Threat-based Cybersecurity

# DoDCAR

DoD Cybersecurity Analysis & Review

Office of the National Manager for NSS

NATIONAL SECURITY AGENCY CYBERSECURITY

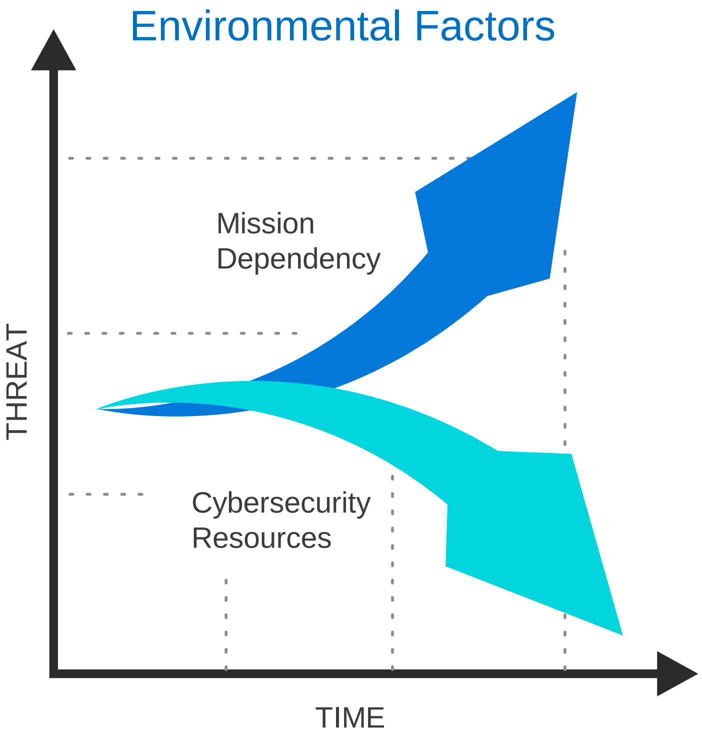
# Problem Space

## Cyber Threat and Mission Dependency

***Cyber threat increases exponentially as our reliance on IT and Cyberspace increases to keep pace with global mission demands***

## Cybersecurity Resources

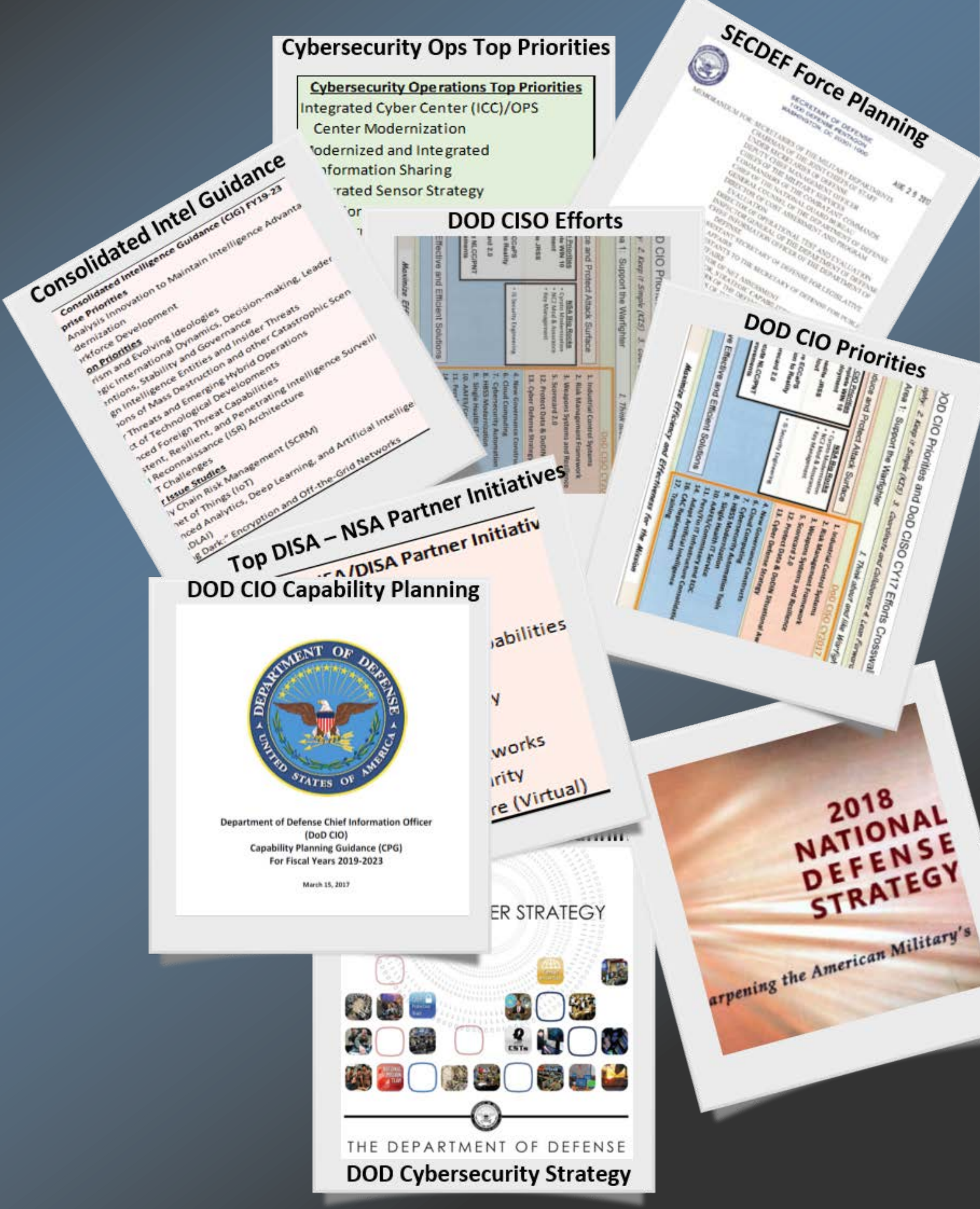
***The USG resources to include expertise and expenditures are fail in comparison to what is required to ensure mission dependency in the face of a capable adversary***



