



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL



Cybersecurity for Weapon Systems: Architecting Mission Assurance & Cyber Resilience

Course Description:

Modern military platforms are no longer just mechanical assets—they are software-defined, hyper-connected, autonomous edge nodes. As adversary threats evolve toward **agentic cyber attacks, C2 hijacking, supply chain interdiction, and signal disruption**, cybersecurity can no longer be an afterthought or a "check-the-box" compliance task tacked on at the end of a project. It is a fundamental operational capability, equal in priority to kinetic lethality, survivability, and range.

Designed specifically for **Systems Engineers, Lead Architects, and Defense Project Managers**, this intensive 6-day hands-on course bridges the critical gap between customer specifications, defense regulatory frameworks, and real-world cyber-resilient design.

Participants will master how to decipher complex military security requirements, navigate defense standards (NIST, DoD, NATO STANAG, DO-326A), conduct threat modeling on platform interfaces, and architect layered "defense-in-depth" solutions that satisfy performance, cost, and mission constraints.

Through practical specification analysis, architectural trade-off exercises, and Red/Blue team response simulations, this course equips engineering leads to



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

deliver mission-capable weapon systems engineered to withstand, operate through, and recover from sophisticated cyber threats.

Key Learning Objectives

By the end of this course, engineering and management professionals will be able to:

- **Decode & Translate Customer Needs:** Analyze military tender specifications to isolate hidden cybersecurity requirements, link them directly to threat vectors, and map them to actionable engineering parameters.
- **Navigate Regulatory Standards:** Seamlessly transition customer specifications into concrete design baselines using defense standards (NIST 800-171, DoD 8500, NATO STANAGs) alongside aviation and commercial frameworks (FAA, DO-326A, ISO).
- **Engineer Resilient Architectures:** Apply *Defense-in-Depth* and Zero Trust principles to combat platforms, land/air/naval vehicles, radar, C2 links, and SCADA/ICS sub-systems.
- **Execute Platform Threat Modeling:** Perform asset mapping, trust-boundary definitions, and STRIDE risk modeling tailored specifically to embedded military hardware, tactical radios, and mission software.
- **Balance Trade-offs & Engineering Constraints:** Evaluate technical controls (encryption, anti-tamper, IAM) against real-world project variables including SWaP (Size, Weight, and Power), operational latency, budget, and schedule.
- **Validate & Manage Mission Continuity:** Oversee Verification & Validation (V&V) planning, Red/Blue team exercise integration, and incident response strategy to ensure operational survival under sustained cyber attack.

Target Audience

- **Systems Engineers & System Architects** designing defense platforms, tactical networks, sensors, and weapon subsystems.
- **Defense Project Managers & Program Directors** managing compliance, schedule, budget, and customer deliverables for military contracts.



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

- **Software & Hardware Engineering Leads** building embedded systems, firmware, or command-and-control software for defense applications.
- **Quality Assurance & Compliance Engineers** responsible for airworthiness, military standard compliance, and security verification testing.

Course Duration: 6 days

Detailed Agenda

Day 1: Introduction to Cybersecurity and Understanding Customer Requirements in Weapon Systems - An Engineer and Project Manager's Perspective

In this module, systems engineers and project managers will receive a focused and accessible introduction to the world of cybersecurity in the context of weapon systems. We will focus on understanding the main threats and their implications for

systems, and more importantly, how these threats translate into security requirements from customers.

The goal is to provide participants with the ability to identify the main cybersecurity elements in customer specifications and understand the justification for these requirements.

Topics and standards to be taught in this module:

- Basic overview of basic cybersecurity concepts relevant to weapons systems (confidentiality, integrity, availability)
- Identification of key threat types (without deep technical diving) and their relationship to compromising military systems
- Analysis of typical customer specifications in the military industry and understanding the cybersecurity clauses included in them
- The relationship between threats and security requirements in the customer specification - why does the customer require specific protections?



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

- Examples of security requirements in customer specifications and their implications for system design
- Practice in analyzing customer specifications and identifying basic cybersecurity requirements
- Understanding the importance of cybersecurity as part of the quality and performance requirements of military systems
- Introduction to cyber threats targeting weapons systems
 - o Overview of cyber threats specifically targeting weapons systems.
 - o Overview of cyber threats unique to military systems, their sources, and adversary motivations.
 - o Types of Cyber Threats: A discussion of the unique threats facing military platforms such as counterfeiting
 - o Command and Control hijacking, supply chain vulnerabilities, and the role of state actors, GPS.
 - o Threat Classification Using the CIA Principle: Understanding the concepts of Confidentiality, Integrity, and Availability, through the lens of weapons and defense systems, including specific examples such as radar jamming, data compromise, and service disruption.

