RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ANF-F03

Achieving Defendable Architectures via Threat-Driven Methodologies

Michael Muckin
LM Fellow, Cyber Architect
Lockheed Martin

Scott Fitch
LM Fellow, Cyber Architect
Lockheed Martin

The system shall encrypt data at rest.

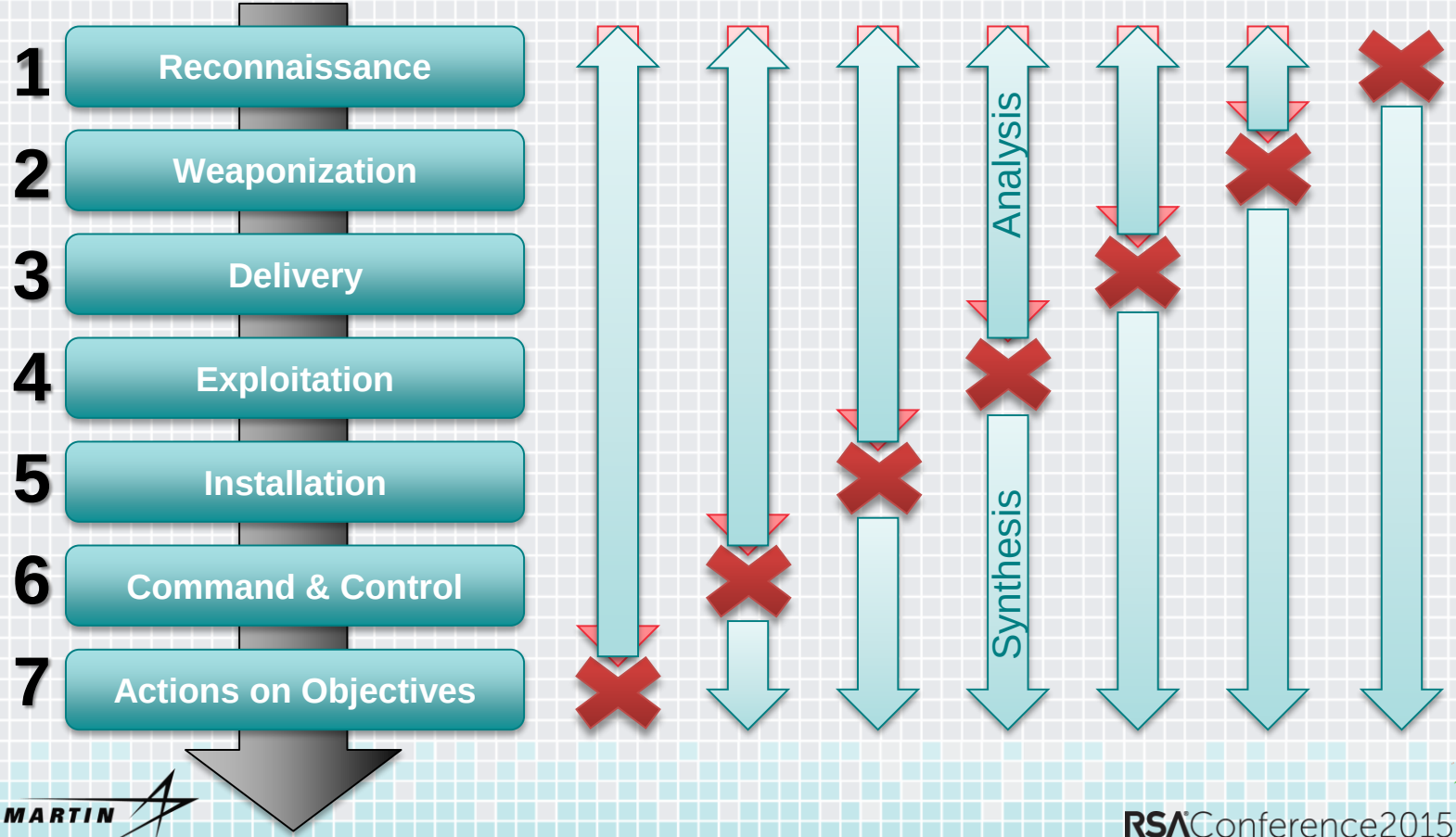
Why?

