2020 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
GROUND SYSTEMS CYBER ENGINEERING TECHNICAL SESSION
AUGUST 11-13, 2020 - NOVI, MICHIGAN

Demystifying Cyber Systems Engineering

Cheri Lofy[1], Dr. Mark Vriesenga[2]

[1]Electronic Systems, BAE Systems, San Diego, CA 92127
[2]FAST Labs Cyber Technology, BAE Systems, San Diego, CA 92127

ABSTRACT

As the United States' (US) Department of Defense (DoD) works to maintain our battlefield superiority in the ground domain, we rapidly integrate new electronic capabilities into vehicles that communicate and cooperate over vehicle-to-infrastructure networks. These new capabilities contribute to increasing the potential attack surface, as described in the 2018 Government Accountability Office (GAO) report on Weapon System Cyber Security [1]. To understand the increasingly complex attack surface and to reduce ground platform exposures through cyberspace, we need new engineering analysis and design techniques.

Today, most engineering methodologies treat cybersecurity as an add-on to traditional process flows. For example, until recently, the International Council on Systems Engineering (INCOSE) gave little attention to cybersecurity in their industry definition of the Vee-Model used widely in defense contracting. We argue that until we give cybersecurity first-class status and give it equal importance to the functional requirements, the products and services delivered may have sub-optimal defensive and resilience properties, making them vulnerable to attack through cyberspace.

This paper introduces BAE Systems' approach to making cybersecurity and resiliency first-class system properties in the engineering process. Our approach, called Cyber Systems Engineering (CSE), combines best practices from Risk Management Framework (RMF) for defensive design and supplementing methods derived from the application of 'offensive thinking to solve defensive problems.' We improve cyber readiness and survivability by combining offensive and defensive techniques throughout the engineering lifecycle. We have already applied CSE (in whole and part) on over 50 DoD programs; our combined approach using defensive and offensive skills strengthen as we identify best practices for DoD programs.

1. INTRODUCTION

The importance of cybersecurity is increasing as foreign adversaries rely on cyberattacks to neutralize the United States' (US) battlefield superiority. Today, cyberattacks are occurring with increased frequency, speed, and agility, making it challenging to guarantee mission assurance. The cyber threat is dynamic; our adversaries correctly anticipate defense-in-depth solutions, successfully identify vulnerabilities in defensive controls, and deploy innovative exploitation techniques to penetrate hardened systems. Our adversaries operate inside our observe, orient, decide, act (OODA) loop, using modern cyber techniques to compromise our platform systems. Figure 1 shows the dynamics of a 'Penetrate and Patch' cycle creating an operations tempo that is detrimental to the long-term security posture of the system.

To address this 'Penetrate and Patch' issue, we need a new generation of engineering methods to design system defenses that operate inside the adversary's OODA loop. These methods must predict 'where' an adversary is likely to attack and 'how' the attack may occur. The resulting defensive solution, informed by the 'dark art' of offensive cyber, anticipates the cyber adversary and allows defenders to operate using a 'Predict and Protect' operations tempo.

To achieve a 'Predict and Protect' operations tempo, security professionals need to rethink the traditional security engineering techniques that unintentionally constrain current defense-in-depth solutions. Specifically, most security engineering techniques leverage decades of historical lessons learned and best practices to establish a foundation for cyber hygiene, but do not integrate current offensive experience and lessons learned into the process. While defense-only techniques are still necessary, they do not adequately deter sophisticated cyber adversaries. Our adversaries continue to learn, adapt, and apply new offensive methods for cyberattack entry and exploitation.

To counter the sophisticated cyber adversary, we add offensive cyber knowledge to the defensive security engineering process, allowing the development of novel and advanced security solutions. These solutions disrupt both current and anticipated attack vectors resulting in a significantly enhanced security posture. This paper introduces BAE Systems' approach to making cybersecurity and resiliency first-class system properties in our corporate engineering process. Our approach, called Cyber Systems Engineering (CSE), combines best practices from Risk Management Framework (RMF) for defensive design and new methods derived from the application of 'offensive thinking to solve defensive problems.' By combining both offensive and defensive techniques into the engineering lifecycle, we increase cyber readiness and provide more cyber survivable products and services for the warfighter.

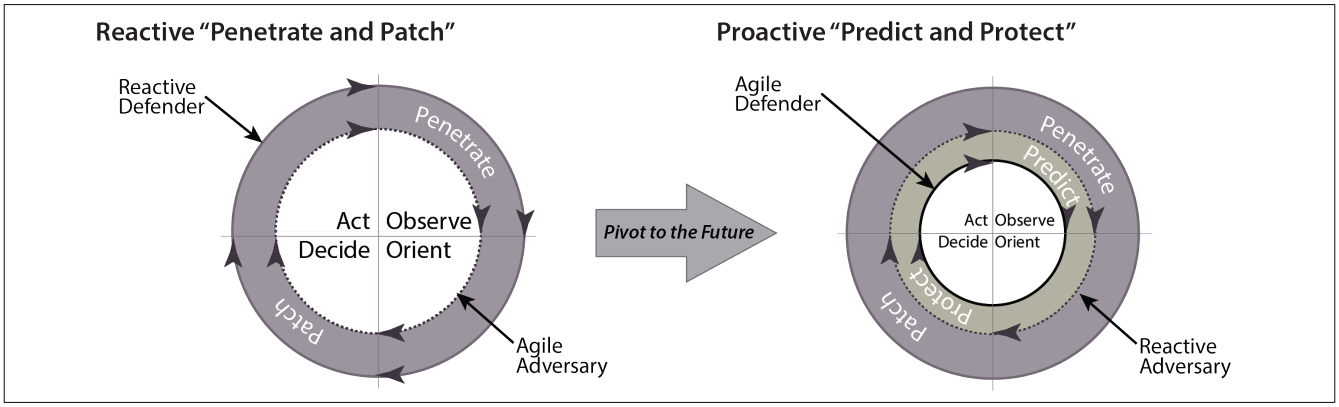


Figure 1 – Shifting the Basis for Cyber Defense. *Today's security engineering techniques are based on historical attack patterns and lead to a 'Penetrate and Patch' ops-tempo. Future security engineering techniques will anticipate attack patterns and lead to a more secure 'Predict and Protect' ops-tempo allowing the defender to be more agile than the adversary.*

2. PRIOR SOLUTIONS

The Department of Defense (DoD), Federal/Civil Agencies, and Intelligence Community (IC) have over two decades of thought leadership and experience in the domain of cyber defense methodologies, tools, and techniques. In the early 1990s, overarching security frameworks including DITSCAP, NIACAP, and NISCAP provided the first-ever information systems accreditation methodologies and guided the development of corresponding engineering analysis and design techniques. DIACAP, NIST SP 800 Series, and DCID 6/3 frameworks superseded these methodologies in the mid-2000s as emphasis shifted to information assurance controls as the primary expression of security requirements. Figure 2 shows this collection of six security policies, standards, and frameworks that set the stage for modern information system security.