Day 2: Translating Customer Requirements into Regulatory Standards and Security Definitions - Tools and Practices for Engineers

In this module, system engineers and project managers will learn how to relate cybersecurity requirements

in a customer specification to relevant regulatory standards (such as (STANAG, FAA, NATO, DoD).

We will focus on understanding the differences between the types of requirements and how to use the standards as a basis for defining concrete security solutions in the system.

The goal is to provide participants with tools and practices to translate customer requirements into clear and measurable security definitions.



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

Topics and standards to be taught in this module:

- Overview of key regulatory standards in the field of cybersecurity for military systems and their relationship to customer requirements
- Understanding the structure and content of standards such as the NIST 800 series (with an emphasis on 800-171), the DoD 8500 series, and relevant NATO and FAA standards
- Working methods for mapping security requirements from customer specifications to relevant clauses in standards
- Translating clauses in standards into specific security definitions for various system components
- Examples of translating customer requirements into concrete security definitions using standards
- Practice in moving from customer requirements to relevant standards and defining basic security solutions
- Understanding the decision-making process regarding the selection of standards according to customer requirements and the nature of the project
- Review of sources for cybersecurity systems requirements for defense
- Regulatory requirements and compliance with standards for military systems: Distinguishing between military and civilian standards, with an emphasis on defense regulations such as DoD, NATO STANAG standards, and requirements FAA.
- Understanding Cybersecurity Expectations for Weapons Systems.
- Customer and Mission Critical Security Requirements: Understand the customer-specific requirements and protocols essential to securing military technologies from cyber threats.
- Cybersecurity Standards Applicable to Defense and Weapons Systems
 - o Overview of Cybersecurity Standards: Analyze military standards such as the NIST 800 series, DoD 8500 series, and Air Force IT documentation. Emphasis on how these standards help ensure resilience against cyberattacks on defense systems.
 - o Civilian Standards and Their Role in Military Contexts: Review standards such as ISO and DO-326A to understand the various applications and unique requirements of defense environments.
 - o Mapping Standards to Defense Platforms: Discuss the specific application of these standards to defense system components, including secure communications, command and control, and data integrity.



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

Day 3: Characterizing Cyber Defense Solutions in Military Systems - Translating Customer Requirements into Architecture and Components

In this module, system engineers and project managers will focus on translating the customer's cybersecurity requirements into a secure system architecture and selecting appropriate security components. We will discuss the principle of "defense in depth" as a central approach in solution design. The goal is to provide participants with the ability to characterize concrete security solutions at the architecture and component level in accordance with customer requirements.

Topics and standards to be learned in this module:

- The principle of "defense in depth" as an approach to characterizing security solutions in accordance with customer requirements
- Identifying potential vulnerabilities in military systems in the context of customer requirements
- Characterizing different layers of protection (access controls, encryption, monitoring, etc.) in accordance with customer requirements
- Selecting appropriate security components (hardware and software) that meet customer requirements and devices Relevant
- Integrate security solutions into the overall system while considering performance and budget constraints
- Practice characterizing basic security solutions for different scenarios according to customer requirements
- Understand the relationship between customer requirements and security architecture and technology selection
- Introduction to cyber defense methods for military systems
 - o Defense in Depth: Concepts and strategies for implementing multiple layers of defense in weapon systems to reduce the risk of attacks.
 - o Cyber Defense Frameworks and Methodologies: Review of risk-based methodologies tailored to protect defense systems from cyber threats, while ensuring missions and operational security against adversary cyber attacks.



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

Day 4: Threat Analysis and Risk Assessment as a Tool for Characterizing Security Requirements with Customers

In this module, system engineers and project managers will learn how to use threat analysis and risk assessment as a central tool for characterizing security requirements with customers. We will focus on simple and practical models (such as the CIA triad in an expanded form) that will help understand the risks relevant to the system according to customer requirements and translate them into detailed security requirements.

Topics and Standards to be Learned in this Module:

- Using basic threat analysis (without complex models) to understand the customer's security needs
- Identifying critical assets in the system according to customer requirements and their value
- Assessing the potential impact of threats on these assets in the context of customer requirements
- Translating identified risks into concrete security requirements in the system specification
- Using the results of the risk analysis to justify security requirements to the Customer
- Practice in basic threat analysis and translating the results into security requirements with customers
- Understanding the connection between risk analysis and prioritizing security requirements in the project
- Threat Analysis for Defense and Weapon Systems
 - Threat Modeling Specific to Military Platforms: Introduction to threat modeling frameworks, such as STRIDE, with specific examples for military



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

platforms like armored vehicles and missile systems.

