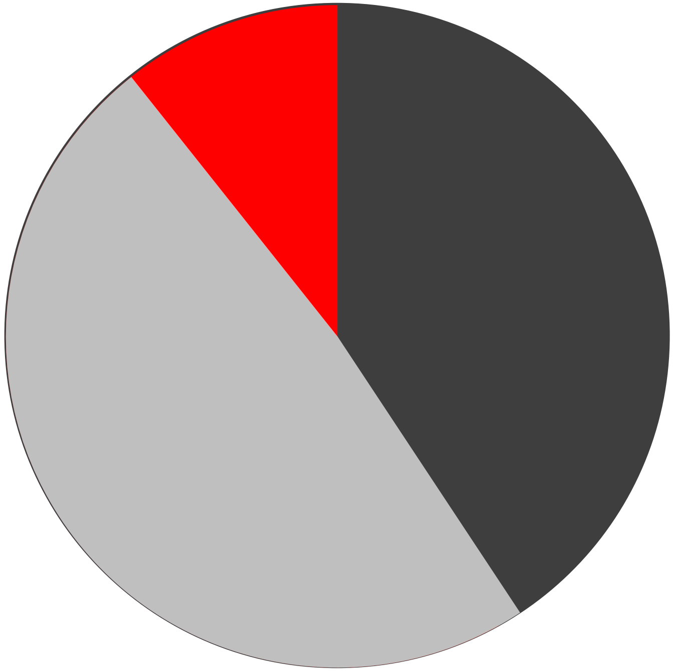
Goal 4: Detect vulnerabilities and harden on the fly

- **Information Security Continuous Monitoring**
- **Auditing by independent agents**
- **Red Teams – Bug Bounties**



Continuous Monitoring

- Focused on a handful of controls – “At all times”
- Shifts non ISCM controls to program managers



All security controls grouped by area of oversight/governance

🟥 **ISCM** (& some FIAR controls)

