

Mission-Oriented Cybersecurity Requirements

Paul M. Kodzwa

Frank B. Gray

Marion L. Williams

Cost Analysis and Research Division

IDA | Presentation Overview

- Bottom Line Up Front
- Motivation & Background
- DoD Cybersecurity T&E Community Perspectives
- Taxonomy of Cyber Threats/Munitions
- Cybersecurity Control and Requirement Limitations
- Mission-Based Cybersecurity Illustration and Prerequisites
- Conclusions

IDA | Bottom Line Up-Front

- Past cybersecurity T&E experience (workshops, test events, pilots and interviews) have indicated:
 - Cybersecurity is disconnected from combat missions and associated tasks
 - Current Risk Management Framework (RMF) analogous to Building Standards and Codes or Specification Compliance – necessary but not sufficient
 - DoD acquisition process structured around mission capability, requirements and cost trade space
 - Mission-Based Cybersecurity T&E requires:
 - Defined threat
 - **Well-defined, mission-oriented cybersecurity requirements**
 - Designed-in countermeasures that allow mission execution in contested cyber environments
 - Mission-centric test System of Systems (SoS) architectures that can support both interoperability and cybersecurity testing

**Cybersecurity cannot be tested into a system
It must be designed/built in from meaningful SoS-based requirements**

IDA | Motivation

- Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) FY 2011 Annual Report
 - *“Requirements for T&E in the defensive cyber domain for MDAP and MAIS programs are not fully understood”*
 - *“Thorough cyber testing needs to be incorporated into weapon system and operational support system development”*
- Defense Science Board – Resilient Military Systems and the Advanced Cyber Threat (2013)
 - *“Intelligence Community must be tasked with specific collection, analysis and reporting requirements on the cyber threat vectors, priorities and activities of U.S. adversaries”*
 - *“The Department must write achievable and testable requirements”*
- Director, Operational Test and Evaluation (DOT&E) FY 2014 Annual Report
 - FY2012 – FY2013: Operational testers found 400 cybersecurity vulnerabilities across 33 programs – *“89% could have been found earlier in system development”*

Increasing concern towards weapon system cybersecurity

IDA | Background

- Response 1: DoD Instruction 5000.02 “Operation of the Defense Acquisition System” – January 2015 requires acquisition programs to:
 - *“resource and ensure threat-appropriate Red Team/Penetration testing to emulate the threat of hostile penetration of program information systems in the operational environment;”*
 - *“develop a strategy and budget resources for cybersecurity testing....[including]...as much as possible, activities to test and evaluate a system in a mission environment with a representative cyber threat capability;”*
 - *“[use] threats ... [that are] ... selected [from] the best current information available from the intelligence community;”*
 - *“[as] a minimum [requirement], [assess] software in all systems ... for vulnerabilities....Higher criticality systems will also require penetration testing from an emulated threat in an operationally realistic environment during OT&E;” and,*
 - *“[develop] testable measures for cybersecurity and interoperability... [these measures should include those that allow the evaluation of the system’s] operational capability to protect, detect, react, and restore to sustain continuity of operation.”*
- Response 2: DoD Instruction 8500.01 “Cybersecurity” – March 2014 generally directs programs to:
 - *categorize system cybersecurity compromise mission impacts;*
 - *define system cybersecurity requirements or controls and associated evaluation and monitoring strategy based on an understanding of the threat environment;*
 - *translate system cybersecurity requirements into contractor specifications;*
 - *continually assess system performance relative to cybersecurity requirements; and*
 - *implement corrective actions to address cybersecurity performance shortfalls as they are identified.*
- Response 3: Cybersecurity Guidebooks
 - DoD Cybersecurity T&E Guidebook (July 2015)
 - DoD PM Cybersecurity Guidebook (September 2015)

Weapon systems must allow operators to “fight through” attacks

- DoD has also funded multiple pilot events, workshops and studies to inform acquisition program cybersecurity efforts, examples:
 1. Computer Network Defense Demonstration Effort (2008)
 2. Computer Network Defense Tabletop Exercise (2009)
 3. InterTEC Cyber Event (2011)
 4. DT&E Cyber Workshop (2012)
 5. Defense Science Board - Resilient Military Systems and the Advanced Cyber Threat (2012)
 6. InterTEC Cyber Event (2013)

Common Finding: Cybersecurity must be designed/built in from meaningful requirements

IDA | DoD Cybersecurity T&E Community Perspectives

- The vast majority of vulnerabilities found by threat team during operational test events are relatively basic (DoD Red Teams)
- Current cybersecurity metrics are generic
 - Metrics should focus on mission impact and provided in requirements documents
- Cybersecurity is often evaluated once important vulnerabilities are “baked in”
- Program offices rely on the Risk Management Framework
 - Necessary but not sufficient
- Common agreement: cyber attacks must be evaluated from a mission perspective
 - No generally accepted approach

Threat
Definition

Countermeasure
Development

Countermeasure
Effectiveness
Assessment

Current: Evaluate perimeter vulnerabilities

Recommended: And evaluate built-in countermeasure effectiveness

IDA | Taxonomy of Cyber Threats/Munitions

DOT&E FY15 Annual Report:

Most common vulnerabilities found and targeted by operational testers:

- Exposed or poorly-managed credentials
- Systems not configured to identified standards
- Systems not patched for known vulnerabilities
- System/network services and trust relationships that provide avenues for cyber compromise

Adapted from Defense Science Board

Tier	Description
1	Publicly available general cyber munitions that target well-known vulnerabilities and have very limited reconnaissance/intelligence-based targeting.
2	Custom-developed general cyber munitions that target publicly known vulnerabilities with very limited reconnaissance/intelligence-based targeting.
3	Specialized cyber munitions that exploit obscure vulnerabilities with considerable reconnaissance-based targeting.
4	Specialized cyber munitions intended to exploit vulnerabilities gleaned from advanced intelligence and testing activities.
5	Specialized cyber munitions intended to exploit vulnerabilities inserted into targeted systems during design, development, or production.
6	Full-spectrum cyber munitions (Tiers 1-5) that can be integrated into large-scale military, political, or economic campaigns

