KENNETH KASUBA

DIRECTOR OF SECURITY & AI RESEARCH

contact@kennethkasuba.com • linkedin.com/in/kenneth-kasuba • Honolulu, HI

EXECUTIVE PROFILE

Principal-level security leader with 15+ years across application security, penetration testing, cloud infrastructure, and AI/ML system defense. Architected secure-by-design patterns for enterprise agentic AI deployments and defined AI governance strategy for organizations adopting LLM-based systems. Led red teaming engagements that bypassed production LLM safety controls. Published two original AI security frameworks. Three-time promotion track to Principal reporting directly to CTO. Background spans NCC Group, Leviathan Security Group, and Certus Cybersecurity.

CAREER HIGHLIGHTS

- **Built AI Purple Ops** — an open-source, research-grade LLM security testing framework with 200+ adversarial test cases spanning prompt injection, data poisoning, GCG suffixes, encoding bypasses, Unicode smuggling, and RAG poisoning. Used by security teams for repeatable, evidence-backed AI assessments.
- **Published STRATA-8** in Towards AI — a novel bottom-up discovery framework for AI agent security that fills the gap between traditional threat models (STRIDE, MAESTRO, MITRE ATLAS) and real-world agentic AI deployments. Adopted as a practical methodology for mapping trust boundaries and privilege drift.
- **Bypassed production LLM safety controls** during red teaming engagements at Certus — demonstrated training-data poisoning chains, unauthorized code execution, and canary validation bypasses via direct API manipulation; drove remediation across model-serving and API gateway infrastructure.
- **Discovered critical vulnerability chains at NCC Group** — IDOR exposing hundreds of clients' financial records, XXE-to-SSRF chains yielding full backend access and session token exfiltration, and JWT key-confusion attacks (RS256→HS256) that triggered complete authentication architecture redesigns.
- **Promoted three times in under three years** at Certus Cybersecurity — Security Engineer → Senior → Principal — earning a direct reporting line to the CTO and ownership of the company's AI security and DevSecOps practice areas.
- **Led SOC 2, ISO 27001, and FedRAMP readiness** across production environments; conducted FedRAMP-aligned reviews of AWS and Azure infrastructure that achieved full compliance posture.

CORE COMPETENCIES

- AI/ML Security Architecture
- LLM Red Teaming & Adversarial Simulation
- Agentic AI Threat Modeling
- AI Governance & Risk Assessment
- Prompt Injection & Data Poisoning Defense
- Application Security (AppSec)
- Penetration Testing (Web, API, Network, Cloud)
- Cloud Security Architecture (AWS, GCP, Azure)
- DevSecOps & Secure SDLC
- Zero Trust Architecture
- Kubernetes & Container Hardening
- Vulnerability Management
- SAST / DAST / IAST / SCA
- Security Program Management
- SOC 2 / ISO 27001 / FedRAMP / NIST 800-53
- NIST AI RMF
- OWASP Top 10 & LLM Top 10
- MITRE ATT&CK / ATLAS
- Cross-Functional Leadership
- Executive & Board-Level Reporting

PROFESSIONAL EXPERIENCE

Director of Security & AI Research
Feb 2026 – Present

Tyrian Institute of AI and Cybersecurity
Honolulu, HI

- Direct the institute's security research program and cross-functional client delivery pipeline — from executive risk framing through technical validation to board-ready reporting.
- Architect cloud-native research infrastructure on AWS with identity segmentation, hardened CI/CD, isolated attack simulation environments, and tamper-evident evidence workflows.
- Define AI governance strategy and operationalize security architecture reviews for organizations deploying LLM-based systems, agentic AI workflows, and RAG pipelines — aligned with NIST AI RMF and OWASP LLM Top 10.
- Establish institute-wide standards for research integrity, responsible disclosure, and evidence handling aligned with enterprise procurement and audit expectations.

Principal Security Engineer
Feb 2022 – Nov 2025

Certus Cybersecurity
Remote

Security Engineer → Senior Security Engineer → Principal Security Engineer · Direct report to CTO

- Defined secure-by-design architecture for agentic AI and GenAI systems — model governance, MLOps pipeline controls, and threat models hardening LLM integrations against prompt injection, data poisoning, and code execution.
- Led AI red teaming engagements that bypassed LLM canary validations and demonstrated training-data poisoning; drove remediation across model-serving and API gateway layers.
- Delivered OWASP Top 10, OWASP LLM Top 10, and ML pipeline application security assessments across enterprise web apps and APIs — XSS, CSRF, SSRF, IDOR, XXE, JWT flaws.
- Authored custom Semgrep rules, SCA scans, and SBOM generation to embed shift-left security into CI/CD; integrated DAST, SAST, and IAST into GitHub Actions and GitLab CI.
- Hardened AWS/GCP IAM and IaC — enforced least-privilege roles, scanned Terraform/CloudFormation templates, eliminated over-permissive policies.
- Secured Kubernetes (EKS) — remediated misconfigured initContainers, enforced Pod Security Standards, tightened OPA/Gatekeeper and RBAC to close RCE and privilege-escalation paths.
- Led SOC 2, ISO 27001, and FedRAMP readiness; advised on GDPR, NIST 800-53, and HIPAA control families.

Security Consultant
Feb 2021 – Mar 2022

NCC Group North America
Remote

Promoted within 5 months · Recognized by Regional VP for exceptional deliverables

- Exposed IDOR in a GraphQL billing API — exfiltrated two years of financial records for hundreds of clients; drove object-level authorization across all endpoints.
- Chained XXE + SSRF to reach internal metadata services, harvest session tokens, and demonstrate full backend compromise.
- Executed JWT key-confusion attack (RS256→HS256) to forge admin tokens; triggered complete auth architecture redesign.
- Conducted FedRAMP-aligned AWS/Azure reviews — identified public S3 buckets, wildcard IAM, absent CloudTrail; remediated to full compliance.
- Automated recon with Nmap, Wireshark, and custom Python tooling — cut manual testing time 50%.

Associate Security Consultant
Feb 2020 – Apr 2020

Leviathan Security Group
Seattle, WA

- Performed web application penetration tests — CSRF, XSS, SQLi, XXE, insecure file uploads — and source code reviews for OAuth2/JWT flaws, hardcoded secrets, and CORS misconfigurations.

IT Security Consultant

Feb 2018 – Jan 2020

PC Doctors Inc.

Wilkes-Barre, PA

- Delivered infrastructure assessments for law firms and healthcare providers — Nessus scanning, network topology mapping, AWS cloud migrations.

Technical Service Engineer

May 2017 – Feb 2018

Web.com

Dallas, PA

- Triaged production PHP/MySQL incidents, performed malware remediation on compromised web servers, administered Linux/Windows virtual infrastructure.

Technical Manager

Aug 2010 – May 2017

PC Doctors Inc.

Wilkes-Barre, PA

- Managed security and network engineering team — infrastructure audits, VPN deployments, security appliance installations, chain-of-custody protocols. Promoted to supervisor within two years.

CERTIFICATIONS

Certified Information Systems Security Professional (CISSP)

ISC2 • Issued 2020 • ID 633076

AWS Certified DevOps Engineer — Professional (DOP-C01/C02)

Amazon Web Services • Issued 2022 • ID YXM6W1F19BFQQYW8