Brady Bruton

Abilene, TX • bradybruton@mac.com • linkedin.com/in/bradybruton

---

Security Analyst - Information Security

Driven and efficient Security Analyst with 15+ years of experience in IT and networking with extensive people and project management skills. Several years in firewall administration, active directory and file share security with extensive knowledge in endpoint detection, vulnerability management, rapid incident response and penetration testing.

WORK EXPERIENCE

First Financial Bank • Abilene, Tx
Security Administrator Team Lead • Full-time • 12/2023 - Present

- Manage long-term projects and interpersonal communications between 4-5 departments and about 20+ vendor relationships through attention to detail and expert prioritization to ensure daily operational success
- Installed an IDS system using packet brokers and Corelight, leveraging AI with Suricata signature matching and Zeek logs to analyze and alert on traffic patterns and anomalies
- Onboarded Varonis to secure file shares and protect hundreds of thousands of sensitive organization-wide exposed files and inconsistent permissions in just a few short months
- Successfully implemented DMARC email enforcement to reduce fraud and email spoofing, blocking around 6k malicious emails per month
- Administer WAF and firewall policies during an SD-WAN migration initiative and HA failover installation to maximize availability, redundancy and uptime

Security Admin I/II • 11/2022 - 12/2023

- Onboarded new MSSP and set up SIEM and all connections to it, providing correlation analysis, rapid incident response, more than doubling our network visibility and implementing 24/7 MSSP support
- Oversees EDR solutions, manage endpoints, live response, malware infection mitigation and leveraging proxies for web content filtering and data loss prevention
- Perform timely threat-hunting based on current threat intelligence in order to stay ahead of potential security incidents using various tools and security systems and platforms
- Streamlined our EDR policies to enhance detection and reduce false positives, resulting in fewer production issues in our environment and adoption across all compatible endpoints
- Administer password vault, VPN, O365 email management, Abnormal for BEC attacks and UEBA analytics & entrusted with the highest level of security for all passwords, access to emails and files for the entire organization

Gateway Cabling LLC • Abilene, Texas
Lead Technician • Full-time • 11/2017 - 12/2022

- Managed multiple 5-10 worker crews all over the state of Texas for various installs, troubleshooting and consulting jobs
- Installed & configured networking equipment (phones, IP cams, APs, POS, racks, servers, fiber/cat6)
- Terminated and fusion spliced fiber optics, Cat6, and soldered A/V connectors. Built out LAN rooms, cable management, diagramming connections, floor plans and doing regular site surveys

Brady Cases LLC • Abilene, Texas
Owner • Full-time • 09/2007 - 11/2018

- Started & operated my own business for 11 years & grew to an internationally-renowned brand
- Designed and constructed tens of thousands of custom ATA cases for the music industry, production, government and other industries
- Web design and maintenance, CRM, IT, 3D renderings, payroll, excel documents, marketing, social media, HR, inventory and ordering, quotes, and much more
- Spearheaded the successful management of a large team, resulting in optimized production processes and a positive work environment for nearly 100 individuals

EDUCATION

Studies in Business Administration
Hardin-Simmons University • 08/2004 - 05/2005

High School Diploma
Abilene High School

SKILLS

Hard Skills

- Adept in basic Python/Bash/ JavaScript
- Advanced in File Security
- Expert in SIEM analysis and EDR Management
- Highly experienced in Incident Response
- Proficient in Mac, Linux, Windows and Wireshark
- Skilled with Firewall Administration
- Skilled with Project Management and Team Coordination

Soft Skills

- Conflict Resolution
- Goal-setting
- Interpersonal Communication

Personal

- Cycling
- Photography
- Studio Musician
- Triathlons

CERTIFICATIONS

CompTIA PenTest+ • 07/2024 - 07/2027

CompTIA Cybersecurity Analyst (CySA+) • 12/2023 - 12/2029

CompTIA Security+ • 07/2023 - 12/2029

CompTIA Network+ • 08/2022 - 12/2029