# Strategic Direction

To support the Defense Department's missions in cyberspace, endless guidance is published to bolster collective cybersecurity practices and protect our national interests. For example, the DoD cooperates with USG departments and agencies, the private sector, and foreign allies to share information, build alliances, and promote accountability.

**Are we really giving clear guidance?**



Cybersecurity Ops Top Priorities

Cybersecurity Operations Top Priorities

Integrated Cyber Center (ICC)/OPS Center Modernization

SECDEF Force Planning

Consolidated Intel Guidance

DOD CISO Efforts

DOD CIO Priorities

Top DISA – NSA Partner Initiatives

DOD CIO Capability Planning

Department of Defense Chief Information Officer (DoD CIO) Capability Planning Guidance (CPG) For Fiscal Years 2019-2023

March 15, 2017

2018 NATIONAL DEFENSE STRATEGY

Sharpening the American Military's

THE DEPARTMENT OF DEFENSE

DOD Cybersecurity Strategy

# Against the adversary, perspective is EVERYTHING.

5 Executives

4 Operations

3 Incident Responders

2 System Admins

1 Architects & Engineers

# Technical Cyber Threat Framework

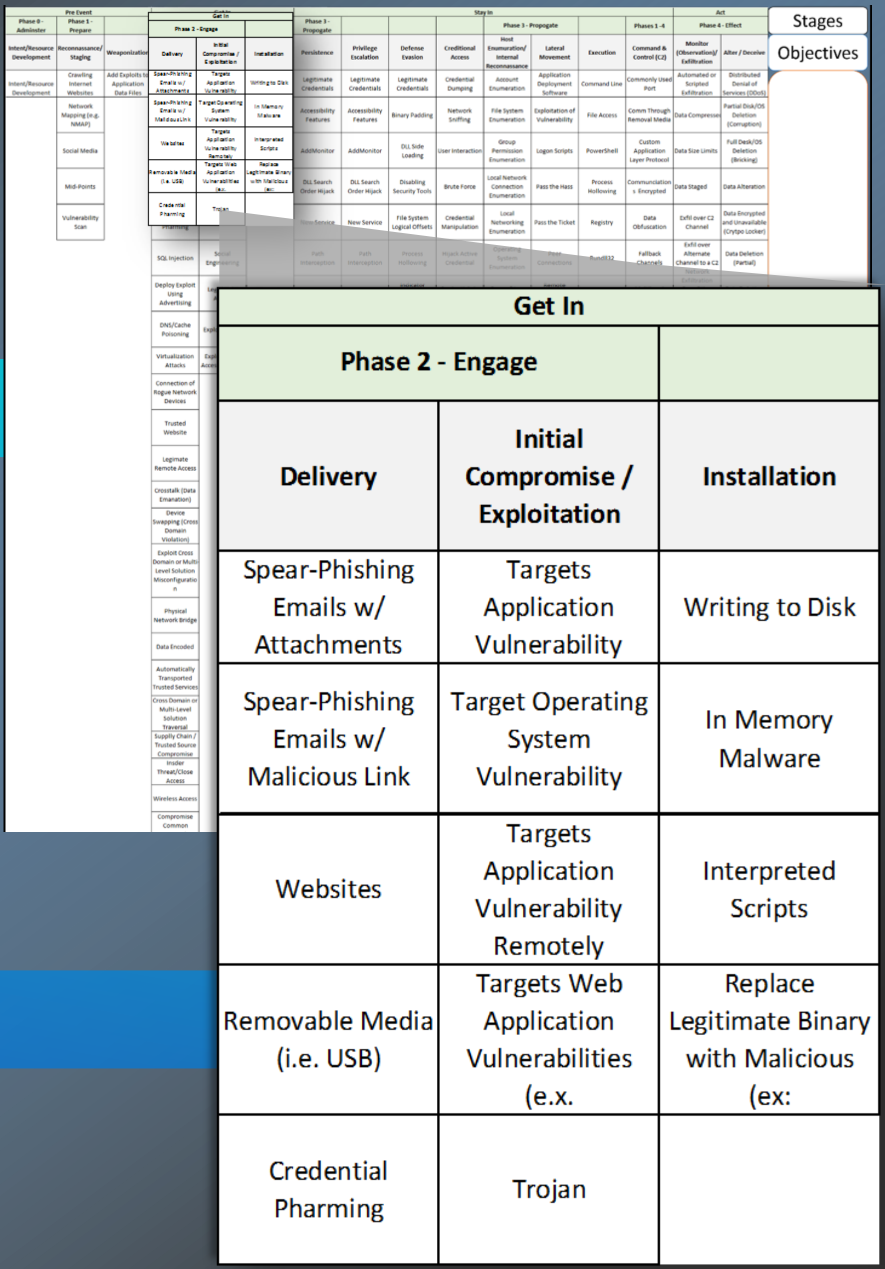
Public dissemination of the lexicon allows for collaboration with whole-of-community.

