A Methodology for Developing Effective and Efficient Cybersecurity Architectures for Data Centers

William Belei
Peter Katsumata
The Aerospace Corporation

Ground Systems Architecture Workshop
March 2-5, 2020

Approved for public release. OTR 2020-00269.

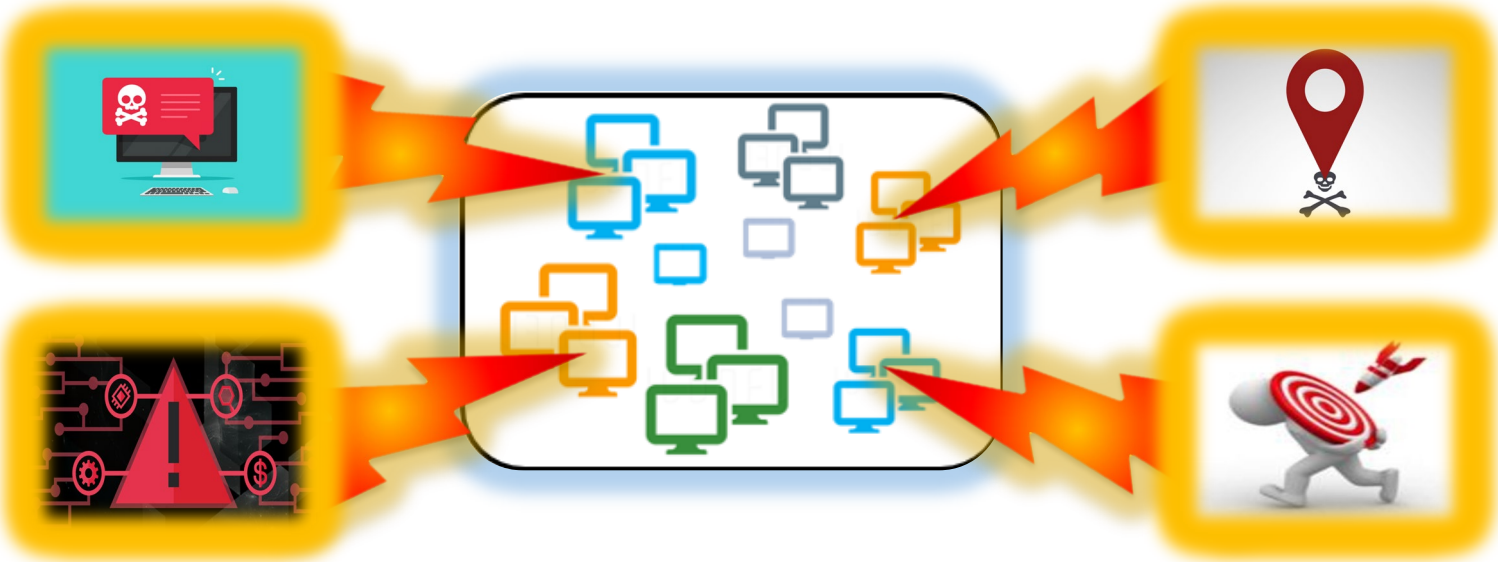
Agenda

- Introduction
- Cybersecurity Strategy Development
- Use Case Methodology
- Summary

Introduction

Many current IT architectures are deprecated and decentralized

- Many legacy systems were developed as isolated systems and prior to threat escalation, forcing programs to bolt on cybersecurity as an afterthought
- Current systems' Cybersecurity Architectures are often:
  - ***Inadequate*** *– sizeable gaps in basic cybersecurity capabilities are not uncommon*
  - ***Inefficient*** *– lack of centralization prevents efficient cyber and IT management*
  - ***Expensive*** *– vast majority of cyber resources are used for compliance (ATO) activity ... no resources left for cyber risk reduction activities*



Current system cybersecurity focused on individual subsystem protection

Introduction

Architecting a cybersecurity enterprise is key

- Proposed Way Forward: Enterprise cybersecurity architectures should prioritize the pursuit of three key principles/characteristics:
  - *being Cybersecurity Holistic*
  - *operating in an Enterprise-Centric Manner*
  - *establishing the foundation for Compliance Process Efficiency (this presentation does not further expound on how to pursue this principle)*

- Backdrop: Industry is moving to more rapid and flexible acquisition strategies
  - *Establish higher level requirements at the start of the project as general guidance*
  - *Enter spiral or agile development phases*
  - *Develop more detailed requirements as the project progresses*
  - *Generating exhaustive and detailed cybersecurity requirements at the start of an acquisition is incompatible with the above … but loose guidance to the developer such as "Apply the RMF" has also proven ineffective ➔ middle ground approach*
    - Develop and document high-level cybersecurity capabilities
      - *High-level descriptions of activities that accomplish cybersecurity objectives*
      - *Written at a level that is high enough and generic enough (e.g., agnostic to any tools or technologies) to "begin the conversation"*
      - *Project stakeholders work together in subsequent spirals/sprints/etc. to develop the lower level details/requirements*

Start by "documenting high-level cybersecurity capabilities" … but how do we do this?

