24
Sp
Securepassage

The School Behavioral Threat Assessment Solution

A TOOL FOR PROACTIVE CAMPUS VIOLENCE PREVENTION

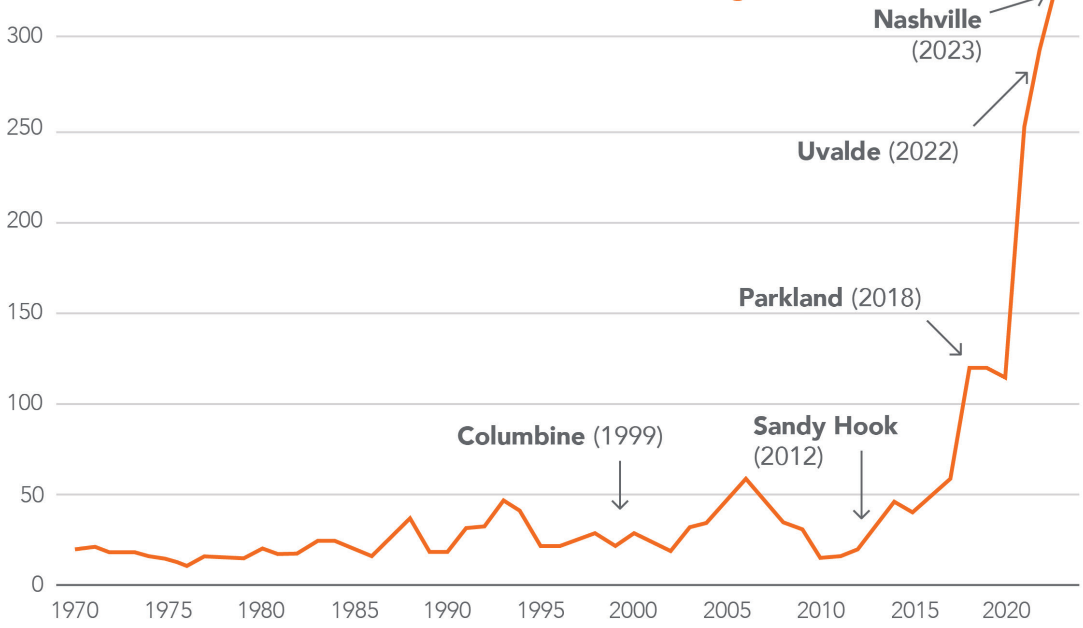
Introduction

The Rise of Campus Violence

In the 25 years since two teenagers killed a teacher and 12 of their fellow students and wounded 21 others at Columbine High School in Littleton, CO, large-scale attacks on K-12 school campuses in the U.S. have become both deadlier and more frequent.

That trend started accelerating exponentially in 2018. According to the K-12 School Shooting Database, in 2023 alone there were a record 346 campus shooting incidents *(see chart below)*. And those grim statistics do not even account for non-firearm violence like stabbings or blunt-force traumas.

Number of Incidents by Year



Shooting Incidents by Year 1970 - 2023. Source: K-12 School Shooting Database.

The deadliest threats are known as "targeted violence," and they rarely come out of the blue. In fact, individuals who commit targeted violence – as opposed to spontaneous or impulsive violence – typically exhibit some kind of concerning behavior days, weeks or sometimes even years before the attack itself.

Assessing School Threats

The first organization to perceive the utility of investigating prior signs of targeted violence in schools was the U.S. Secret Service. Thanks to its core mission of protecting American presidents from would-be assassins, the agency excels at the science of assessing human behaviors, communications and actions for early indications of a threat.

Following the Columbine tragedy a joint team of Secret Service and U.S. Department of Education (DOE) experts spent two years combing through historical data on school shootings, looking for patterns and trends that could lead to more effective approaches for proactively identifying and preventing, rather than merely responding to, school mass casualty events.

In May 2002 the agencies published a landmark report, *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates*, which found that “incidents of targeted violence in school were rarely impulsive; that the students who perpetrated these attacks usually planned out the attack in advance – with planning behavior that was oftentimes observable; and that, prior to most attacks, other children knew that the attack was to occur.”

Based on their findings about the prior ‘knowability’ of these acts, the report’s authors advocated for applying long-accepted risk assessment principles to schools, while simultaneously stressing the importance of fostering safe school climates where students would feel empowered to share their concerns.

With a safe climate and the right assessment procedures and reporting policies in place, the report concluded 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 Case for Behavioral Threat Assessments

The use of risk assessments in the American criminal justice system dates back to the early 1900s, when parole officers were seeking reliable ways of predicting the behavior of soon-to-be released prisoners.

In the intervening 100-plus years risk assessments have been applied to many other security realms, accompanied by the evolution of more systematic, comprehensive and 'predictive' assessment techniques that rely heavily on quantifiable evidence and data analysis.

Efforts to adapt modern behavioral threat assessment methodologies to school environments began soon after Columbine. For example, the Virginia Center for School and Campus Safety (VCSCS), created in 2000 under the Virginia Department of Criminal Justice Services, was an early pioneer in the development of comprehensive school safety policies, procedures, resources and training, including behavioral assessments. Today it is the go-to service center for K-12 schools, institutions of higher learning and law enforcement agencies – not just for the state but nationwide.

While the 2002 Secret Service/DOE report crystalized the need for behavioral threat assessments, it took the 2018 surge in high-profile campus violence to accelerate the trend. Current campus threat assessment methodologies are variously described as guidelines, frameworks or models, but they all still rely on the Secret Service's 'identify-assess-manage' construct to more predictively and proactively prevent school violence *(see sidebar on page 6)*.

Do Assessments Work?

The body of empirical research on school threat assessment effectiveness is sparse, but what little there is supports the argument that assessments can prevent violence in many cases.

The best-known example of empirical testing came from the work of Dr. Dewey Cornell of the University of Virginia, who examined more than 23,000 student threat assessments conducted in Florida schools during the 2021-2022 academic year. (One of the largest school shootings in U.S. history had taken place in February 2018 at Marjory Stoneman Douglas High School in Parkland, Florida.)

Dr. Cornell's research, underwritten by the U.S. Department of Justice, found that "the ongoing implementation of school threat assessment in Florida has been widely, but not uniformly, successful," leading to effective interventions in the majority of cases. From a safety perspective, relatively few threats (5.9%) were carried out and very few (0.23%) resulted in someone being seriously injured. As for effectiveness, 90% of assessed students were able to remain in their original schools.

