VENDOR SECURITY ASSESSMENT

CoSN K-12CVAT Lite

School ThreatSim — Vendor Assessment Response

VERSION 4.1

COMPLETED BY

School ThreatSim

DATE

April 2026

PREPARED BY

Adam Robison, Founder & CSSO

CONTACT

schoolthreatsim@gmail.com

General Information

Field	Response
DATE-01	04/2026
GNRL-01 Vendor Name	School ThreatSim
GNRL-02 Product Name	School ThreatSim — Scenario-Based Safety Decision Training Platform (v1.0)
GNRL-03 Product Description	A web-based, scenario-driven decision training platform designed for K-12 school security staff and administrators. Users engage in timed, branching scenarios that simulate real-world school safety situations. No student data is collected or processed.
GNRL-04 Privacy Notice URL	https://schoolthreatsim.com/#/trust
GNRL-05 Vendor Contact Name	Adam Robison
GNRL-06 Vendor Contact Title	Founder & Certified School Security Officer (CSSO)
GNRL-07 Vendor Contact Email	schoolthreatsim@gmail.com
GNRL-08 Phone	Available upon request
GNRL-09 Vendor Data Zone	United States
GNRL-10 Institution Data Zone	United States

Documentation

Code	Question	Response	Additional Information
DOCU-01	Have you undergone a SSAE 18 audit?	No	School ThreatSim is a small, early-stage vendor. A formal SSAE 18 audit has not been completed. Infrastructure relies on SOC 2-certified providers (Supabase/AWS, Netlify).
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	No	Not yet completed. Planned as the platform scales.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	Not applicable at current scale.

Documentation

Code	Question	Response	Additional Information
DOCU-04	Do you conform with a specific industry standard security framework?	Partial	We follow NIST Cybersecurity Framework principles informally. Formal certification is planned as the product matures.
DOCU-05	Are you compliant with FISMA standards?	No	FISMA is not currently applicable; no federal government data is processed.
DOCU-06	Would you sign the Student Data Privacy Consortium (SDPC) statement?	Yes	School ThreatSim does not collect or process student data. We are willing to sign applicable SDPC agreements for districts that require it.

Company Overview

Code	Question	Response	Additional Information
COMP-01	Describe your organization's background and ownership structure.	School ThreatSim is an independently owned, single-entity LLC founded in 2025. There are no parent companies, subsidiaries, or multinational agreements. All operations are US-based.	Founder: Adam Robison, Certified School Security Officer
COMP-02	How long has your organization conducted business in this product area?	School ThreatSim was founded in 2025. The founder has 10+ years of K-12 school security experience as a CSSO.	Scenario content is CSSO-authored based on real-world school safety protocols.
COMP-03	Do you have existing K-12 customers?	In evaluation/pilot phase	The platform is in active pilot with K-12 district contacts. Customer list available upon request.

Company Overview

Code	Question	Response	Additional Information
COMP-04	Have you had a significant cybersecurity incident disrupting availability for longer than 8 hours?	No	No incidents to date.
COMP-05	Have you had a security event in the last 5 years impacting privacy, operations, or data?	No	No security events to date. Platform launched in 2025.
COMP-06	Do you have a formal risk management and cybersecurity program in place?	Partial	Formal policies are in development. We follow documented secure development practices and rely on infrastructure-level controls from Supabase and Netlify.
COMP-07	Do you have dedicated customer support and product management?	Yes	The founder serves as primary support and product contact. Response time: within 24 hours.
COMP-08	Do you have dedicated software and systems development teams?	Yes — small team	Development is led by the founder with contracted engineering support.
COMP-09	Additional environment information	School ThreatSim runs on a serverless architecture (Netlify Functions + Supabase PostgreSQL). No student PII is collected. Staff training data (name, email, role, scenario scores) is stored in Supabase (AWS us-east-1). All traffic is HTTPS.	