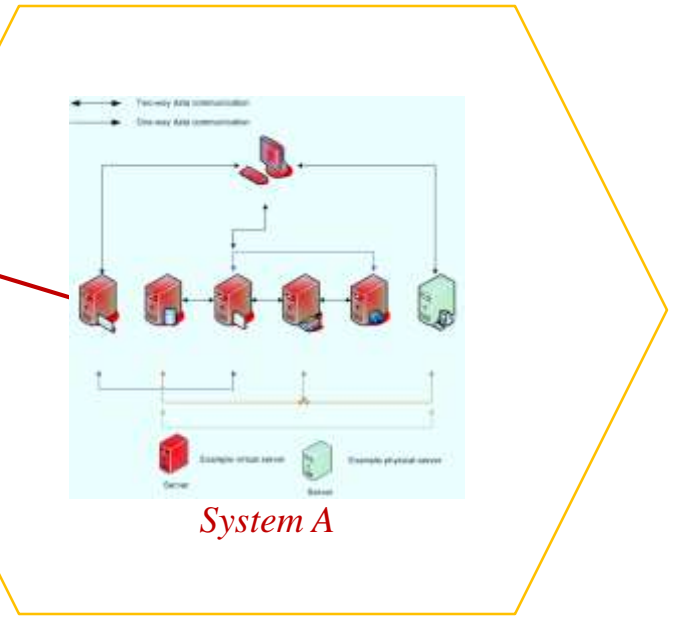
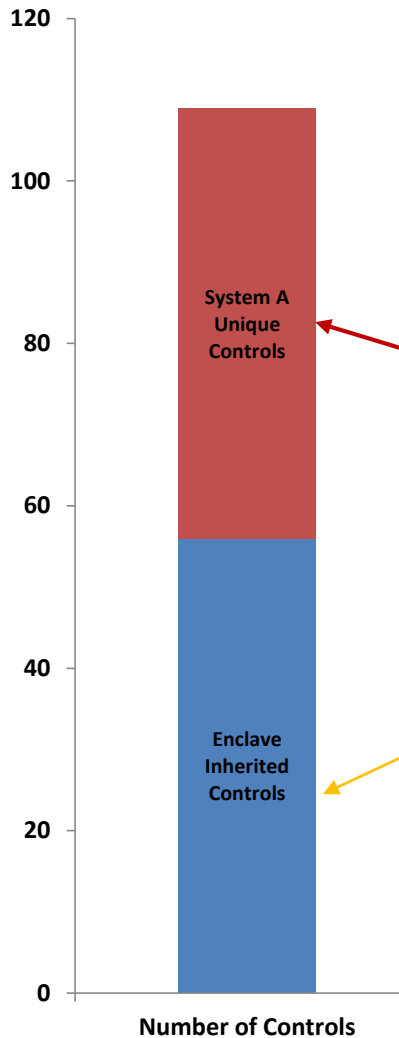
Current Approach: Identify Vulnerabilities

Recommended: And demonstrate mission impact

IDA | Control Implementation Realities

- Ideal Condition: System compliance with all relevant cybersecurity “building standards and codes”
- Event/Workshop Lessons Learned
 - Cybersecurity is part of the SoS mission capability tradespace
 - It is a “team sport” – systems can inherit key security features
 - Mission performance can override control compliance
 - Programs may not select all salient cybersecurity controls
 - Programs may not recognize which cybersecurity controls are the most relevant

Control Implementation Realities

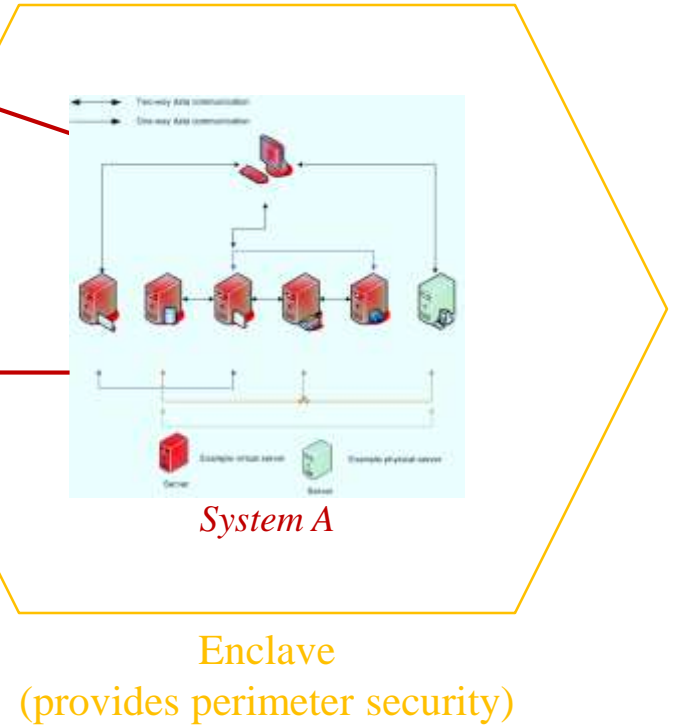
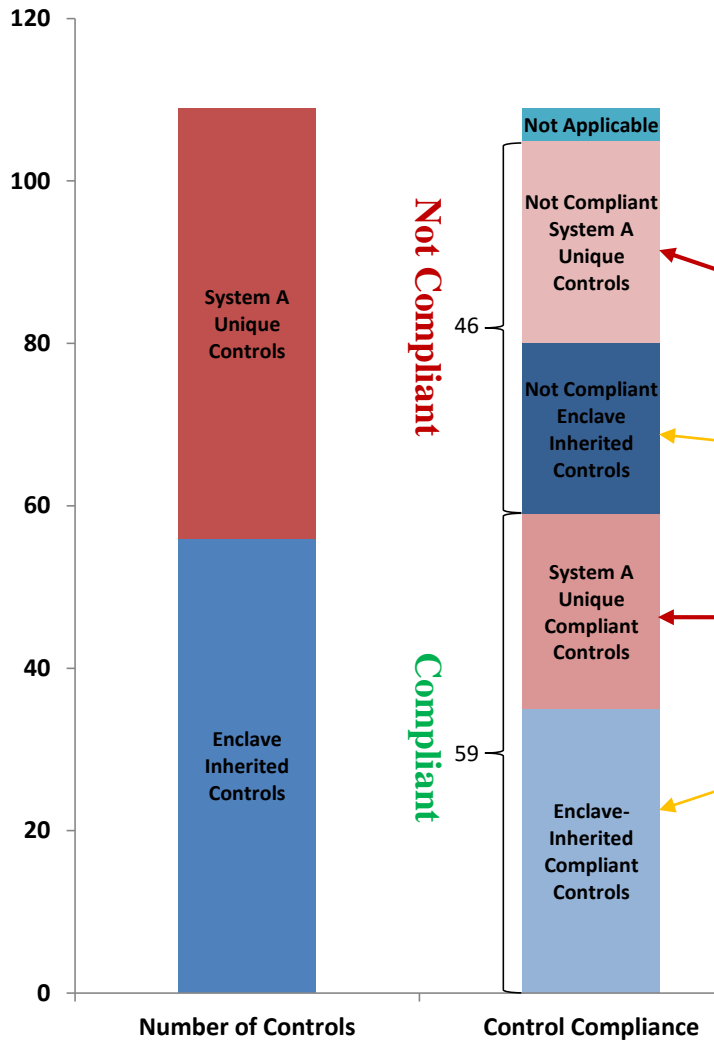


