Brent Harrell

www.linkedin.com/in/brent-harrell • https://bitsofharmony.com/security
Red Team Maturity Model: https://redteammaturity.com

EXPERIENCE

Principal Red Team Consultant January 2024 - Present
CrowdStrike |Remote

- **Leading, defining, and executing** a full spectrum of offensive security operations, including adversary emulation, internal red team exercises, and large language model (LLM) penetration tests.
- **Founding member** of the CrowdStrike Professional Services AI Red Team, defining core workflows, reporting practices, and driving learning and adoption across the Red Team.
- **Authored** a customer-facing workshop covering the theory behind LLMs, state-of-the-practice attack methodologies, and mitigation strategies. Called the best material on LLMs to date by multiple customers.
- **Giving back to the community** through blog authorship, thought leadership on the CrowdStrike Adversary Universe podcast, and community presentations at BSidesLV and DEF CON Red Team Village.
- Received the **2024 Red Team MVP** award on a team of over 50 operators for continuous contributions to the team's knowledge, thought leadership, and execution on strategic objectives outside of routine exercises.

Red Team Lead, Principal Engineer May 2022 – January 2024
Humana |Remote

- **Created and published** the first standard-format **Capability Maturity Model for Red Teams**, lauded and/or adopted by multiple Fortune 500 companies as a benchmark to share Red Team progress with leadership.
- **Built a new internal Red Team**, providing mentorship on a broad range of offensive disciplines and soft-skills. **Defined core processes and standard operating procedures** to enable enduring success.
- Delivered critical findings through Red Team operations and unique approaches to Purple Team activities. **Began an internal process** to track defensive concerns, **covering over 60%** of the most pressing issues in the first year.
- **Established strong partnerships and trust** with defensive partners in incident response, engineering, and leadership that the Red Team will provide actionable data; consistently validated through routine feedback.
- **Contributed to the security community** through emulated malware development and release of the RTCMM.
- **Increased** information sharing from the Red Team **more than 10-fold** in my first year through lunch and learns, conference presentations, and training series targeted at general and technical audiences.

Lead Offensive Security Engineer January 2021 – May 2022
The MITRE Corporation |McLean, VA

- USSF Red Team Lead. **Led engineers** targeting Windows/Linux environments using various command and control frameworks. **Received a commendation** for support to the DoD Hack-a-Sat 2 event execution.
- **Co-led a development team of 10 engineers** for MITRE Engenuity ATT&CK Evaluations resulting in successful execution of evaluations against MSSPs and EDR vendors.
- **Led CALDERA development efforts** in the area of operator improvements. **Increased CALDERA capabilities from a single exfiltration-related ability to nearly all ATT&CK exfiltration techniques**.
- **Created and led a 10-part training program** combining lectures and demonstrations, adopted as a recurring class that was lauded by engineers of all levels as **the clearest presentation of offensive materials** they have received.

System Security Engineer November 2017 – January 2021
Modern Technology Solutions, Inc | Alexandria, VA

- **Worked across engineering disciplines** to guide execution through the early stages of the program. Praised by the program manager for effective communication **leading to a demonstrable shift in security culture**.
- Decomposed complex cyber-physical systems to **identify risk and engineer mitigations** at the appropriate system level. Engaged program management and engineering teams to ensure minimal disruption to operations.
- **Led standardization efforts** for the team of system security engineers. Planned and hosted a multi-day security summit, with the resultant recommendations adopted by the Air Force Rapid Capabilities Office's chief engineer.
- **Mentored new and struggling team members** on security engineering practices and **established standard operating procedures** that created cohesion across engineers supporting diverse, sensitive programs.

Cybersecurity Analyst April 2016 - November 2017
K2 Group, Inc | Washington, DC

- Single-handedly authored a comprehensive assessment on vulnerabilities in a critical Air Force system, briefed to the Secretary and Chief of Staff of the Air Force and all relevant combatant commanders, **leading to an initial $500 million budget increase for cybersecurity** on the system.
- Supported the Air Force Red Team with threat modeling, vulnerability assessments, and cyber threat intelligence (CTI) leading to successful exploit development and/or engagements.

CONFERENCE PRESENTATIONS *(most slides available on GitHub)*

- **DEF CON Red Team Village Workshop**
- **Financial Services and Healthcare ISAC Summits 2023**
- **Red Team Summit** (panel)
- **BSides Las Vegas** (2x)
- **Humana Cybersecurity Awareness Week** (2x - technical and general sessions)
- **Safebreach Validate East**

PUBLICATIONS AND CVEs

Red Team Capability Maturity Model | https://www.redteammaturity.com
Published on Multiple Organizational Blogs (links available on my personal site) | https://bitsofharmony.com

CVE-2021-41315 (Privilege Escalation) | **CVE-2021-41316** (Argument Injection)

EDUCATION

Bachelor of Science in Computer Science, *Summa Cum Laude* | University of Maryland, Global Campus

Bachelor of Arts in Political Science and International Affairs, *Summa Cum Laude* | Florida State University

CERTIFICATIONS AND COURSES

- Modern Initial Access Training
- Sektor7 Malware Development Essentials, Intermediate, and Advanced
- Evasion Techniques and Breaching Defenses (OSEP) (course only)
- Penetration Testing with Kali Linux (OSCP)
- Certified Information System Security Professional (CISSP) (voluntarily expired)