In 2014, the Risk Management Framework (RMF) [2] became the common foundation for defensive cybersecurity across government organizations. It is a collection of best practices for information system security and distills two decades of lessons learned and best practices into a cohesive defensive security approach. Applied appropriately, RMF provides a reliable foundation for system hardening and cyber hygiene.

Today, we are witnessing the next fundamental shift in cyber defense strategy. This shift recognizes that for two decades, we built security solutions based on best practices derived from the analysis of historical cyberattacks. The next generation of defensive techniques will anticipate cyberattacks as we understand them through the lens of modern offensive cyber operations. As a foundation for innovation, tools like Cyber Kill Chain [3], Cyber Table Top Exercises [4], ATT&CK Framework [5], Attack Tree Modeling [6], and Cyber Resilience-in-Depth [7] are providing catalysts for change.

While these catalysts provide the foundation for next-generation cyber defense, they do not offer a cohesive, consistent, and repeatable methodology for designing and deploying anticipatory security solutions. The remainder of this paper describes BAE Systems' Cyber Systems Engineering (CSE) method that blends offensive and defensive

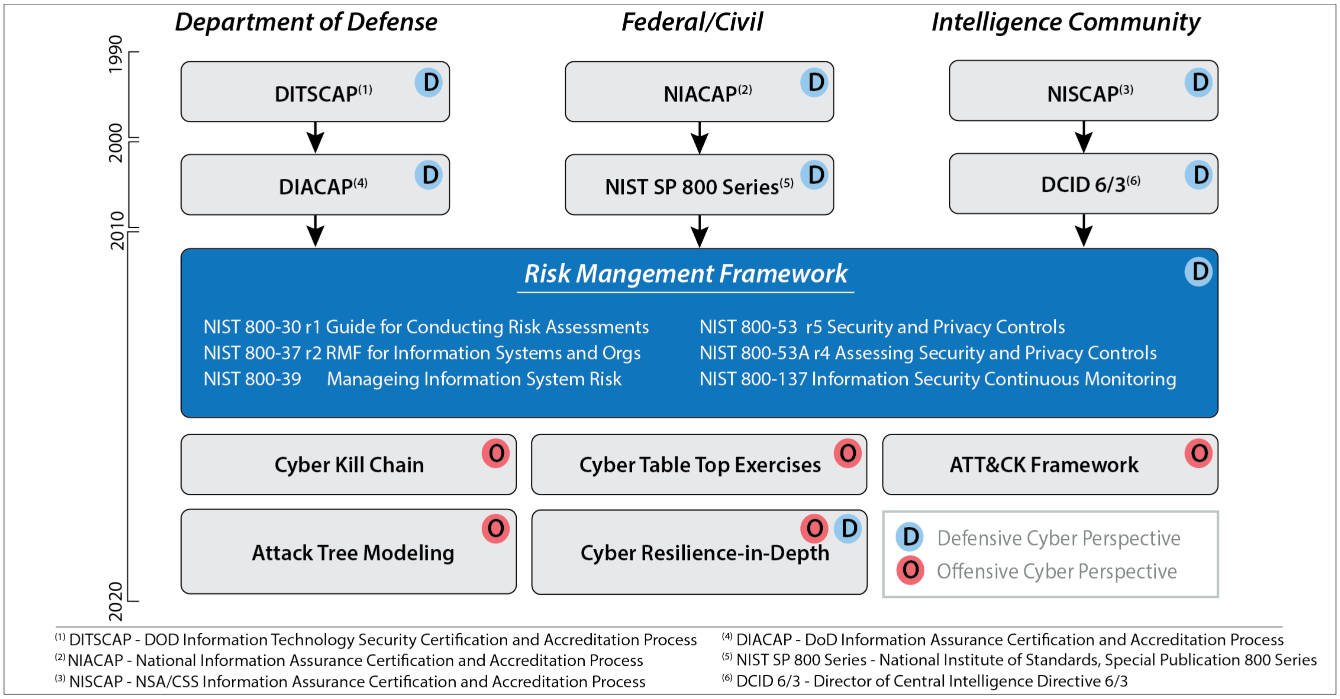

Department of Defense
Federal/Civil
Intelligence Community
1990
2000
2010
2020
DITSCAP(1) D
NIACAP(2) D
NISCAP(3) D
DIACAP(4) D
NIST SP 800 Series(5) D
DCID 6/3(6) D
Risk Mangement Framework D
NIST 800-30 r1 Guide for Conducting Risk Assessments
NIST 800-37 r2 RMF for Information Systems and Orgs
NIST 800-39 Manageing Information System Risk
NIST 800-53 r5 Security and Privacy Controls
NIST 800-53A r4 Assessing Security and Privacy Controls
NIST 800-137 Information Security Continuous Monitoring
Cyber Kill Chain O
Cyber Table Top Exercises O
ATT&CK Framework O
Attack Tree Modeling O
Cyber Resilience-in-Depth O D
D Defensive Cyber Perspective
O Offensive Cyber Perspective
(1) DITSCAP - DOD Information Technology Security Certification and Accreditation Process
(2) NIACAP - National Information Assurance Certification and Accreditation Process
(3) NISCAP - NSA/CSS Information Assurance Certification and Accreditation Process
(4) DIACAP - DoD Information Assurance Certification and Accreditation Process
(5) NIST SP 800 Series - National Institute of Standards, Special Publication 800 Series
(6) DCID 6/3 - Director of Central Intelligence Directive 6/3

Figure 2 – Defenses for Historical Attacks. *Today, most security engineering techniques are based on best practices for defending against historical attacks. While these techniques provide necessary cyber hygiene, they frequently do not defend against new and emerging adversarial tactics, techniques, and procedures.*

thinking to create next generation ‘Predict and Protect’ security solutions.

