

Jason Ratcliffe

Lead Information Security Engineer, Cloud

San Antonio, TX · [linkedin.com/in/jasonratcliffe](https://www.linkedin.com/in/jasonratcliffe) · jasonratcliffe.dev (contact form)

SUMMARY

Experienced Platform Security Engineer with over 18 years of applied enterprise security experience in secure infrastructure design, risk and vulnerability management across complex systems and networks. Proven track record of “moving the needle”, leading technology transformation, streamlining business processes, and enhancing security controls at an enterprise scale. Influential security professional providing thought leadership across Information Security, Information Technology and Chief Technology Office business units.

CERTIFICATIONS

- CISSP
- AWS Solutions Architect – Associate
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Penetration Tester (GPEN)
- GIAC Certified UNIX Security Administrator (GCUX)
- Red Hat Certified System Administrator (RHCSA)

SKILLS

- Cloud Governance / Compliance
- Security Architecture & Design
- IAM / Privileged IAM Delegation
- Cryptography / SSH Keys
- Prisma Public Cloud / Prisma Compute
- Terraform
- GitLabCI
- Docker
- Bash
- PowerShell
- Python (Beginner)
- Scaled Agile Framework (SAFe)
- Coaching / Mentoring
- Adaptability / Problem-Solving

LEADERSHIP EXPERTISE

- **2018 – “Vigilant Eagle” award:** Enterprise Security Group award for leadership, mitigating USAA’s risk exposure in the public cloud, and building a high performing cloud security team (1 of 10 awardees out of ~500 teammates).
- Thought leader providing guidance and strategy to ensure Information Security preparedness for technology transformation from monolithic architectures to containers and public cloud.
- Created agile teams operationalizing security enablement/remediation, DevSecOps, and Emerging Technology to support Board-of-Director level strategic digital transformation efforts.
- Security Tech Lead for an annual \$10M Public Cloud Security Program of dedicated and matrixed security engineers, with three priorities: Safe Landing controls for new workloads, enabling new business-driven use cases securely, and remediating legacy workloads across AWS, Azure and GCP.
- Lead three Public Cloud Security engineering teams across AWS, Azure and GCP – including new AWS capabilities (PCI, Resilience Automation, Modern Auth), a risk mitigation strategy for USAA’s two Azure tenants, and the resurgence of GCP at USAA for GenAI use cases.
- Guided and developed over 20 engineers transitioning into USAA’s Public Cloud Security and Information Security teams, resulting in multiple team promotions, successful internal and external career moves, and speaking engagements.
- Developed training plans and mentored Information Security engineers interested in cloud security.
- Partnered with SANS to provide feedback on their Cloud Security suite of courses.

CLOUD SECURITY ENGINEERING EXPERTISE

- **2018 – “Innovator of the Year”:** Enterprise Security Group award for developing custom detections within USAA's public cloud environment (annually 1 out of 500 employees selected within department).
- **Public Cloud Account Metadata:** Enterprise application to track and manage USAA's public cloud estate, used daily by 40+ Cloud Security Engineers and 3,000+ developers.
- **S3 Malware Scanning:** Serverless malware scanning solution inspecting 30M+ S3 objects per day.
- **VPC Endpoint Policy Orchestration:** First iteration of a scalable, preventative data perimeter using orchestrated VPC endpoint policies – presented at AWS re:Inforce 2023.
- **Safe Landing Framework:** Service Catalog of approved cloud services with guardrails – 200+ services Safe Landed across AWS, Azure and GCP.
- Former Member of the Palo Alto Cloud Advisory Board helping shape future Palo Alto cloud security products.
- Developed and implemented USAA's “Safe Landing” framework for allowed services within AWS, Azure and GCP, providing a Service Catalog to customers – over 200 services have been Safe Landed across the three major CSPs.
- Developed and implemented least-privilege IAM access patterns at enterprise scale – two AWS Organizations with 450+ member accounts, one Google Cloud Identity and Workspace domain, one GCP domain with 220+ projects, and two Azure tenants with 10+ subscriptions.
- Translated business requirements into security requirements in “crawl, walk, run” iterations – enabling Exploratory environments while enforcing guardrails with SCPs (e.g. restrict IGW), VPC Endpoints, GuardDuty, AWS Config, AMI tagging, and SSM State Manager and Session Manager.
- Translated regulatory scrutiny for USAA's multi-cloud journey into controls – crypto requirements by data sensitivity (client/server-side encryption), AWS managed or customer managed keys, and IAM Role federation with Okta.
- Led a cloud security “tiger team” to identify and remediate critical misconfigurations with custom and open-source tools across 70+ GCP projects, 45+ AWS accounts and 50+ Azure subscriptions.
- Implemented multiple Azure ExpressRoute circuits with VNet Peering supporting Data Scientists, and the first Direct Connect/Transit Gateway in AWS for Firewall and Networking team testing.
- Developed tactical solutions: centralized CloudTrail logs to S3 consumed by the on-premises SIEM, enforced VPC flow logs for GuardDuty, converted IAM Users to Roles, hardware MFA for root, joined accounts into the AWS Organization with SCPs, removed public S3 buckets, enforced encryption, and removed Security Groups open to 0.0.0.0/0.