- o Understanding the Security Scope and Environment for Defense Platforms:
How to define secure boundaries and identify critical operational interfaces vulnerable to cyberattacks.

- **Asset Mapping and Threat Analysis for Defense Systems**

- o Identifying and classifying critical assets in defense platforms, including data, software, and communication interfaces.

- o Developing Threat Scenarios: Creating scenarios to evaluate potential cyberattacks, identify attacker motivations, and define effective controls.

- o Risk Management and Prioritization: Assessing and prioritizing threats based on their potential impact on weapon system functionality and mission-critical capabilities. Developing strategies for rapid response and damage mitigation.

Day 5: Defining Defense Controls and Cybersecurity Solutions According to Customer Specifications - Engineering and Management Considerations

In this module, system engineers and project managers will learn how to define concrete defense controls and cybersecurity solutions according to customer specifications, while considering engineering (such as performance, integration) and management (such as cost, schedules) considerations. We will discuss different types of defense controls and the criteria for selecting the most appropriate solutions for customer requirements and project constraints.

Topics and Standards to be Learned in this Module:

- Overview of key defense control types (technical and managerial) relevant to military systems
- Criteria for selecting defense controls and cybersecurity solutions according to customer requirements (functionality, cost, performance, ease of



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

implementation)

- Defining requirements for the integration of security solutions into the overall system
- Engineering considerations in implementing defense controls (impact on performance, resource consumption)
- Management considerations in selecting security solutions (cost, availability, support)
- Practice in defining basic defense controls for given customer requirements
- Understanding the decision-making process regarding the selection of security solutions while considering customer requirements and project constraints
- **Cybersecurity Controls for Military Platforms**
 - Overview of Defense Controls: Understanding controls such as encryption techniques, access management, and intrusion detection systems unique to military environments.
 - Defense in Layers and Redundancy: How layered defense is critical for preventing, detecting, and responding to cyberattacks on military systems.
- **Cyber Architecture for Weapon Systems**
 - Designing Resilient Architectures: Focusing on designing cyber-resilient architectures with redundancy, segmentation, and defenses capable of withstanding sophisticated cyberattacks.
 - Discussion on maintaining operational capability even when parts of the system are compromised.
 - SCADA/ICS Security for Defense: Overview of strategies for securing SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems) for critical military assets such as missile control, submarine operation, and other command and control systems.



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

Day 6: Verification, Testing, and Documentation of Security Solutions

According to Customer Requirements - The Role of Engineers and Project Managers

In this module, system engineers and project managers will learn about the importance of verifying and testing the security solutions defined according to customer requirements. We will focus on their role in planning and managing verification and testing processes, as well as the importance of complete documentation of security solutions for the customer. In addition, incident response and mission continuity are also discussed in details. The goal is to equip participants with the ability to ensure that the implemented solutions indeed meet customer requirements.

Topics and Standards to be Learned in this Module:

- Importance of verifying and testing security solutions according to customer requirements
- Role of system engineers and project managers in planning and managing verification and testing processes
- Overview of basic testing methods for verifying security solutions
- Importance of complete and accurate documentation of security solutions for the customer
- Preparing specification and definition documents for security solutions according to customer requirements
- Practice in writing basic test requirements for security solutions
- Understanding the process of delivering security solution documentation to the customer
- Validation and Testing of Cyber Defenses in Military Systems



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

- Regulatory Requirements for Validation: Understanding the importance of validating that defense systems meet cybersecurity requirements against a range of threats.
- Testing Considerations for Military Platforms: Addressing the unique challenges of testing military systems, such as testing under operational load, ensuring availability during critical operations, and planning for deployments in harsh environments.
- Response Planning and V&V Testing
 - Overview of Red Team/Blue Team Exercises: Introduction to active defense strategies, such as simulated attack exercises, to assess the resilience of defense systems.
 - Cyber Incident Response Planning in Military Systems: Discussion of effective response plans for cyber incidents affecting military operations – focusing on how to contain and mitigate the threat while maintaining mission-critical capabilities.
 - Maintaining System Functionality During Attacks: Techniques for ensuring operational continuity and mission assurance even under sustained cyberattacks.
- Incident Response & Mission Continuity
 - Cyber incident response planning
 - Military-specific considerations
 - How to test incident response?
 - Maintaining mission continuity during attacks
 - Resilience testing
 - Documentation



When innovation meets expertise...