24
Bt
Behavioral Threat
by
24
Sp
Securepassage

Behavioral Threat Assessment

Safety Through Insight

The first organization to discern the presence of prior signs of targeted violence in schools was the U.S. Secret Service (USSS), which – thanks to its core mission of protecting American presidents from would-be assassins – excels at the science of assessing human behaviors, communications, and actions for early indications of threat. Following the Columbine tragedy, a joint team of USSS and U.S. Department of Education (DOE) experts spent two years combing through historical data on school shootings, looking for patterns and trends that would lead them to a more effective approach to proactively identify and prevent – rather than merely respond to – school mass casualty events. Those findings were conglomerated into a report, *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates*, concluding that "it may be possible to prevent some future school attacks from occurring – and that efforts to identify, assess, and manage students who may have the intent and capacity to launch an attack may be a promising strategy for prevention."

The Secure Passage Approach

We are passionate about public safety in general, and school safety in particular. More than a decade ago, we designed and launched our first school safety solution for managing campus risk, based on in-depth discussions with district leaders, school administrators, security directors and district police chiefs, campus law enforcement personnel, counselors, teachers, and operations staff.

In 2018, Haystax (now Secure Passage) developed its first behavioral threat assessment application for schools at the request of a district security director who was already using our core school safety platform apps to protect nearly 30,000 students, plus more than 2,000 staff and faculty, at dozens of campuses and facilities. The behavioral assessment app is still in use today and has provided the district with a robust platform for identifying, assessing, and managing behavioral threats of all types and a secure repository of data, plus supporting records, on all open and closed cases.

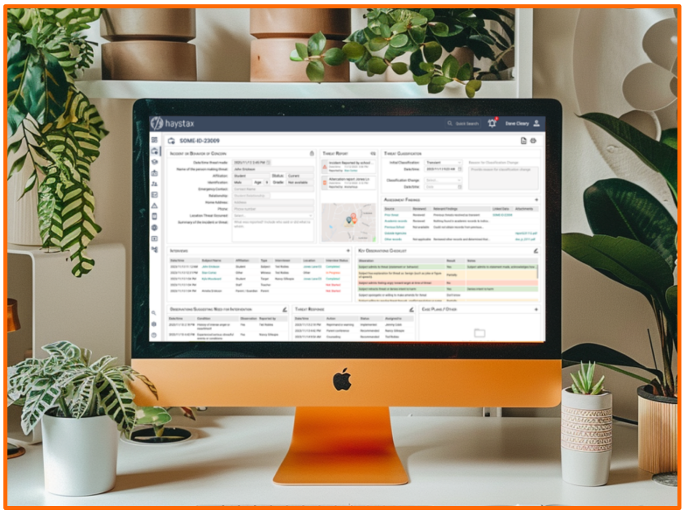
Overview: School Behavioral Threat Assessment

Our newest solution, the School Behavioral Threat Assessment (SBTA), has been designed from the ground up to provide administrators, security directors, mental health professionals, and other assessment team members with the intelligence and insights they need to make evidence-based decisions regarding emerging campus security threats in time to avert a more serious crisis – providing *Safety Through Insight*.

Behavioral Threat Assessment

Safety Through Insight

The SBTA Solution



- Configured to reflect the unique requirements of each district or state, taking account of existing systems, workflow, investigative approaches, assessment frameworks and team structures.
- Built with functionalities and workflows that are housed in a series of tightly integrated applications, wrapped in a case management module that support incident reporting, verification, investigation, assessment, recommendation, and resolution.
- Allows users to analyze data across multiple cases to glean deeper insights on emerging trends and shifts in behavioral threat assessment patterns, and to report tailored results to a broad array of stakeholders.
- Built on a separately hosted SaaS platform that employs robust data encryption protocols and strict user access controls, all data resident in the SBTA 'ecosystem' is secured against unauthorized access. Personally Identifiable Information (PII) and other sensitive information is kept behind a wall, ensuring compliance with current regulations regarding student privacy and mental health.
- Generate reports from asset, assessment, incident, and event data and share with school leadership and the community stakeholders, as you require.
- Case Management-Friendly – At the heart of our solution is a task-centered case management module that enables users to:
    - Review and validate incoming incident reports.
    - Open a case.
    - Enter information on students, staff, or other individuals relevant to the case.
    - Eliminate information silos by designating team members and their roles.
    - Assign member tasks using preset templates or create custom tasks.
    - Upload files and integrate third-party data as supporting evidence.
    - Evaluate the threat using a commonly accepted assessment framework.
    - Determine the response – and intervention if any.
    - Implement the chosen response.
    - Submit the case for review, and make further amendments, if needed.
    - Close the case.
    - Analyze case records and submit reports to key stakeholders.