System A

Enclave
(provides perimeter security)

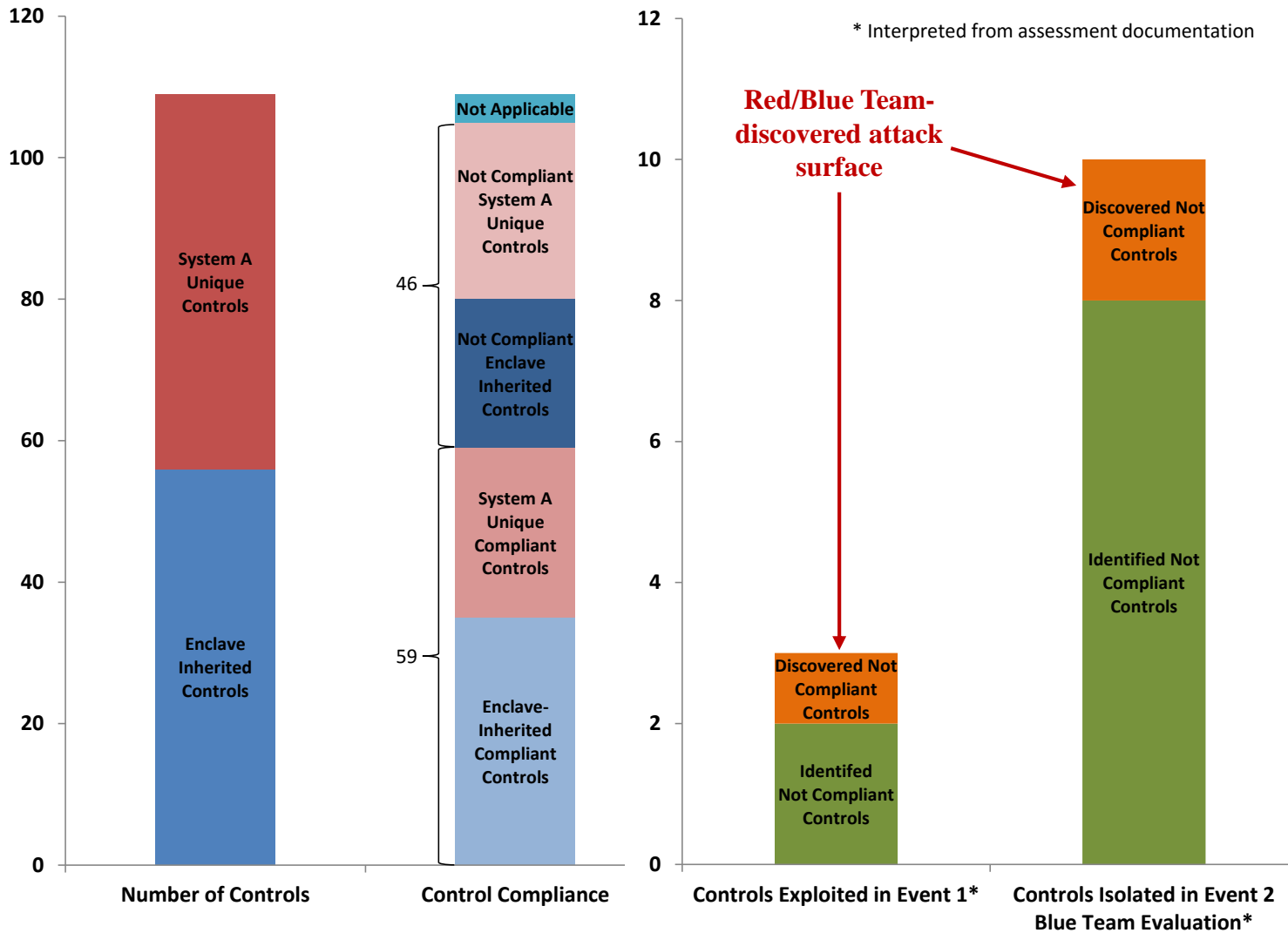
50% of System A controls reliant on enclave for compliance

Control Implementation Realities



Not Compliant Controls Result from Mission Considerations

Control Implementation Realities



Do these vulnerabilities really matter?

