CURRICULUM VITAE · SEPTEMBER 2026

Ryan James York

Security engineer and founder · Hardware security · cryptographic provenance · 2D carbon thin films

SSX360 Corp., Honolulu, Hawai'i, USA · mission@ssx360.com · https://ryanjamesyork.com · https://www.linkedin.com/in/ryanjamesyork · ORCID https://orcid.org/0009-0007-5979-7949

Summary

Born in Makiki, Honolulu, Hawai'i, in 1995. Security engineer and founder of SSX360 Corp., building cryptographic provenance and independent audit tooling for AI-agent payment systems; leads authorized security assessments and vulnerability research across the logistics, finance and climate domains. Hands-on with post-quantum signatures (FIPS 204 ML-DSA, FIPS 205 SLH-DSA), hardware signing devices, adversarial evaluation of machine-learning models, and hardened container infrastructure. Built a control plane that governs and audits what development teams ship, with software and hardware mapped ahead of multiple compliance layers. Leads a 2D carbon thin-film characterisation programme moving from modelled to measured data with academic partners.

Positions

2024 – present — **Founder & Chief Executive Officer**, SSX360 Corp. (Delaware; Honolulu, Hawai'i). Cryptographic provenance and independent audit tooling; open protocol Matrix Scroll; MCV-1 criteria for machine-verifiable evidence; research platform for 2D-carbon security hardware.

2019 – 2024 — **Chief Real Estate Officer**, CPY Partners. Opened and ran the firm's research and development wing, a quantitative investment team drawn from MIT and Northeastern University.

Affiliations

2026 – — **Innovator member**, Cyber Risk Institute (CRI), the coalition of financial institutions that maintains the CRI Profile; participation through SSX360 Corp.

Selected work

- Designed the full system architecture for AP2 agent-payment policy enforcement: mandate chain verification, cryptographic audit trails, hardware-signed approvals.
- Flashed, penetration-tested and patented an encrypted internal hardware signing device built on an NFC/SE050 secure element.
- Implemented post-quantum signature support targeting FIPS 204 ML-DSA and FIPS 205 SLH-DSA alongside Ed25519.
- Fine-tuned internal machine-learning prediction models for production use across finance, logistics and climate workloads.
- Built a deterministic synthetic corpus, learned inversion and signed release gate for the amorphous-carbon Raman inverse problem (Findings 2026.2–2026.4; preprint v1.1, 2026).

Systems built

- **Matrix Scroll** – open-source provenance protocol (Apache-2.0, PyPI): commit-time Ed25519 signing, MCP trust scanner (top of Show HN on release), CI gating.

- **Encrypted Team Workspace** – zero-knowledge Kanban, chat and file sharing; server stores only ciphertext; libsodium with Argon2id, 1 MiB secretstream chunks with reorder and truncation detection, single-use invites bound to keyed BLAKE2b digests.
- **ZERO_G** – hardware security appliances for regulated work: AES-256 at rest, air-gapped USB workflows, on-device semantic search, tamper-evident audit logs; renderer treated as untrusted; configurations aligned to CMMC, HIPAA and SOC 2 use cases.
- **LAMBDA_ANGELS** – MCP safety gate for autonomous coding agents: natural-language goals to DAG plans, unsafe dispatches blocked before any model token is spent, repository policies on paths, egress and execution limits; 209 unit tests, property-based fuzzing, Pyright strict.
- **CRUCIBLE** – CI-ready adversarial evaluation harness for tabular ML models: YAML attack cards in network-isolated Docker workers, schema-validated JSON reports, release gating on regression diffs.
- **RECON_MCP** – OSINT and threat-intelligence MCP server: twenty tools across GitHub, arXiv, SEC EDGAR, USPTO and a local vector corpus, with per-source rate limiting.

Competencies

Cryptography	FIPS 204 ML-DSA, FIPS 205 SLH-DSA, Ed25519, AES-256, libsodium, Argon2id, end-to-end encryption, tamper-evident audit logs, hardware secure elements (NFC/SE050)
Security engineering	Threat modelling (STRIDE), secure SDLC, application security, secure code review, SAST/DAST, supply-chain security, secrets management, CI security gates
AI and agent security	Adversarial ML evaluation, red-team harnesses, policy-as-code, MCP server security, autonomous-agent safety gates, AP2 payment policy enforcement
Infrastructure	Docker isolation and egress control, air-gapped workflows, Linux hardening, IAM, structured audit logging
Intelligence and OSINT	GitHub, arXiv, Semantic Scholar, SEC EDGAR, USPTO, Hugging Face, vector-corpus search, rate-limited collection, incident-response readiness
Compliance	NIST SP 800-171, CMMC, HIPAA, SOC 2, FIPS 140-3 awareness, audit-evidence workflows
Materials	Raman spectroscopy of sp^2 carbon, Ferrari–Robertson analysis, synthetic-corpus benchmarking of inversion pipelines

Publications and findings

2026	R. J. York, "A deterministic synthetic corpus and learned inversion for the amorphous-carbon Raman inverse problem, admitted through a signed release gate," preprint v1.1, 3 September 2026. `https://ryanjamesyork.com/files/york-2026-raman-inverse-problem-v1.1.pdf`
2026	Findings 2026.1–2026.5, *ryanjamesyork.com*, each with Markdown source and SHA-256 digest. `https://ryanjamesyork.com/findings`

Current as of September 2026. The canonical version of this document is `https://ryanjamesyork.com/cv`; a signed PDF is served beside it.