The Threat Driven Approach

System Threat Analysis

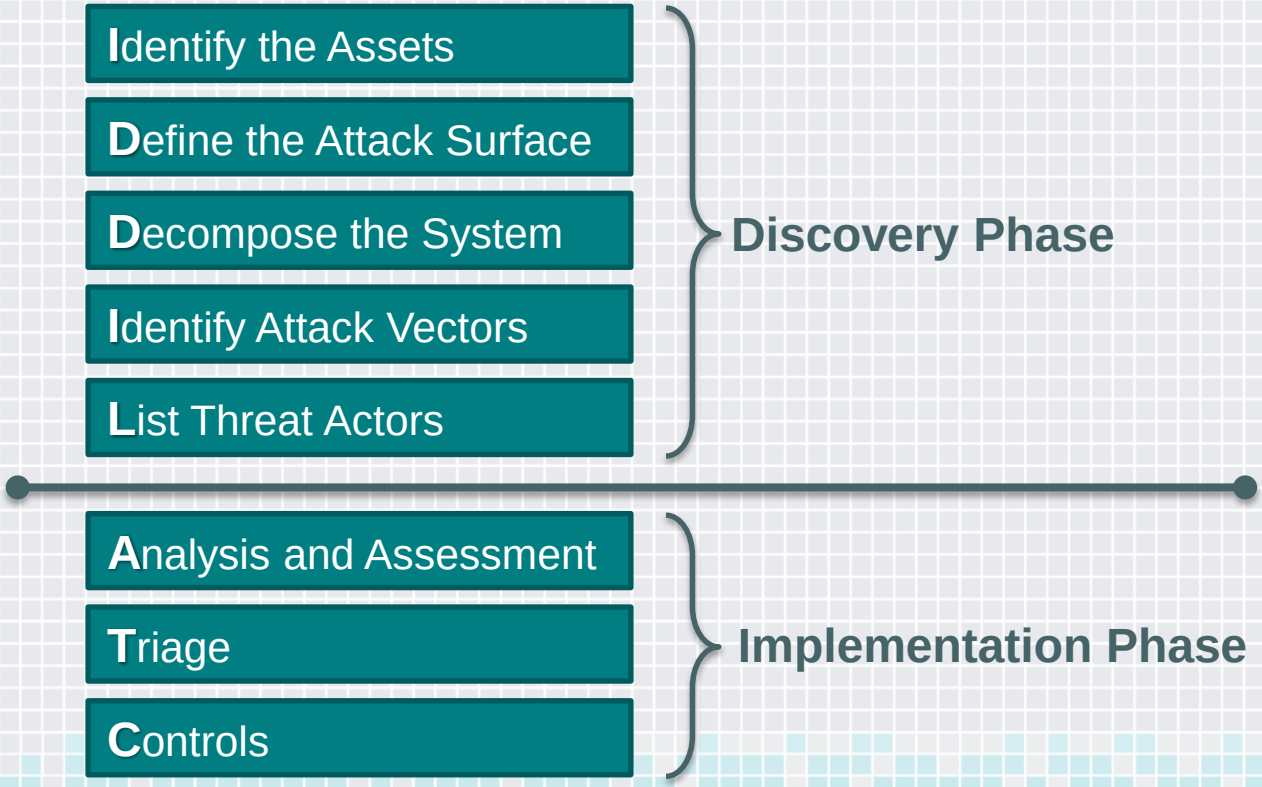
Threat Intelligence

Threat Intelligence

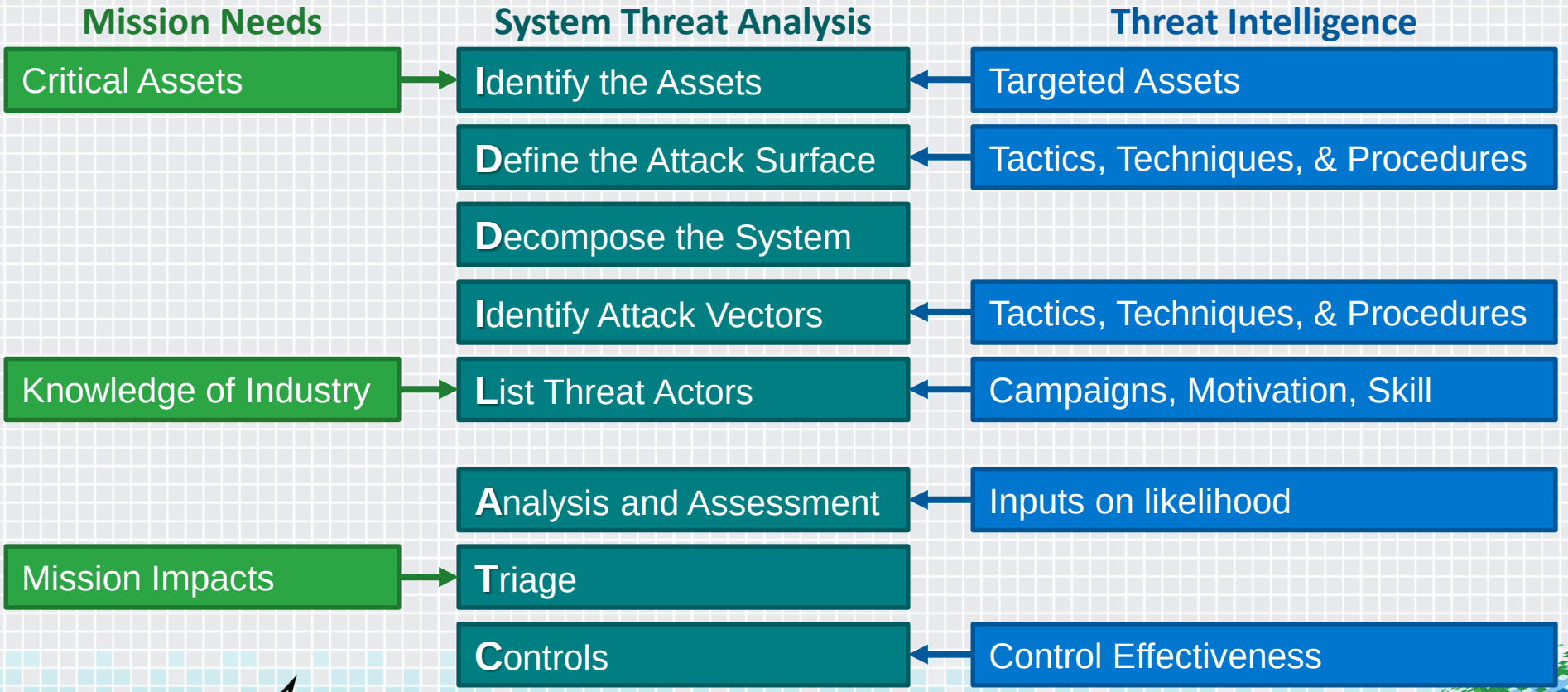


System Threat Analysis Methodology

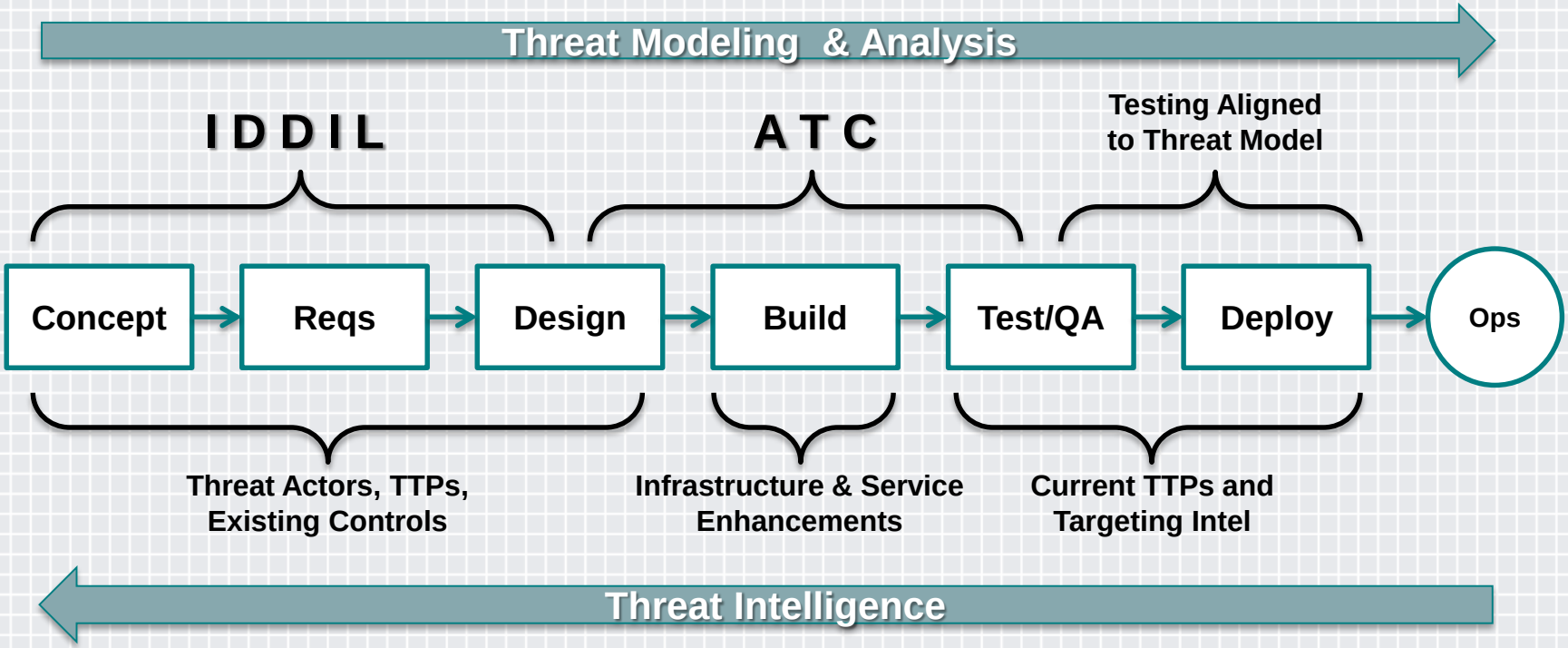
*There are no **IDDIL** (idle) Threats; they **ATC** (attack)*



System Threat Analysis Methodology

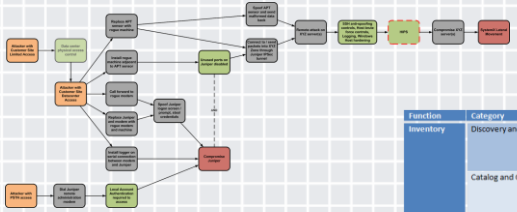


Threat Methodology Integration



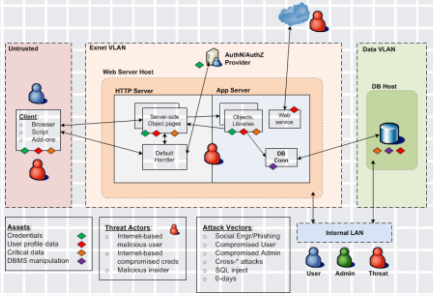
Threat Methodology Practices

- Threat Models
- Attack Trees
- Threat Profiles
- Cyber Kill Chain®
- Controls Effectiveness Matrix