3. REQUIREMENTS FOR A SOLUTION

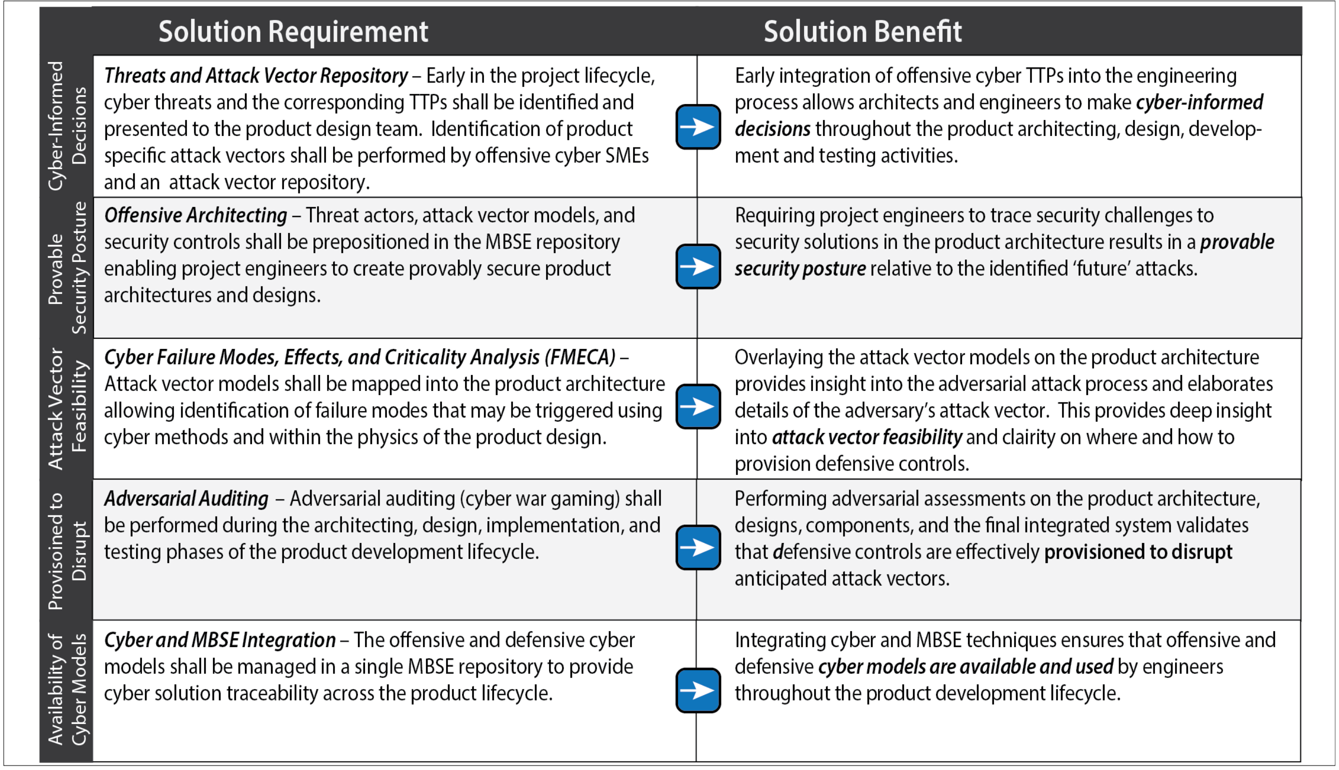
The challenge for the next generation of cyber defense methodologies is to develop security solutions allowing us to defend inside the cyber adversary's OODA loop. Solving this challenge seems intractable from a strictly defensive viewpoint as it requires 'predicting the future.' However, from an offensive viewpoint, the solution is finite and bounded. Specifically, the physics of the environment and the system constrain the adversarial cyber operations. This important fact means that:

- **Accessibility** - The adversary's access to the targeted system limits the selection of relevant and viable tactics, techniques, and procedures (TTPs).
- **Determinism** - The adversary's attack procedures (attack vectors) are limited by the physics of the system's vulnerability, making attack procedures directed, and finite.
- **Disruption** – Most attack procedures require multiple steps, and each step has to be successful for the attack to succeed.
- **Similarity** - Attack vectors are the same for everyone (friend and foe), making them predictable for the known attack surface.

With this offensive perspective, predicting an adversary's actions with reasonable accuracy becomes a tractable problem.

Table 1 lists five foundational requirements that we implement in our CSE methodology. These requirements enable an offensive perspective throughout the product development lifecycle that mitigates both known and anticipated attacks. In addition to these requirements, we also require that the CSE methodology 1) overlay and augment our corporate engineering processes, 2) be tailorable to support large and small programs, and 3) support both waterfall and Agile project management methods.

Table 1 – Requirements for Cyber Systems Engineering. *Modern cyber systems engineering methods combine offensive and defensive techniques resulting in the ability to predict adversarial TTPs and defend using well placed and properly configured security controls.*



	Solution Requirement		Solution Benefit
Cyber-Informed Decisions	***Threats and Attack Vector Repository*** – Early in the project lifecycle, cyber threats and the corresponding TTPs shall be identified and presented to the product design team. Identification of product specific attack vectors shall be performed by offensive cyber SMEs and an attack vector repository.	→	Early integration of offensive cyber TTPs into the engineering process allows architects and engineers to make ***cyber-informed decisions*** throughout the product architecting, design, development and testing activities.
Provable Security Posture	***Offensive Architecting*** – Threat actors, attack vector models, and security controls shall be prepositioned in the MBSE repository enabling project engineers to create provably secure product architectures and designs.	→	Requiring project engineers to trace security challenges to security solutions in the product architecture results in a ***provable security posture*** relative to the identified ‘future’ attacks.
Attack Vector Feasibility	***Cyber Failure Modes, Effects, and Criticality Analysis (FMECA)*** – Attack vector models shall be mapped into the product architecture allowing identification of failure modes that may be triggered using cyber methods and within the physics of the product design.	→	Overlaying the attack vector models on the product architecture provides insight into the adversarial attack process and elaborates details of the adversary’s attack vector. This provides deep insight into ***attack vector feasibility*** and clairity on where and how to provision defensive controls.
Provisoined to Disrupt	***Adversarial Auditing*** – Adversarial auditing (cyber war gaming) shall be performed during the architecting, design, implementation, and testing phases of the product development lifecycle.	→	Performing adversarial assessments on the product architecture, designs, components, and the final integrated system validates that *d*efensive controls are effectively **provisioned to disrupt** anticipated attack vectors.
Availability of Cyber Models	***Cyber and MBSE Integration*** – The offensive and defensive cyber models shall be managed in a single MBSE repository to provide cyber solution traceability across the product lifecycle.	→	Integrating cyber and MBSE techniques ensures that offensive and defensive ***cyber models are available and used*** by engineers throughout the product development lifecycle.