Cybersecurity Strategy Development

Cybersecurity measuring stick selection

- The Community Gold Standard Framework Version 2.0 from the National Security Agency
- Center for Internet Security (CIS) Top 20 Critical Security Controls 7.0 (formerly the SANS Top 20)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 1 - *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
- NIST SP 800-53 Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (aka the NIST Cybersecurity Framework (CSF))

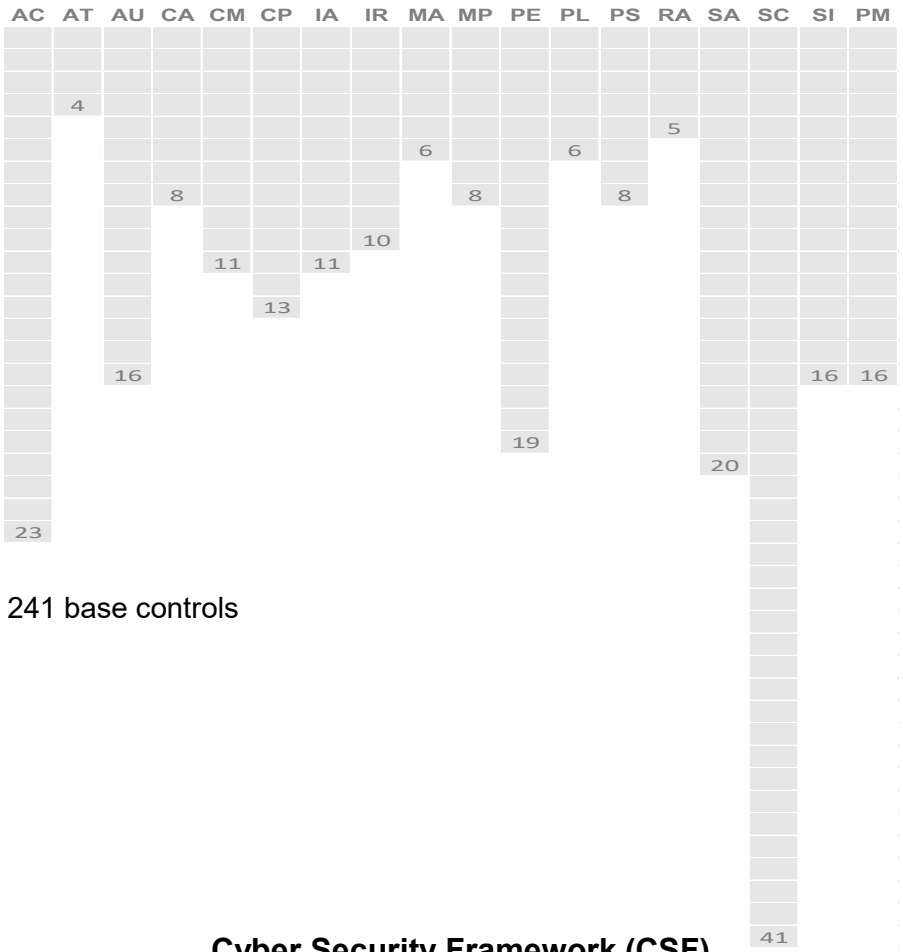
CSF has taken on added prominence in Fed Gov & DoD with Executive Order 13800 & NIST SP 800-37 Rev 2

Cybersecurity Strategy Development

Cybersecurity measuring stick selection continued …

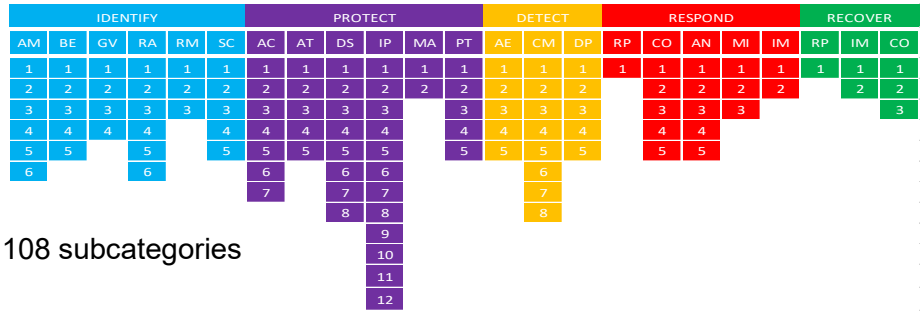
- Original inclination to use the RMF's 800-53 control catalogue, however, project funding and aggressive schedule forced us to find an alternative
- CSF offered some key advantages:
  - *Essentially covers the same broad cybersecurity spectrum as the RMF yet abstracts at a higher/more appropriate level*
  - *NIST has included a mapping to/from CSF subcategories to RMF controls*

