Donny Schreiber

Cloud & Infrastructure Security Engineer | DevSecOps | Cloud & Application Security

Boulder, CO | career@dschreib.com | linkedin.com/in/donaldschreiber

Security engineer with **10+ years** across endpoint, network, cloud, infrastructure, application, and product security — including **4 years securing AWS at enterprise scale** in AWS Professional Services. Builds production security automation, internal tooling, and infrastructure-as-code in **Python, Terraform, AWS CDK, and GitHub Actions**: policy-as-code guardrails, shift-left DevSecOps pipelines orchestrating 15+ SAST/DAST/IaC/secrets scanners, cloud IAM/PAM, detection & response, and GenAI/LLM and AI-assisted-developer security. Secured **$4B+ in regulated infrastructure** across healthcare, financial services, government, defense, and telecom; published 3 official AWS Prescriptive Guidance documents and open-source Terraform on aws-samples.

CORE SKILLS

Cloud & Infrastructure: AWS, Terraform, AWS CDK, CloudFormation, Docker, Kubernetes / Amazon EKS, container security, cloud security posture management (CSPM), hardening baselines, drift detection, AWS RAM, VPC / Network Firewall, Transit Gateway

Cloud Security, IAM & PAM: IAM least-privilege design, Service Control Policies, privileged access management (PAM), preventative guardrails, AWS Config (custom rules), Security Hub, GuardDuty, KMS, Secrets Manager, zero trust architecture, workload / non-human identity, SSO & federation (Cognito, OIDC, OAuth 2.0, SAML), MFA

DevSecOps & CI/CD: GitHub Actions, GitLab CI/CD, SAST / DAST, Checkov, TFSec, Terrascan, Semgrep, Bandit, GitLeaks, secrets management, SARIF, detection-as-code, PR-based IaC / HCL review

Detection, IR & Threat: Threat detection & response, incident response (NIST 800-61r2), MITRE ATT&CK, threat modeling (STRIDE), SIEM (Splunk / SPL, LogRhythm), EDR (Cybereason), digital forensics, vulnerability & risk management, query languages (SQL, Splunk SPL)

Languages & Automation: Python, Bash, PowerShell, TypeScript, SQL · API integrations, internal tooling, ETL & dashboards/reporting, toil reduction

AppSec & Product Security: Secure code review, product & deliverable security reviews, secure-by-design architecture review, security tooling & libraries, supply-chain security

Endpoint, Identity & Network: Windows / Linux / macOS administration, Active Directory, Group Policy, MDM & device trust, least-privilege enforcement, Palo Alto NGFW, GlobalProtect VPN, network segmentation, DNS, TLS

GenAI Security: Amazon Bedrock, OWASP LLM Top 10, Model Context Protocol (MCP) security, multi-agent / agentic AI, RAG, AI coding-assistant security (Copilot, Claude, Cursor), LLM API integration & AI/ML service-identity governance

Compliance: HIPAA, HITRUST, PCI DSS, SOC 2, NIST 800-53, FedRAMP, IRS Pub 1075

Familiar with: Go, HashiCorp Vault

PROFESSIONAL EXPERIENCE

Amazon Web Services (AWS) — Professional Services

Security Consultant II (Jan 2024 – Present) · Security Consultant I (Jun 2022 – Jan 2024) · Colorado · Jun 2022 – Present

- Authored a **policy-as-code foundation** for a HITRUST-certified healthcare SaaS using **AWS CDK (Python)** — 5 reusable L3 constructs (Service Control Policies, AWS Config rules, Security Hub automation, automated remediation); cut audit prep from 8 weeks to **under 1 week** and removed 65% of compliance overhead.
- Developed **15+ AWS Config custom rules** (Guard DSL) detecting IAM privilege escalation, cross-account trust gaps, CloudTrail tampering, and missing MFA — integrated into enterprise security assessments.
- Built **multi-account, multi-region Amazon VPC IPAM automation** in Terraform — 67 hierarchical pools, 874 network resources, cross-account sharing via AWS RAM; **published to aws-samples and as AWS Prescriptive Guidance**.
- Built a **shift-left DevSecOps suite** orchestrating **15+ scanners** (Bandit, Semgrep, Checkov, TFSec, Terrascan, GitLeaks, ESLint, Safety) through GitHub Actions with intelligent change detection (40–60% CI cost reduction); cut a financial-services platform's security validation from **2 weeks to 4 hours** for a $60B+ trading system.
- Engineered **iSQA**, a production Python tool with 100+ context-aware analysis patterns that automates security-questionnaire and assessment review — **eliminated 3,000+ annual review hours** across the global ProServe practice and cleared a one-year backlog.
- Built **IAMulator**, a GenAI tool that generates least-privilege IAM policies from natural language and flags excess permissions in existing policies — used across 7+ engagements; **~75% faster** policy development.
- Led **18 product / deliverable security reviews** across 9 development teams for a ~$26M connected-home IoT platform (AWS's largest telco engagement); built **ASHparser** (Python) automating scan-output consolidation — **500%+ throughput** vs. manual review; surfaced and mitigated 190 threats and 100 vulnerabilities.