4. THE CYBER SYSTEMS ENGINEERING METHOD

Our cyber adversaries are more determined than ever to neutralize US battlefield superiority through the use of offensive cyber operations. The Department of Defense is challenging its contractors to develop platforms and systems that better defend against historical, current, and anticipated adversarial cyberattacks. Over the past five years, BAE Systems developed and piloted an engineering process that adds offensive and defensive cybersecurity activities to the traditional methodologies giving cybersecurity 'first-class status' in the development lifecycle.

Figure 4 (upper) provides an overview of our Cyber Systems Engineering (CSE) process overlay. The overlay comprises fifteen (15) processes representing a mix of offensive (red dot) and defensive (blue dot) activities that enable 'offensive thinking to solve defensive problems.' We align these processes with six traditional lifecycle management (LCM) phases that commonly define engineering methods. The CSE activities are modular and allow tailoring to meet the needs of projects using waterfall or Agile methods.

4.1. Requirements Engineering

During the Requirements Engineering phase, cyber engineers extract both offensive and defensive information needed to inform and guide the product development teams. This extraction process includes

1. Modeling of cyber threats in the product's operating environment,
2. Modeling of attack vectors that define the step-by-step attack process, and
3. Identification and extraction of relevant defensive security controls.

We produce the threat and attack vector models using a brainstorming session with offensive cyber experts followed by rounds of adversary modeling. The resulting adversary models provide a foundation used to guide engineering decisions in down-stream lifecycle activities throughout the product development lifecycle. This early identification and extraction of offensive cyber information is a crucial activity in CSE since it enables the project team to make cyber-informed decisions.

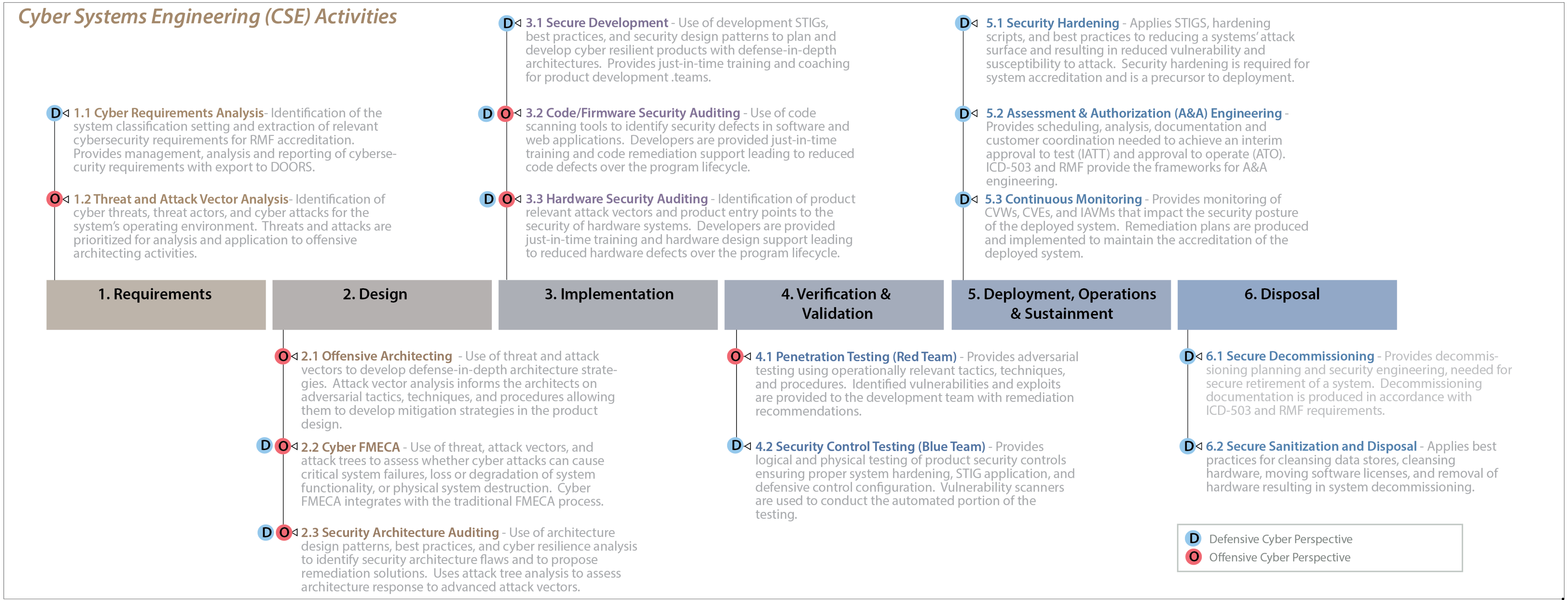
4.2. Architecture and Design

In the Architecture and Design phase, cyber engineers perform three essential activities. The Offensive Architecting activity prepositions offensive and defensive cyber data (e.g., threat and attack models, security controls, security requirements) in the project's model-based engineering (MSBE) repository. This cyber data allows system architects and design engineers to work with cyber data and trace it to the corresponding architecture and design views.

Next, we perform Cyber Failure Modes, Effects, and Criticality Analysis (Cyber FMECA) to identify significant product failures that may be triggered by a successful cyberattack vector. This Cyber FMECA activity allows engineers to understand the attack vector details better, assess the viability of each attack vector, and alter the system design to neutralize each attack vector. The result is a product architecture that has improved defensive capabilities for the set of anticipated cyberattacks.

Finally, in the Security Architecture Auditing activity, cyber engineers conduct a wargame using the product architecture. We perform this activity as a 'discovery workshop' where the product design team presents technical design artifacts, and cyber engineers develop new attack vectors. This activity provides an 'out-of-the-box' adversarial assessment of the product design and leads to the discovery of novel attack approaches. At the end of the auditing workshop, design engineers change the product design to address the newly discovered security concerns resulting in a hardened product design.

