

# Aaron Rinehart

**Global Fortune 4 Cybersecurity Leader | Published Author | Keynote Speaker**

Fairfax, VA 22032

[aaron@sce.dev](mailto:aaron@sce.dev)

+1573-823-6864

“A high energy, passionate, visionary technology leader with a track record of proven experience in delivering excellence on the impossible, executing transformational change, and aligning technology with core business value.”

Pioneer | DevSecOps | SRE | Chaos Engineering | Founder | CTO | Architect| Advisor | Keynote Speaker | Published Author | Mentor

Global Fortune 4 Leader | Published Author | Keynote Speaker| Servant Leader

Aaron Rinehart has spent his career solving complex challenging engineering problems and transforming cyber security practices across a diverse set of industries: healthcare, insurance, government, aerospace, technology, higher education, and the military. Aaron has been expanding the possibilities of chaos engineering in its application to other safety-critical portions of the IT domain, most notably in cybersecurity. He began shaping the application of chaos engineering within cyber security during his tenure as the Chief Security Architect at a Fortune 4, UnitedHealth Group (UHG). Rinehart is a frequently requested speaker at respective media outlets and conferences, most notably RSA, O'Reilly's Velocity, Blackhat/DefCon, GOTOgoto;, OWASP Global, and QCon. Rinehart has been interviewed and quoted in various publications including the Huffington Post, ABC News, TechTarget, DarkReading, SecurityWeekly, IEEE, and the Washington Post.

For more info follow him on Twitter @aaronrinehart

Authorized to work in the US for any employer

## Work Experience

---

### **Chief Technology Officer, Co-Founder**

Verica, Inc. - Fairfax, VA

January 2019 to September 2022

Served as CTO and Co-Founder of a venture backed software startup from Series Seed to Series A funding stage. My role was to balance build highly performant and autonomous business functions such as Engineering, Marketing, Sales, and other critical functions within the business. At Verica.io we brought a series of products for critical software infrastructure components such as Kubernetes and Kafka to market that made up our continuous verification platform. The primary goal of the product was its ability to proactively uncover system weaknesses and security flaws before they disrupted business outcomes. As the next step in the evolution of chaos engineering, continuous verification provides a disciplined methodology to prevent availability and security incidents. In addition to building high performing business functions I was responsible for bringing in over 3 million dollars in Annual Recurring Revenue (ARR). In order to do so this involved being able to extrapolate customer specific engineering pain and map it to the value our series of products provided to alleviate that pain.

## **Chief Enterprise Security Architect**

UnitedHealth Group - Optum

October 2015 to January 2019

- UHG and its technical service arm, Optum, provides health benefits and services to more than 85 million patients worldwide and is the largest U.S. health insurer. In 2018, while in this role, UnitedHealth Group was Fortune 4, contained 380+ business entities, operated globally, a annual revenue of \$201B and 270,000 employees world-wide.
- As the Chief Enterprise Security Architect I was the executive leader responsible for the leadership and transformation of the Enterprise Security Architecture Domain of Practice; to craft new capabilities and services that smoothly support UHG's rapid global growth. Accountable for setting the future direction of the security solutions architecture strategy for the company. The Chief Security Architect was charged to support company SVP technology executives and capital committee on major technology investments in the company often for capital projects up to 300 million with an overall security program budget just short of \$1B.
- Led, directed, and delivered multiple digital transformations for UHG, including the Public Cloud, DevSecOps, Site Reliability Engineering and inspired an Open-Source Software culture by delivering the company's first open-source software public contribution.
- Created many programs to set and maintain global UHG cyber security strategy. These included: global maps of security capability and maturity; security growth strategy; self-service security architecture requirements portal; baselines; rationalization and refinement of security policies, standards, and guidelines; refinement of exception request process; more. Directed team providing security architecture consulting for applications being developed throughout UHG. Technical, architectural, regulatory and policy requirements. Primary author interpreting laws, regulations, and contracts (HIPAA, HITRUST, NIST, ISO27001, PCI, IRS1075, others) into corporate policies and technical requirements for both in-house and web/cloud/mobile applications.