Application / Service Security

Code	Question	Response	Additional Information
HLAP-01	Does your system support role-based access control?	Yes	Three roles: User (staff), Admin (district admin), Super Admin. Admins can only view data within their own district.
HLAP-02	Do you enforce additional controls for privileged access users?	Yes	Admin accounts require secure login credentials. Super admin access is developer-only.
HLAP-03	Can employees access protected data remotely?	Yes — with controls	All access requires authenticated login via HTTPS. No plaintext access.
HLAP-04	Is an audit log of access maintained?	Partial	Session logs and score records are maintained per user. Formal audit log tooling is planned.
HLAP-05	Would you share system schematics/data flow diagrams if necessary?	Yes	Available upon request for qualified procurement reviewers.
HLAP-06	Has your system been tested for input validation errors?	Partial	Input validation is implemented at the API layer. Formal third-party penetration testing is planned.
HLAP-07	Is district data segmented from other organizations?	Yes	Each district's data is logically separated by district_id at the database level. Cross-district access is not possible for standard accounts.
HLAP-08	Do you have a quality multi-tenancy environment?	Yes	Multi-tenant by design. Each district's users, admins, and data are scoped to their own district.

Authentication, Authorization, and Accounting

Code	Question	Response	Additional Information
HLAA-01	Do you have strong authentication including MFA?	Partial	Email/password authentication is enforced via Supabase Auth. MFA support is planned. Admin accounts require strong passwords.
HLAA-02	Does your web interface support standards-based SSO?	Planned	OAuth integration is on the product roadmap. Currently email/password only.
HLAA-03	Does the system support external auth services (Active Directory, LDAP)?	No — planned	Not currently supported. SSO/SAML planned for district-level deployments.

Authentication, Authorization, and Accounting

Code	Question	Response	Additional Information
HLAA-04	Do district staff have access to audit logs for their users?	Partial	District admins have access to user session and performance data through the admin dashboard. Full audit logging planned.

Business Continuity Plan

Code	Question	Response	Additional Information
HLBC-01	Do you have a documented Business Continuity Plan?	Partial	An informal BCP exists. Formal documentation is in development. Infrastructure reliability relies on Netlify (99.9% uptime SLA) and Supabase (AWS-backed).
HLBC-02	Is there a documented communication plan for impacted clients?	Partial	The founder directly communicates with affected districts in the event of an outage. A formal plan is being documented.
HLBC-03	Is the BCP reviewed at least annually?	Yes	Reviewed by the founder annually and updated as the platform evolves.
HLBC-04	Does your organization regularly test failover/recovery?	Partial	Supabase provides automated backups. Manual recovery testing is conducted. Formal DR testing is planned.

Change Management

Code	Question	Response	Additional Information
HLCH-01	Do you have a documented change management process?	Yes	All platform changes go through version-controlled releases (GitHub). Releases are reviewed before deployment to production.
HLCH-02	Will the district be notified of changes impacting security or availability?	Yes	Districts are notified via email for any changes impacting service availability or data handling.
HLCH-03	Do you have a policy for managing known vulnerabilities and zero-day risks?	Partial	Dependencies are monitored via automated tooling (npm audit). Patches are applied promptly. Formal vulnerability response policy is in development.

Data

Code	Question	Response	Additional Information
HLDA-01	Do you logically separate institution data from other customers?	Yes	Data is segregated by district_id at the database level.
HLDA-02	Is sensitive data encrypted in transit?	Yes	All data is transmitted over HTTPS/TLS 1.2+.
HLDA-03	Is sensitive data encrypted at rest?	Yes	Supabase (PostgreSQL on AWS) uses AES-256 encryption at rest.
HLDA-04	Do backups leave the United States?	No	All data and backups remain in AWS us-east-1 (United States).
HLDA-05	Do you have a documented media handling/data sanitization process?	Partial	Data deletion is available upon customer request. Formal sanitization procedures are in development.
HLDA-06	Is institution data visible in system administration modules?	Limited	Only authorized super admin accounts can view cross-district data for support purposes. This access is logged.

Database

Code	Question	Response	Additional Information
HLDB-01	Does the database encrypt specified data elements at rest?	Yes	Supabase PostgreSQL (AWS-hosted) applies AES-256 encryption at rest.