Cyber Systems Engineering (CSE) Activities



1. Requirements

D 1.1 Cyber Requirements Analysis- Identification of the system classification setting and extraction of relevant cybersecurity requirements for RMF accreditation. Provides management, analysis and reporting of cybersecurity requirements with export to DOORS.

O 1.2 Threat and Attack Vector Analysis- Identification of cyber threats, threat actors, and cyber attacks for the system's operating environment. Threats and attacks are prioritized for analysis and application to offensive architecting activities.

2. Design

O 2.1 Offensive Architecting - Use of threat and attack vectors to develop defense-in-depth architecture strategies. Attack vector analysis informs the architects on adversarial tactics, techniques, and procedures allowing them to develop mitigation strategies in the product design.

D O 2.2 Cyber FMECA - Use of threat, attack vectors, and attack trees to assess whether cyber attacks can cause critical system failures, loss or degradation of system functionality, or physical system destruction. Cyber FMECA integrates with the traditional FMECA process.

D O 2.3 Security Architecture Auditing - Use of architecture design patterns, best practices, and cyber resilience analysis to identify security architecture flaws and to propose remediation solutions. Uses attack tree analysis to assess architecture response to advanced attack vectors.

3. Implementation

D 3.1 Secure Development - Use of development STIGs, best practices, and security design patterns to plan and develop cyber resilient products with defense-in-depth architectures. Provides just-in-time training and coaching for product development .teams.

D O 3.2 Code/Firmware Security Auditing - Use of code scanning tools to identify security defects in software and web applications. Developers are provided just-in-time training and code remediation support leading to reduced code defects over the program lifecycle.

D O 3.3 Hardware Security Auditing - Identification of product relevant attack vectors and product entry points to the security of hardware systems. Developers are provided just-in-time training and hardware design support leading to reduced hardware defects over the program lifecycle.

4. Verification & Validation

O 4.1 Penetration Testing (Red Team) - Provides adversarial testing using operationally relevant tactics, techniques, and procedures. Identified vulnerabilities and exploits are provided to the development team with remediation recommendations.

D 4.2 Security Control Testing (Blue Team) - Provides logical and physical testing of product security controls ensuring proper system hardening, STIG application, and defensive control configuration. Vulnerability scanners are used to conduct the automated portion of the testing.

5. Deployment, Operations & Sustainment

D 5.1 Security Hardening - Applies STIGS, hardening scripts, and best practices to reducing a systems' attack surface and resulting in reduced vulnerability and susceptibility to attack. Security hardening is required for system accreditation and is a precursor to deployment.

D 5.2 Assessment & Authorization (A&A) Engineering - Provides scheduling, analysis, documentation and customer coordination needed to achieve an interim approval to test (IATT) and approval to operate (ATO). ICD-503 and RMF provide the frameworks for A&A engineering.

D 5.3 Continuous Monitoring - Provides monitoring of CVWs, CVEs, and IAVMs that impact the security posture of the deployed system. Remediation plans are produced and implemented to maintain the accreditation of the deployed system.

6. Disposal

D 6.1 Secure Decommissioning - Provides decommissioning planning and security engineering, needed for secure retirement of a system. Decommissioning documentation is produced in accordance with ICD-503 and RMF requirements.

D 6.2 Secure Sanitization and Disposal - Applies best practices for cleansing data stores, cleansing hardware, moving software licenses, and removal of hardware resulting in system decommissioning.

D Defensive Cyber Perspective
O Offensive Cyber Perspective

CSE Collaboration Lab

BAE Systems Cyber Lab

Provides a BAE Systems hosted lab environment enabling broad access to cyber SMEs and enabling deep analysis of system documentation, hardware and software (U/S/TS/SCI).

CSE Toolset

The following tools are used for Defensive CSE activities:

- RMF Requirements Extractor
- Cyber Threat and Attack Catalog
- IBM Rational DOORS
- No Magic MagicDraw/Sparx Enterprise Architect
- Amenaza SecuriTree
- Reliasoft XFMEA
- Tenable ACAS Nessus/Retina
- HP Fortify/HP WebInspect
- Synopsys Coverity
- eMASS, Xacta
- Microsoft Office & Adobe Reporting
- RMF Document Templates and Accelerators

The following toolsets are used for Offensive CSE activities:

- Open Source Intelligence (OSINT) Reporting
- SecuriTree Attack Tree Modeling and Analytics
- XFMEA Cyber FMECA Analysis
- HP Fortify/WebInspect Code Scanners
- Application and Protocol Fuzzers
- IDAPro/Binary Ninja/BinDiff Reverse Engineering
- OllyDBG/ImmunityDBG/WinDB/GDB Debuggers
- Kali Linux
- HackRF and Inspectrum/GQRX
- Hardware Expressions of Malware
- Microsoft Office & Adobe Reporting

Cyber Resilience Capability Group

Cyber Resilience Capability Group (CRCG)
Cyber Resilient by Design

Provides an environment for training and sustaining the BAE Systems Cyber Systems Engineers capability:
- CSE career lattice
- CSE toolsets
- CSE processes and handbooks
- Cyber/IA Community of Practice (Cyber/IA COP)
- Internal cyber training courses (CEH, CISSP, ISSEP, OSCP, etc.)

Figure 4 – The Cyber Systems Engineering Methodology. *The Cyber Systems Engineering methodology provides an integrated set of offensive and defensive engineering activities that augment both traditional waterfall and modern agile engineering processes. These activities are selected and tailored based on specific project needs resulting in affordable and efficient defense-in-depth solutions.*

4.3. Implementation

The Implementation phase begins with Secure Development where the cyber engineers work with developers and coach them on how to develop a secure product. Because many attack vectors rely on software defects to succeed, we give special attention to the software elements of the product design. These software elements include micro-controller firmware, embedded operating systems, embedded software applications, server operating systems, server applications, and web applications.

As we implement the product, we continuously test it for security defects. The Code/Firmware Security Auditing activity uses both manual and automated code scanning to identify and remediate software defects as they occur in the software baseline. In many cases, we perform this checking as part of Agile continuous integration (CI), where we build, functionally test, and security test the software baseline, daily. Agile CI allows early identification of software defects and provides an opportunity to deliver just-in-time training to the project's software development team.