### Notable projects

- Pioneering the application of Netflix's Chaos Engineering into Cyber Security. We wrote the first open source software tool ChaoSlingr which demonstrated the value in this practice.
- Built the UHG Security Champions Program
- Provided primary security engineering and design services to aid in the delivery of UHG's startup entity Harken Health. This included enabling the startup within UHG transform into the AWS cloud successfully ahead of UHG corporate that created a model forward for the rest of the company to adopt the cloud.
- Supported 10+ M&A Technical Security Operations every year while at the organization to include the merger of Catamaran into OptumRX making OptumRX the second largest drug fulfillment entity.
- Provided primary security risk assessment and design services for the redesign of UHG Claims Highway in the Mainframe to a microservices architecture running on OpenShift.
- Provided support for delivering security capabilities within the Optum Cloud Scaffolding automation framework.
- Proactively identified a major leakage of secrets into Public Github. Managed the remediation with chief counsel and led the solutioning effort for implementing a secrets management solution within UHG based on Hashicorp's Vault.
- Led the evaluation, procurement and implementation of Contrast's Interactive Application Security Testing (IAST) tooling which saved the company millions of dollars monthly by providing a more self-service methodology for application testing services.
- Delivered a CI/CD Jenkins pipeline Dynamic Application Security Testing (DAST) security service based on the Open Source tool Gauntl for software engineering teams to perform self-service pipeline driven

dynamic runtime security testing. This was a key enabler in transforming the company into a DevSecOps culture.

- Led the coordination and delivery of several Chef Inspec auditing baselines that enabled engineering teams to have an automated way to assess the security and compliance of common building components such as VMs. The outcome of this project led to UHG's accelerated delivery of several State Healthcare Exchanges include the Vermont Healthcare Exchange.

### **Sr. Enterprise Information Security Architect/SME**

The College Board - Washington, DC

June 2014 to October 2015

- Served as lead enterprise security resource for solving complex security engineering problems.
- Supporting multiple PCI-DSS audits and technical solutions engineering
- Projects included migrating a legacy on-premise organization ERP system to a cloud based solution, enabling employee BYOD security, modernizing corporate IT infrastructure, and designing core security components for AWS cloud for engineering teams to consume such as CloudHSM, logging, etc., designing a process for managing insecure software dependencies such as Apache Struts, aiding penetration testers for post-penetration test remediation activities, supporting the incident management team in triaging incidents as well as finding solutions to the problems once identified
- Supported the transformation of the organizations flagship product the "SAT" high stakes college entrance exam into a digital testing platform on AWS. My focus in this effort was the threat and risk assessment of the system through providing guidance to engineering teams for delivering the new platform securely.

### **Lead Security Architect and Sr. Information System Security Officer- (Sr. ISSO)**

Dept of Homeland Security- TSA - Emerging Technologies (ETB) - KCG Contractor - \*TS-SCI Clearance - Washington, DC

May 2012 to March 2014

- Primary responsibility was to support the mission of the DHS and TSA Emerging Technologies agenda. My role incorporated the assessment of risk and identification of security challenges in emerging technology capabilities the agency was adopting. Once the challenges were understood I worked with a cross functional team of engineers to build and deliver the capability for agency consumption.
- Projects included adopting Cisco's Identity Services Engine (ISE), upgrading the agencies wifi wireless infrastructure, building the first private cloud within DHS based on Microsoft System Center stack, solving for in-airport connectivity issues for critical TSA security equipment, modernizing the agencies mobile device management solution, upgrading the agencies secure web filter technology and several others
- Duties involved threat modeling, security risk assessment, conducting security scans, reviewing network traffic, creating System Security Plans( included security control details, network design, system design, data flow, key configuration,etc.), stewarding the solutions we built through the agencies Authority to Operate (ATO) process, and other security engineering + compliance related tasks.
- Collaboration projects with In-q-tel in the design and delivery of a secure push-to-talk solution based on Voxer with other agencies.

### **Lead Software Engineer/Senior Security Officer (ISSO) - ManTech CTR**

NASA Goddard Space Flight Center - Safety & Reliability Engineering Code 300 - Greenbelt, MD

November 2009 to May 2012

- Primary responsibilities were the buildout and delivery of full-stack software solutions for the Safety & Reliability functions at NASA Goddard Space Flight Center. In addition to serving as the Lead Software

Engineer I also became the organizations Sr. ISSO responsible for the security and compliance of its systems.

