SECURITY SERIES · SEC-05

# SEC-05 — Internal Security and Counterintelligence

Detection · Compartmentalization · Remediation

*Detecting compromise before it costs the group everything*

**BOTTOM LINE UP FRONT**

SEC-05 is the group's second line of defense against insider compromise — detecting the signs, bounding the damage through compartmentalization, and running a real audit that ends in remediation. It is not the individual-level cultivation-recognition training taught in SEC-12, and it does not replace it; the two are meant to run together.

## Why This Matters

Individual awareness training reduces cultivation attempts. It does not guarantee none succeed. A patient, competent effort can still succeed against one member — and without a second line of defense, that single compromise reaches everything that member can see.

> *"A compromised member can only hand over what they actually know — compartmentalization decides how much that is."*

## THE KEY CONCEPTS

| | |
|---|---|
| **Compromise (as a rate)** | Not a failure of vigilance — given enough time, some percentage of any group's people will eventually be cultivated, coerced, or worn down. |
| **Behavioral & Procedural Indicators** | Behavioral: sudden secrecy, unexplained spending, a shift in mood. Procedural: access-seeking outside a member's actual role. |
| **Compartmentalization** | Structuring who knows what by actual role-based need, not trust or seniority — a bound on damage, not a statement about trust. |
| **Structured Audit** | A scheduled review producing a documented finding and one of three concrete remediation steps, not a vague impression. |

## COURSE LESSONS

**Lesson 1: Detecting Indicators of Compromise**
The two categories of warning signs, and the pattern-over-single-tell principle that separates real signal from ordinary noise.

**Lesson 2: Compartmentalization and Need-to-Know**
Bounding damage by mapping who actually needs to know what, and holding that line against social pressure.

**Lesson 3: Running the Structured Security Audit**
From detection to remediation: review cadence, a full worked case, and the three concrete outcomes an audit must produce.

## DOCTRINAL SOURCES

| Source | Publisher | Relevance |
|---|---|---|
| No single named field manual cited in this build | FFTP synthesis | Content synthesizes general counterintelligence tradecraft rather than one named manual; add a citation once a source is confirmed. |