Brady Bruton

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

Threat Hunter - Information Security

Threat Hunter who enjoys asking questions security tools were not designed to answer. Combines threat intelligence, enterprise telemetry, and behavioral investigation to uncover adversary activity and security gaps beyond existing detections.

WORK EXPERIENCE

Fulcrum Technology Solutions – Remote

Threat Hunter • Full-time • Jan 2026 – Present

- Develop and execute intelligence-driven and hypothesis-based threat hunts using enterprise telemetry, MITRE ATT&CK, adversary TTPs, and behavioral analysis to identify attacker activity and security gaps beyond commercial security detections
- Produce tailored cyber threat intelligence, dark web assessments, and hunting packages from OSINT, commercial intelligence, and customer-specific requirements to drive proactive hunting and informed security decisions
- Lead enterprise threat hunting engagements from planning through executive reporting, delivering technical findings, threat intelligence, and remediation recommendations directly to security leadership, including recurring CISO briefings
- Build scalable threat hunting capabilities through documented methodology, reusable hunt queries, AI-assisted threat research workflows, and knowledge management resources that improve analyst consistency and customer coverage
- Identify adversary tradecraft including living-off-the-land techniques, credential abuse, shadow IT, unauthorized remote management tools, and policy weaknesses through behavioral and hypothesis-driven hunting rather than IOC-only detection

Security Analyst II • Full-time • Sep 2024 – Jan 2026

- Led investigation and triage of alerts across varied customer environments using multiple SIEM, EDR/XDR, and SOAR platforms
- Performed targeted threat hunts using customer telemetry, intel feeds, and tool-based anomaly detection
- Reviewed Tier 1 escalations; validated alerts, guided remediation, and documented outcomes
- Assisted in detection tuning, rule creation, and process automation to improve SOC efficiency & response time
- Collaborated with clients during active incidents and postmortems; wrote investigation summaries and runbooks

First Financial Bank Texas – Abilene, TX • Hybrid

Security Administration Team Lead • Full-time • Nov 2023 – Sep 2024

- Managed cross-department security projects and vendor relationships across 4–5 internal teams
- Oversaw Corelight and Suricata-based IDS deployment with Zeek integration for layered detection
- Led onboarding and tuning of Varonis and Valimail to improve visibility and reduce fraud risk
- Directed operational readiness and tool rollout during SD-WAN, HA failover, and MSSP transitions
- Mentored junior analysts, delegated investigations, and developed response runbooks and playbooks

Security Administrator I/II • Full-time • Nov 2022 – Nov 2023

- Led alert response and malware triage through EDR tools and endpoint live investigations
- Managed onboarding of a new MSSP and integrated SIEM pipelines for full visibility and 24/7 support
- Administered security systems including password vaults, email security (Abnormal), and proxies
- Refined EDR policies to reduce false positives and expand coverage across endpoints
- Performed threat hunting, escalation validation, and vulnerability triage using multiple toolsets

Gateway Cabling LLC – Abilene, TX

Lead Technician • Full-time • Nov 2017 – Dec 2022

- Managed field tech teams and hands-on deployments for fiber optics and network infrastructure across Texas
- Provided consulting, installation, and troubleshooting for networking hardware and low-voltage systems

Brady Cases LLC – Abilene, TX

Owner • Full-time • Sep 2007 – Nov 2018

- Founded, built, and scaled a globally recognized manufacturing brand for custom ATA road cases
- Led all operations including design, IT systems, team management, and marketing for international clients

PLATFORMS & TECHNICAL SKILLS

Threat Hunting & Response: Intelligence-driven and hypothesis-based hunting • MITRE ATT&CK • Behavioral analysis • Incident response • Alert triage • Detection tuning • Malware analysis • Digital forensics

Endpoint & Network Security: CrowdStrike Falcon • SentinelOne • Microsoft Defender for Endpoint • Cortex XDR • Carbon Black • Tanium • ExtraHop • Corelight/Zeek • Suricata

SIEM, XDR & Security Analytics: Splunk • Microsoft Sentinel • Google SecOps/Chronicle • Elastic Security • Exabeam • Cortex XSIAM/XSOAR • QRadar

Identity, Exposure & Email Security: Tenable • Varonis • Entra ID • Okta • Delinea Secret Server • Obsidian Security • Valence Security • Proofpoint • Mimecast • Abnormal Security

Security Operations: Cross-platform telemetry analysis • Query development • Customer-specific threat intelligence • Dark web monitoring • Executive reporting • Detection validation • Runbook and hunt-methodology development • Bring-your-own-stack MSSP environments

Forensics & Utilities: Wireshark • CyberChef • Autopsy • CAPEv2 • DeepBlueCLI

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

CompTIA PenTest+: Jul 2024 – Jul 2027
CompTIA CySA+: Dec 2023 – Dec 2029
CompTIA Security+: Jul 2023 – Dec 2029
CompTIA Network+: Aug 2022 – Dec 2029
Blue Team Level 1 (BTL1): Jun 2025
LogRhythm Security Analyst (LRSA): Oct 2025
OffSec TH-200: In progress; expected Q3 2026
Hack The Box CDSA: Exam scheduled

EDUCATION

Hardin-Simmons University — Studies in Business Administration | Aug 2004 – May 2005
Abilene High School — High School Diploma

ADDITIONAL

Endurance Sports: Ironman triathlete • Ultrarunner • Ultra-distance cyclist