Risk Management Framework (RMF)



241 base controls

Cyber Security Framework (CSF)



Cybersecurity Strategy Development

Cybersecurity measuring stick selection continued …

Risk Management Framework (RMF) ~800+ controls (241 base controls + 741 enhancements)

Cyber Security Framework (CSF) 108 subcategories (AKA controls)

The CSF abstracts cybersecurity at a much higher level than the RMF

Cybersecurity Strategy Development

Enterprise considerations

- Assembled a diverse team of cybersecurity SMEs, directed them to leverage their experience, available industry guidance, and ultimately use the CSF as a measuring stick to develop an enterprise cybersecurity architecture that:
  - *Provides the foundational cybersecurity protections for the data center's infrastructure and*
  - *Efficiently extends those integrated & holistic collection of cybersecurity protections for tenant applications to subscribe to*

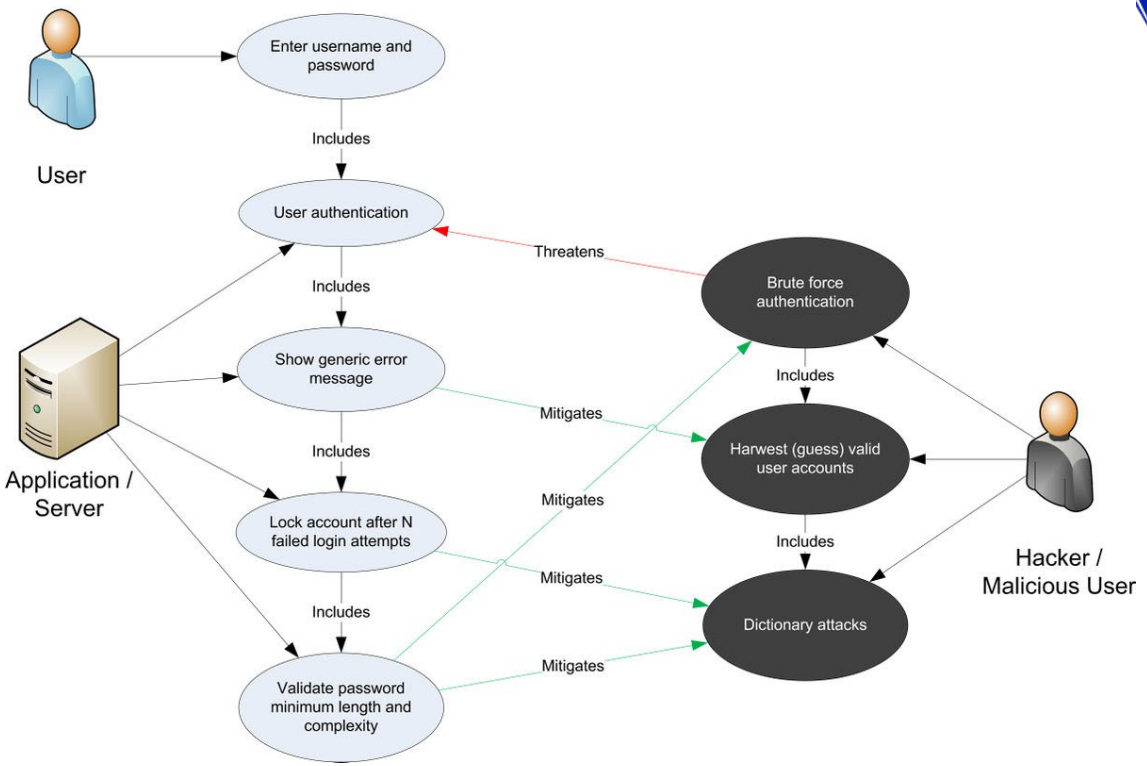
➔ 29 Enterprise Cybersecurity Services (ECSs)