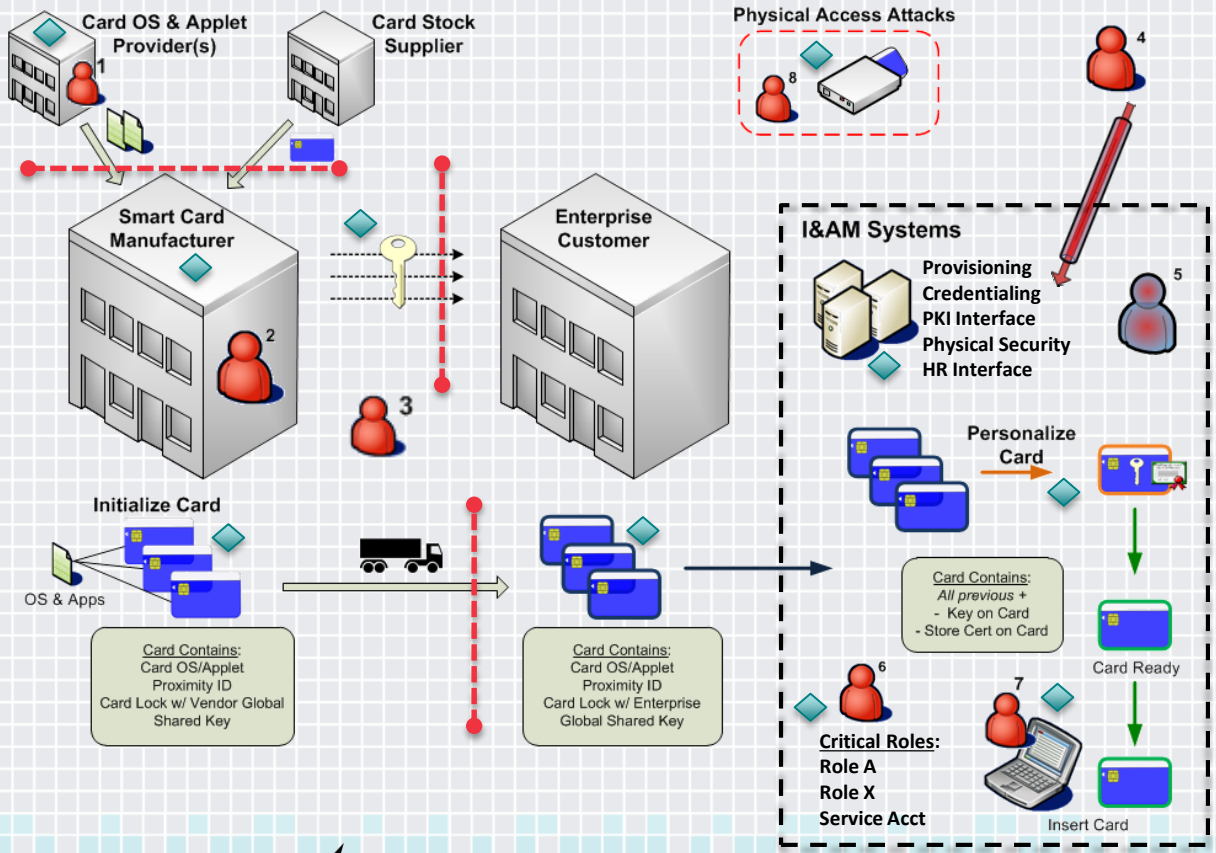


Function	Category	Implementation	Effectiveness
Inventory	Discovery and Reconcile	System X	●
		Control Q	○
		Process 1	○
	Catalog and Organize	System X	○
		Technology T	●
		System Z	○
		Process 2	●
	Rogue Detection	System M	○
		Technology R	△
	Decommission/Shutdown/Remove	Process 2	○
		System T	○

● Fully achieves control function's objective
◐ Partially achieves control function's objective
○ Does not achieve control function's objective
△ Control function capability gap