- Duties included the build out of the organization's internal program web infrastructure, transition to an IP6 based network infrastructure, Code 300 System Engineering (\*NIX), ISO 9000 audit, ISO 27001 audit, running security scans, handling security incidents, engineering management for a small team of engineers,
- Notable project included the early adoption, testing and assessment of NASA's Cloud Nebula project, which later became known to the industry as OpenStack. Contributing to the CIS hardening benchmark for Mac OSX maintained by NASA at the time, collaborating with firmware engineers writing HSIC Hardware Description Language (VHDL) on Xilinx FGPAs, building the technology infrastructure to support NASA's Supply Chain Engineering Conference, and supporting other software and security engineering efforts for NOAA and NASA projects such as Geostationary Operational Environmental Satellite (GOES), JWST, LISA

### **DBA; Director of App Engineering**

University of Missouri Health System - Biodesign Surgical Research Program - Columbia, MO  
August 2008 to December 2009

- Primary responsibilities included the fullstack engineering and operations of the University of Missouri Health System web/mobile applications and databases. This involved building out the servers, designing the web applications, building the apps and running them in production.
- Notable projects included the building of software designed to detect Hospital Acquired Pneumonia, web application for supporting the Biodesign Surgical Research Program, web application to gather survey input from patients test the effects of Temperature and Pressure on Patient Mood and its relationship to eye diseases, a EMR solution for the organization based on OpenEMR, a software application for Clinical Trial administration using OpenClinica

### **Strategic Software Implementation Consultant**

Nolij Corporation - Beverly, MA  
August 2007 to August 2008

Nolij Corporation was a small startup software company out of Beverly, MA. It was founded by one of the creators of the popular education platform Blackboard. The software products offered by Nolij included its Document Imaging Management software that was specifically designed to integrate with Student Information System data stores within Higher Education. Our primary clientbase during my tenure was mostly top tier university and elite Ivy League schools such as Dartmouth, Harvard, Pepperdine, URI, MIT, etc.

- Primary responsibilities included the integration of Nolij Corporations Document Imaging Software based in Java and VB.net with Student Information System Data stores at higher education clients. This ranged from Peoplesoft Oracle integration, Microsoft SQL, Uniqery, Sybase and many other relational data stores. In addition to integration my role was to author custom interfaces and business logic for each institution to find, retrieve and display their student data alongside key student document artifacts. Occasionally supported the core product teams in building out core product functions

Notable Projects - Implemented subversioning of code, build an internal resource for sharing customer integration documentation and reusable code artifacts

### **Non-Commissioned Officer (NCO) - Systems/Network Engineering Mgr (Corporal)**

United States Marine Corps (USMC) - various

May 2001 to August 2008

Primary responsibilities included:

- Leadership of the Data Engineering group within MCHQ 4th Marine Division HQ Battalion Communications Platoon. Ensuring mission preparedness by proactively inventorying equipment, assessing configuration, conducting end-to-end readiness exercises the entire system from the satellites down to the data network and ultimately serving up mission critical IT services such as email, logistics applications, mapping software, etc.
- Building and delivering training to new marines on mission essential IT systems
- Primary 4th Marine Division HQ resource for missions and exercises

Notable Projects - Led the design and delivery of a complete Disaster Relief Communications System for the Republic of the Seychelles (Africa) on behalf of the United States Department of Defense. This project included safety critical communications systems such as satellites, phones, radios and computers designed with the intention of supporting the nation during a national disaster. Over several months I led the design, build and delivery on this system in country as a representative of the US Govt.

Camp Lemonier Djibouti, Africa - S6 Served as the lead information technology resource for Camp Lemonier S-6 in Djibouti Africa during - Operation Enduring Freedom.

Combined Joint Task Force- Horn of Africa - J6 Communication Operations - Provided key technology support for Joint services operations such as implementing mission essential mapping software systems, mission air support traffic and control system support, troubleshooting mission critical communications ranging from satellites, multiplexers, system servers and Secret/TopSecret networks

Marine Forces Pacific Communications Exercise - Osan, South Korea

- Served as the data communications leader for the rollout of forward operating location IT operations. Was responsible for designing, planning and delivering an expedient delivery of data communications in the field to support the Joint Military Operations Exercise with the South Korean Navy and Marine Corps.