The general conclusion from Dr. Cornell and other school shooting investigations is that assessments can be effective, provided they are thoughtfully designed and implemented, and properly staffed.

Assessment Teams are Vital

Behind every successful assessment is a multi-disciplinary (and sometimes multi-jurisdictional) team with a clearly designated leader. This team has the heavy responsibility of evaluating threats, selecting appropriate responses and implementing tailored plans to prevent further violence.

This team has the heavy responsibility of evaluating threats, selecting appropriate responses and implementing tailored plans to prevent further violence.

An assessment team is typically led by a senior administrator and includes an investigator (e.g., a school resource officer or other sworn law enforcement personnel), a representative of the school administration and a mental health specialist, plus other individuals who regularly interact with students, such as teachers, guidance counselors, sports team coaches and even custodial staff.

The team should make an effort to build relationships outside the campus perimeter, especially with law enforcement agencies but also with local clergy, sports and community leaders and others who may be familiar with a particular student or group of students.

One team member should also be designated as the single point of contact for any reports originating from students or family or the community, and his or her identity should be widely publicized, both on-campus and beyond.

To date, according to the advocacy group Everytown for Gun Safety, nine U.S. states have adopted laws requiring school threat assessment teams: Florida, Kentucky, Maryland, Ohio, Pennsylvania, Rhode Island, Texas, Virginia and Washington. Several other state legislatures are considering such measures.

THE NTAC ASSESSMENT MODEL

One of the most commonly used methodologies for conducting behavioral threat assessments in U.S. schools today is the National Threat Assessment Center (NTAC) model for comprehensive targeted violence prevention, developed in the aftermath of Columbine by a unit of the same name under the Secret Service.

The model specifies eight steps to creating a targeted-violence prevention plan:

STEP 1 Establish a multi-disciplinary threat assessment team that will direct, manage and document the threat assessment process.

STEP 2 Define behaviors, including those that are prohibited and should trigger immediate intervention as well as other concerning behaviors that require a threat assessment.

STEP 3 Establish and provide training on a central reporting system, ensuring that it provides anonymity to those who report concerns and is monitored by personnel who will follow up on all reports.

STEP 4 Determine the threshold for law enforcement intervention, especially if there is a safety risk.

STEP 5 Establish threat assessment procedures that include practices for maintaining documentation, identifying sources of information, reviewing records and conducting interviews. Investigative themes guiding the assessment process include motivations, threatening communications, inappropriate interests, access to weapons, stressors, signs of despair, tendencies towards violence, concerning behaviors, signs of attack planning and lack of social connections or relationships.

STEP 6 Develop post-assessment risk management options, including individualized risk mitigation and stress reduction plans. Notify law enforcement immediately if the student is thinking about an attack, and ensure the safety of potential targets.

STEP 7 Create and promote a safe school climate by encouraging communication, intervening in conflicts and bullying and empowering students to share their concerns.

STEP 8 Provide training for all stakeholders, including school personnel, students, parents and law enforcement.

NTAC provides greater flexibility and open-endedness in conducting behavioral threat assessments in schools than some of the other more structured and guided approaches. In addition, NTAC typically involves a broader community of interest while other approaches rely primarily on school personnel, at least for the less serious cases. The choice of models will depend on the specific needs and preferences of the school district, as well as the level of experience and support available for conducting threat assessments.

The Secure Passage Approach

At Secure Passage, 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.

At Secure Passage, we are passionate about public safety in general, and school safety in particular.

In 2014, we deployed the platform as a statewide solution in Florida. Known as the Florida Safe Schools Assessment Tool (FSSAT), the solution initially focused on managing school asset information and conducting physical security assessments at approximately 4,200 public schools and 700 charter schools across all 67 districts in the state. FSSAT capabilities have since grown to encompass incident alerting, mobile field reporting, event scheduling, safety drill management and digital monitoring and analysis of third-party data.

In addition to Florida, our school safety solution has been deployed in K-12 districts and regional government agencies in California, Texas, Virginia, Arizona, Indiana and elsewhere.

Our company's history with behavioral threat assessments dates back even further. In 2008 we were tasked by the Pentagon with providing evidence-based analytics for assessing terrorist risk, and in 2011 we started working with the Gates Foundation to assess a growing number of personal threats to Bill and Melinda Gates and their family members. Within two years our data scientists had additionally developed a software-based predictive model for identifying potential insider threat behaviors, which has been used by leading banks, government agencies and other large organizations.

In 2018 we developed our 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, across several dozen campuses and facilities.

That behavioral assessment app is still in use today and has provided the district's leaders with a robust platform for identifying, assessing and managing behavioral threats of all types, plus a secure repository of data and supporting records on all open and closed cases.

Overview: Secure Passage School Behavioral Threat Assessment

Our newest solution, the School Behavioral Threat Assessment, or 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.

The solution can be configured to reflect the unique requirements of each district or state, taking into account existing policies, systems, workflows, investigative approaches, assessment frameworks and team structures.

All functionalities and workflows within the SBTA platform are housed in a series of tightly integrated modules, wrapped in a case management application, that support the nationally recognized 'identify-assess-manage' behavioral assessment framework first promulgated by the Secret Service *(see sidebar next page)*.

Additionally, the SBTA allows users to analyze data across multiple cases to glean deeper insights on emerging trends and shifts in behavioral threat patterns, and to report relevant results to a broad array of stakeholders.

Because it is 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.