Case Study



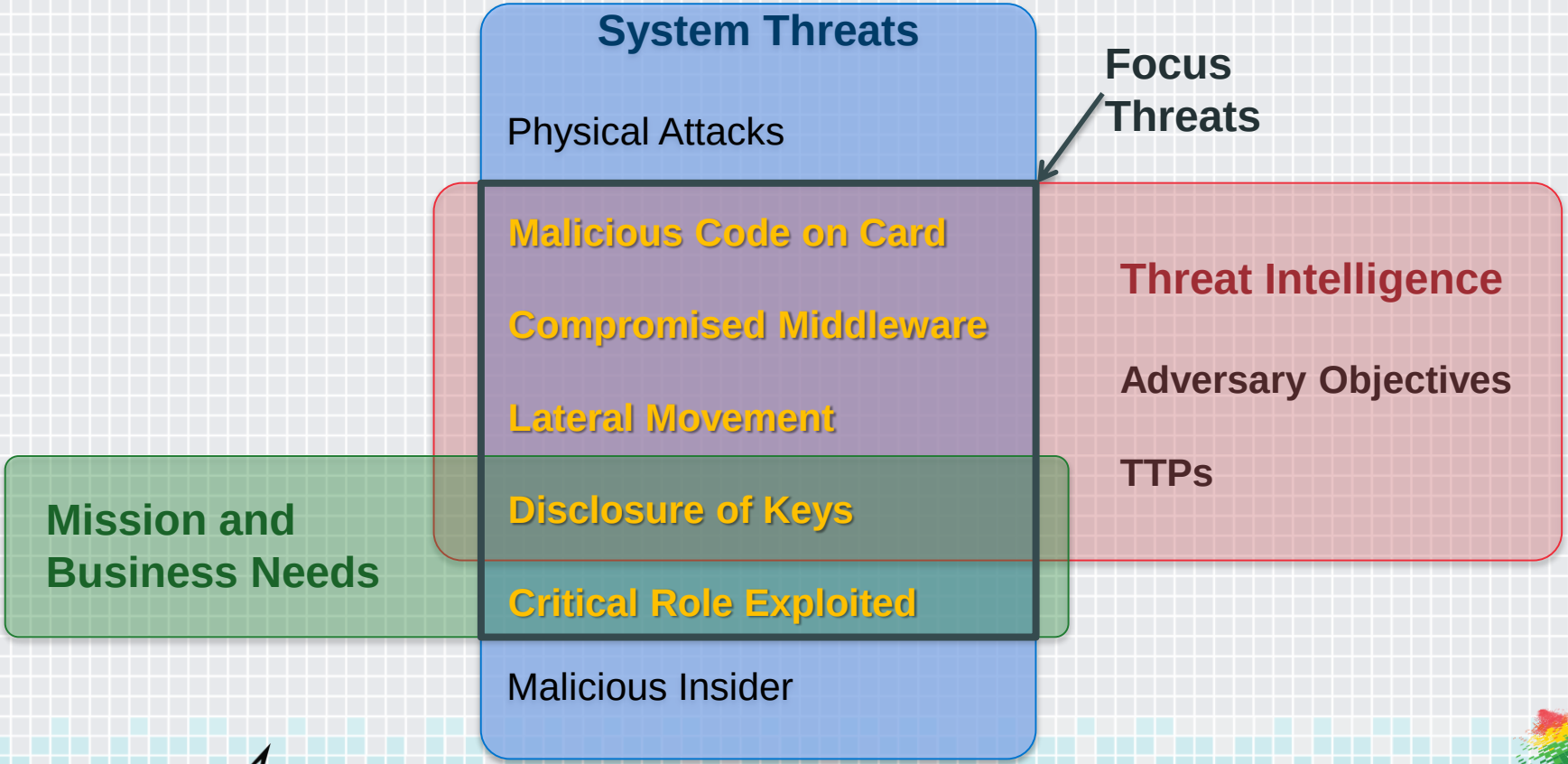
Assets:

- Smart Card
  - OS and Applet
  - ID codes
- Keys
- I&AM Systems
- Workstations
- Facilities

Threat Actors/Attack Vectors:

1. Man-in-Manufacturer (a)
2. Man-in-Manufacturer (b)
3. Interception of Master Key
4. Compromise of I&AM System
5. Malicious Insider
6. Compromise Critical Role
7. Compromise middleware
8. Physical attacks

