FOR MEMBER USE ONLY
SECURITY SERIES

SEC-06 Applied OPSEC: Analytical Method and Field Application

Analytical Method and Field Application -- seven lessons, seven worksheets, one written countermeasure plan.

BOTTOM LINE UP FRONT

OPSEC fails silently. Most households and groups that believe they are operationally secure have never identified their critical information, modeled a realistic adversary, or inventoried the indicators their behavior already broadcasts. SEC-06 runs the complete five-step OPSEC analytical process -- from a named Critical Information List through a documented threat model, a full indicator inventory, a dual-channel exposure audit, and a written countermeasure plan. Every lesson produces worksheet output. By Lesson 7 you have a working OPSEC baseline.

WHY THIS MATTERS

Most preparedness groups make high-stakes security decisions without a documented process. SEC-06 gives you a repeatable, auditable method that holds up under scrutiny.

When a threat assessment is wrong, the consequences fall on your people. The OPSEC process prevents that by forcing the analysis into daylight where assumptions, gaps, and leaps become visible and correctable. By the end of this course you have a documented baseline -- CIL, threat matrix, indicator inventory, exposure audits, and countermeasure plan -- that is auditable, challengeable, and updatable.

► **There is no other course in the preparedness space that runs the complete OPSEC five-step analytical process from doctrinal sources, applied to household and group security. This is the only one.**

THE SEVEN LESSONS

1	**The OPSEC Process** The five-step analytical cycle, why sequence is mandatory, and what each step produces. Introduces Worksheet 1-A: first-draft critical information baseline.
2	**Critical Information** EEFI identification, the adversary test, category classification, and producing a finalized Critical Information List of fewer than 12 items. Worksheet 2-A.
3	**Threat Identification** Adversary tiers, capability versus intent, and mapping collection disciplines to your critical information. Worksheet 3-A: threat matrix.
4	**Vulnerabilities and Indicators** Cataloging every observable indicator and solving the aggregation problem -- why individually harmless details are dangerous in combination. Worksheet 4-A.
5	**Your Digital Signature** Platform inventory, username linkage, EXIF and metadata, device emissions, cross-referenced against your CIL. Worksheet 5-A.
6	**Your Physical Signature** Property, vehicle, routine, and disposal signatures. What an external observer sees, and how physical patterns combine into exploitable profiles.
7	**Applying Countermeasures** Action, control, and deception measures. Prioritization matrix, digital and physical action tables, and a recurring review schedule.

HOW EACH LESSON WORKS

Doctrine first	Every concept is grounded in its source: DoDD 5205.02E, AR 530-1, JP 3-13.3, DoDM 5205.02-M. You learn why the method works, not just what the steps are.
Application second	Each lesson translates the concept to a realistic household or group security scenario, with a worked case study and a field drill tied to the companion guide worksheet.
Knowledge checks	Questions test application, not recall. Correct answers include the full reasoning. Wrong answers direct you back to the relevant section.
Prerequisites	SEC-02: Know What You're Showing, or equivalent. No prior intelligence or military background required. Estimated completion: 18-22 hours over 3-5 weeks self-paced.