



THREAT SUPPRESSION, INCORPORATED

THREAT SUPPRESSION®

Corporate Headquarters: 525 North Tryon Street, Suite 1600 | Charlotte, NC 28202 | USA

Corporate Mailing Address: Post Office Box 57 | Fort Mill, SC 29715 | USA

Phone: 800.231.9106 **Web:** www.ThreatSuppression.com **E-Mail:** info@ThreatSuppression.com

Grab the Snake by the TALE™: Threat Assessment for Law Enforcement

Executive Summary:

Threat information rarely arrives as a complete, clear account. Investigators may receive a concerning message, a reported grievance, fixation on a target, a sudden behavioral change, unusual preparation, or a third-party concern. The challenge is to determine what those fragments mean, what must be verified, what information should be shared, and what action is justified.

Grab the Snake by the TALE gives law-enforcement personnel a practical framework for turning scattered information into disciplined threat-assessment work. Participants learn to recognize warning behavior, evaluate the context and credibility of information, connect indicators across people and systems, and select lawful, proportionate next steps. The course applies research and operational material involving adolescent and adult perpetrators, school and workplace violence, active assailant behavior, domestic terrorism, and homegrown violent extremism.

THE CHALLENGE: Law enforcement officers encounter a variety of complaints made about threats. It is often difficult to discern the immediacy and urgency of threats. This training provides an overview of threat assessment and different tools available for law enforcements officers, from patrol officers to criminal investigators.

Instructional Team:

This course is taught by Dr. Angelo Sambunaris, a 40-year practicing forensic psychiatrist and professor of neuropharmacodynamics. Dr. Sambunaris is a retired Lieutenant Colonel, with multiple years of service with the 19th Special Forces group and the U.S. Public Health Service. Dr. Sambunaris is the chief hostage negotiator with the North Fulton County SWAT Team in Atlanta, Georgia. The course is also co-taught by Dr. Mike Clumpner, who has a PhD in homeland security and is an ATAP board-certified threat manager (CTM). Dr. Clumpner is also a 17-year law enforcement veteran, certified criminal investigator, and has spent more than 20 years researching mass violence attacks.

Course Overview:

Length	16 hours (two days)
Format	Dual instructor-led presentation with facilitated discussion, multiple case-based examples, guided investigative questions, threat-information timelines, and practical decision exercises.
Audience	School and higher education administrators, SROs, counselors, social workers, BTAM team members, law enforcement investigators, and intelligence analysts.
Class Size	Host-specific. The lecture format has no fixed enrollment limit; final attendance and room requirements are confirmed during scheduling. For best interaction and participation, courses are recommended capped at 50 students.
Prerequisites	No specialized prerequisites. Participants should have a working knowledge of criminal investigation, school safety, or public safety operations.
Cost	\$19,999 for two instructors for two days. Travel and lodging are additional; government discounts and virtual delivery rates are available.

What Participants Will Learn:

The TALE™ Framework

T — Track the signal	Recognize concerning communications and behaviors, including grievances, fixation, leakage, target references, escalation, and changes from baseline. Preserve source, timing, context, and reporting details.
A — Assess the threat	Evaluate credibility, intent, capability, access, target specificity, preparation, time frame, protective factors, and signs of acceleration. Separate what is known from inference and uncertainty.
L — Link the information	Connect relevant people, locations, communications, online activity, prior incidents, capability indicators, associates, grievances, and possible reconnaissance. Look for convergence across information sources.
E — Engage and act	Select lawful, proportionate, operationally sound steps such as interviewing, corroborating, notifying, referring, protecting, disrupting, documenting, and reassessing. Threat assessment is an ongoing process, not a one-time label.

What the Course Covers

- Threat leakage, common communication channels, and the seven-step leakage pathway of warning behavior.
- Warning behaviors and pre-attack indicators, including fixation, identification, novel aggression, pathway behavior, last-resort behavior, and energy-burst behavior.
- Patterns and differences across adolescent active assailants, adult workplace offenders, domestic terrorists, and homegrown violent extremists.
- Grievance development, target selection, surveillance, capability development, preparation, and escalation.
- Threat-assessment team roles, activation triggers, investigative responsibilities, information sharing, documentation, and case management.