⬛ **FIAR PM Managed**

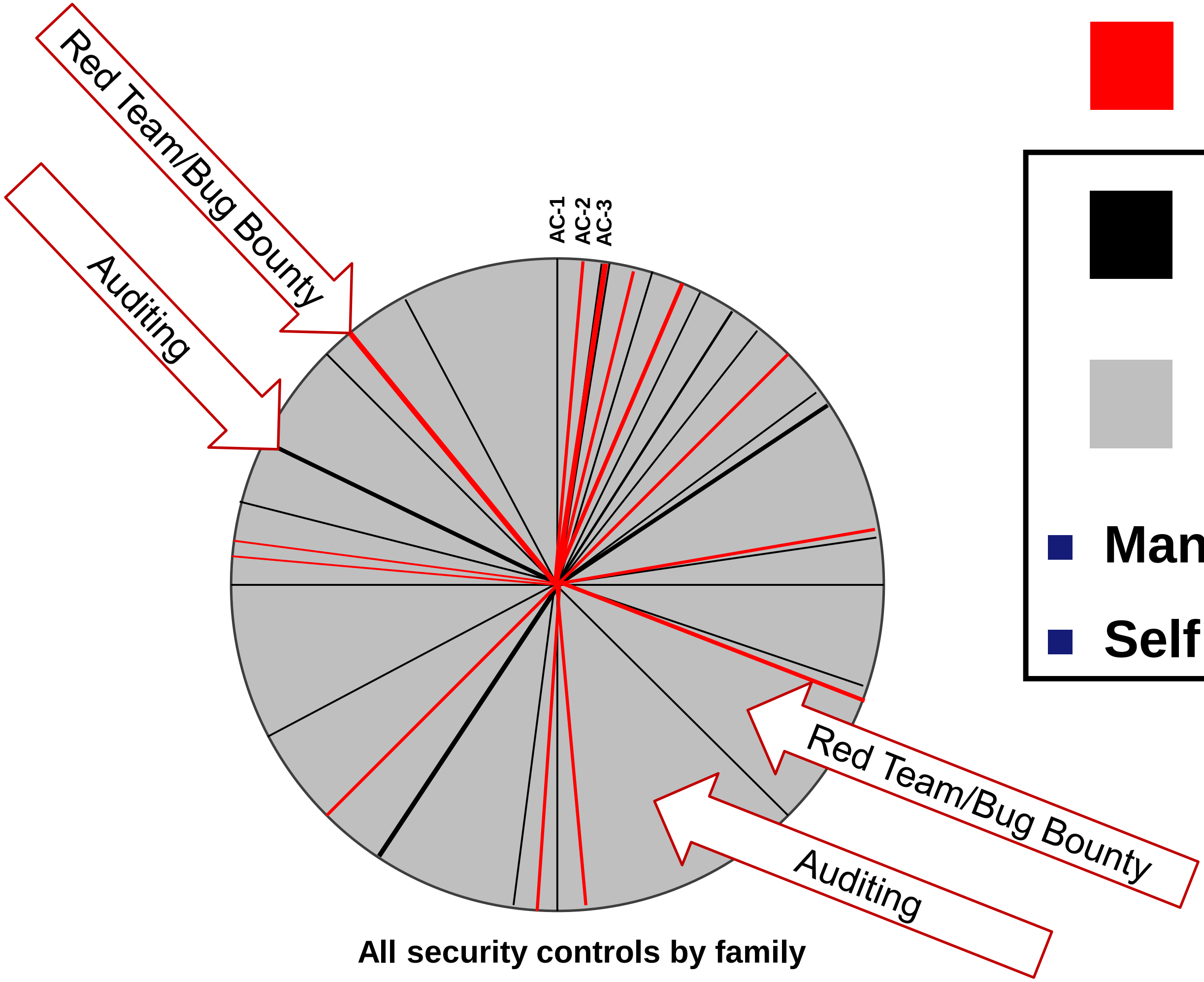
▩ **Non- FIAR PM Managed**

- **Managed by exception**
- **Self reporting**

Continuous Monitoring

- Begin with a subset of controls
  - We use the “Dirty 36”
  - Forms the starting point for ISCM, ATO consideration
  - May be more or less, depending on the system, its criticality, etc.
- ISCM becomes the basis for continual authorization, continual monitoring
  - Controls tested daily, weekly monthly…. ATO decision is based on the system’s ongoing risk level and risk tolerance of the AO
  - High risk systems are issues ATOs with short expiration dates to drive the risk level down and provide more oversight

Continuous Monitoring



All security controls by family

🟥 ISCM & some FIAR controls

⬛ FIAR PM Managed

⬜ Non- FIAR PM Managed

- Managed by exception
- Self reporting

Desired Future State

- Security focused on vulnerabilities as a key risk driver
  - Manage vulnerabilities & risk across the IT's life cycle
  - Information security continuous monitoring (ISCM) the norm
  - Robust Symmetric & Asymmetric vulnerability detection
    - External, independent testing through Bug Bounty/Red Team
    - Independent Security Control Assessor audits
- Cybersecurity workforce realignment
  - Align systems engineering with security engineering pre PMO
  - Institutionalize culture of "Sense and Respond"
- Automate cybersecurity functions
  - Real or near real time monitoring and alerting
  - System testing

Bug Bounties

- Provides an incentive to find vulnerabilities
- One time pass to baseline
- Goal is to have perpetual BB
    - Consider limiting to critical IT
    - Budget for fixes

Auditing

- Compliance is still a necessary evil
- Cannot let compliance drive security $$ for the sake of compliance – make risk based decisions
- The bulk of compliance falls on the program manager
    - Best source to allocate resources to make mission – compliance decisions
- Leverage outside audit agents the same as a SCA

Critical Initiatives for Success

- Initiative 1: Vulnerability Based Risk Management
- Initiative 2: Cybersecurity Workforce Realignment
- Initiative 3: Automation of Cybersecurity Functions

Initiative 1: Vulnerability Based Risk Management

"…controls are necessary, but not sufficient, and penetration test results—rather than compliance documentation—are better indicators of a system's security."

GAO report on cybersecurity in the DoD

- **Implement a Bug Bounty (BB) for each of the next 4 years**
  - **Test 5 Priority 1 systems per year**
  - **Leverage lessons learned to harden across the enterprise**
- **POM for a "continual" BB program**
  - **Leverage SCA audits for non BB controls such as FIAR compliance**
- **Migrate systems to continual authorization/monitoring with BB as a key driver of vulnerability management**

Initiative 2: Cybersecurity Workforce Realignment

"…there are one million open cybersecurity positions today, it will grow to 3.5 million by 2021."