FUNCTIONAL MODULES

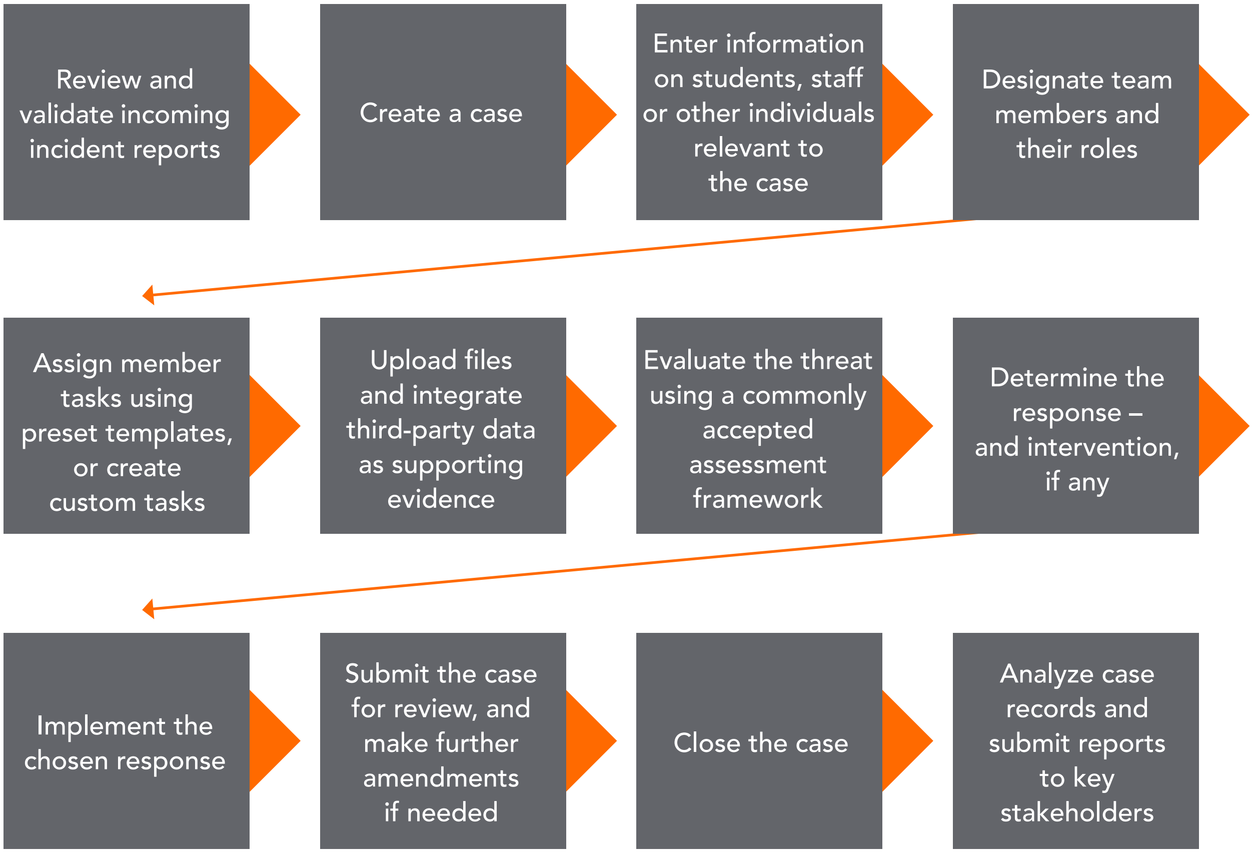
Individual SBTA modules and their roles are as follows:

- The *Case Management* app provides high-level data on all in-progress and closed cases as well as rapid access to each individual case.
- Next is a series of modules for managing data on *Students, Staff, Other Individuals* (e.g., law enforcement) and *School Facilities* involved in specific cases.
- The *Tasks* module enables team leads to assign individual tasks to assessment team members and others, and monitor progress on each task.
- The *Assessments* module houses various forms used in interviews and mental health assessments.
- The *Threat Reports* module is the environment for: a) capturing significant incidents, such as tips generated via third-party data sources like anonymous reporting apps, emails, texts, phone calls or direct conversations; and b) storing alerts from SROs and campus security personnel equipped with the *Field Reports* mobile app. This module also serves as a repository for any additional incoming evidence regarding threatening statements, behaviors or actions.
- The *Events* module is used in a supporting role to verify the existence of scheduled events where some threat incidents may have taken place.
- Third-party data with potential relevance to a particular case – such as news reports, social media posts or other online or third-party information – is collected via the *Data Streams* module, and data that may yield useful evidence is then uploaded to the *Threat Reports* module.

Key information on case lists, people, incidents, tasks, interviews, assessment findings and observations is displayed on the SBTA *Dashboard* for easy visualization and overall case management. The same data is also viewable on a built-in *Map*, providing geo-visual context for the district and its surrounding regions. For seamless navigation, each data type is tagged and hyperlinked so that data can be entered once but then be accessible across every module in the platform and in the *Dashboard*.

Case Management

At the heart of our solution is the task-centered case management app, which enables users to:



Review and validate incoming incident reports

Create a case

Enter information on students, staff or other individuals relevant to the case

Designate 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

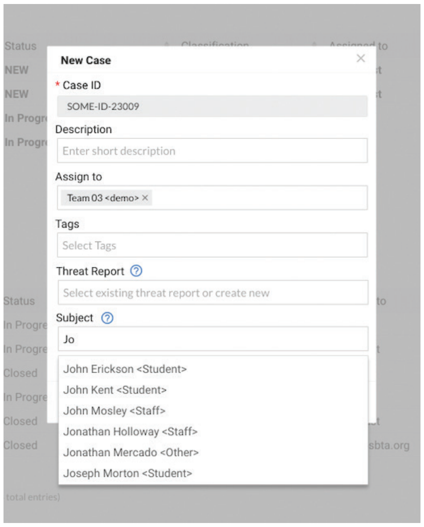
Determine the response – and intervention, if any

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



New Case

* Case ID: SOME-ID-23009

Description: Enter short description

Assign to: Team 03 <demo> ×

Tags: Select Tags

Threat Report: Select existing threat report or create new

Subject: Jo

John Erickson <Student>
John Kent <Student>
John Mosley <Staff>
Jonathan Holloway <Staff>
Jonathan Mercado <Other>
Joseph Morton <Student>