IDA | Cybersecurity Requirement Limitations

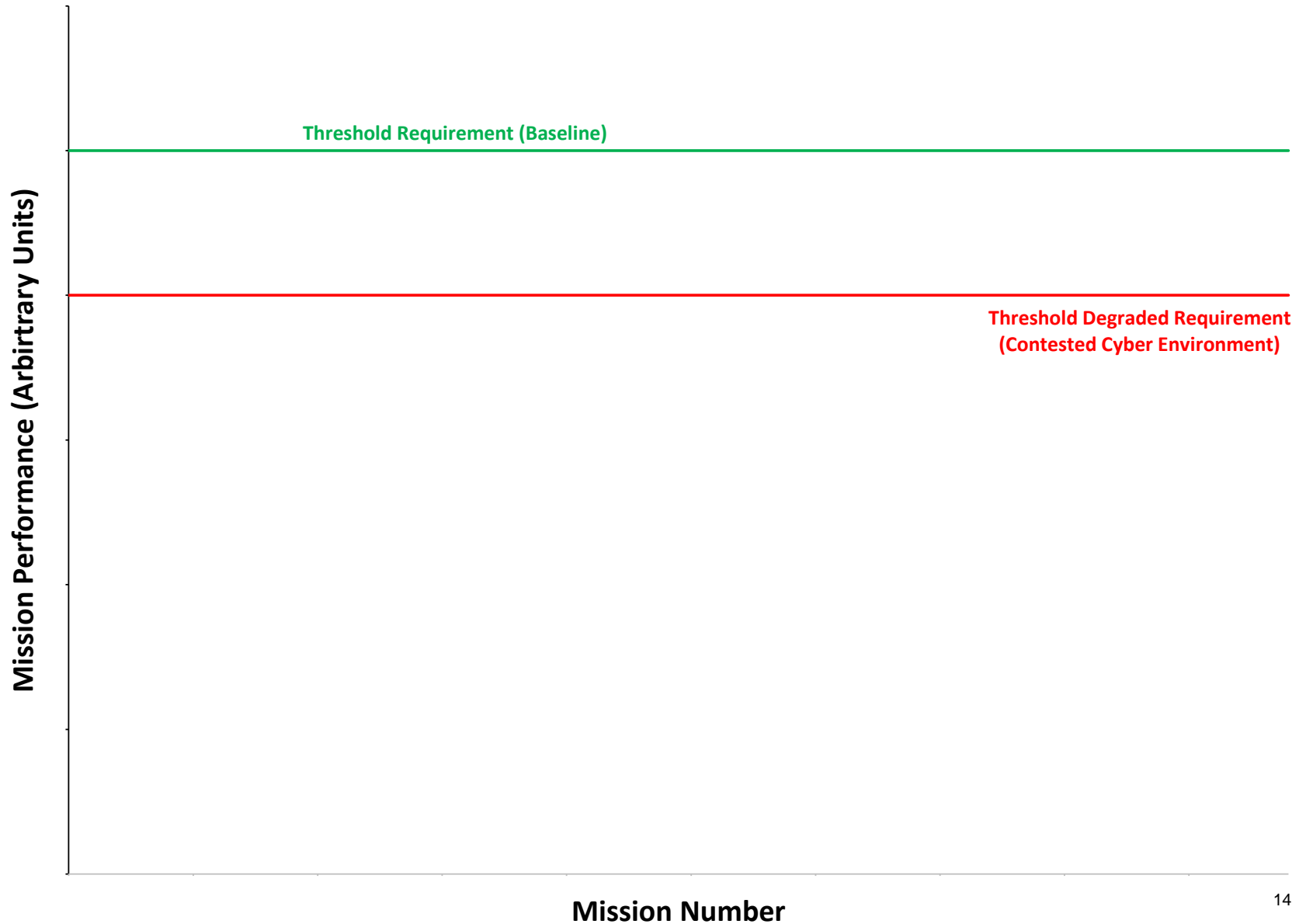
- February 12, 2015 Joint Capabilities and Integration Development System (JCIDS), mandates that programs implement a waivable System Survivability Key Performance Parameter (KPP)
 - Intended to ensure system performance in a contested cyber environment
 - Current guidance is to structure requirement around RMF controls
 - Insufficient granularity to support countermeasure development and mission-based performance evaluations
- Pilot events and workshops indicate that cybersecurity requirements should require acceptable mission performance in a contested cyber environment defined by specific threats
 - *The system under test shall be sufficiently resilient to cyber attacks and disruptions such that the capability is degraded by no more than 20% in the presence of DIA-validated cyber threats*

