CAMERON BABCOCK

PHONE: 831-574-9662
TS/SCI + FSP last active 2024
Cameron@RealAmericanSecurity.com

CERTIFICATIONS: GSEC, NET+, GCFA, GCFE, CISSP, GCIH, GSTRT, GCIA

Principal Software Engineer with 10+ years in Windows kernel development, EDR architecture, and offensive cyber tooling. Recognized by NNSA Deputy Director for presidential cyber policy contributions. Proven track record leading DoD/DoE CNO operations and architecting enterprise security solutions.

EXPERIENCE

Principal Software Engineer – Sophos / SecureWorks 2024-CURRENT

- Architected and developed enterprise EDR software across kernel- and user-mode components in modern C++, allowing the platform to compete, and outperform established security vendors
- Spearheaded adoption of AI agents and agentic development workflows across the agent and kernel teams, modernizing a nearly 100,000-line legacy codebase and driving compliance with new post-acquisition linter and engineering standards.
- Engineered proactive threat detection mechanisms capable of identifying shellcode injection and zero-day exploits through behavioral analysis and capture, before execution
- Designed high-fidelity agent telemetry systems that improved endpoint visibility while reducing operational costs by roughly 50% compared with competitor approaches
- Created AI powered crash dump analysis utility that enables real-time bug identification in production environments and detection of potential EDR bypass attempts
- Served as Principal Engineer on Windows agent development for both Taegis and Sophos endpoint platforms.
- Conducted security assessments and code reviews uncovering APT-level attack techniques, subsequently implementing hardening measures to strengthen endpoint protection against advanced threats

Senior CNO Software Engineer – Raytheon Cyber 2022-2024

- Architected and developed Computer Network Operations (CNO) toolsets including custom implants, command-and-control infrastructure, and specialized loaders with comprehensive threat modeling and operational security considerations
- Led R&D efforts within the Windows CNO group, driving development of advanced evasion techniques across Windows, macOS, iOS, and Linux through hardware virtualization and hypervisor-based obfuscation and anti-analysis mechanisms.
- Transformed development lifecycle by implementing automated testing infrastructure including custom loader frameworks and C2 emulators, accelerating QRC validation and establishing CI/CD pipelines within existing operational constraints

Software Engineer/Systems Vulnerability Analyst–National Security Agency 2020-2022

- Recognized as part of 3-person team cited by name in presidential cyber policy initiatives and by NNSA Deputy Director in formal discussions on U.S. national cyber strategy.
- Acted as deputy lead for red team and blue team operations assessing cyber defense capabilities across DoD and DoE enterprises, focusing on zero-day threats and advanced persistent threats, resulting in detection frameworks adopted across multiple organizations.
- Led research into supply chain attack methodologies through binary manipulation, compiler tampering, and code injection techniques to replicate and defend against SolarWinds-class compromise vectors
- Authored technical analysis reports on software security assessment tools published to DoD, DoE stakeholders and presented by branch chief at DEF CON security conference
- Conducted reverse engineering and vulnerability research on critical applications to identify security flaws and detect malicious subversions within production codebases. As well as performed CNO duties.
- Performed security audits and penetration testing of Java, .Net and other Web applications, and assisted creators of OWASP WebGoat training software for Java web application security.
- Oversaw development of Juliet Test Suite, a NIST/NSA test suite and review library for CWE’s

Prior Experience 2014-2020

- Software Engineer – World Vision Technologies (Defense Language Institute Contractor) (2018-2020)
- Security Researcher/Software Engineer – Devs of the West (2014-2018)

Education

- Bachelor of Science in Computer Science – California State University Monterey Bay

Technologies

C++, C, CPPUNIT, C#, Unit Testing, .Net, Java, AWS, Azure, GCP, Ghidra, IDA, IDA PRO, Confluence, Wiki, SVN, git, LibSSL, openSSL, BoringSSL, Android, Windows, Windows Server Administration, Linux Server Administration, Java, JUNIT, HTML, SQL, Blazor, Razer, Nodejs, Javascript, Active Directory, Jenkins, Ruby, Groovy, RAII, Object Oriented Programming, Functional Programming, TCP, IP, TCP/IP, UDP, Network Forensics, X86, X86-64, Assembly, Powershell, Bash, Scripting, Docker, Virtualization, UNIX, Network Programming, Network Engineering, CVS, System Architecture, Test Driven Development (TDD), AGILE, Scrum, Protocol Analysis, Source Management Tools, JIRA, Socket Programming, VMWare ESXi, Hyper-v, Postgres, ARM, Vulnerability Research, Vulnerability Analysis, Fuzzing, Rust, Exploit Development, PE Files, QT, Metasploit, Pentesting, Subversion, Makefiles, VSBUILD, Multi-threaded Programs, Algorithms