Finally, as the product matures, we audit the hardware implementation using adversarial assessment techniques. We apply these assessment techniques at the chip, board, assembly, bus, and platform levels of abstractions as described in Demystifying Platform Cyber Resilience [7]. The use of specialized equipment is sometimes needed when performing these tests to determine whether hardware test points are active, hardware buses are protected, and whether side channels may be transporting sensitive data. In addition to the physical hardware assessment, we also evaluate whether unsecured trust relationships between hardware elements of the system exist. Where exploitable trust relationships exist, we update the product's hardware and software design, and we apply preventative security controls to disrupt anticipated adversarial attack vectors.

4.4. Verification and Validation

In the Verification and Validation phase, cyber engineers conduct both offensive and defensive testing of the final as-built product to ensure that the product meets the set of design specifications and the operational needs of the user. By using Red and Blue Teams in the verification and validation process, we gain a deep understanding of product vulnerabilities and how adversarial TTPs can be applied to exploit them. When used frequently in the product lifecycle, the process enables the rapid convergence of the security architecture to a near-optimal state.

In the Penetration Testing (Red Team) activity, offensively trained CSEs (e.g., penetration testers) conduct a simulated cyberattack on the as-built product. Penetration testers creatively discover, evaluate, and exploit configuration errors, software defects, unsecured trust relationships, default system behaviors, and unintended emergent behaviors. At the end of the Red Team activity, the penetration testers produce an assessment report documenting the discovered security issues and providing recommendations for corrective action. This report is delivered to the development team and supports the final product hardening before formal accreditation and deployment into operations.

In the Security Control Testing (Blue Team) activity, we inspect the defensive security controls relative to the anticipated attack vectors. This activity extends the traditional RMF testing by ensuring that the control provisioning extends beyond the default 'out-of-the-box' configurations. Individually, we configure the defensive controls to meet the specific operational environment's demands, the anticipated threat actors, and the anticipated attack vectors. This activity prevents security controls from misconfiguration in their final deliverable state. Additionally, once the Red Team develops an assessment report for the discovered security issues, the Blue Team must then develop response strategies and apply fixes to defend against the identified security issues.

4.5. Deployment, Operations, and Sustainment

In the Deployment, Operations, and Sustainment phase, cyber engineers complete the final hardening of the product, produce the final accreditation package, and begin the RMF continuous monitoring activities. The Security Hardening activity includes taking action on 1) defensive best practices described in Secure Technical Implementation Guides (STIGS) [8] and 2) addressing the findings discovered during the Penetration Testing activity.

By performing defensive and offensive hardening, we achieve a balance of historical best practice and predictive defensive practice.

Next, the cyber engineers complete the Assessment and Authorization activity resulting in an RMF accreditation package. The package is presented to the government for approval and leads to the products' formal authorization to operate (ATO). This activity, defined by the RMF, is a standard across DoD, FedCiv, and IC programs to establish a foundational level of product security. In our experience, CSE does not replace RMF. Instead, CSE augments the early product engineering activities and improves the quality of the architecture and designs documented in the RMF accreditation package.

The last activity in this lifecycle phase is Continuous Monitoring, where we monitor the product's security logs for signs of compromise. RMF also defines the activity and requires constant adjudication of security warnings and alerts in the context of the deployed product.

CSE augments this activity by creating new attack vector models and assessing them against the deployed product architecture. These attack vectors are added to a central repository managed in the CSE toolset and are used to develop, test, and deploy product patches and updates.

4.6. Disposal

The Disposal phase of CSE provides Secure Decommissioning of the product and Secure Sanitization and Disposal of the products' hardware, software, and data components. These two activities account for the methods and techniques used to handle, transport, package, store, or destroy retired products. These include the data and information holdings associated with the system or contained in system elements. These two activities can be time-consuming and complicated when the decommissioned product had classified system elements or operated in a classified environment. To accomplish both activities in this phase, we follow government guidelines and best practices defined by NIST and NSA for secure system decommissioning.

4.7. CSE Toolset

Figure 4 (lower) shows the core toolset used on the majority of our DoD and IC programs. This toolset is a mix of commercial, open-source, and custom-built applications that provide accelerators for the CSE activities, making them fast and affordable. We select tools that are best in class and provide realistic emulation of both offensive and defensive operations.

In addition to the core toolset, one of the significant challenges in implementing CSE is the availability of domain-relevant and validated threat and attack vector models. Generally, this information is held by a few subject matter experts who are well versed in the 'dark art' of offensive cyber operations and penetration testing. To resolve this challenge, a central data store, called the Cyber Threats and Attacks Catalog (CTAC), provides a common knowledge repository across projects. This catalog is program neutral and supports the robust extraction of offensive and defensive information needed to guide the CSE activities. The CTAC is used in the Requirements Engineering phase of CSE and ensures that a robust and correct set of adversarial models is selected to guide the product development process.

5. TAILORING CYBER SYSTEMS ENGINEERING FOR PROJECTS

In most government and contractor environments, a broad spectrum of development approaches are used to design, architect, design, and develop warfighting products. These approaches range from the “Vee” (e.g., waterfall) to iterative-incremental (e.g., spiral, rapid prototyping) to Agile (e.g., Scrum, Kanban, eXtreme Programming). We designed Cyber Systems Engineering as a modular set of activities tailored to suit specific program needs and to make our security engineering processes portable across development approaches.

Figure 5 shows a process for tailoring CSE. The process begins with a System Criticality Assessment and a Cyber Threat Assessment. In the criticality assessment, we determine the value of the product to a foreign adversary. The RMF provides best-practices for establishing the system classification; however, it generally evaluates the system from a stand-alone perspective. CSE builds on these best practices and adds evaluation criteria based on how the product connects to its operating environment. Specifically, when low and high criticality products are connected, both systems' criticality should be elevated to a high level. This design principle is important because cyber adversaries commonly compromise low criticality systems to provide a foothold from which to exploit more critical systems.

In the Cyber Threat Assessment, we evaluate the product’s operating environment to identify potential threat actors and access the final deployed product. In cases where the system has little threat exposure and access, we reduce the scope of offensive cyber activities in the CSE implementation. In this tailoring step, it is essential to consider both current and future applications of the product. If a product is designed initially for a low risk operating environment, we should be careful about deploying it to a high-risk operating environment without reapplication of the offensive CSE activities.

In the Cyber Security Value Proposition assessment, we decide how much security the product needs. Future-proofing against all anticipated cyberattacks can be expensive and only applies to high-value, mission-critical systems, and limited access systems (e.g., military satellites, missile systems, UAVs).