Joint Navy & Marine Corps Special Forces Naval Exercise - Coronado Bay, CA and Camp Pendleton

- Successfully designed and delivered operational core computer network and system communications during Navy and Marine corps Special Forces combined exercise

## **Oracle DBA Database Software Engineer**

University of Missouri Systems - Enterprise Application Services

May 2006 to August 2007

Primary Responsibilities

- Writing business logic to support various business functions within the University of Missouri student administration. PeopleTools, PL/SQL, SQR, SQL, COBOL, Informatica ETL, PeopleSoft Campus Solutions
- Building ETL mappings using Informatica between legacy Mainframe COBOL Student Information Systems to Oracle Peoplesoft Student Information Systems
- Performing data cleanup operations during cross university system sync operations
- Supporting the Peoplesoft Implementation team in authoring various business logic for custom integration projects
- Troubleshooting database server maintenance, migration, and performance issues

## Education

---

### **B.S. in Economics**

University of Missouri - Columbia, Missouri, US  
2006

### **Diploma in Engineering**

US Marine Corps Communications & Electronics School  
2001

## Skills

---

- Product Security
- Pragmatic Security Architecture
- Public Speaking
- Tech Transformation
- Security Ops & Crisis
- Fortune 5 Senior Leadership
- Engineering Leadership Management
- B2B Sales Ops
- Resilient Security Program Design
- Cloud Security
- Board Member
- Chaos Engineering
- DevSecOps
- Building High Performance Teams
- Complex Systems & Orgs
- Site Reliability Engineering
- Raising Venture Capital Northwestern University of Missouri, St Johns, USAF Air War College, and others. Employment History [Summarized. Full Details at [www.linkedin.com/in/aaronsrinehart/](http://www.linkedin.com/in/aaronsrinehart/)]
- Cybersecurity
- Computer Networking
- Network Firewalls
- NIST Standards
- Information Security
- DevOps
- Agile
- Linux

## Links

---

[DevOps.com](http://DevOps.com)

[OpenSource.com](#)

[Verica.io](#)

<http://www.linkedin.com/in/aaronsrinehart>

## Military Service

---

**Branch: United States Marine Corps**

Service Country: United States

Rank: E-4

May 2001 to August 2008

## Certifications and Licenses

---

**CISSP**

**GSEC**

**GIAC Certification**

## Publications

---

**O'Reilly Security Chaos Engineering**

<https://www.oreilly.com/library/view/security-chaos-engineering/9781492080350/>

November 2020

Information security is broken. Users and customers continually entrust companies with vital information, and companies continually fail to maintain that trust. Year after year, the same attacks are successful. But the impact has become greater. Those who build, operate, and defend systems need to acknowledge that failure will happen. People will click on the wrong thing. The security implications of code changes won't be clear. Things will break.

In this report, Aaron Rinehart and Kelly Shortridge explain how engineers can navigate security in this new frontier. You'll learn the guiding principles of security chaos engineering for harnessing experimentation and failure as tools for empowerment--and you'll understand how to transform security from a gatekeeper to a valued advisor. Case studies from Capital One and Cardinal Health are included.

- Apply chaos engineering and resilience engineering to securely deliver software and services
- Transform security into an innovative and collaborative engine for enhancing operational speed and stability
- Anticipate and identify security failure before it turns into an incident, outage, or breach
- Harness failure to continuously improve your security strategy
- Learn your systems' ability to handle security-relevant failures such as system exploitation and server failures
- Apply a series of controlled experiments in engineering testing processes

**Security Chaos Engineering • Kelly Shortridge, Aaron Rinehart & Mark Miller • GOTO 2022**

<https://www.youtube.com/watch?v=0T0IOXjL660>

May 2022

Kelly Shortridge - Co- Author of Security Chaos Engineering and Senior Principal, Product Technology at Fastly  
Aaron Rinehart - Co- Author of Security Chaos Engineering and Co-Founder & CTO at Verica  
Mark Miller - Co-Author of Epic Failures in DevSecOps and Vice President, Community Engagement and Outreach at The Linux Foundation

DESCRIPTION What's the state of the art in modern security practices? The authors of the book Security Chaos Engineering, Aaron Rinehart and Kelly Shortridge talk to Mark Miller about the shift in the mental model that one has to undertake to reap its benefits. Their approach paves a new way that allows security engineers to uncover bugs in complex systems by chaos experiments before an actual attack. The interview is based on Kelly's and Aaron's book "Security Chaos Engineering": <https://www.verica.io/sce-book>