- Designed a **zero-trust-aligned cloud security framework** for a multi-agency state government under simultaneous **IRS Pub 1075 + HIPAA** — Landing Zone Accelerator customization, attribute-based access control, SCP-enforced isolation, and **12+ NIST 800-61r2 incident-response playbooks** (ransomware, cryptojacking, credential compromise, EC2 forensics).
- Performed **STRIDE threat modeling** identifying 127 threats across a financial-services **Amazon Bedrock** GenAI platform, enabling FINRA model-risk approval for AI securing $60B+ institutional portfolios.
- Led the security architecture review for an **AWS re:Invent 2025** GenAI session (70,000+ attendees) — assessing an **AI coding-assistant** architecture (Amazon Q, Model Context Protocol, multi-agent) against OWASP LLM Top 10, securing AI-assisted developer workflows.

Recognition: Security Bar Raiser · GenAI Security Maven · 3× AWSome Builder · AppSec Guardian · 94th-percentile Amazon Q contributor (1,006 participants) · Top 8% Lakera GenAI Security (20,000+ participants).

Zayo Group — Tier 1 Fiber Provider (146,000+ route miles, 400+ global markets)

Network Security Engineer (Apr 2021 – Jun 2022) · Cyber Security Analyst III (Jul 2019 – Apr 2021) · Boulder, CO · Jul 2019 – Jun 2022

- One of two engineers accountable for **all corporate and data-center security** at a global Tier 1 fiber provider — administered Palo Alto NGFW policy, application controls, and GlobalProtect VPN alongside a Cisco ASA fleet across Windows / Active Directory environments and geographically distributed perimeters.
- Built **Splunk** dashboards, alerting logic, and ETL pipelines spanning NGFW, email, **Cybereason EDR**, and Google Workspace — **70% MTTR reduction** via proactive threat hunting across 5,000+ endpoints.
- Led end-to-end **email security transformation** — vendor RFP, contract negotiation, and migration to Abnormal Security, measurably reducing phishing exposure.
- SME for Google Workspace, Cybereason EDR, and MDM during a hiring freeze; architected the corporate MDM program from scratch and co-authored the Organization of Information Security policy aligned to **ISO 27001 A.6**.

KIOSK Information Systems

Cybersecurity Administrator & Security Analyst · Louisville, CO · Jan 2017 – Jul 2019

- Delivered **managed security services (MSP/MSSP-style)** for 10 distinct client organizations (10,000+ endpoints) — AV, encryption, file-integrity monitoring, firewall, and DLP across a heterogeneous portfolio.
- Ran the full email-security lifecycle (RFP, selection, negotiation, migration) and launched an MDM program with no prior organizational precedent.
- Authored Tier 3 escalation runbooks that reduced on-call load and improved security-operations agility.

Earlier

- **Hewlett Packard Enterprise** — Cybersecurity Intern, USPS Enterprise Security · Colorado Springs, CO · 2016 — competitively selected for HPE's 12-week CSIP; delivered a technical white paper and presentation to C-suite and senior security leadership.
- **Front Range Community College** — Cybersecurity & Networking Work-Study · Westminster, CO · 2015–2017 — built hands-on lab curricula; co-authored a 51-page VMware ESXi reference guide.

SELECTED PUBLICATIONS & OPEN SOURCE

- **AWS Prescriptive Guidance:** Hierarchical, Multi-Region IPAM Architecture on AWS using Terraform — docs.aws.amazon.com/prescriptive-guidance/latest/patterns/multi-region-ipam-architecture.html
- **AWS Prescriptive Guidance:** PAM-Centric Baseline with SSM, IAM, KMS, and CloudWatch
- **AWS Prescriptive Guidance:** Deliverable Security Review (DSR) Report Template — ProServe security-delivery standard
- **Open source:** aws-samples/sample-amazon-vpc-ipam-terraform — github.com/aws-samples/sample-amazon-vpc-ipam-terraform

CERTIFICATIONS

AWS Certified Security – Specialty | AWS Certified Solutions Architect – Associate | AWS Certified AI Practitioner | AWS Certified Cloud Practitioner | EC-Council C|CISO | Certified Threat Hunter

EDUCATION

Associate of Science, Cybersecurity — Front Range Community College · 2015–2017

ADDITIONAL

Professional drummer, Kroenke Sports & Entertainment (Denver Nuggets / Colorado Avalanche / Colorado Rapids), 2015–2022 — including the Avalanche's 2022 Stanley Cup championship. WiCyS hackathon facilitator (70+ students, CU Boulder).