

Austin R. Mann

Vice President, CyberSecurity Engineering

| Network Security | Intrusion Detection | Forescout / NAC | Hybrid Cloud
austinmann.net | firemann816@hotmail.com | LinkedIn

PROFESSIONAL PROFILE

Senior cybersecurity engineer with 20+ years of experience securing enterprise, financial-services, healthcare, federal, on-prem, cloud, and hybrid environments. Specialized in intrusion detection, network security monitoring, Forescout/NAC, SIEM/IDS telemetry, endpoint visibility, packet analysis, segmentation, and security architectures. Known for translating complex technical risk into practical remediation plans, supporting regulated environments, and improving security posture across large, distributed networks.

CORE COMPETENCIES & TECHNICAL EXPERTISE

Security Engineering, Intrusion Detection, IDS/SIEM Analysis, Incident Response, Threat & Vulnerability Analysis, Zero Trust, Network Segmentation, Host Posture Assessment, Endpoint Visibility Platforms & Tools: Forescout CounterACT, Splunk, SentinelOne EDR, JAMF, ServiceNow, Snort/Snort Rules, Packet Analysis, Cisco Security Products, Cisco IOS, Extrahop, Armitis, Ansible Cloud, Infrastructure & Compliance: AWS, Azure, Aviatrix, Hybrid Architecture Migration, Server Hardening, Financial Services Security, HIPAA, DISA STIG Alignment.

PROFESSIONAL EXPERIENCE

Vice President, CyberSecurity Engineering / Regions Bank | Oct 2024 - Present | Network Security

- Recruited back to Regions Bank to support enterprise network security engineering within a regulated financial-services environment.
- Administer and engineer Forescout capabilities supporting endpoint visibility, access control, compliance monitoring, and network segmentation.
- Re-addressed Forescout platform IPv4 infrastructure to remove blockers for a broader enterprise network segmentation initiative.
- Upgraded Forescout from 7.x to 8.5.x and built a dedicated lab environment for validation, troubleshooting, and controlled change testing.
- Use Splunk, SentinelOne EDR, JAMF, ServiceNow, and endpoint telemetry to support investigations, operational workflows, and remediation efforts.

CyberSecurity Engineer / Alchemy Global Networks | Jan 2022 - Oct 2024

- Oversaw Forescout CounterACT deployment for a U.S. Federal Government agency, supporting network visibility, access control, and security posture management.
- Identified, prioritized, and communicated 50+ critical security risks quarterly, contributing to a documented 15% reduction in incident response time.
- Administered Forescout platform updates to keep network topology, endpoint posture, and operational workflows aligned with current requirements.
- Supported cybersecurity policy improvement, operational best practices, team collaboration, client-facing reporting, and security training material development.

Network Intrusion Detection Engineer / Regions Bank | Nov 2017 - Dec 2021

- Monitored network traffic, endpoint logs, and IDS/SIEM alerts to detect, report, and mitigate threats to financial networks.
- Managed intrusion prevention systems and tuned IDS signatures to align with observed attack patterns and recommended mitigation actions.
- Implemented Forescout CounterACT to monitor endpoint compliance and control network access for noncompliant devices.
- Collaborated with SIEM administrators to integrate IDS telemetry, accelerate response workflows, and improve threat visibility.
- Supported hybrid-cloud migration efforts for DLP and IDS platforms while serving as an escalation point for CyberSecurity Operations Center analysts.

PROFESSIONAL EXPERIENCE (CONTINUED)

Senior Consultant / eLoyalty / TTEC | Oct 2011 - Nov 2017

- Participated in 30+ concurrent projects over five years, with average budgets generally ranging from \$500K to \$2.5M.
- Installed, upgraded, secured, and documented Cisco Unified Communications products, aligning platforms with DISA STIGs and monitoring requirements.
- Developed and executed User Acceptance Test Plans and conducted audits of the TTEC Cloud Based Contact Center as a Service platform.

Network Engineer / Preston Health | Oct 2009 - Oct 2011

- Designed and maintained healthcare network, systems, and clinical devices while safeguarding sensitive data through anti-malware, host firewall, and encryption controls.
- Executed secure backup strategy across four locations and led a \$100K+ server and desktop refresh through an independent bid process.

Network Engineer / Marshall Medical Centers | Oct 1999 - Oct 2009

- Scaled, secured, and monitored a hospital network from under 100 to 1,200+ nodes, supporting clinical operations and revenue-cycle improvements.
- Supervised Network Support Technicians and administered firewall and encryption controls to protect healthcare information.
- Received CNSS and NSA recognition for meeting CNSS 4011 and 4013a requirements.

EARLY EXPERIENCE & LEADERSHIP

Technical Trainer, CompUSA (Jun 1998 - Oct 1999): Delivered technical training to diverse audiences in-house and at client locations. | Firefighter/EMT, Cocoa Fire Rescue (Dec 1989 - Jun 1997): Served on focused emergency-response teams under adverse conditions, performing search, rescue, and first-responder medical care.

CERTIFICATIONS & TECHNICAL EDUCATION

Current: AWS Certified Cloud Practitioner; AWS Certified Solutions Architect - Associate; Microsoft Certified: Azure Fundamentals; Aviatrix Certified Engineer; Forescout Certified Administrator; CompTIA CyberSecurity Analyst (CySA+); GIAC Security Essentials (GSEC); GIAC Intrusion Analyst; Splunk Fundamentals 01; ExtraHop Foundations.

Historical: 10+ legacy credentials including Cisco CCNP suite, VMware VCP, Microsoft MCSE, CompTIA A+, Network+, and Security+.