Technology moves quickly, so do I

Austin R. Mann

September 2021

Intrusion Detection / Cyber Security \ Network Administration

3108 Sunrise Dr. Guntersville AL 35976
firemann816@hotmail.com \ also LinkedIn
SUBMITTED IN CONFIDENCE | *References Available Upon Request.*

Summary of Qualifications:

Intrusion Detection Engineer with twenty years experience in Information Services. Career achievements include numerous vendor certifications with focus on securing enterprise networks. Specializations include Intrusion Detection, Analysis and Response. Experience with On Prem, Cloud, and hybrid architectures.

Skills & expertise:

Forescout CounterACT | Cisco Security Products | Network Deployment & Design | Intrusion Detection | Threat and Vulnerability Analysis |Host Posture Assessment | Server Hardening | Snort |Snort Rules| Splunk | Cisco IOS | Amazon Web Services | AWS | Zero Trust Architectures | Network Segmentation | Packet Analysis | Incident Response |

Professional Experience:

Network Intrusion Detection Engineer / Regions Bank / Nov 2017 – Present

Monitor and analyze network traffic, network or end point logs, IDS\SIEM alerts to detect, report, and mitigate threats to financial networks. Manage and maintain intrusion and event detection architecture. Monitor internal network end points for compliance with corporate security policy, denying network access to noncompliant end points. Tune IDS Signatures to match observed attack patterns and agreed upon mitigation actions. Participate in the investigation and remediation of security incidents. Perform, review and communicate security project tasks. Work with SIEM admins to feed IDS telemetry to their platform. Engage SIEM Admins to customize automation and orchestration actions. Collaborate with SIEM admins to automate initial responses to detected malicious traffic. Support escalations from CyberSecurity Operations Center analysts. Supported migration of Data Loss Prevention platform from on prem to AWS hosted successor. Support migration to hybrid architecture of current IDS platform from on place to cloud for management plane. Create IDS shift logs, review shift logs from adjacent teams. Communicate intrusion detection practices with adjacent teams.

Senior Consultant | eLoyalty - Ttech | Oct 2011- Nov 2018
Install, upgrade, secure, and document Cisco Unified Communications products. Secure Cisco Unified Communications platform to align with DISA STIGs. Ensure Unified Communications elements integrate into management and monitoring platforms. Develop and execute User Acceptance Test Plans to ensure the solution meets customer requirements and scope of work. Perform project work either remotely or onsite in the customer's environment. Travel to client locations serving in a customer facing capacity. Conduct audits of TTEC Cloud Based Contact Center as a Service platform. Participate in over thirty concurrent projects in a five-year period, average budget generally ranging from $500K to $2.5M.

Network Engineer | Preston Health | Oct 2009 - Oct 2011
Design and maintain a healthcare delivery network, computer systems, and related clinical devices. Install and centrally manage anti-malware software, host based firewalls and data encryption programs, to protect sensitive data. Developed and executed a secure backup strategy in each of our four locations. Installed and supported secure billing systems, trained coworkers in HIPPA practices and compliance. Employer was audited annually by governing bodies, and consistently found deficiency free. Independently executed a bid process to acquire new servers and desktops across our locations during a tech refresh valued over $100,000.

Network Engineer | Marshall Medical Centers |Oct 1999 - Oct 2009
Supervise, develop, and evaluate our Network Support Technicians under direction from our Chief Information Officer. Design and deploy an IP addressing scheme for our growing healthcare system allowing us to add clinical devices to the network. Network enabling our clinical systems increased the quality of patient outcomes while speeding the revenue cycle. Grew the network from under 100 devices to over 1200 nodes during my tenure. Scaled, secured, documented, and monitored our network while supporting the business objectives. Collected network data to evaluate and optimize network performance. Evaluated and purchased network monitoring software. Installed, and administered firewalls and data encryption programs to safeguard protected healthcare information. Upgraded all network hardware during product life cycles. Developed vendor relationships to ensure their product implementations met solution definition, our project budget, and was deployed in accordance with our governing policies. Train end users in proper use of hardware and software. Received letters of recognition from Committee on National Security Systems (CNSS) and the National Security Agency (NSA) for meeting CNSS 4011 and 4013a requirements.

Technical Trainer | CompUSA | June 1998 - Oct 1999
Communicate and convey technical information to varying sizes of student audiences. Deliver training in employer’s training center, or client locations. Taught a variety of students of diverse backgrounds with varying skill levels. Solicit feedback and reviews from students to ensure customer satisfaction and knowledge transfer.

Firefighter/EMT | Cocoa Fire Rescue | Dec 1989 - June 1997
Work as a member of a focused team under adverse conditions. Perform search and rescue during lifesaving operations. Deliver first responder medical care, ensure continuity of care by higher medical authorities.

Technical Education / Industry Vendor Certifications:

Current:

Aviatrix (May 2020 to Present) — Aviatrix Certified Engineer, ACE.

Forescout: (February 2018 to Present)

- Forescout Certified Administrator

CompTIA: (August 2018 - Present)

- Cybersecurity Analyst

SANS (November 2018 - Present)

- GIAC Security Essentials (GSEC)
- GIAC Intrusion Analyst Certification

Amazon Web Services: (July 2018 - Present)

- Certified Cloud Practitioner
- Solutions Architect Associate *(In Progress)*

Splunk

- Fundamentals 01

Extrahop

- Foundations

Historical:

Cisco Systems: (June 2000 to August 2018)

- *Cisco Certified Network Associate*
- *Cisco Certified Network Professional.*
- *Cisco Certified Network Professional – Security.*
- *Cisco Certified Network Professional – Voice.*
- *Cisco Certified Network Professional – Collaboration.*
- *Cisco Web Security Field Engineer*
- *Cisco Advanced Security Architecture Field Engineer*

VMware: (August 2013 to August 2017)

- *VMware Certified Professional, 5.5 - Data Center Virtualization.*
- *VMware Certified Professional, 6.0 - Cloud Management & Automation.*

Microsoft: (September 1999 to September 2004)

- *Microsoft Certified Systems Engineer. (Windows NT4.0 & Windows 2000)*

CompTIA: (September 2000 to September 2002)

- *CompTIA A+, Network+, Security +*