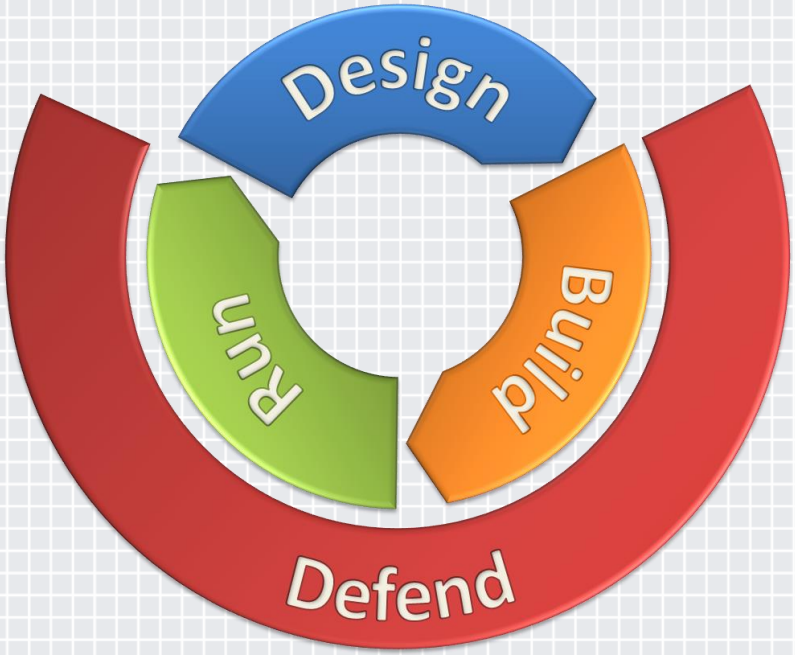
Determining Focus Threats



Addressing Threats

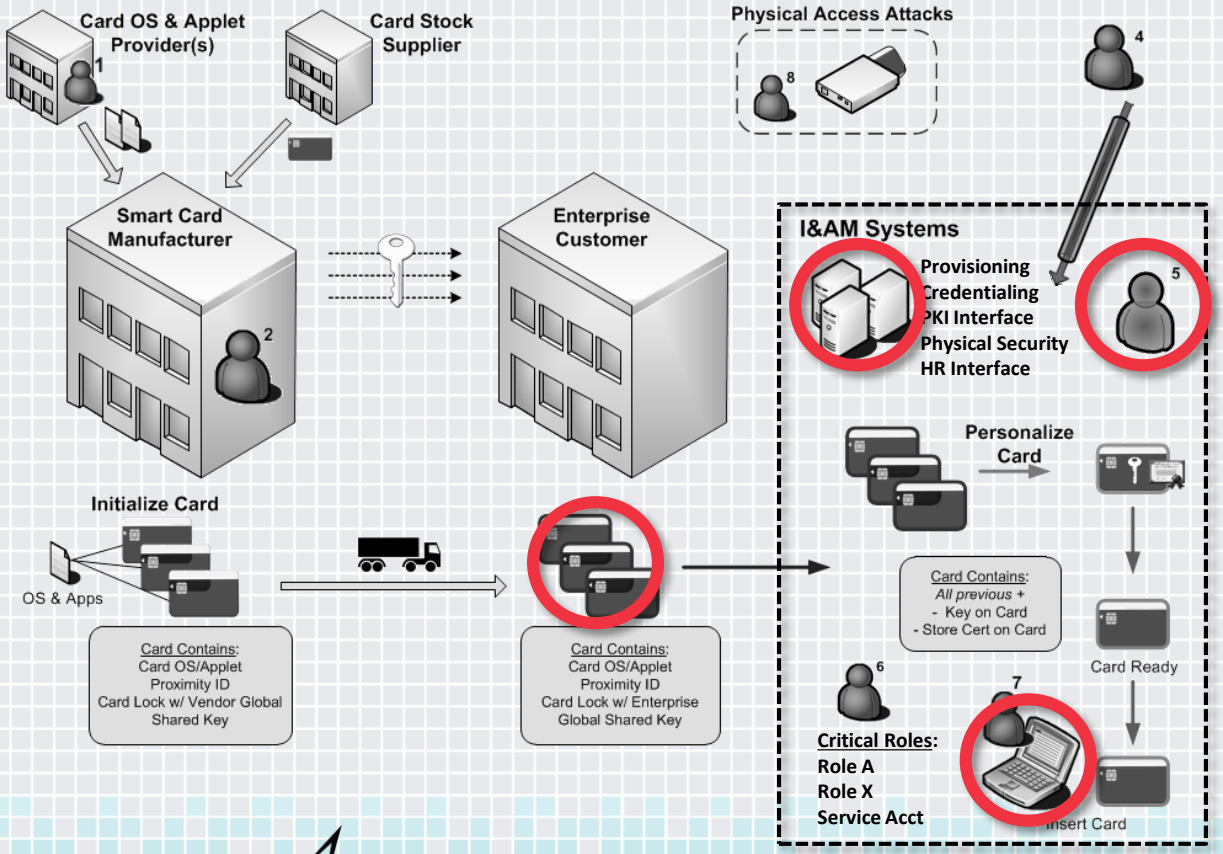
Asset/ Objective	Threat Types	Resultant Condition(s)	Attack Surface/ Vector	Controls
SmartCard OS	• Tampering • Disclosure • Elevation of Privilege • Lateral Movement	Dependent upon # of cards and level of access of user	• Card • Card OS code • APDU manipulation	• Code Audits • Contract language • Privileged account restrictions
Critical Role	• Spoofing • Repudiation • Elevation of Privilege • Lateral Movement	Unauthorized, privileged and potentially untraceable activity to critical infrastructure	• I&AM Systems • Specific interfaces • Specific services • Targeted user and service accounts	• Admin gateways • Multi-factor AuthN • Local accounts wherever possible • Privileged account password controls
Workstation	• Disclosure • Elevation of Privilege • Lateral Movement	Exfil data and/or credentials; Use machine as foothold for further actions	• SmartCard • Middleware • Memory	• System patching • HIPS • Memory protections • Penetration testing / assessment • Configuration controls

