DAVID ALEXANDER ("ALEX") STEIN

Cloud Architecture | Cyber Security Engineering | Network Infrastructure | Regulatory Compliance
Richmond, VA | 804.852.0855 | DAStein86@gmail.com

PROFESSIONAL SUMMARY

Cloud architect, cyber security engineer and US Army Veteran with 16+ years across infrastructure, network engineering, and high-level security operations. Designed and built a complete AWS-native production environment from inception and stood up a full regulatory compliance program (SOC 2 Type 2, PCI DSS, GDPR, CCPA) at an insurance technology SaaS organization. Background spans MSP/MSSP service delivery, U.S. Army Cyber operations, and enterprise network architecture across multinational environments.

TECHNICAL SKILLS

Cloud: AWS (ECS, EC2, ECR, Secrets Manager, Amplify, VPC, IAM, S3, RDS, Lambda, CloudFront, KMS, WAF, Cloudwatch, CloudTrail), GCP (Compute, IAM, Cloud Storage, Cloud Run, Vertex AI, Colab), Microsoft 365 & Azure (Entra ID / Active Directory, Exchange, Security, Intune, Sharepoint, Virtual Machines)
Security & Compliance: SOC 2 Type 2, PCI DSS, GDPR, CCPA, HIPAA, ISO, NIST; pentesting, vulnerability management; incident response and forensics; endpoint and email security; IDS/IPS, WAF, Firewall
Networking: Cisco IOS routing/switching (Catalyst, Nexus, Meraki), Cisco ASA NextGen firewalls with SourceFire, site-to-site VPN, MPLS network segmentation, wireless implementation & optimization
Identity & Endpoint: Active Directory, Microsoft Entra ID, Conditional Access, Group Policy, SCCM, Intune, Defender, Microsoft Purview, Citrix XenApp, JAMF, Mosyle, Apple Business Manager, Google Workspace, IAM
Infrastructure: Windows Server (2008 R2 – 2022), Exchange Server, Exchange Online, Microsoft 365, SQL Server, IIS, VMware vSphere, Windows / macOS / Linux
Scripting / Coding: PowerShell, Bash, Javascript, Python, Infrastructure-as-Code (IaC) using SST & Pulumi

PROFESSIONAL EXPERIENCE

Director of Information & Security

2022 – Present

***Buddy** - Richmond, VA - Insurance technology ecommerce and administrative SaaS platform*

- Designed and built the company's complete AWS production environment from inception, including an automated CI/CD pipeline, IaC deployment workflows, VPC architecture, IAM strategy, encryption standards, network segmentation, and high-availability patterns for an insurance platform handling regulated data.
- Built and operated Buddy's internal IT infrastructure platform, including centralized endpoint administration (workstation provisioning, patch testing and distribution, endpoint security and EDR), identity and access management for corporate users, networking and connectivity tooling, and helpdesk and ticketing systems.
- Established the company's information security and regulatory compliance program from zero to fully qualified across SOC 2 Type 2, PCI DSS, GDPR, and CCPA — sole owner across policy authorship, control implementation, audit coordination, and ongoing evidence management.
- Operationally hybrid AWS/GCP cloud architecture; maintain GCP environment dedicated to AI/ML development workloads using Vertex AI and associated compute services.
- Partner with the development team on secure SDLC practices, security review of architectural changes, infrastructure-as-code patterns, and integration of security tooling into development workflows.
- Lead development of custom AI solutions for the business, including creation and hosting of internal MCP services, chat and RAG application development, external API integration and ingestion pipelines, and cloud-native deployments on AWS and GCP.

Founder & CISO

2018 – Present

***Bluetec** - Richmond, VA · Managed security and technology services firm*

- Lead security engineering and architecture engagements across MSP/MSSP, incident response, vulnerability assessment, and penetration testing for small and mid-market clients.
- Recently led incident response on a Microsoft 365 tenant compromise: forensic investigation under significant audit log limitations, attacker persistence identification, and post-incident rebuild of the tenant's identity and access controls.

- Designed and implemented Microsoft 365 secure configurations across multiple client tenants, including Exchange Transport Rules with Microsoft Purview Message Encryption, Conditional Access, MFA enforcement, and Defender configuration.
- Scaled the practice to 13 concurrent recurring contracts before transferring all recurring contracts to a partner MSP in 2022 to focus on the Buddy role; continue selective project-based engagements.

Senior Network Security Engineer *2018 – 2019*

Lumber Liquidators *- Toano, VA · Publicly traded national retailer, 400+ stores*

- Designed and operated EDR, vulnerability management, and DLP security controls across the enterprise.
- Led the enterprise vulnerability management program: scan coverage, prioritization frameworks, and cross-team remediation tracking across infrastructure and application owners.
- Performed enterprise security assessments, identified and reported critical infrastructure and process gaps to leadership, and developed remediation roadmaps.
- Executed daily security operations including event monitoring, alert triage, and incident response.

Network Engineer *2015 – 2018*

Independent Container Line *- Glen Allen, VA · International shipping enterprise, US and European offices*

- Owned global IT infrastructure spanning multiple US and European offices: WAN architecture, perimeter security, server operations, and end-user computing.
- Designed and operated multi-site Cisco environment including ASA firewalls with SourceFire/FireAMP, Catalyst and Nexus switching, site-to-site VPNs connecting multiple US and European locations.
- Migrated company website and disaster recovery infrastructure to Microsoft Azure; integrated Azure-based DR for domain services and on-premises systems.
- Led Windows 7 to Windows 10 migration across global endpoints using SCCM; maintained Citrix XenApp environment for distributed users.

Migration Project Manager / Deskside Support *2014 – 2015*

VCU Health Systems (Networking Technologies + Support) *- Richmond, VA · Trauma 1 University Hospital*

- Promoted from migration technician to project manager within six months; led a six-technician team through migration of 10,000+ workstations across 30+ departments and statewide locations, closing the project six months ahead of forecast.
- Transitioned to deskside engineering role following project closure: tier 2 and 3 incident response, Active Directory and SCCM administration, and break-fix engineering across multiple departments.

MILITARY SERVICE

First Lieutenant — Cyber & Signal Operations *2013 – 2019*

U.S. Army National Guard, Virginia

- **91st Cyber Brigade, 143rd Cyber Warfare Company (2017 – 2019):** Network Warfare Team Lead in one of the Army's earliest Guard cyber units. Designed and implemented offensive cyber operations training programs for a ~100-person company. Coordinated with the sister 133rd Cyber Security Company on joint operations including those supporting internationally-oriented, federal objectives. Led teams delivering scheduled penetration tests and vulnerability assessments for state and municipal government partners.
- **29th Infantry Division (2013 – 2017):** Signals Officer and Executive Officer in dual-role assignment supporting Division HQ A Co (Operations) and C Co (Signals). Led 45+ Signals personnel; supported Division-level communications across radio, satellite, line-of-sight, and transport encryption systems. Supported 400+ personnel through deployment and garrison operations.

EDUCATION & CERTIFICATIONS

Bachelor of Science, Anthropology — Virginia Commonwealth University, Richmond, VA
Certifications & Clearance: CompTIA Security+ | U.S. Department of Defense Secret Clearance
Honor Graduate - Signal Basic Officer Leadership, Fort Gordon, GA