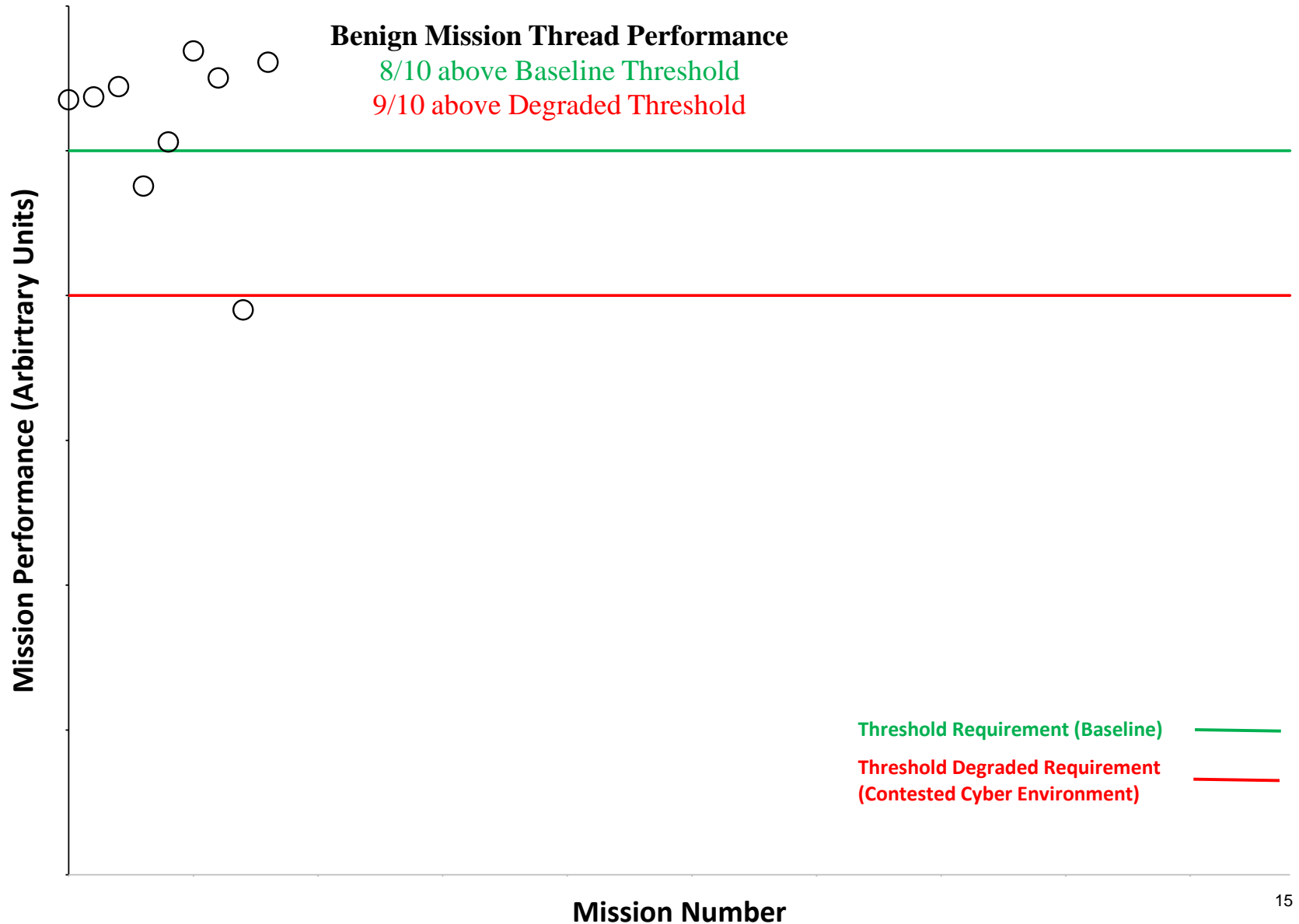
Cybersecurity must be designed/built in from meaningful requirements

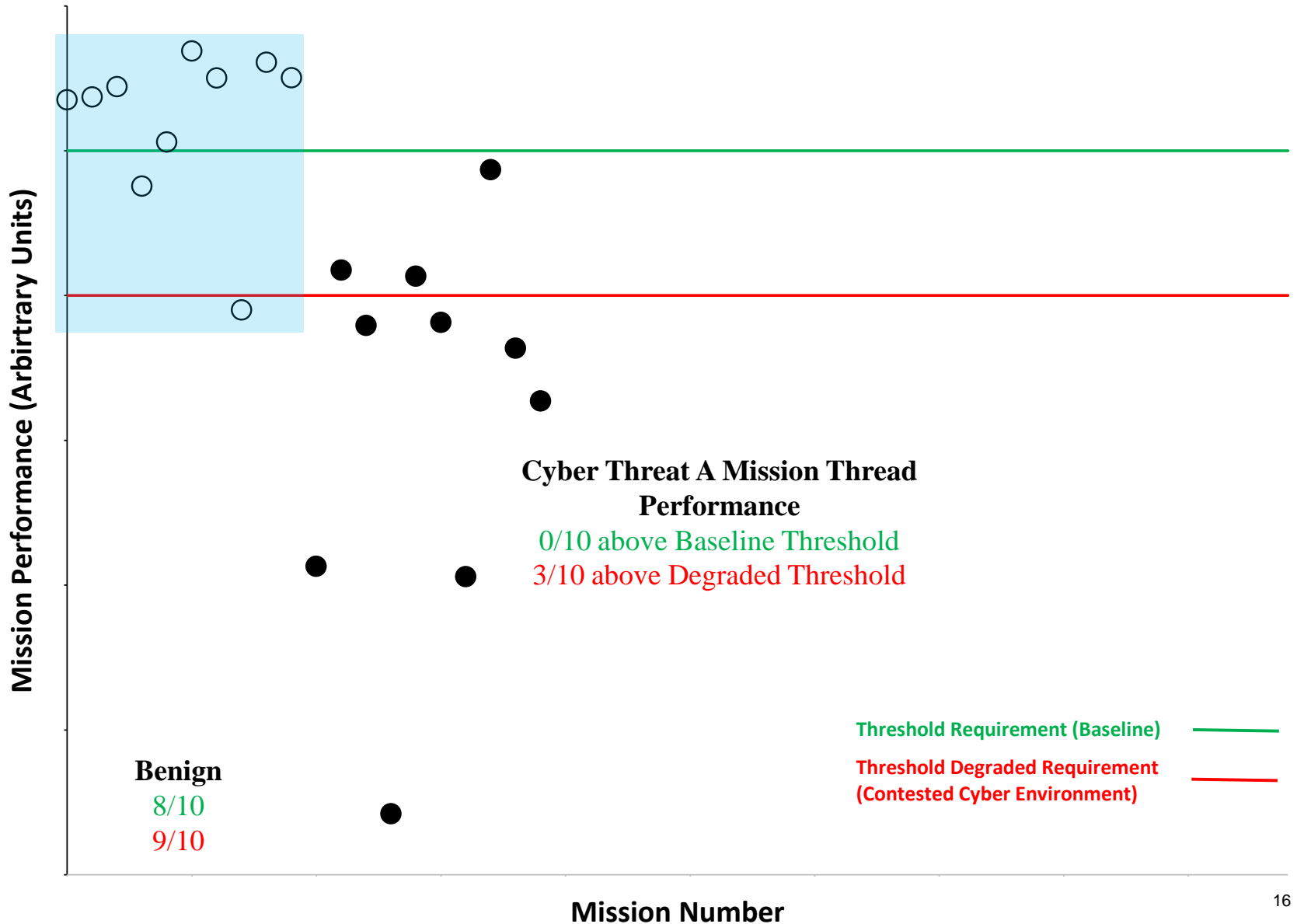
IDA | Mission-Based Cybersecurity T&E Prerequisites