Defend the System as a Whole



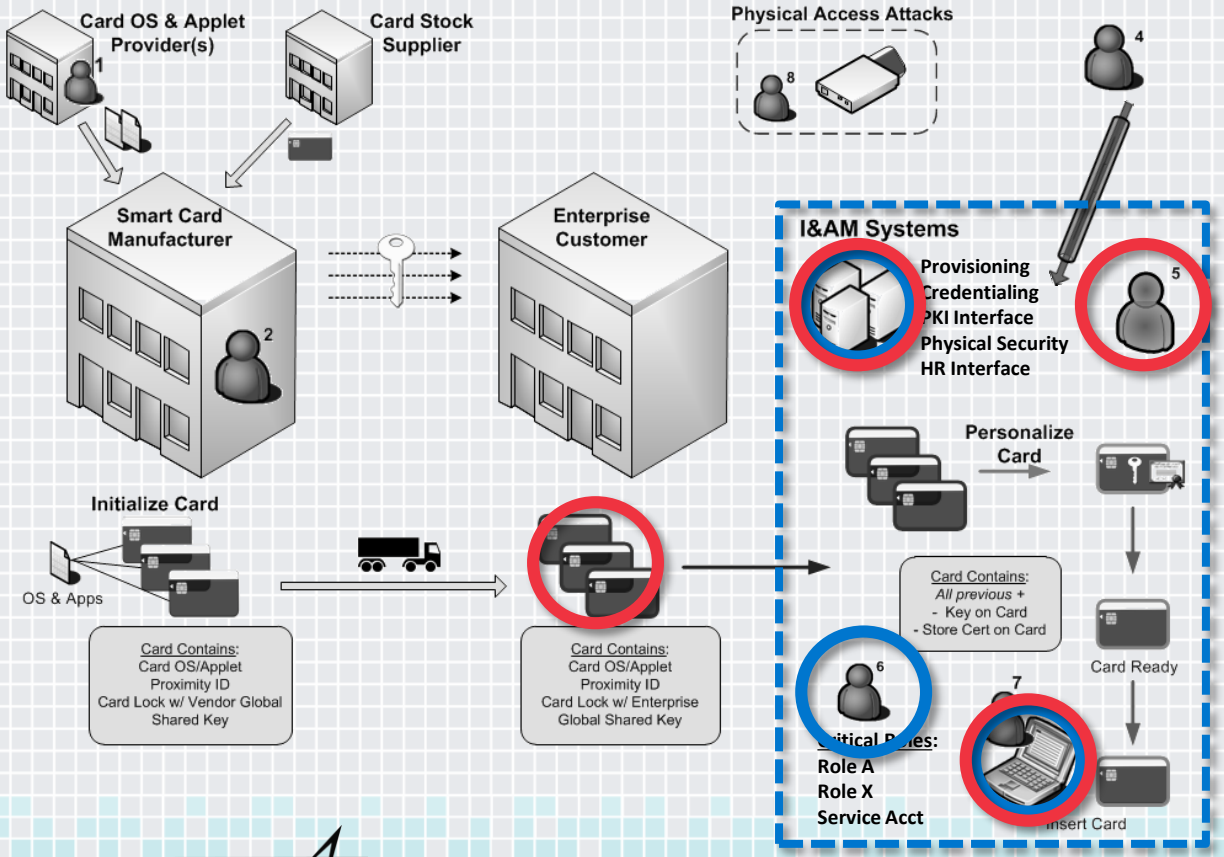
- **Visibility** into current and historical system activity
- **Manageability** of system configuration, updates, and control settings
- **Survivability** to deliver services through attack, detection, and recovery

Designing for Defense



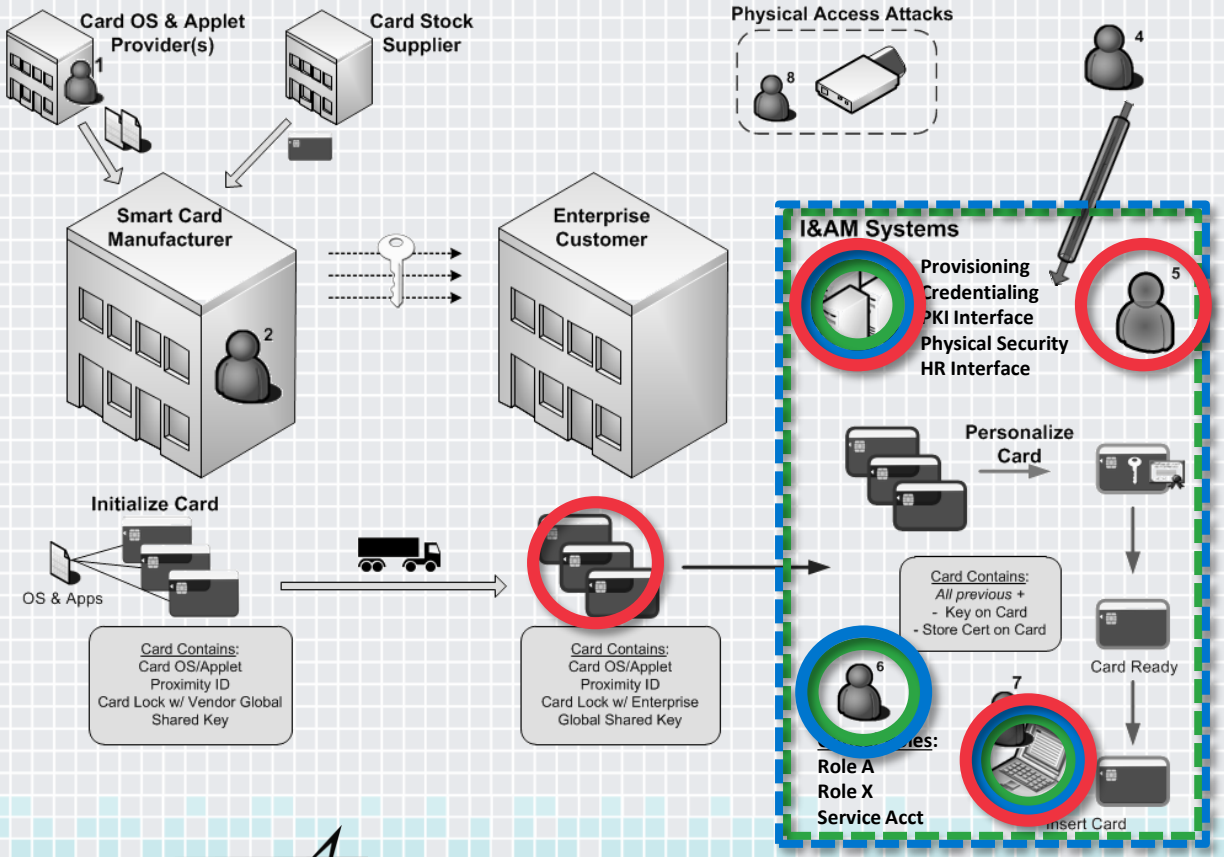
- **Visibility**
  - Server logging
  - Workstation logging
  - Network monitoring
  - Cardstock inventory
  - Insider detection

