

CONTACT

 jonzeolla.com

 /in/jonzeolla

 /jonzeolla

RECOGNITION

Agentic AI Foundation

Ambassador, 2026 to Present

CNCF Ambassador

TAG Security & Compliance, 2023 to 2026

Start-up Innovator of the Year

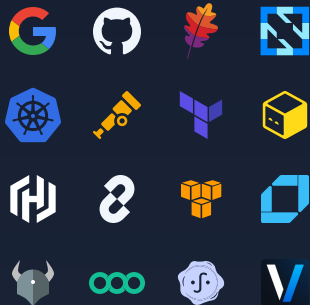
Pittsburgh Tech Council, 2021

SANS Certified Instructor

SEC545: GenAI and LLM Application Security

SEC540: Cloud Native Security and DevSecOps

OPEN SOURCE CONTRIBUTIONS



FOCUS AREAS

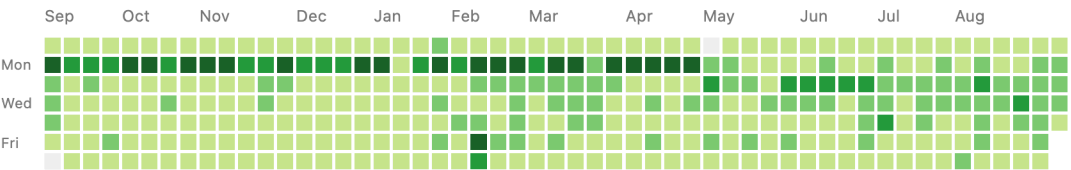
- AI/ML Security
- Cloud Native
- Application Security
- Platform Security
- DevSecOps
- Automated Governance
- Policy as Code
- Guardrails
- Spec Driven Development

Jon is currently building **agent alignment and governance technologies**. As the founder of [Zenable](#), he leads the team in developing self-improving verifiers that ensure coding agents follow each company's evolving requirements.

He has been working with AI and machine learning since 2015 when he was at Carnegie Mellon, applying Petabyte-scale data analysis to improve security automations. That work led him to contribute to dozens of open source projects and initiatives, and he now serves as an [Agentic AI Foundation \(AAIF\) Ambassador](#).

In that role, he helps engineers understand and adopt open protocols for agentic systems, including MCP and A2A, via anything from talks and hands-on workshops to running strategy sessions to help navigate tradeoffs. He's particularly interested in using data and feedback to improve systems and automate repetitive work.

CURRENTLY BUILDING



For more open source, volunteer work, and details on my 100+ presentations, see [jonzeolla.com](#)

EXPERIENCE

- Founder & CEO

2023 to Present

Zenable

→ Making coding agents self-improving via layered feedback loops, automated analysis, and requirement mining from code, docs, and review history

→ Building MCP servers, CLI tools, agentic IDE integrations, GitHub and GitLab reviews, and pre-commit hooks

→ Orchestrating coding agents, leveraging policy as code and spec-driven development to enforce correctness and conformance in AI-assisted workflows

→ Autoformalizing natural-language requirements into deterministic guardrails, mixed with AI-based reviews; heavy focus on context engineering, including RAG and recurring evals of context files against frontier models to improve steering quality
- Co-Founder & CTO

2017 to 2026

Seiso

→ Worked as a forward deployed security engineer at tech startups and software companies; 100% success rate on ISO 27001, SOC 2, PCI, and HITRUST audits

→ Rolled out secure-by-default tooling with SDLC integrations; partnered with dev teams for low-friction product security and compliance

→ Worked with platform teams to build secure-by-default runtimes; co-authored numerous CNCF white papers on cloud native security
- Principal Information Security Engineer

2014 to 2020

Carnegie Mellon University

→ Built distributed systems for automated threat detection and mitigation at scale

→ Led cybersecurity data science for threat intelligence clustering and visualization

→ Apache Metron Committer: shipped big data security monitoring and analytics features
- Senior Security Engineer

2009 to 2014

American Eagle Outfitters & PNC Bank