Enterprise Cybersecurity Services	
Account and Access Control	Network Flow and Packet Analysis
Identity Management	Security Information and Event Management
Vulnerability Management	Incident Management
Network and Endpoint Anti-Malware	Data Center Backup and Recovery
Software Inventory and Control	Segregated Test Environment
Security Configuration Management	Security E-mail Gateway
Network and Endpoint IDS/IPS	Secure Web Gateway
Data Protection	Wireless IDS/IPS
Data Loss Prevention	Breach and Attack Simulation and Penetration Testing
Boundary Protection	Media Sanitization
Network Hardware Port Security	User Entity and Behavioral Analytics
Device Configuration Scanning	Digital Forensics
Device Network Privileges Adjudication	Automated Warning and Intelligence
Device Network Privileges Provisioning	Deep Learning/Artificial Intelligence
Data Inventory Labeling	

Use Case Methodology

Apply Use Case methodology to ECSs

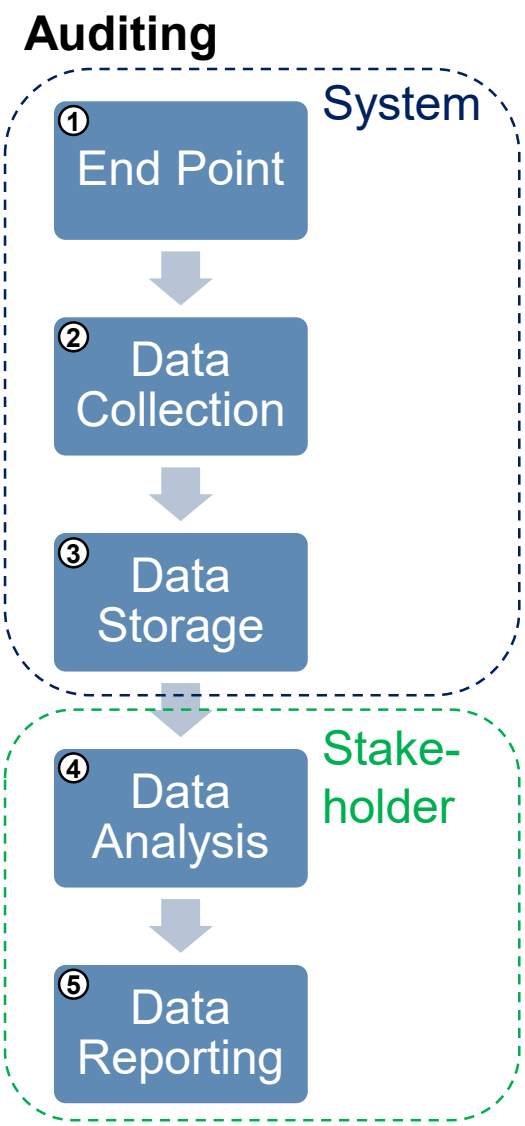
- Common technique to capture functional requirements
- Originally created for software development (the use case technique is well documented in literature)
- Adapted for systems engineering and, to a lesser degree, applied specifically for cybersecurity
- List of actions or event steps typically defining the interactions between a role (e.g., human or other external system) and a system to achieve a goal
- Applied to provide a high-level functional description of each ECS



Provide the concept of the cybersecurity service by describing the major functional activities, and where applicable, inputs, outputs, and pre-requisites.

Use Case Methodology – Cybersecurity Example

Example application of Use Case Methodology to cybersecurity



- Summary: Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures
- Main Success Scenario/Narrative
  1. *End point creates data*
     - Log data from router, switch, etc
  2. *System collects data*
     - SIEM system or equivalent collects log data from end points
  3. *System stores data*
     - ASSUMPTION: Log data stored in DC
  4. *Stakeholder analyzes data*
     - ASSUMPTION: CDCC or MDT analyzes data
  5. *Stakeholder reports data*
     - ASSUMPTION: CDCC or MDT reports findings
- Extensions
  - *2a. Data collected does not meet requirement*
  - *3a. Storage not sufficient for amount collected data*
  - *4a. Data analysts not available*

Summary

Migration to cybersecure, data center based architectures

- Data center based cybersecurity architectures can be vastly more effective and efficient by ensuring they are
  - *Cybersecurity holistic: architectures will include all fundamental cybersecurity capabilities*
  - *Enterprise-centric: architecture will be centralized and integrated across IT enterprise.*

- Presented an approach to rapidly develop cybersecurity architectures that are cybersecurity holistic and well as enterprise-centric based on:
  - *NIST Risk Management Framework (RMF)*
  - *NIST Cybersecurity Framework (CSF)*
  - *Use Case analysis*

- A critical feature of this methodology is that the underlying capabilities of the cybersecurity architecture are expressed in language that is tool/technology agnostic and ready to be provided to a DC developer to initiate a spiral/agile development process

Align data center cybersecurity architectures to "Cybersecurity holistic" and "Enterprise-centric" design principles