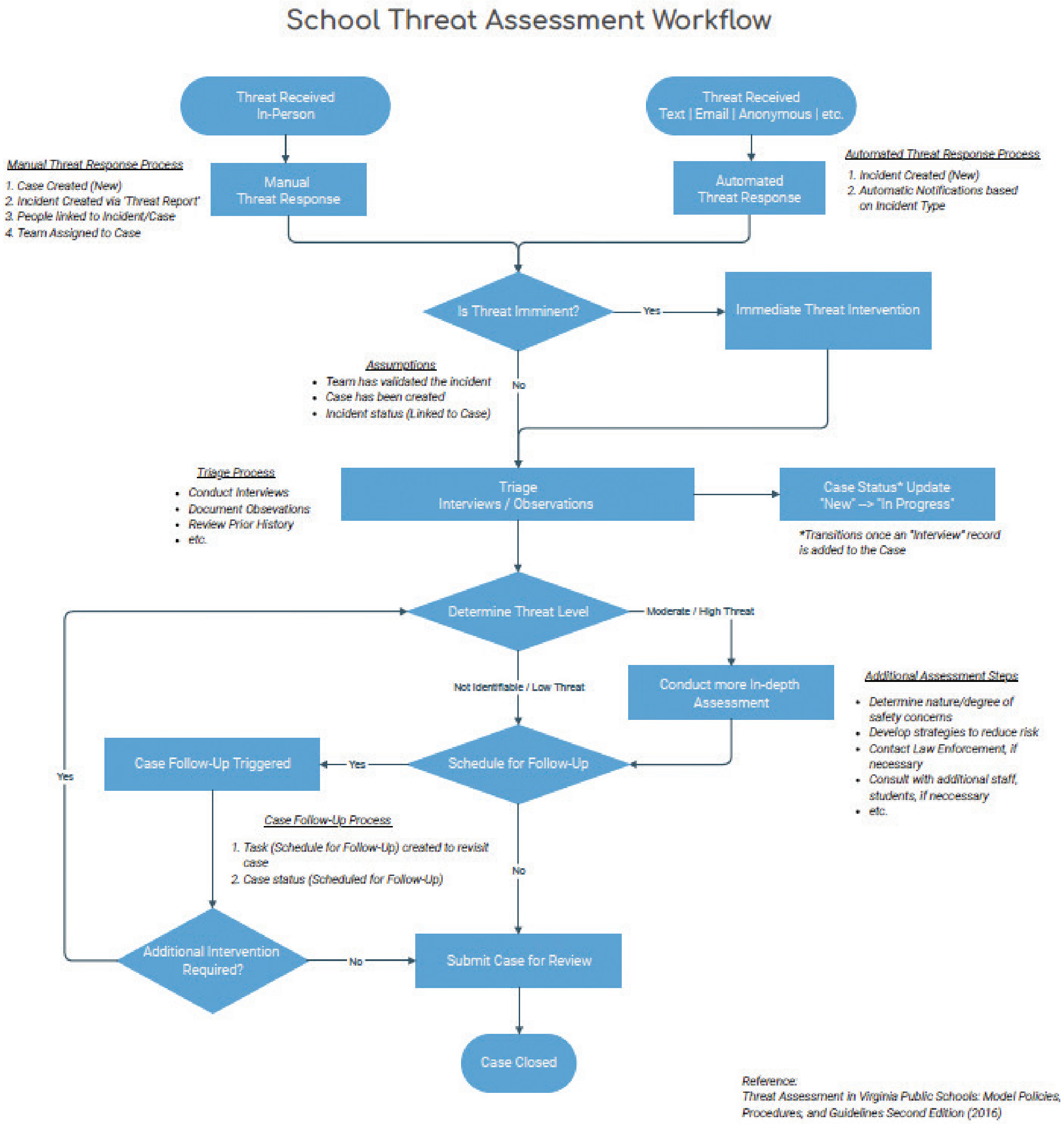
Cases can be created from the Cases list page, and also from an incident or field report.

In order for a case to be created, a report must be received – either by being entered manually or ingested automatically from linked data sources – indicating that an adverse incident or concerning behavior has occurred.

Designated assessment team members are immediately notified, so they can meet to assess the incident's validity. Invalid or not-applicable incidents are archived but if an incident is deemed to pose a valid threat, the team opens a case *(see image at left)*.

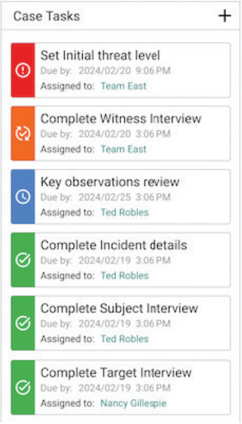
The SBTA assessment workflow *(see image next page)* has been designed to support any size of school district and any number of team members.

A typical case workflow.


School Threat Assessment Workflow
Threat Received In-Person
Threat Received Text | Email | Anonymous | etc.
Manual Threat Response Process
1. Case Created (New)
2. Incident Created via 'Threat Report'
3. People linked to Incident/Case
4. Team Assigned to Case
Manual Threat Response
Automated Threat Response
Automated Threat Response Process
1. Incident Created (New)
2. Automatic Notifications based on Incident Type
Is Threat Imminent?
Yes
Immediate Threat Intervention
Assumptions
Team has validated the incident
Case has been created
Incident status (Linked to Case)
No
Triage Process
Conduct Interviews
Document Observations
Review Prior History
etc.
Triage Interviews / Observations
Case Status* Update "New" --> "In Progress"
*Transitions once an "Interview" record is added to the Case
Determine Threat Level
Moderate / High Threat
Conduct more In-depth Assessment
Additional Assessment Steps
Determine nature/degree of safety concerns
Develop strategies to reduce risk
Contact Law Enforcement, if necessary
Consult with additional staff, students, if neccessary
etc.
Not Identifiable / Low Threat
Yes
Case Follow-Up Triggered
Yes
Schedule for Follow-Up
Case Follow-Up Process
1. Task (Schedule for Follow-Up) created to revisit case
2. Case status (Scheduled for Follow-Up)
No
Additional Intervention Required?
No
Submit Case for Review
Case Closed
Reference:
Threat Assessment in Virginia Public Schools: Model Policies, Procedures, and Guidelines Second Edition (2016)

The team leader's first act is to assign tasks to individual team members. Task examples include:

- Importing and reviewing relevant information on alleged perpetrators, such as their attendance records and grades, records of prior incidents and counselor evaluations.
- Scheduling and conducting interviews with the alleged perpetrator plus any intended victims, and collecting statements from students, staff and others (e.g., law enforcement, parents, etc.) who may have witnessed the threat or possess knowledge of important aspects of the case.
- Reviewing social media posts or other evidence for additional context surrounding the incident.
- Collecting videos, documents or other case-relevant files.



Case Tasks +

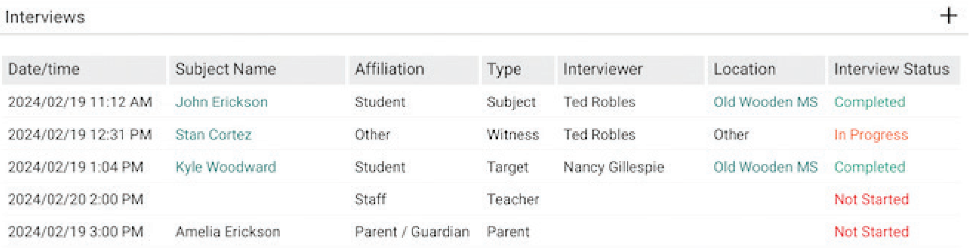
- ⓘ Set Initial threat level
  Due by: 2024/02/20 9:06 PM
  Assigned to: Team East
- Complete Witness Interview
  Due by: 2024/02/20 3:06 PM
  Assigned to: Team East
- Key observations review
  Due by: 2024/02/25 3:06 PM
  Assigned to: Ted Robles
- ✓ Complete Incident details
  Due by: 2024/02/19 3:06 PM
  Assigned to: Ted Robles
- ✓ Complete Subject Interview
  Due by: 2024/02/19 3:06 PM
  Assigned to: Ted Robles
- ✓ Complete Target Interview
  Due by: 2024/02/19 3:06 PM
  Assigned to: Nancy Gillespie

Color-coded task lists make it easy to track assignees, schedules and progress.