Designing for Defense



- **Visibility**
- **Manageability**
  - Rules based on new threat intel
  - Control points for tactical mitigations
  - System patching
  - Controlled admin access

Designing for Defense



- **Visibility**
- **Manageability**
- **Survivability**
  - System segmentation
  - Strong admin authentication
  - Separate card use from issuance
  - Assured system recovery

System Threat Analysis + **Threat Intelligence**

Use **IDDIL/ATC** to select **protection** and appropriate compensating controls
Design the system to be **defended** through **visibility**, **manageability**, and **survivability**

Building Defendable Architectures and Applying Threat-Driven Methodologies

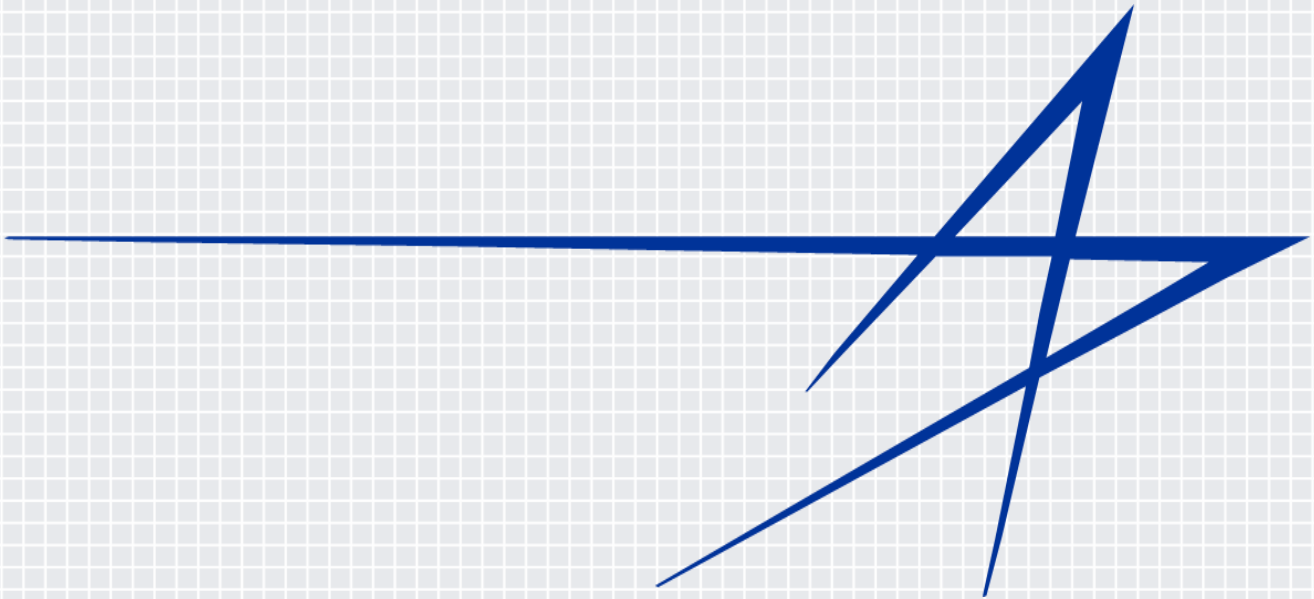
Start identifying your organization's critical **systems** and **assets**

For the next system you build, modify, operate, or assess

Use **IDDIL/ATC** to select **protection** and appropriate compensating controls
Design the system to be **defended** through **visibility**, **manageability**, and **survivability**

As your cyber defense capabilities mature

Integrate **threat intelligence** into design, development, and operations



http://lockheedmartin.com/cyber