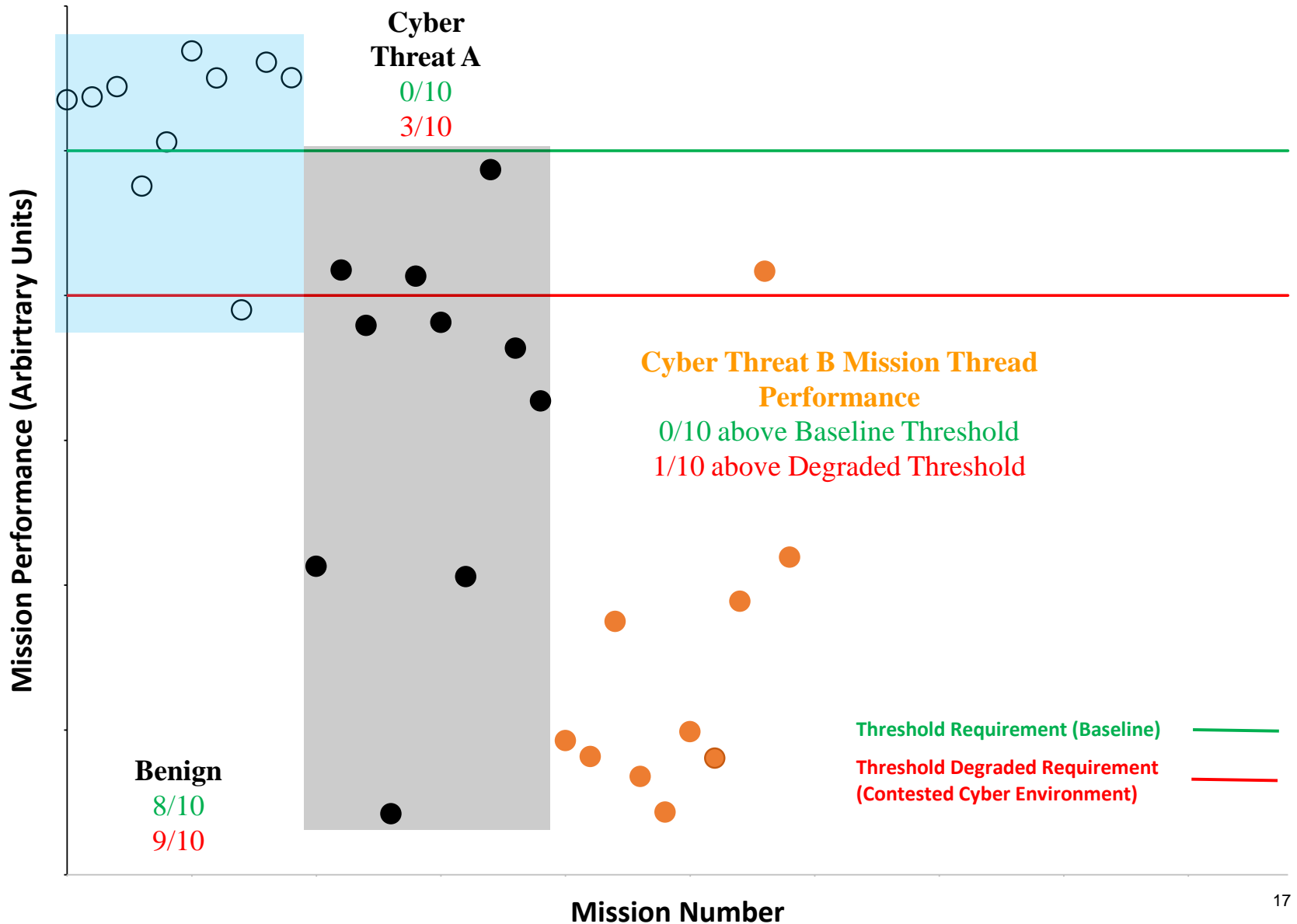
- Defined threat
 - Most relevant and critical threat exploits
 - Delivery mechanisms
 - Potential mission impacts
- Mission-Oriented Requirements
 - Analogy: Electronic Warfare
 - Move from perimeter defense to evaluating of threat mission impacts
- Designed-in countermeasures
 - Test objective is to verify that countermeasures support mission execution in contested cyber environments
- Mission-centric SoS test architectures
 - Must support both interoperability (baseline) and cybersecurity testing
 - Allow for complete corruption/destruction of key systems and reversion to original configuration