## Characterizes adversary activity

*NSA/CSS Technical Cyber Threat Framework v1 can be used as reference for US Government Collaboration with partners and stakeholders in discussing adversary activities through the adversary lifecycle.*

## Five appendices are included:

1. *One page view of the Threat Framework*
2. *Stages and Objectives*
3. *Action Definitions*
4. *How terms relate to various stages and objectives*
5. *References and License Information*



Stages

Objectives

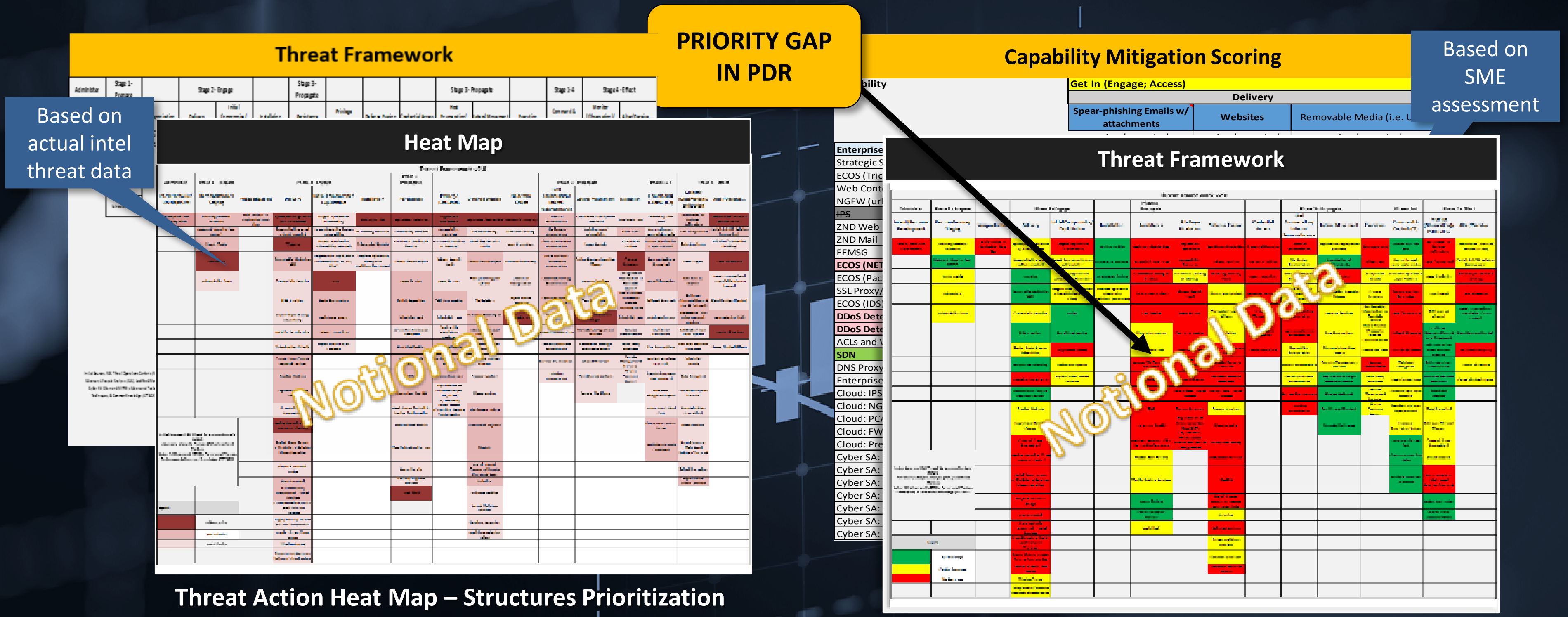
| Pre Event | | | Get In | | | Stay In | | | | | | | | Act | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phase 0 - Administer | Phase 1 - Prepare | | Phase 2 - Engage | | | Phase 3 - Propogate | | | | Phase 3 - Propogate | | | Phases 1 -4 | Phase 4 - Effect | |
| Intent/Resource Development | Reconnassance/ Staging | Weaponization | Delivery | Initial Compromise / Exploitation | Installation | Persistence | Privilege Escalation | Defense Evasion | Creditional Access | Host Enumuration/ Internal Reconnassance | Lateral Movement | Execution | Command & Control (C2) | Monitor (Observation)/ Exfiltration | Alter / Deceive |
| Intent/Resource Development | Crawling Internet Websites | Add Exploits to Application Data Files | Spear-Phishing Emails w/ Attachments | Targets Application Vulnerability | Writing to Disk | Legitimate Credentials | Legitimate Credentials | Legitimate Credentials | Credential Dumping | Account Enumeration | Application Deployment Software | Command Line | Commonly Used Port | Automated or Scripted Exfiltration | Distributed Denial of Services (DDoS) |
| | Network Mapping (e.g. NMAP) | | Spear-Phishing Emails w/ Malicious Link | Target Operating System Vulnerability | In Memory Malware | Accessibility Features | Accessibility Features | Binary Padding | Network Sniffing | File System Enumeration | Exploitation of Vulnerability | File Access | Comm Through Removal Media | Data Compresses | Partial Disk/OS Deletion (Corruption) |
| | Social Media | | Websites | Targets Application Vulnerability Remotely | Interpreted Scripts | AddMonitor | AddMonitor | DLL Side Loading | User Interaction | Group Permission Enumeration | Logon Scripts | PowerShell | Custom Application Layer Protocol | Data Size Limits | Full Desk/OS Deletion (Bricking) |
| | Mid-Points | | Removable Media (i.e. USB) | Targets Web Application Vulnerabilities (e.x. | Replace Legitimate Binary with Malicious (ex: | DLL Search Order Hijack | DLL Search Order Hijack | Disabling Security Tools | Brute Force | Local Network Connection Enumeration | Pass the Hass | Process Hollowing | Communciation s Encrypted | Data Staged | Data Alteration |
| | Vulnerability Scan | | Credential Pharming | Trojan | | New Service | New Service | File System Logical Offsets | Credential Manipulation | Local Networking Enumeration | Pass the Ticket | Registry | Data Obfuscation | Exfil over C2 Channel | Data Encrypted and Unavailable (Crytpo Locker) |
| | | | SQL Injection | Social Engineering | | Path Interception | Path Interception | Process Hollowing | Hijack Active Credential | Operating System Enumeration | Peer Connections | Rundll32 | Fallback Channels | Exfil over Alternate Channel to a C2 | Data Deletion (Partial) |
| | | | Deploy Exploit Using Advertising | | | | | | | | | | | Network Exfiltration | |
| | | | DNS/Cache Poisoning | | | | | | | | | | | | |
| | | | Virtualization Attacks | | | | | | | | | | | | |
| | | | Connection of Rogue Network Devices | | | | | | | | | | | | |
| | | | Trusted Website | | | | | | | | | | | | |
| | | | Legimate Remote Access | | | | | | | | | | | | |
| | | | Crosstalk (Data Emanation) | | | | | | | | | | | | |
| | | | Device Swapping (Cross Domain Violation) | | | | | | | | | | | | |
| | | | Exploit Cross Domain or Multi-Level Solution Misconfiguration | | | | | | | | | | | | |
| | | | Physical Network Bridge | | | | | | | | | | | | |
| | | | Data Encoded | | | | | | | | | | | | |
| | | | Automatically Transported Trusted Services | | | | | | | | | | | | |
| | | | Cross Domain or Multi-Level Solution Traversal | | | | | | | | | | | | |
| | | | Suppily Chain / Trusted Source Compromise | | | | | | | | | | | | |
| | | | Insider Threat/Close Access | | | | | | | | | | | | |
| | | | Wireless Access | | | | | | | | | | | | |
| | | | Compromise Common | | | | | | | | | | | | |