Datacenter

Code	Question	Response	Additional Information
HLDC-01	Will any institution data leave the United States?	No	All data stored in AWS us-east-1 (Virginia, USA).
HLDC-02	Does your company own the physical data center?	No	School ThreatSim uses Supabase (AWS) and Netlify — both reputable cloud providers with US-based data centers.
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report?	Yes	Supabase is SOC 2 Type 2 certified. Netlify has SOC 2 compliance. Reports available upon request from providers.

Disaster Recovery Plan

Code	Question	Response	Additional Information
HLDR-01	Do you have a Disaster Recovery Plan?	Partial	Informal DRP exists. Formal documentation in progress. Supabase provides automated daily backups with point-in-time recovery.
HLDR-02	Are any DR locations outside the United States?	No	All infrastructure is US-based.
HLDR-03	Is the DRP reviewed at least annually?	Yes	Reviewed by the founder annually.

Firewalls, IDS, IPS, and Networking

Code	Question	Response	Additional Information
HLFI-01	Are you utilizing a WAF or SPI firewall?	Yes	Netlify provides DDoS protection and edge security. Supabase includes network-level firewall controls.
HLFI-02	Do you have a documented policy for firewall change requests?	Partial	Infrastructure firewall changes are managed through Netlify and Supabase provider controls. Internal policy documentation in development.
HLFI-03	Do you have automated threat monitoring?	Partial	Supabase and Netlify provide platform-level monitoring and alerting. Application-level SIEM is planned.
HLFI-04	Is there 24x7x365 monitoring in place for intrusions?	Partial	Supabase (AWS) and Netlify provide continuous infrastructure monitoring. Application-level 24/7 monitoring is planned as the platform scales.

Physical Security

Code	Question	Response	Additional Information
HLPH-01	Does your organization have physical security controls and policies?	Yes — via providers	School ThreatSim does not operate physical data centers. Physical security is managed by Supabase (AWS) and Netlify, both of which maintain rigorous physical security controls.
HLPH-02	Are employees allowed to store customer data on personal devices?	No	All data remains within the cloud infrastructure. No local storage of customer data is permitted.

Policies, Procedures, and Processes

Code	Question	Response	Additional Information
HLPP-01	Can you share an org chart, mission statement, and security policies?	Yes — upon request	Available to qualified procurement contacts. Contact: schoolthreatsim@gmail.com
HLPP-02	Are security principles designed into the product lifecycle?	Yes	Security is a core design consideration. HTTPS-only, input validation, role-based access, and dependency monitoring are built into the development workflow.
HLPP-03	Do you have a formal documented incident response plan?	Partial	An informal IRP exists. Formal documentation is in development. The founder is the primary incident response contact.
HLPP-04	Do you have a documented information security policy?	Partial	Core security practices are documented. A formal, comprehensive ISP is in development.

Systems Management & Configuration

Code	Question	Response	Additional Information
HLSY-01	Do you employ network and administrative segmentation?	Yes — via providers	Administrative and application environments are logically separated. Netlify Functions (serverless) are isolated from frontend assets. Database access is restricted to API layer only.
HLSY-02	Do you have standard hardened configurations for servers?	Yes — via providers	Server hardening is managed by Supabase (AWS) and Netlify. No self-managed servers.
HLSY-03	Do you encrypt company-owned mobile devices?	N/A	School ThreatSim has no company-owned mobile devices used for data access.

Vulnerability Scanning

Code	Question	Response	Additional Information
HLVU-01	Have systems had a third-party security assessment in the last year?	No	Planned as the platform scales. Infrastructure providers (Supabase, Netlify) maintain regular third-party assessments.

Vulnerability Scanning

Code	Question	Response	Additional Information
HLVU-02	Are applications scanned for vulnerabilities?	Partial	Automated dependency scanning (npm audit) is run on each build. Full DAST scanning is planned.
HLVU-03	Are systems scanned for vulnerabilities?	Yes — via providers	Supabase (AWS) and Netlify conduct regular infrastructure vulnerability scanning.

Completion & Contact

Completed by	Adam Robison, Founder & CSSO, School ThreatSim
Contact	schoolthreatsim@gmail.com
Date	April 2026

"K-12CVAT documentation available upon request."