Validated LVC environments essential for all pre-requisites

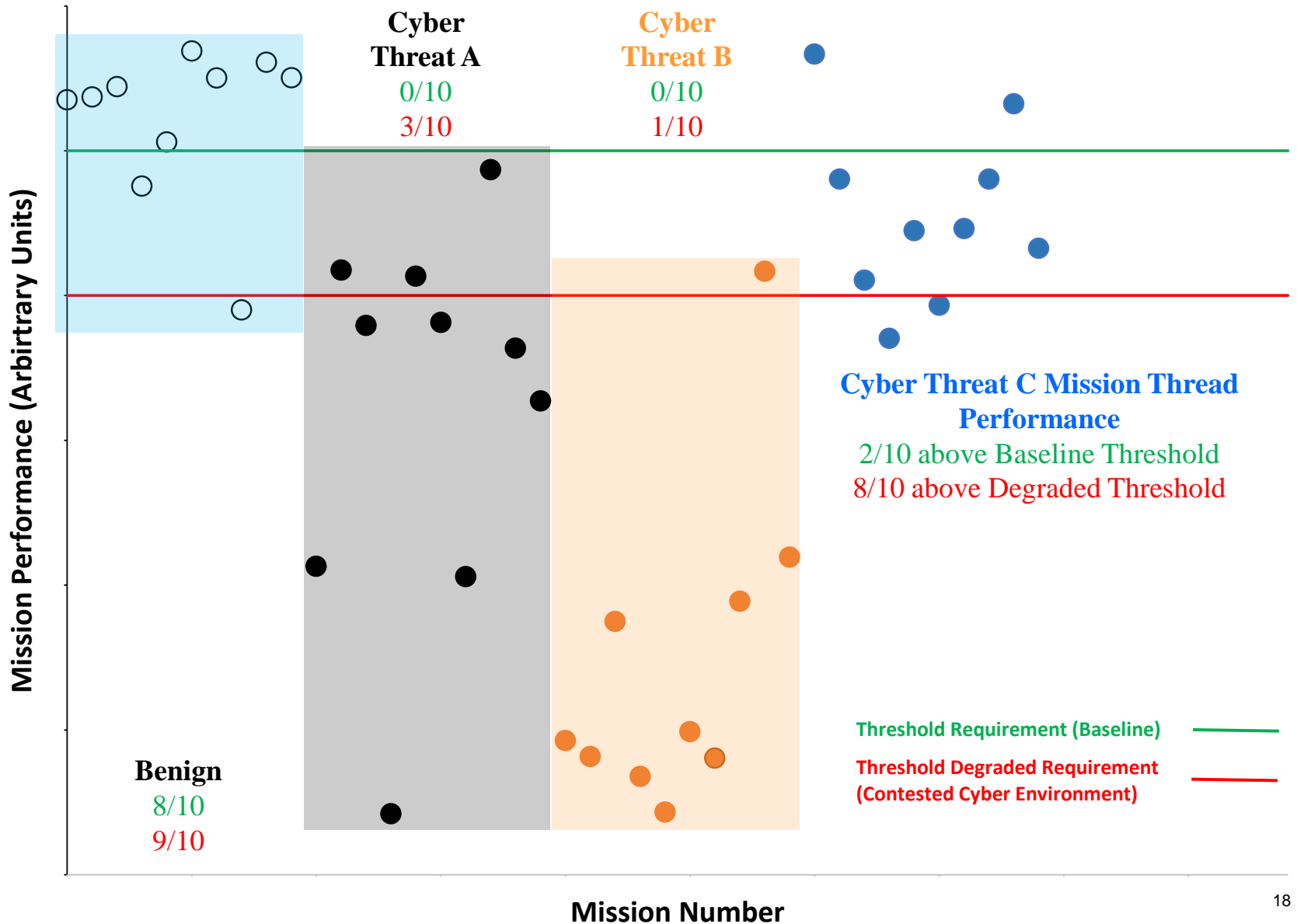




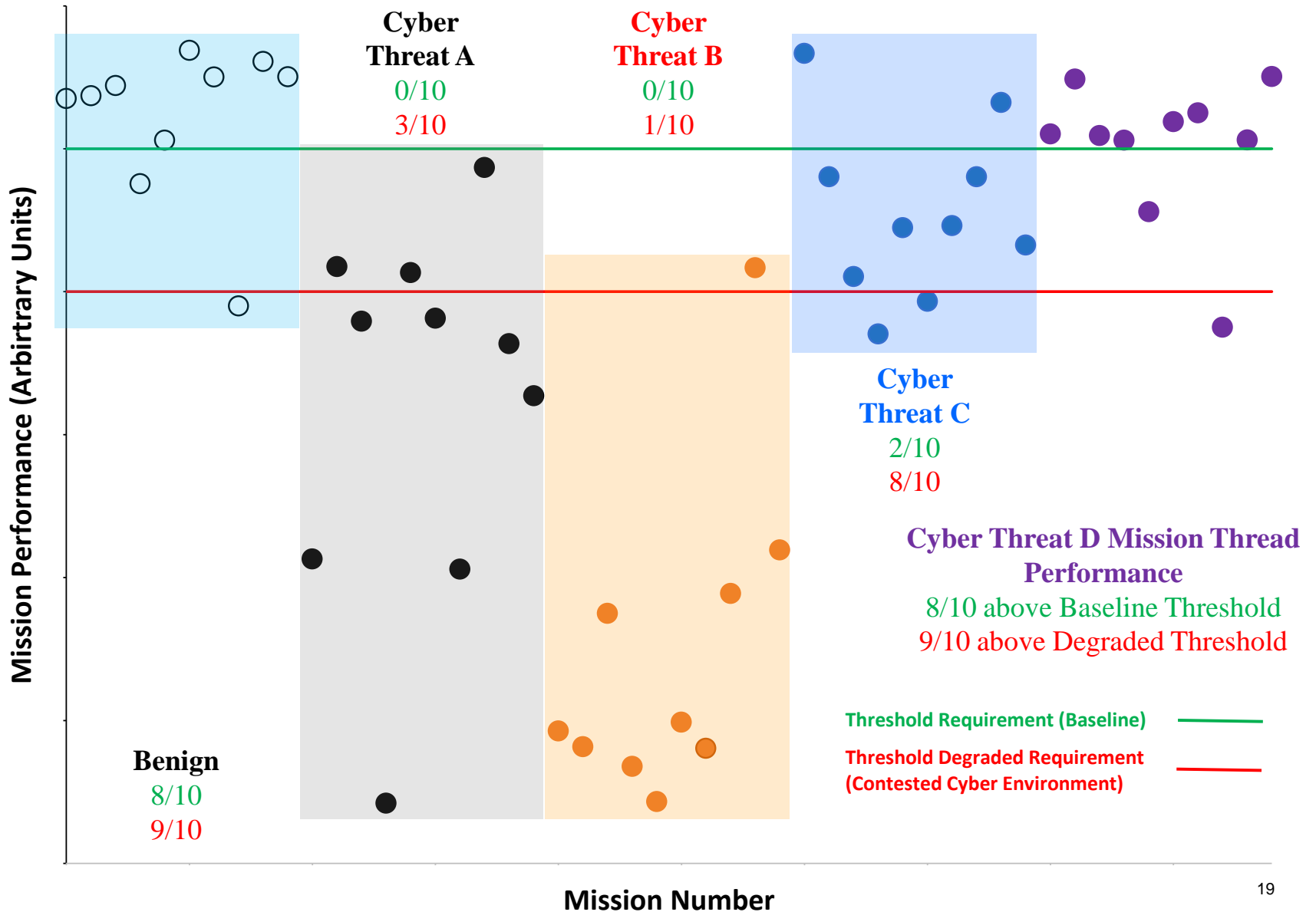




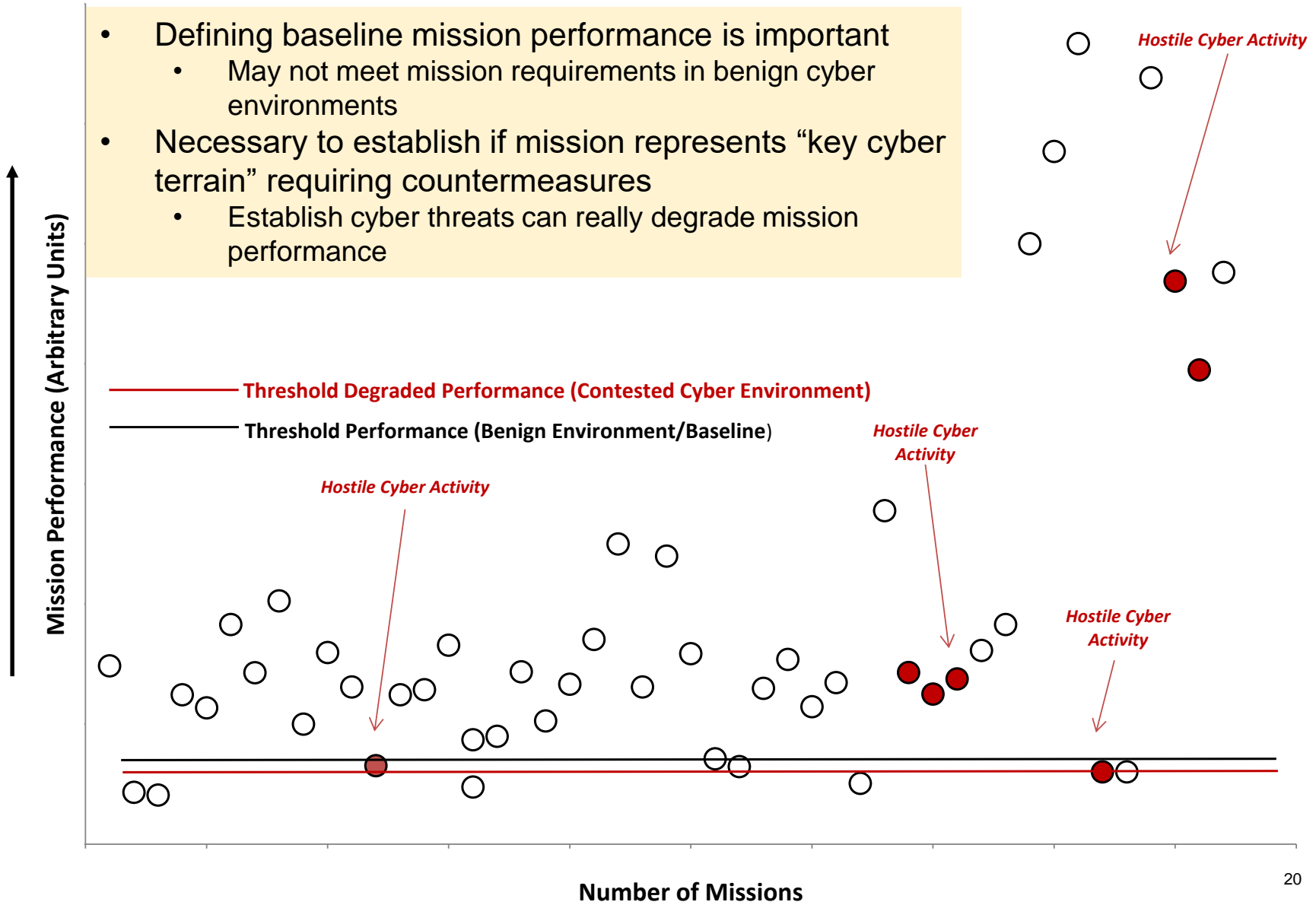
Mission-Based Cybersecurity T&E Illustration



Mission-Based Cybersecurity T&E Illustration



- Defining baseline mission performance is important
 - May not meet mission requirements in benign cyber environments
- Necessary to establish if mission represents “key cyber terrain” requiring countermeasures
 - Establish cyber threats can really degrade mission performance



- Past cybersecurity T&E experience (workshops, test events, pilots and interviews) have indicated:
 - Cybersecurity is disconnected from combat missions and associated tasks
 - Current Risk Management Framework (RMF) analogous to Building Standards and Codes or Specification Compliance – necessary but not sufficient
 - DoD acquisition process structured around mission capability, requirements and cost trade space
 - Mission-Based Cybersecurity T&E requires:
 - Defined threat
 - **Well-defined, mission-oriented cybersecurity requirements**
 - Designed-in countermeasures that allow mission execution in contested cyber environments
 - Mission-centric test System of Systems (SoS) architectures that can support both interoperability and cybersecurity testing

**Cybersecurity cannot be tested into a system
It must be designed/built in from meaningful SoS-based requirements**