| Get In | | |
|---|---|---|
| Phase 2 - Engage | | |
| Delivery | Initial Compromise / Exploitation | Installation |
| Spear-Phishing Emails w/ Attachments | Targets Application Vulnerability | Writing to Disk |
| Spear-Phishing Emails w/ Malicious Link | Target Operating System Vulnerability | In Memory Malware |
| Websites | Targets Application Vulnerability Remotely | Interpreted Scripts |
| Removable Media (i.e. USB) | Targets Web Application Vulnerabilities (e.x. | Replace Legitimate Binary with Malicious (ex: |
| Credential Pharming | Trojan | |

# DODCAR

## THREAT COVERAGE, PRIORITIZATION & GAP IDENTIFICATION

( NOTIONAL DATA )



Threat Action Heat Map – Structures Prioritization

Security Capability Coverage – effectiveness for PDR

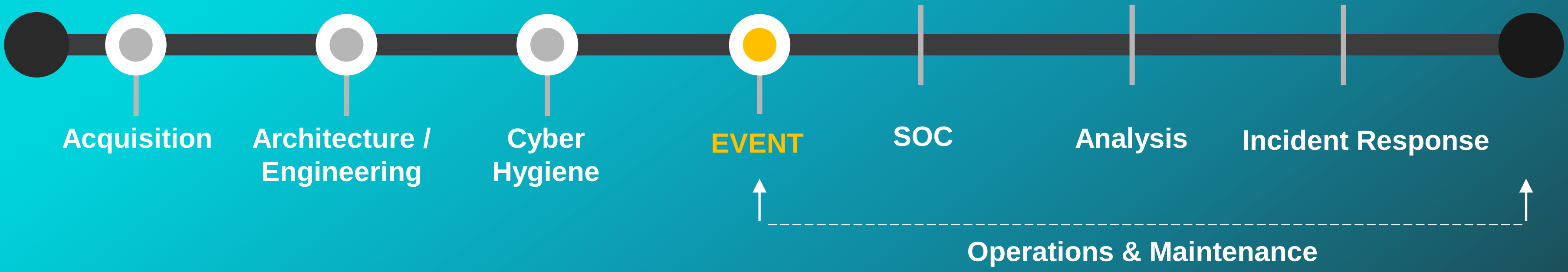
Threat Framework

Threat Action Heat Map

Capability Mitigation Scoring