Results from the criticality, threat, and value assessment are combined and tracked in an Excel workbook to provide a recommended set of CSE activities. The workbook accounts for the fact that some CSE activities have interdependencies and must be selected together. For example, Threat and Attack Vector Analysis must precede a Cyber FMECA since the offensive models are required during the FMECA analysis. We document the final set of tailored CSE activities in the product’s systems engineering management plan (SEMP) to record the selection decisions.

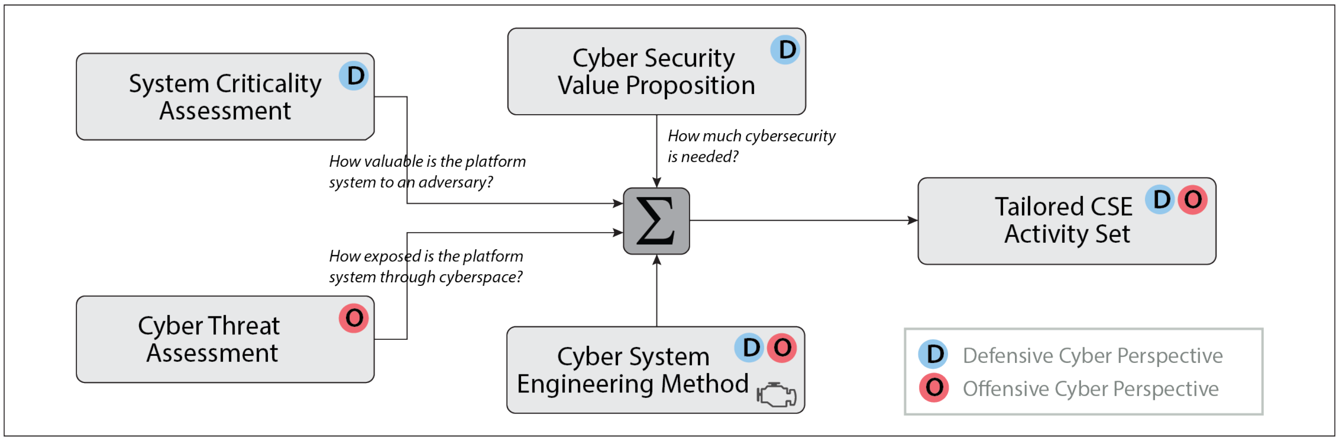

System Criticality Assessment
D
Cyber Security Value Proposition
D
How valuable is the platform system to an adversary?
How much cybersecurity is needed?
Σ
Tailored CSE Activity Set
D
O
How exposed is the platform system through cyberspace?
Cyber Threat Assessment
O
Cyber System Engineering Method
D
O
D Defensive Cyber Perspective
O Offensive Cyber Perspective

Figure 5 – Tailoring the CSE Methodology. *The Cyber Systems Engineering methodology is a modular set of activities that can be tailored to support both waterfall and modern agile engineering processes.*

6. LESSONS LEARNED AND BEST PRATICES

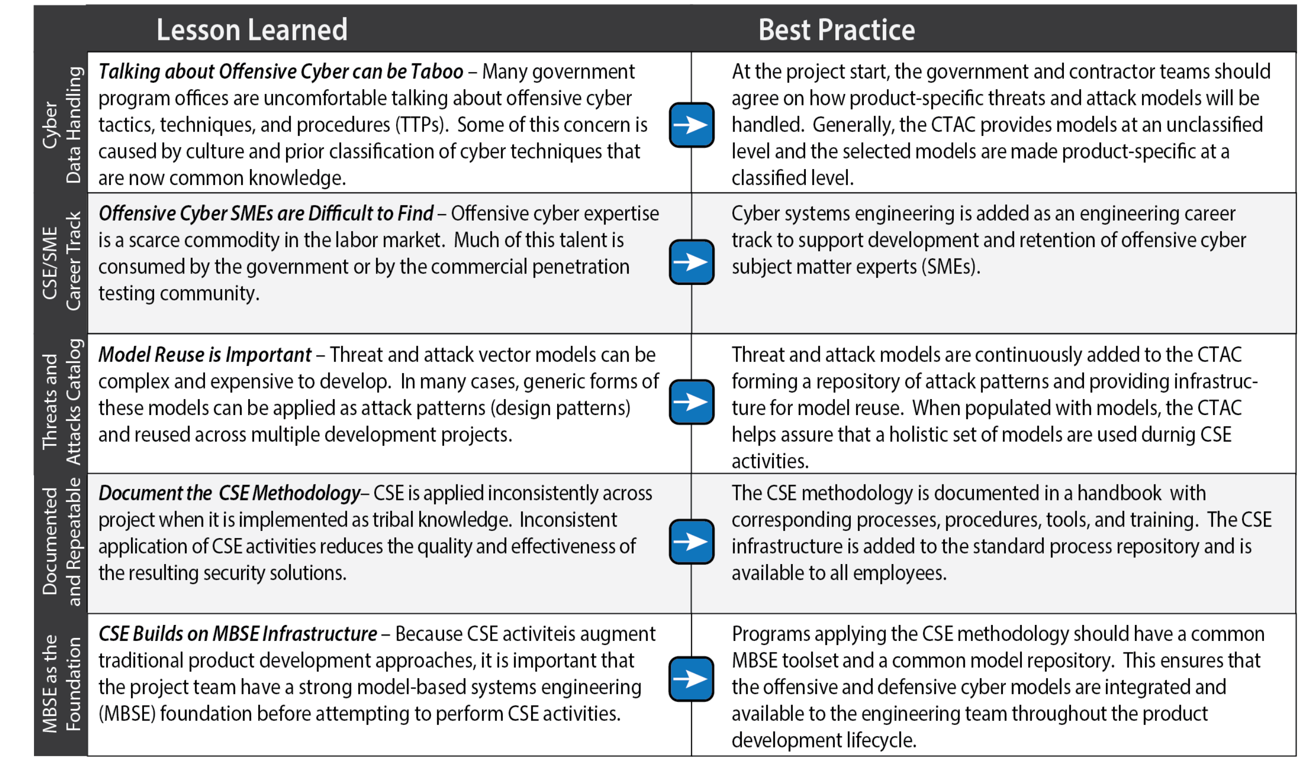
Over the past five years, we have applied (in whole and in part) the Cyber Systems Engineering methodology on over 50 product development programs. This experience provides many lessons and best practices that shape the current version of the CSE methodology.