WORK EXPERIENCE

United Services Automobile Association (USAA) – San Antonio, TX

Lead Information Security Engineer – Cloud

07.2018 – Present

- Led implementation of AWS Resilience Hub within USAA's AWS Organization resulting in the ability to automate onboarding of applications and reporting on their resilience posture to satisfy a regulatory finding.
- Led USAA's first no-notice penetration test exercise within USAA's GCP organization to illustrate gaps in security posture to secure funding and team to safe land USAA's GCP platform environment.
- Identified and led triage activities for NOBLR's AWS Organization (M&A) resulting in a security posture assessment and remediation team to secure their application and services.
- Led holistic triage and remediation of Google's Cloud Identity and Workspace platform – unmanaged identities, unapproved OIDC clients, Shadow IT applications with no governance, excessive IAM entitlements, and usage of non-USAA owned and managed identities.
- Led USAA's first safe landed production AWS use case – Post Catastrophe Aerial Imagery (PCAI) – leveraging DynamoDB, Lambda, S3, SQS, KMS and IAM Roles to quickly capture damage after a catastrophe.
- Secured funding for a multi-cloud monitoring SaaS application – Palo Alto's Prisma Public Cloud (RedLock); automated enrollment of all AWS, GCP and Azure accounts for continuous monitoring.
- Developed and facilitated the implementation of governance processes for USAA's public cloud strategy – reducing cloud accounts on corporate credit cards, a Cloud Review Panel, and closing of unauthorized cloud accounts in AWS, GCP and Azure.

Lead Information Security Analyst

03.2016 – 07.2018

- Created framework and process to build and integrate CIS baseline across enterprise technologies resulting in more fine-grained security controls and enhanced monitoring.
- Led enterprise adoption of SELinux for container orchestration (Red Hat's OpenShift), and later the entire 20,000+ server fleet, to allow developers to fail fast and deliver value-add applications to customers quicker while enforcing mandatory access controls.
- Instrumental in planning, funding, and implementing a SecOps team to enhance security controls within the GitLabCI pipeline – TwistLock's Vulnerability Management and Configuration Management.

Senior Information Security Analyst

06.2013 – 03.2016

Information Security Analyst

08.2008 – 06.2013

Security Support Specialist

06.2007 – 08.2008

- Led and implemented Centrify's Active Directory Bridging for Unix/Linux on over 10,000 systems, reducing managed individual user identities from roughly 35,000 to nearly 2,000 – saving over 200 hours per month in identity administration.
- Implemented MFA for privileged user accounts with BeyondTrust's PowerBroker for Unix/Linux.
- Led complete transformation of Unix/Linux server hardening standards utilizing CIS best practices and Qualys' Policy Compliance tool, automating server monitoring and reducing configuration/patching drift.
- Presented USAA's risk for SSH keys at an enterprise scale, directly resulting in the funding and implementation of SSH's Universal Key Management application – inventoried over 150,000 unique SSH key pairs and removed over 40,000 unused authorizations.
- Implemented BeyondTrust's PasswordSafe (Privileged Session Management) to manage delegation of elevated privileges within cloud applications, servers, and other technologies.

EDUCATION & TRAINING

The University of Texas at San Antonio – BBA, Infrastructure Assurance – Magna Cum Laude, May 2007

- SANS SEC545 – Cloud Security Architecture & Operations
- SANS DEV540 – Secure DevOps & Cloud Application Security
- LASCON – AI SecureOps: Attacking & Defending AI Applications and Services

BLOG POSTS AND EXTERNAL COLLABORATION

- Public Cloud Account Metadata – <https://aws.amazon.com/blogs/architecture/how-to-track-aws-account-metadata-within-your-aws-organizations/>
- S3 Malware Scanning – <https://aws.amazon.com/blogs/architecture/how-usaa-built-an-amazon-s3-malware-scanning-solution/>
- VPC Endpoint Policy Orchestration – <https://aws.amazon.com/awstv/watch/7bfd0425cfb/>