Security Capability Coverage

# DoDCAR Feedback Loop



Acquisition

Architecture / Engineering

Cyber Hygiene

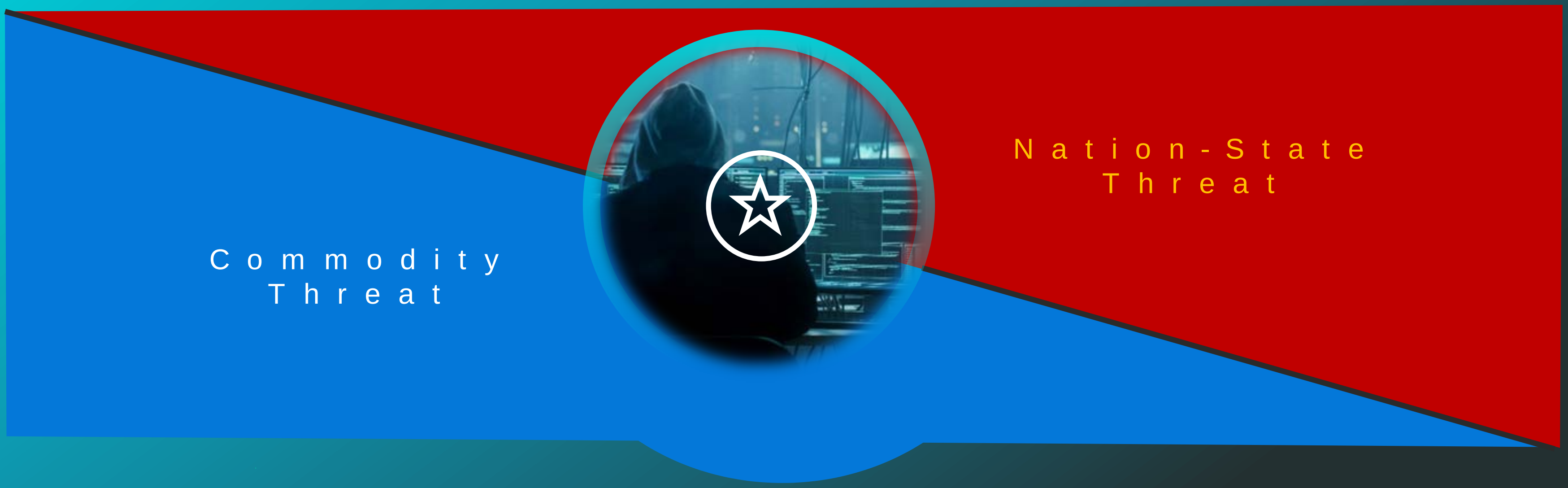
EVENT

SOC

Analysis

Incident Response

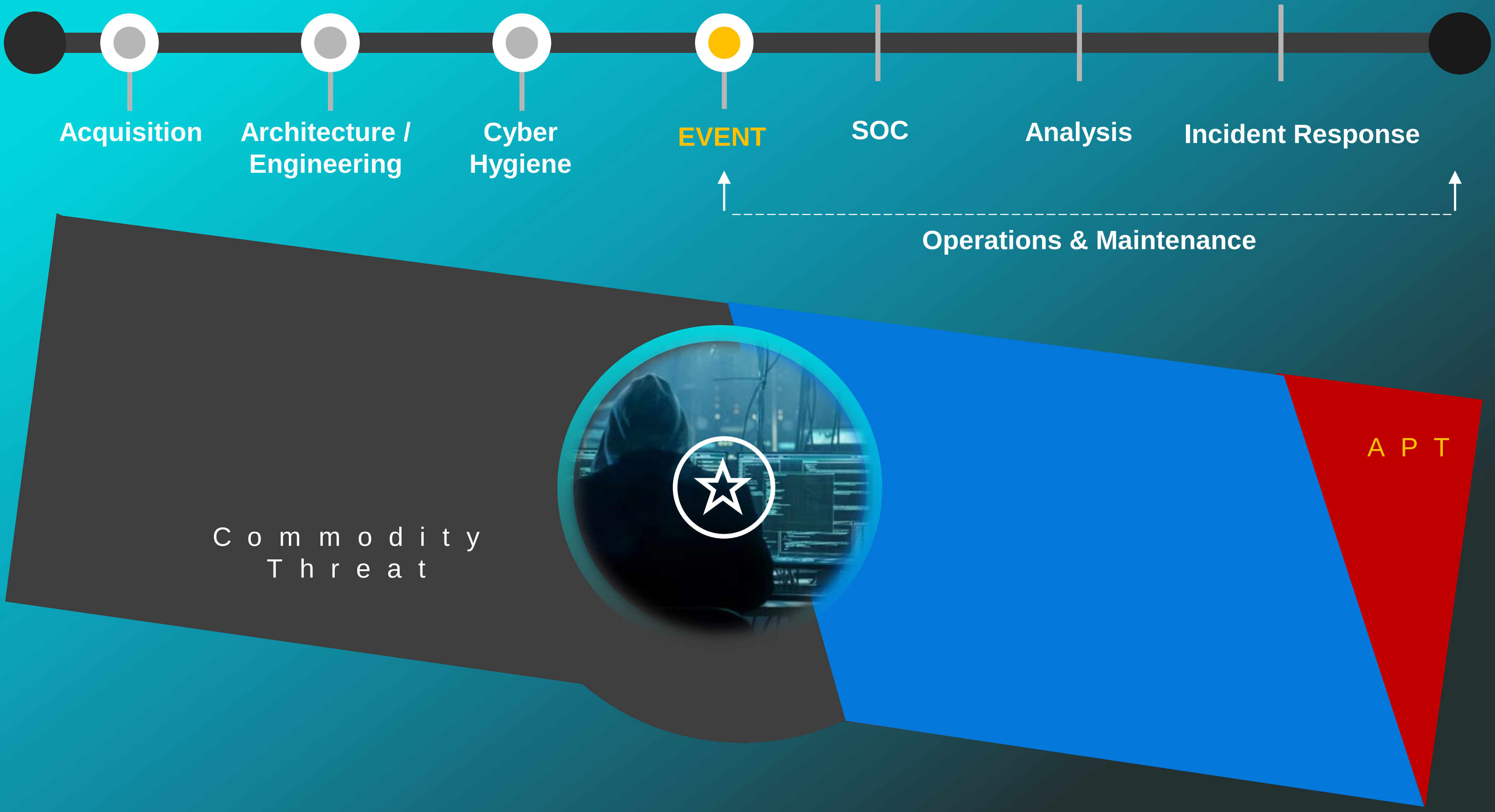
Operations & Maintenance



Commodity Threat

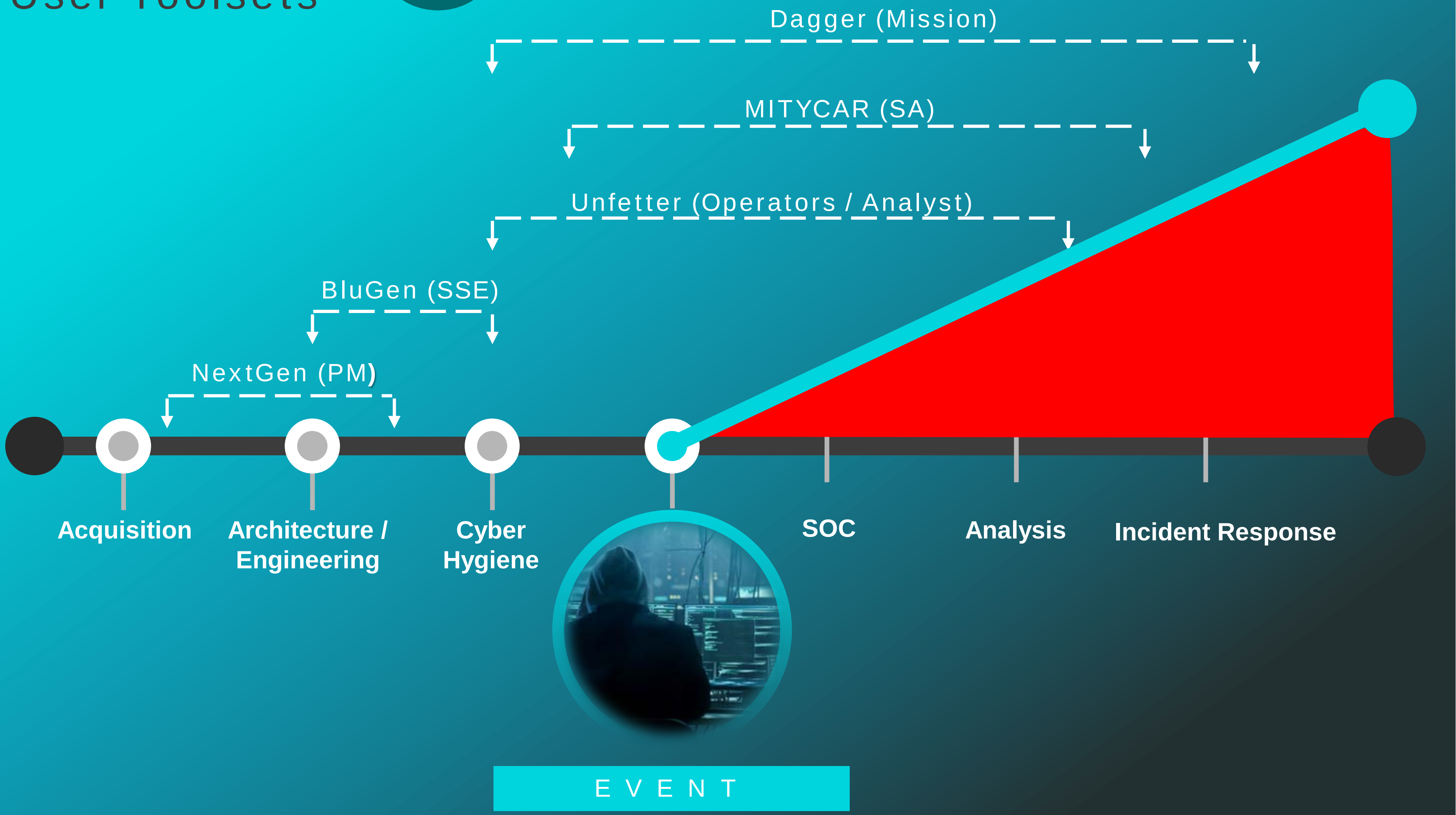
Nation-State Threat

# DoDCAR Feedback Loop



# DoDCAR

User Toolsets



Dagger (Mission)