Table 2 lists five lessons learned and best practices derived from applying CSE to production programs. Each item in this table derives from a significant challenge experienced in product development programs, and each item focuses on developing and integrating offensive knowledge into best practice applications. Of particular interest is the first item labeled 'talking about Offensive Cyber can be Taboo.' We find that the program sponsor is uncomfortable discussing relevant cyber threats and attack vectors in many programs. This discomfort is partly due to prior classifications of offensive cyber information and partly due to lingering uncertainty about what can and cannot be shared. On this topic, we believe

1. The physics of cyberattack is the same for everyone – friend and foe,
2. Our cyber adversaries are good at guessing product vulnerabilities, and
3. Our cyber adversaries are good at developing exploits and attack vectors.

We believe the truth of these assertions provide strong motivation for the entire defense community to rethink what offensive cyber information can and should be shared so our defensive strategies can evolve. Our CSE methodology takes steps in this direction as a feasibility pilot to show the application of offensive thinking throughout the lifecycle; however, a DoD/IC comprehensive initiative focused on institutionalizing these practices might be the next transformational step in defensive cybersecurity.

Table 2 – Lessons Learned and Best Practices. *The Cyber Systems Engineering methodology has evolved over 5-years based on lessons learned and the identification of best practices for security solution development.*



	Lesson Learned	Best Practice
Cyber Data Handling	***Talking about Offensive Cyber can be Taboo*** – Many government program offices are uncomfortable talking about offensive cyber tactics, techniques, and procedures (TTPs). Some of this concern is caused by culture and prior classification of cyber techniques that are now common knowledge.	At the project start, the government and contractor teams should agree on how product-specific threats and attack models will be handled. Generally, the CTAC provides models at an unclassified level and the selected models are made product-specific at a classified level.
CSE/SME Career Track	***Offensive Cyber SMEs are Difficult to Find*** – Offensive cyber expertise is a scarce commodity in the labor market. Much of this talent is consumed by the government or by the commercial penetration testing community.	Cyber systems engineering is added as an engineering career track to support development and retention of offensive cyber subject matter experts (SMEs).
Threats and Attacks Catalog	***Model Reuse is Important*** – Threat and attack vector models can be complex and expensive to develop. In many cases, generic forms of these models can be applied as attack patterns (design patterns) and reused across multiple development projects.	Threat and attack models are continuously added to the CTAC forming a repository of attack patterns and providing infrastructure for model reuse. When populated with models, the CTAC helps assure that a holistic set of models are used durnig CSE activities.
Documented and Repeatable	***Document the CSE Methodology***– CSE is applied inconsistently across project when it is implemented as tribal knowledge. Inconsistent application of CSE activities reduces the quality and effectiveness of the resulting security solutions.	The CSE methodology is documented in a handbook with corresponding processes, procedures, tools, and training. The CSE infrastructure is added to the standard process repository and is available to all employees.
MBSE as the Foundation	***CSE Builds on MBSE Infrastructure*** – Because CSE activiteis augment traditional product development approaches, it is important that the project team have a strong model-based systems engineering (MBSE) foundation before attempting to perform CSE activities.	Programs applying the CSE methodology should have a common MBSE toolset and a common model repository. This ensures that the offensive and defensive cyber models are integrated and available to the engineering team throughout the product development lifecycle.

7. CONCLUSIONS

As our foreign adversaries continue to develop offensive cyber capabilities focused on neutralizing our battlespace superiority, we as a defense community need to shift from 'Penetration and Patch' strategies to 'Predict and Protect' strategies. Historically, this shift was viewed as impossible when viewed from only the defender's perspective. However, when viewed from a defensive and offensive perspective, new engineering techniques become apparent that allow us to defend at the speed of the attack. At BAE Systems, we found that a necessary first step to addressing this need is to demystify platform cyber defense and platform cyber resilience [7]. The second step, documented in this paper, is to lay-flat a Cyber Systems Engineering methodology that defines a balanced approach to using 'offensive thinking to solve defensive problems.'

In this paper, we described several key concepts used to design and develop next-generation defensive security solutions. These concepts include:

- The CSE methodology gives first-class status to security engineering and provides a full lifecycle focus on product security.
- Offensive and defensive models can be combined to enable new advancements in security engineering.
- The application of offensive cyber models to enable 'Predict and Protect' security solutions and to allow defense inside the adversary's OODA loop.
- Model-Based Engineering provides foundational infrastructure and enables the advancement of security engineering practices.

Building on our CSE successes, BAE Systems continues to innovate and advance the science and technology of security engineering. We are prototyping new tools and techniques, allowing engineering teams to make informed cyber decisions daily. The resulting integrated processes and tools provide a measurable and repeatable approach to designing and developing highly defendable products with a fast track to operational accreditation.

8. REFERENCES

[1] GAO U.S. Government Accountability Office. “Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities”, October 9. 2018. https://www.gao.gov/products/GAO-19-128 (accessed May 27, 2020).

[2] Joint Task Force. “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy” NIST SP 800-37 Rev. 2, December 2018. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final (accessed May 27, 2020).

[3] Lockheed Martin Corporation. “The Cyber Kill Chain®” July 4, 2015. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed May 27, 2020).

[4] Deputy Assistant Secretary of Defense. “Department of Defense Cyber Table Top Guidebook” Version 1.0, July 2, 2018. https://www.dau.edu/cop/test/DAU Sponsored Documents/The DoD Cyber Table Top Guidebook v1.pdf (accessed May 27, 2020).

[5] The MITRE Corporation. “ATT&CK^{TM} Framework”, January 5, 2018. https://attack.mitre.org (accessed May 27, 2020).

[6] Wikipedia. “Attack Tree” March 7, 2020. https://en.wikipedia.org/wiki/Attack_tree (accessed May 27, 2020).

[7] C. Lofy and M. Vriesenga. “Demystifying Platform Cyber Resilience”, August 13, 2019. https://www.baesystems.com/en/download-en/20191030185537/1434638247099.pdf (accessed May 27, 2020).

[8] DoD Cyber Exchange. “Security Technical Implementation Guides (STIGs)”, June 19, 2019. https://public.cyber.mil/stigs/ (accessed May 28, 2020).