- Workplace, educational, and public-sector violence concerns, including bullying, harassment, stalking, domestic disputes, and employee conflict.
- The limits of profiling and single-factor explanations, including the need to assess evidence in context rather than rely on diagnosis, identity, or appearance.

Practical Application

Participants work through case material and structured decision points. They build threat-information timelines, separate facts from assumptions, identify information gaps, develop investigative questions, and explain why information does or does not support a credible threat concern. Exercises address digital information in context, cross-agency information sharing, decision documentation, and reassessment triggers.

Learning Objectives:

At the conclusion of the program, participants will be able to:

1. Explain the purpose and limits of behavior-based threat assessment and describe why profiling and single-indicator judgments are unreliable.
2. Recognize threat leakage and warning behaviors and distinguish them from generalized concern or protected expression.
3. Apply the TALE framework and leakage pathway to organize and assess reported information.
4. Evaluate threat credibility using intent, capability, access, specificity, preparation, time frame, corroboration, and protective factors.
5. Identify indicators of target selection, pre-attack information gathering, preparation, and escalation.
6. Develop investigative questions that test the reliability, meaning, and context of threat information.
7. Connect relevant information across people, places, communications, online activity, grievances, and prior conduct.
8. Identify threat-assessment team roles, activation triggers, information-sharing needs, and reassessment requirements.
9. Document facts, assumptions, uncertainties, actions, and rationale, then communicate a concise threat picture and recommended next steps.

Host Agency Requirements:

The host agency is responsible for providing a suitable classroom or virtual learning environment, a computer, projector, and audio for in-person delivery. The host should confirm that the classroom is available for the full scheduled program and that participants can engage in confidential, professional discussion of sensitive material. If the course is delivered virtually, the host should provide a reliable platform, a technical point of contact, and a participant environment that supports discussion and case-study review.

Because this course addresses behavioral threat assessment and adolescent violence, the host should identify applicable reporting procedures, emergency contacts, behavioral threat assessment team members, and local policies before delivery. Hosts should also determine how questions involving a specific student, employee, patient, or community member will be referred for appropriate clinical, legal, or investigative review. The course is lecture and discussion based; live weapons, tactical equipment, or a practical response area are not required unless a separate exercise or practical component is commissioned.

Threat Suppression provides education and preparedness support. This presentation is not clinical diagnosis, psychotherapy, legal advice, or a substitute for agency policy, medical or mental-health care, legal counsel, or a formal threat assessment conducted by qualified professionals. The host remains responsible for its own policies, reporting obligations, clinical governance, operational decisions, and compliance with applicable law.

About Threat Suppression:

Threat Suppression, Incorporated is a research-driven safety, security, and public-safety training and consulting firm founded in 2012. The company is a leading provider of integrated active assailant training for the Department of War, providing more than 165 classes at 45 major installations. The company has invested more than 50,000 hours in internal active assailant research. Threat Suppression serves as a principal member of NFPA 3000 and participates in multiple state and federal ASHE workgroups that shape national active assailant preparedness standards and policy.

The company's leadership has commanded active assailant events and was lead author on the 2021 Oxford High School mass shooting after-action report, one of the most comprehensive analyses of an active assailant incident response. Threat Suppression provides active assailant preparedness, rescue task force training, emergency management support, behavioral threat assessment and management, exercises, after-action reviews, and physical security services to federal agencies, military installations, public safety organizations, healthcare systems, schools, and private organizations. Our work combines operational experience, applied research, and field-tested instruction.

To Schedule or Learn More:

Phone: 1-800-231-9106

Email: info@ThreatSuppression.com

Course Page: <https://www.threatsuppression.com/threat-assessment-for-law-enforcement>

Website: www.threatsuppression.com