MITYCAR (SA)

Unfetter (Operators / Analyst)

BluGen (SSE)

NextGen (PM)

Acquisition

Architecture / Engineering

Cyber Hygiene

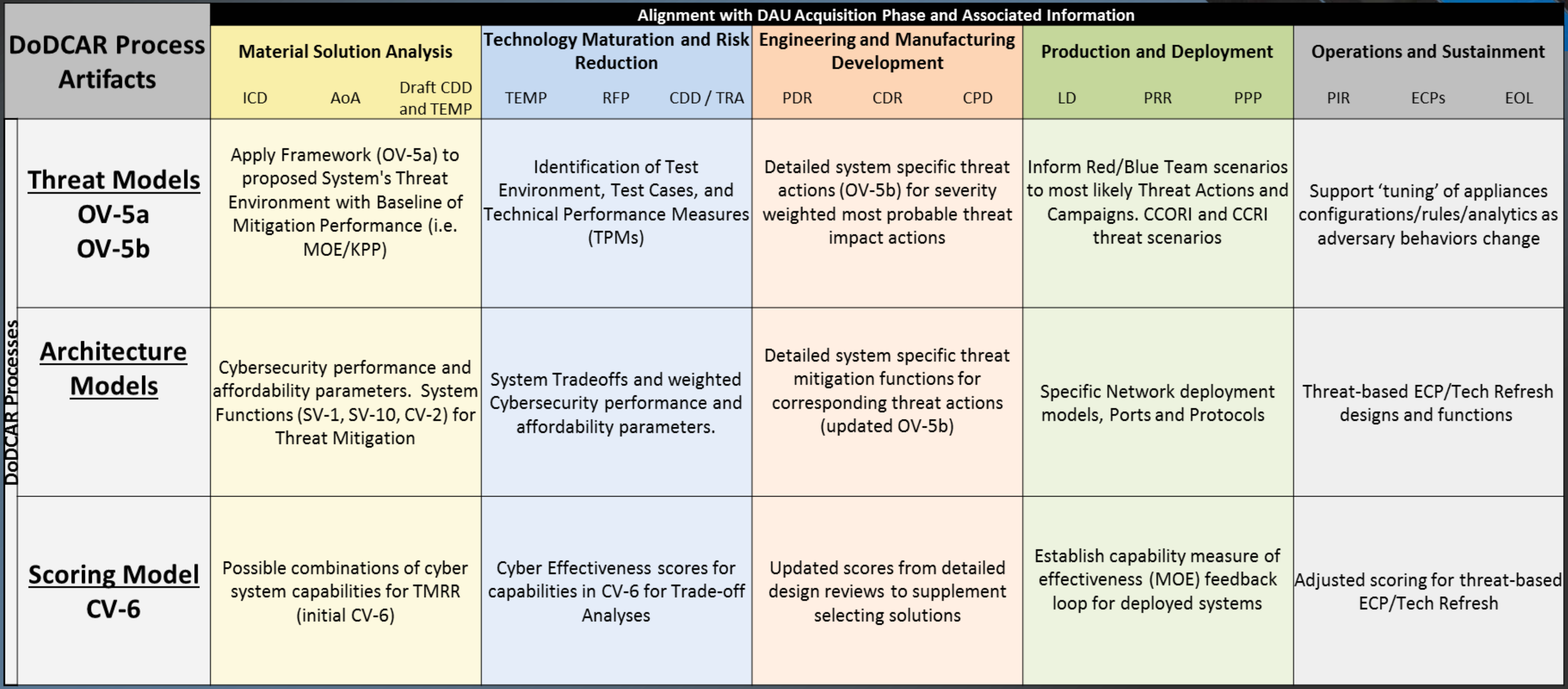
SOC

Analysis

Incident Response

EVENT

# DoDCAR's Contribution to Acquisition



Alignment with DAU Acquisition Phase and Associated Information

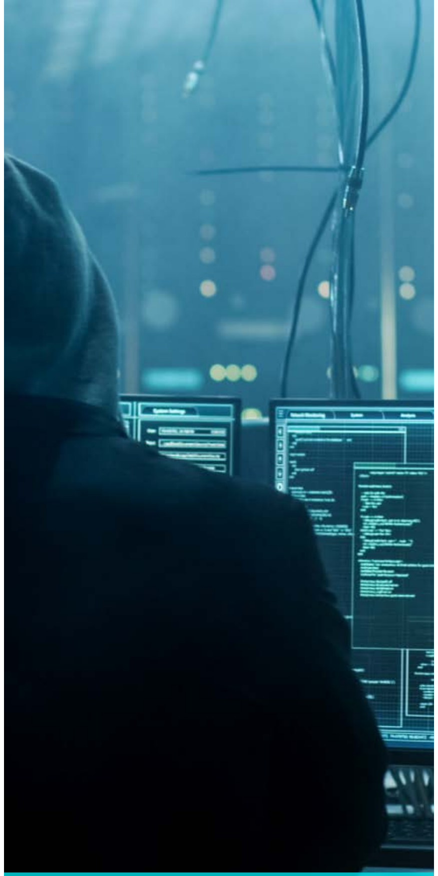
| | DoDCAR Process Artifacts | Material Solution Analysis | Technology Maturation and Risk Reduction | Engineering and Manufacturing Development | Production and Deployment | Operations and Sustainment |
|---|---|---|---|---|---|---|
| | | ICD<br>AoA<br>Draft CDD and TEMP | TEMP<br>RFP<br>CDD / TRA | PDR<br>CDR<br>CPD | LD<br>PRR<br>PPP | PIR<br>ECPs<br>EOL |
| DoDCAR Processes | **Threat Models**<br>**OV-5a**<br>**OV-5b** | Apply Framework (OV-5a) to proposed System's Threat Environment with Baseline of Mitigation Performance (i.e. MOE/KPP) | Identification of Test Environment, Test Cases, and Technical Performance Measures (TPMs) | Detailed system specific threat actions (OV-5b) for severity weighted most probable threat impact actions | Inform Red/Blue Team scenarios to most likely Threat Actions and Campaigns. CCORI and CCRI threat scenarios | Support 'tuning' of appliances configurations/rules/analytics as adversary behaviors change |
| | **Architecture Models** | Cybersecurity performance and affordability parameters. System Functions (SV-1, SV-10, CV-2) for Threat Mitigation | System Tradeoffs and weighted Cybersecurity performance and affordability parameters. | Detailed system specific threat mitigation functions for corresponding threat actions (updated OV-5b) | Specific Network deployment models, Ports and Protocols | Threat-based ECP/Tech Refresh designs and functions |