Each task *(see image at left)* is given a due date, and automated reminders are sent to each team member (e.g., that the deadline for submitting a witness interview form is approaching). Other notification types include case status changes, such as scheduling shifts or the arrival of new evidence. Depending on the customer's preference, notifications can originate from within the SBTA module or be sent via email or via text message – or all three.

During evidence collection, data for each case can be ingested automatically, entered manually or uploaded as files of any format (e.g., documents, photos and videos).

At this stage, teams begin interviewing alleged perpetrators, victims or witnesses using forms pre-populated in the SBTA. Interview data can be entered on-screen as an interview is taking place, written down on a pre-printed interview form, or drafted as written notes and entered later in the app. All interviews are logged for future reference *(see image below)*.

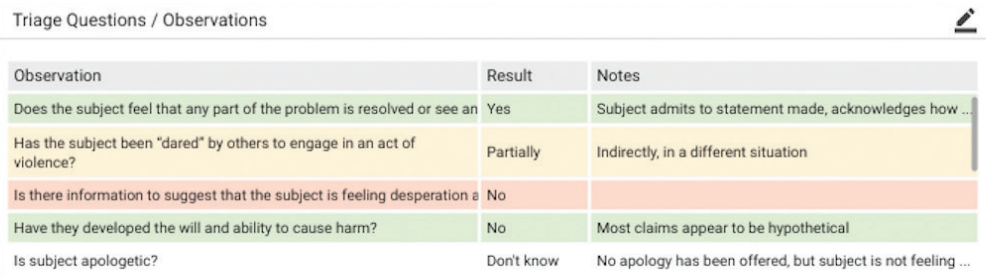


Interviews +

Date/time	Subject Name	Affiliation	Type	Interviewer	Location	Interview Status
2024/02/19 11:12 AM	John Erickson	Student	Subject	Ted Robles	Old Wooden MS	Completed
2024/02/19 12:31 PM	Stan Cortez	Other	Witness	Ted Robles	Other	In Progress
2024/02/19 1:04 PM	Kyle Woodward	Student	Target	Nancy Gillespie	Old Wooden MS	Completed
2024/02/20 2:00 PM		Staff	Teacher			Not Started
2024/02/19 3:00 PM	Amelia Erickson	Parent / Guardian	Parent			Not Started

Interview status for a case, updated in real time.

Team members also begin recording their key observations, which provide critical context surrounding the case. One example would be a school principal who knows both the perpetrator and victim in a case and could attest to any prior incidents involving both students. Team observations are captured on a checklist *(see image below)*.

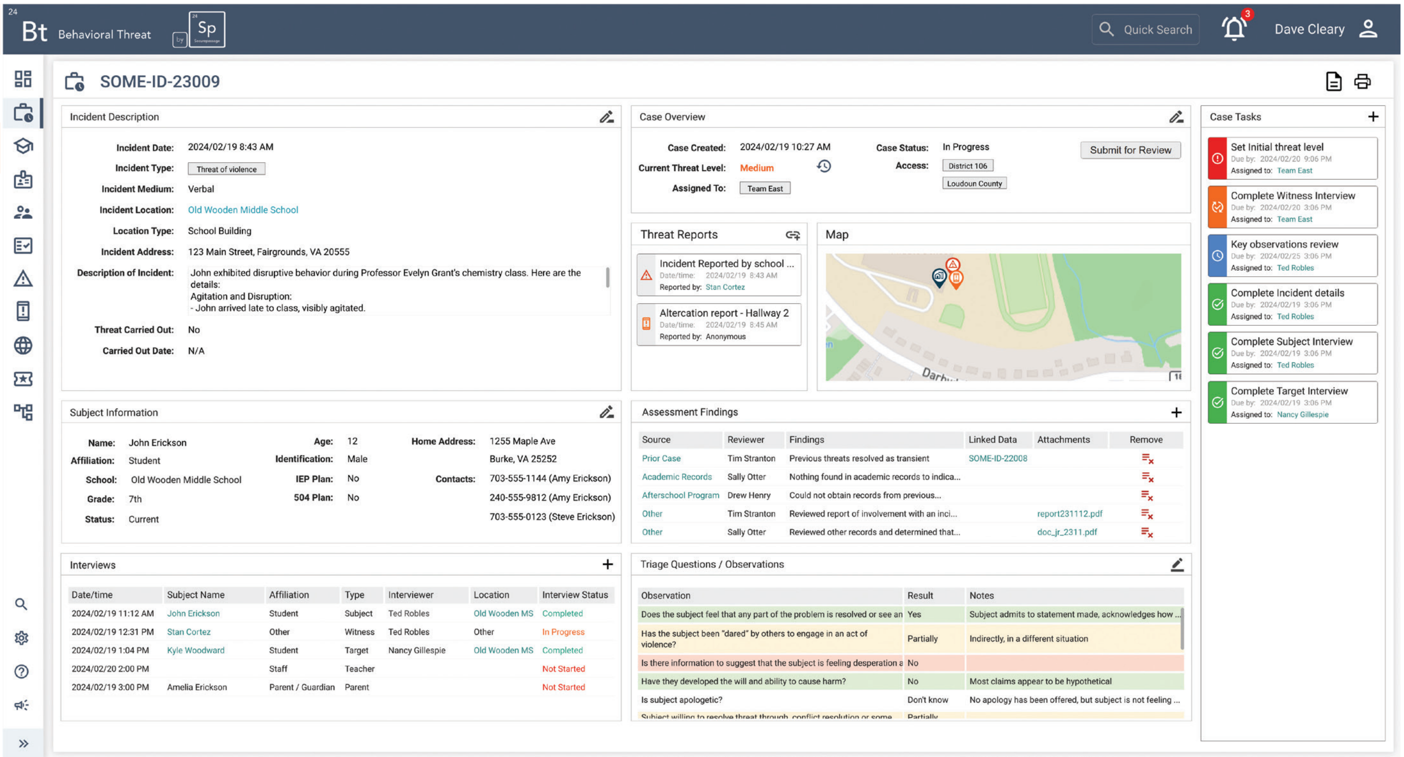


Triage Questions / Observations

Observation	Result	Notes
Does the subject feel that any part of the problem is resolved or see an	Yes	Subject admits to statement made, acknowledges how ...
Has the subject been "dared" by others to engage in an act of violence?	Partially	Indirectly, in a different situation
Is there information to suggest that the subject is feeling desperation a	No	
Have they developed the will and ability to cause harm?	No	Most claims appear to be hypothetical
Is subject apologetic?	Don't know	No apology has been offered, but subject is not feeling ...