CSO Online 2018

- **Rethink how we staff ISSM/Os across the enterprise**
- **Build a cybersecurity engineering division that works concurrently with the system engineering division**
- **PMOs only start to "bend metal" once a solution has passed the engineering and cybersecurity engineering design phase**
  - **Manning comes from the ISSM/Os in PMOs now**
  - **Cybersecurity is "baked in" from the start, not bolted on after**
  - **Independent tests performed by the SCA measure success**
- **Reduction in the # of cybersecurity personnel goes down**

Initiative 3: Automation of Cybersecurity Functions

"Cyberattacks have become increasingly automated…To successfully protect against attacks, it is essential to fight fire with fire."

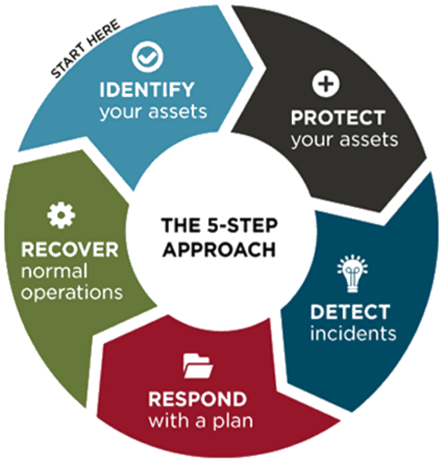
Palo Alto Networks 2018

- Leverage automation to enable real or near real time monitoring
  - Enable emerging technology such as AI to assume repetitive roles such as audit log reduction, monitoring
  - Monitor the enterprise for rapid interpretation of potential vulnerabilities before they become an issue
- Automate testing in development and production
  - Discover "coded" vulnerabilities before BB
  - Testing performed daily to discover deltas from desired state
- Reduce the need for cybersecurity personnel at the PMO level

U.S. AIR FORCE

Putting it all together

Strategy:


START HERE

IDENTIFY your assets

PROTECT your assets

DETECT incidents

RESPOND with a plan

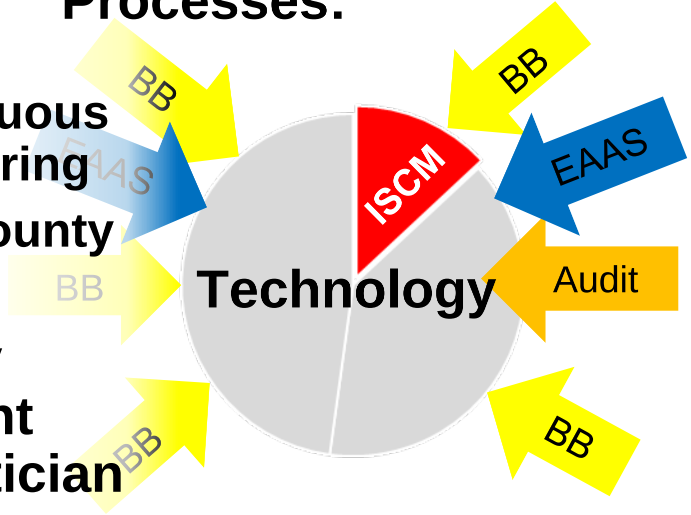
RECOVER normal operations

THE 5-STEP APPROACH

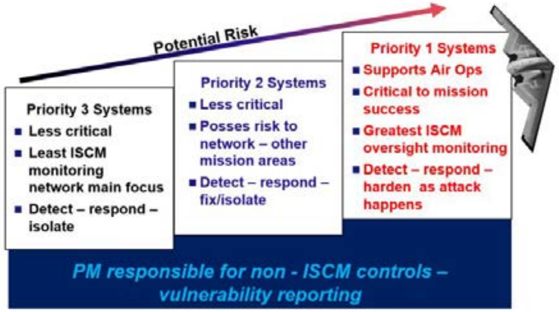
- Identify
- Protect
- Detect
- Respond
- Recover

Processes:

- Continuous Monitoring
- Bug Bounty
- Cyber Ready Vigilant Logistician



Align Resources:


Potential Risk

Priority 3 Systems
- Less critical
- Least ISCM monitoring network main focus
- Detect – respond – isolate

Priority 2 Systems
- Less critical
- Posses risk to network – other mission areas
- Detect – respond – fix/isolate

Priority 1 Systems
- Supports Air Ops
- Critical to mission success
- Greatest ISCM oversight monitoring
- Detect – respond – harden as attack happens

PM responsible for non - ISCM controls – vulnerability reporting

- Warfighter
- Supply Chain
- Personnel
- Assets

End Results:

- Find vulnerabilities – not document compliance
- Harden critical systems on the fly
- Culture of Sense and Respond
- Agile cybersecurity

Change cybersecurity culture