| | **Scoring Model**<br>**CV-6** | Possible combinations of cyber system capabilities for TMRR (initial CV-6) | Cyber Effectiveness scores for capabilities in CV-6 for Trade-off Analyses | Updated scores from detailed design reviews to supplement selecting solutions | Establish capability measure of effectiveness (MOE) feedback loop for deployed systems | Adjusted scoring for threat-based ECP/Tech Refresh |

### Security Posture

*Provides a rationale for DoD acquisitions processes by highlighting improvements to enterprise security*

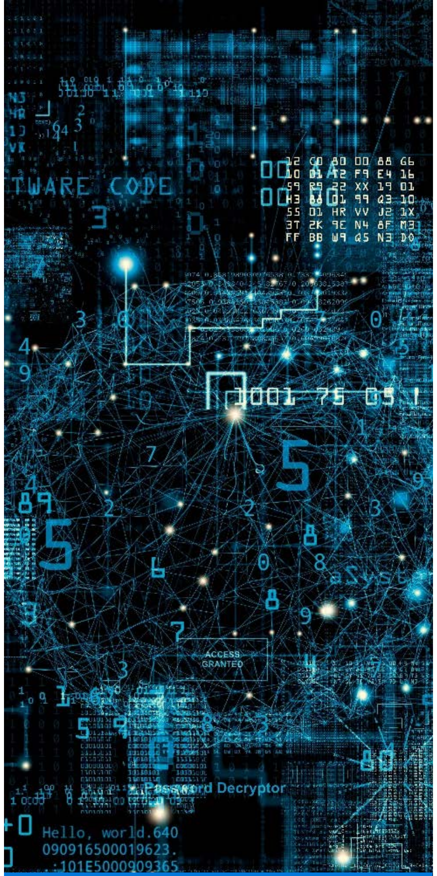
### Costs vs. Coverage

*Supports portfolio managers in balancing capability costs and capability coverage of threat landscape*



### Threat Actions & Heat Maps

*DoDCAR Threat Framework incorporated across the DoD, Intelligence Community, and DHS (GOVCAR)*



### Cyber Competency Scoring

*Scoring and analysis results feed the DoD Cybersecurity Portfolio Manager’s Cyber Competency Scoring process*

# DoDCAR Influence on DoD Cybersecurity Portfolio

# DoDCAR

## Accomplishments

Evolves the DoD's cybersecurity posture by creating an implementation roadmap for the DODIN based on an holistic review of the security architecture.

Creates a solid rationale using the Adversary Lifecycle as a framework, informed by current classified and unclassified threat intelligence data.

### Broad Adoption

Adoption of Threat Framework for EO13587 Independent Assessments

### Military Readiness

Command Cyber Operational Readiness Inspections (CCORI)

### IT Modernization

Reduction of Cyber Vulnerabilities, Enhanced Security & Maximized ROI through end-point and perimeter security modernization

### Threat Driven Model

Provides Decision Makers Across Federal Government Insight & Knowledge to Make Well-Informed, Prioritized Cybersecurity Investment Decisions

### NIST Coordination

To Establish Data-Driven Threat-Based Cybersecurity as an Industry Best Practice