An assessment team member's observations provide critical context.

Once available evidence, interview transcripts and observations have been collected, the team meets to: a) consider the circumstances under which the threat was made and the threatening individual's intentions; and b) classify the threat using one of several available assessment frameworks. The full range of details on each case can be viewed on a dashboard-style page *(see image next page)*.



SOME-ID-23009

Incident Description

Incident Date:	2024/02/19 8:43 AM
Incident Type:	Threat of violence
Incident Medium:	Verbal
Incident Location:	Old Wooden Middle School
Location Type:	School Building
Incident Address:	123 Main Street, Fairgrounds, VA 20555
Description of Incident:	John exhibited disruptive behavior during Professor Evelyn Grant's chemistry class. Here are the details: Agitation and Disruption: - John arrived late to class, visibly agitated.
Threat Carried Out:	No
Carried Out Date:	N/A

Case Overview

Case Created:	2024/02/19 10:27 AM	Case Status:	In Progress
Current Threat Level:	Medium	Access:	District 106 Loudoun County
Assigned To:	Team East		

Submit for Review

Threat Reports

Incident Reported by school ...
Date/time: 2024/02/19 8:43 AM
Reported by: Stan Cortez

Altercation report - Hallway 2
Date/time: 2024/02/19 8:45 AM
Reported by: Anonymous

Map

Case Tasks

Set Initial threat level
Due by: 2024/02/20 9:06 PM
Assigned to: Team East

Complete Witness Interview
Due by: 2024/02/20 3:06 PM
Assigned to: Team East

Key observations review
Due by: 2024/02/25 3:06 PM
Assigned to: Ted Robles

Complete Incident details
Due by: 2024/02/19 3:06 PM
Assigned to: Ted Robles

Complete Subject Interview
Due by: 2024/02/19 3:06 PM
Assigned to: Ted Robles

Complete Target Interview
Due by: 2024/02/19 3:06 PM
Assigned to: Nancy Gillespie

Subject Information

Name:	John Erickson	Age:	12	Home Address:	1255 Maple Ave Burke, VA 25252
Affiliation:	Student	Identification:	Male		
School:	Old Wooden Middle School	IEP Plan:	No	Contacts:	703-555-1144 (Amy Erickson) 240-555-9812 (Amy Erickson) 703-555-0123 (Steve Erickson)
Grade:	7th	504 Plan:	No		
Status:	Current				

Assessment Findings

Source	Reviewer	Findings	Linked Data	Attachments	Remove
Prior Case	Tim Stranton	Previous threats resolved as transient	SOME-ID-22008		✕
Academic Records	Sally Otter	Nothing found in academic records to indica...			✕
Afterschool Program	Drew Henry	Could not obtain records from previous...			✕
Other	Tim Stranton	Reviewed report of involvement with an inci...		report231112.pdf	✕
Other	Sally Otter	Reviewed other records and determined that...		doc_jr_2311.pdf	✕

Interviews

Date/time	Subject Name	Affiliation	Type	Interviewer	Location	Interview Status
2024/02/19 11:12 AM	John Erickson	Student	Subject	Ted Robles	Old Wooden MS	Completed
2024/02/19 12:31 PM	Stan Cortez	Other	Witness	Ted Robles	Other	In Progress
2024/02/19 1:04 PM	Kyle Woodward	Student	Target	Nancy Gillespie	Old Wooden MS	Completed
2024/02/20 2:00 PM		Staff	Teacher			Not Started
2024/02/19 3:00 PM	Amelia Erickson	Parent / Guardian	Parent			Not Started

Triage Questions / Observations

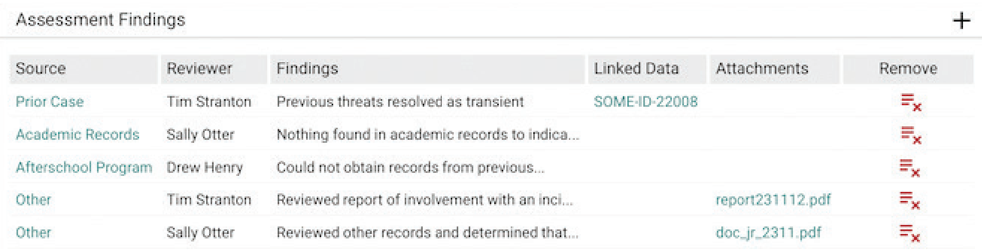
Observation	Result	Notes
Does the subject feel that any part of the problem is resolved or see an	Yes	Subject admits to statement made, acknowledges how ...
Has the subject been "dared" by others to engage in an act of violence?	Partially	Indirectly, in a different situation
Is there information to suggest that the subject is feeling desperation a	No	
Have they developed the will and ability to cause harm?	No	Most claims appear to be hypothetical
Is subject apologetic?	Don't know	No apology has been offered, but subject is not feeling ...
Subject willing to resolve threat through conflict resolution or some	Partially	

The main page for an individual case aggregates all pertinent details on one screen.

Depending on the framework used, a typical assessment threat classification system can be as simple as: 1) Minor; 2) Serious; and 3) Very Serious, or as detailed as: 1) Low Risk Threat; 2) Moderate Risk Threat; 3) High Risk Threat; 4) Imminent Threat; and 5) Not A Threat. Those classified in the realm of "minor," "moderate" or "not a threat" will lead directly to a response without an intervention but including a case follow-up plan. More serious threat classifications will trigger an intermediate step to review observations, and suggest appropriate responses.

For the higher-risk cases there is typically a fork in the road at this stage: threats that are classified as "serious" will lead to the creation of intervention plan as part of the follow-up, but those that are classified as "very serious" or above will trigger a mental health assessment and a detailed safety plan and behavioral intervention plan.

When the threat classification process is complete, the team lead can submit the assessment findings *(see image below)* and response recommendations for review and approval by a supervisor. A case can be sent back for revisions, or approved and closed.



Assessment Findings

Source	Reviewer	Findings	Linked Data	Attachments	Remove
Prior Case	Tim Stranton	Previous threats resolved as transient	SOME-ID-22008		✕
Academic Records	Sally Otter	Nothing found in academic records to indica...			✕
Afterschool Program	Drew Henry	Could not obtain records from previous...			✕
Other	Tim Stranton	Reviewed report of involvement with an inci...		report231112.pdf	✕
Other	Sally Otter	Reviewed other records and determined that...		doc_jr_2311.pdf	✕

Threat assessments can be classified in different ways, depending on district preferences and the assessment framework used.

Data Sources and Integrations

Virtually every existing Secure Passage customer relies on a diverse array of internal and third-party data sources when managing risk. Accordingly, we excel at rapidly configuring our system to securely ingest existing data sets from virtually any source.

In cases where the data volumes and frequency are high (and the data source has an applications programming interface, or API), Secure Passage can ingest, process, filter and display that data. Our engineering team is particularly adept at linking to data sources that are most critical to security incidents, such as computer-aided dispatch (CAD) alerts from regional law enforcement agencies, or local news feeds. Even social media sources can provide valuable context in certain cases.

For one-off data sets or less frequent ingestions, we use specially written import scripts. For example, each Secure Passage SBTA deployment typically includes securely linking to a district's student information system (SIS), regardless of which system is in place. When needed, an assessment team member can query the SIS data from within the SBTA and extract background information on the students linked to a case. Similarly, school personnel and facility data sources can be accessed and imported as needed.

Assessment Team Training

Even when there are no ongoing threats to assess, successful assessment teams meet and train on a regular basis. By getting to know each other and working out each member's exact role in advance, the team will be well prepared when an incident does occur.

It is common for teams to convene once a month, or at least quarterly, to practice their responsibilities and routines, and to work out procedural kinks or fill in missing functions or experts. In addition to its operational role during threat assessment cases, the *SBTA also is the ideal environment for conducting ongoing team training and exercising.*

User Management

Secure Passage has developed comprehensive in-built capabilities for managing all authorized users in the system, including:

- Inviting, registering and managing system users.
- Clearly delineating their levels of access to various apps and specific roles within each app.
- Defining user groups and sub-groups based on school, role, agency or jurisdiction.

For school staff and faculty, information can be ingested automatically from existing district staff data repositories or entered manually. New user accounts must first be registered, which happens after the user receives an email invitation from the system administrator to register with the provided URL. Registration involves creating a password plus a username, which is the user's email address.

The system administrator assigns users one or more roles, which specify the apps and data they can access and the types of actions they can take in each app. Users are also assigned to one or more user groups, to determine which assets and cases they can access.

At the app level, the admin has even finer-grained control over users. Each app has selectable permissions for creating an entry, reading an existing entry (the most common permission granted), editing an entry and deleting an entry (rarely granted to any user besides the admin).

Moreover, Secure Passage can integrate with a district's existing single sign-on (SSO) authentication environment, so that users can access the SBTA with their existing credentials. SSO enables more efficient user onboarding, management and off-boarding.

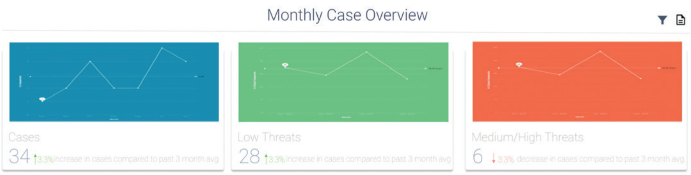
Analytics

Secure Passage has developed its own analytics engine within the platform, which runs continuously in the background. Its sole purpose in SBTA is to extract insights and understand data trends within the district.

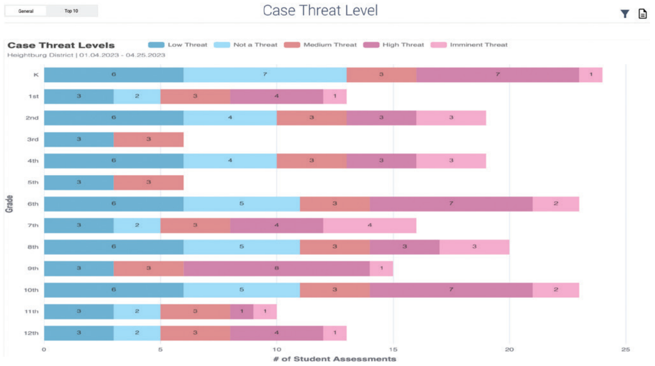
The analytics are viewable in real time or exportable for use in reports, presentations or in-person briefings. Data analyzed includes the ratio of minor to major threat cases, the distribution of case threat levels across the district and types of threats, the relative number of cases at one school compared to others in the same district, types of services provided to students and so on.

Analytics data is presented on-screen in a series of up to five charts, each of which contains a switch and a filter. The switch specifies district overview vs. school overview, or top 10 teams and top 10 schools. Users can then filter by individual school, by grade level, different time periods (from yearly to daily). Visualization options include line charts and bar charts *(see samples below)*.

Analytics charts show multiple data sets and offer a variety of viewing options.

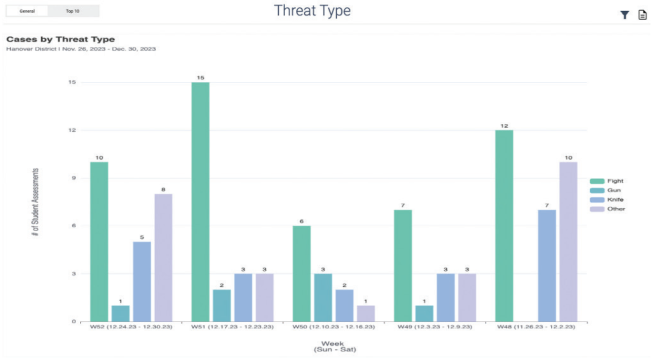

Monthly Case Overview

Cases
34 ↑3.3% increase in cases compared to past 3 month avg
Low Threats
28 ↑3.3% increase in cases compared to past 3 month avg
Medium/High Threats
6 ↓3.3% decrease in cases compared to past 3 month avg


Case Threat Level

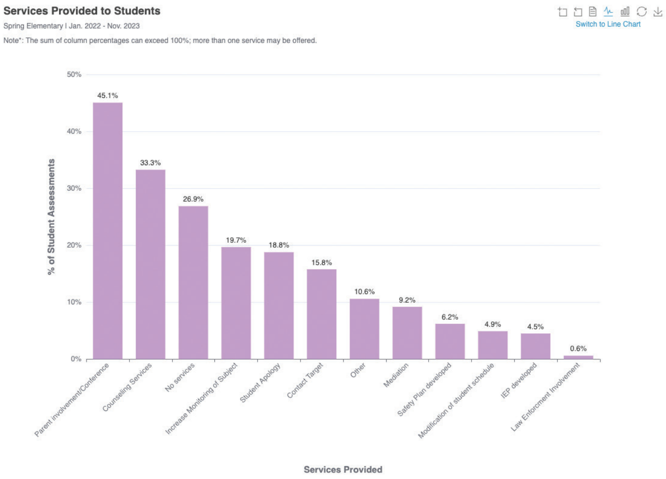
Case Threat Levels

Heightburg District | 01.04.2023 - 04.25.2023


Threat Type

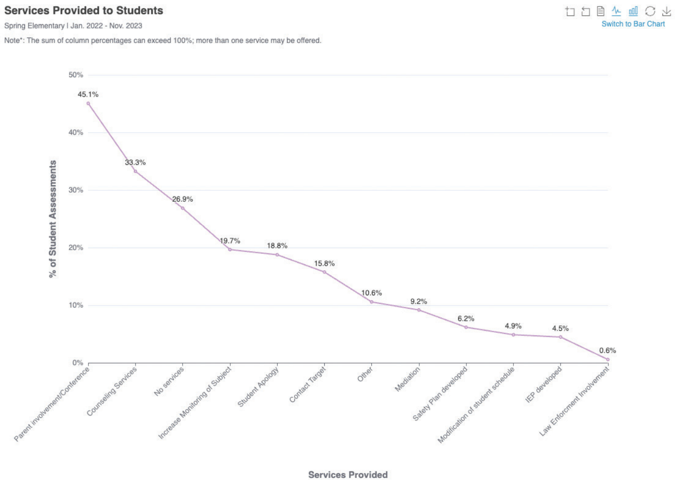
Cases by Threat Type

Hanover District I Nov. 26, 2023 - Dec. 30, 2023


Services Provided to Students

Spring Elementary I Jan. 2022 - Nov. 2023

Note*: The sum of column percentages can exceed 100%; more than one service may be offered.


Services Provided to Students

Spring Elementary I Jan. 2022 - Nov. 2023

Note*: The sum of column percentages can exceed 100%; more than one service may be offered.

Reporting

District assessment teams are often required to download and submit not just reports on individual cases but also summaries of all threat assessment activity over a period of time. The SBTA's reporting engine allows the user to create a variety of reports suitable for any audience, based on how the data has been filtered.

Data can be exported in any format, including .csv, Excel, Word or PDF. All data and graphics contained in a report can be 'flattened' and anonymized so that no sensitive information is at risk of exposure beyond those who are authorized to view it.

IT Security and Data Privacy Benefits

The Secure Passage SBTA solution is unique in several ways. One is its high degree of cybersecurity protections. Given several recent examples of data breaches involving sensitive school facility security and student mental health data, can any district afford not to insist on top-level IT security?

The closed-loop nature of the SBTA means that a district's threat assessment data is far more secure than if it resided on individual computer hard drives or nominally secure school networks, or as printed material stored in physical files. More importantly, Secure Passage is certified as SOC II Type 2-compliant, the gold standard in cybersecurity compliance that holds companies to the most stringent criteria for their security processes, procedures, technologies and guardrails.

Secure Passage is certified as SOC II Type 2-compliant, the gold standard in cybersecurity.

A second key feature is that the SBTA meets the requirements set forth in the Family Educational Rights and Privacy Act (FERPA) by providing strict controls on information access, even for authorized users, plus the ability to provide temporary read-only access to selected data when FERPA law enforcement waivers need to be invoked. These controls apply equally to more serious threat cases, where mental health issues are a factor. Accordingly, Secure Passage has designed its systems and access controls to also be in compliance with Health Insurance Portability and Accountability Act (HIPAA) requirements. In short, our operating principle for data access is 'need-to-know.'

Conclusion
Why Secure Passage?

No school is immune to behavioral threats. As a result, parents, communities and political officials expect educational leaders to work with their mental health and law enforcement partners to ensure they maintain continuous awareness of the scope and severity of potential threats and other adverse behaviors in their areas of responsibility, and can respond in a timely manner.

With jurisdictional authority spread across multiple individuals and agencies – many of them operating under significant budgetary pressures – this is a complex challenge. To succeed, all stakeholders must work collaboratively, implementing consistent threat assessment best practices and response protocols while accommodating the needs of a diverse student population.

Secure Passage has decades of experience developing analytic software for the defense, intelligence, homeland security and public safety communities. Our school safety solutions adhere to nationally accepted risk management standards while reflecting the unique characteristics of the educational environment, including the personal privacy of students.

The Secure Passage School Behavioral Threat Assessment solution supports district and state investigations by providing threat assessment teams with secure access to a single repository containing all information for each individual case, regardless of its source or format. We provide the tools for assigning and carrying out critical tasks and aggregating the resulting data in one place.

Using insights gleaned from multiple sources and presented in the SBTA's single viewing environment, decision-makers can proactively reach evidence-based conclusions regarding the relative severity of a threat and choose the tailored intervention that is most likely to minimize that threat – regardless of whether it is a minor case resolvable through supportive counseling, or a severe threat requiring the intervention of law enforcement and mental health professionals.

In-built analytics and reporting tools can provide instant summaries of all threat assessment activity taking place at a school, district or even an entire state, and the information can be tailored to meet federal reporting requirements as well.

The SBTA solution can be rapidly configured to the exact specifications of each customer, and is typically deployed in as little as a few weeks – empowering those who protect campuses to proactively identify, assess and manage threats – before the unthinkable happens.

Secure Passage: Elemental to Your Security

At Secure Passage, we embody the principle that "It's all security to us." Our core mission revolves around the meticulous identification, organization, and prioritization of key digital and physical security data. By streamlining this information into a secure 'source of truth,' we ensure its ready availability for both routine operations and critical emergency responses.

With a foundation built on decades of expertise in digital security, physical security, intelligence, law enforcement, critical infrastructure, and education, our team members are not just practitioners but innovators. We pride ourselves on contributing a wealth of planning, operational knowledge, and experience to your organization, aiming to seamlessly integrate with your team and enhance your security posture.

24
Sp
Securepassage

securepassage.com

20240430