SIDDARTH KANAPARTHY

Offensive Security Specialist | Red Team Operator | Threat Intelligence Researcher

limeinc.official@gmail.com | (270) 484-0983 | Nashville, TN
lime-sec.netlify.app | github.com/LimeIncOfficial

CLEARANCE: Secret (NATO) — Active | TS/SCI Eligible

SUMMARY

Offensive security professional with operational experience across enterprise red team operations, vulnerability research, threat intelligence, and computer network exploitation. Led red team engagements against Active Directory environments, cloud infrastructure, ICS/SCADA systems, mobile platforms, and air-gapped networks. Extensive experience exploiting known and novel vulnerabilities across Windows, Linux, and network infrastructure. Developed autonomous attack methodologies achieving rapid domain compromise through multi-phase exploitation chains. Built threat intelligence platforms for nation-state APT tracking and dark web collection, producing finished intelligence products aligned to priority intelligence requirements. Delivered technical intelligence briefings to senior federal leadership on time-sensitive national security matters. Pioneering agentic AI applications for autonomous security operations. Strong client-facing communication skills with experience translating technical findings for executive stakeholders. U.S. Army veteran with Intelligence Community collaboration and federal law enforcement support experience.

TECHNICAL SKILLS

Offensive Security & Red Team: Red Team Leadership, Adversary Simulation, Penetration Testing, Computer Network Exploitation, C2 Infrastructure Design, Implant Development, Malleable C2 Profiles, AV/EDR Evasion, OPSEC Methodology, Social Engineering, Physical Security Assessment, Purple Team Collaboration

Testing Domains: Active Directory, Azure, AWS, GCP, Hybrid Cloud, ICS/SCADA, OT Networks, Mobile Applications (iOS/Android), Air-Gapped Systems, Web Applications, REST APIs, Network Infrastructure, Wireless Networks

Vulnerability Research: Font Rendering Libraries, Graphics Libraries, Fuzzing (AFL++, LibFuzzer, honggfuzz), Reverse Engineering, Binary Exploitation, Memory Corruption Analysis, Heap Exploitation, ROP Chain Development, Shellcode Development

Threat Intelligence: OpenCTI, MISP, APT Campaign Analysis, MITRE ATT&CK Framework, Diamond Model, Kill Chain Analysis, Dark Web Intelligence Collection, Nation-State TTP Research, Adversary Emulation, IOC Management, Detection Engineering, Finished Intelligence Production, PIR Development, Intelligence Lifecycle, Threat Landscape Assessment, Indicator Enrichment

Security Operations: SIEM Platforms (Splunk, Microsoft Sentinel, Elastic), Log Analysis, Detection Bypass Testing, Alert Validation, EDR Evasion (CrowdStrike, SentinelOne, Carbon Black, Microsoft Defender), Purple Team Exercises

Intelligence & Forensics: All-Source Intelligence Analysis, Cyber Threat Intelligence (CTI), Cryptocurrency Forensics, Blockchain Analysis, Anti-Money Laundering (AML) Investigations, OSINT Collection, Digital Evidence Handling, Risk Assessment, Compliance Awareness (PCI-DSS, HIPAA, SOC2, NIST)

Emerging Technologies: Post-Quantum Cryptography (ML-KEM, ML-DSA, SLH-DSA), AI/ML Security, Adversarial Machine Learning, seL4 Formal Verification, Secure Boot Architectures, Trusted Platform Module (TPM), RF/SDR Analysis, SATCOM Security

Programming: C, C++, Rust, Golang, Python, PowerShell, x86/x64 Assembly, C#, JavaScript, Ruby, Nim, SQL, Bash, VBA

Tools: Cobalt Strike, Sliver, HAVOC, Mythic, MITRE Caldera, Atomic Red Team, BloodHound/SharpHound, Impacket Suite, Mimikatz/pypykatz, Rubeus, Certify, Responder, CrackMapExec/NetExec, Chisel, Ligolo-ng, Burp Suite Professional, Metasploit Framework, Ghidra, IDA Pro, Binary Ninja, Wireshark, Nmap, Nuclei, SQLMap, ffuf, AutoRecon, RTL-SDR, HackRF

AI & Automation: Claude Code, Model Context Protocol (MCP) Development, Multi-Agent Orchestration,

LLM-Augmented Security Tooling, Autonomous Vulnerability Discovery, AI-Driven Reconnaissance, Prompt Engineering for Security Applications

Platforms: Windows Server, Active Directory, Linux (Kali, Ubuntu, RHEL), macOS, Docker, Kubernetes, Proxmox, VMware ESXi, Tactical Communications Systems

Professional: Technical Report Writing, Executive Briefings, Client-Facing Communication, Stakeholder Management, Risk Assessment, Remediation Guidance, Knowledge Transfer, GRC Awareness, Governance, Security Audit Support

PROFESSIONAL EXPERIENCE

Intelligence & Reconnaissance Specialist

September 2022 — 2025

U.S. Army, 101st Airborne Division (Air Assault) | Fort Campbell, KY

- Served in specialized reconnaissance element within the 101st Airborne Division supporting battalion-level operations and emerging capabilities integration
- Delivered technical threat intelligence briefings to senior federal leadership on time-sensitive national security matters
- Provided cyber threat intelligence support to federal law enforcement and military counterintelligence investigations involving national security concerns
- Developed technical threat assessments integrating multi-source intelligence with signals analysis to support operational planning
- Provided technical expertise on tactical communications systems, mobile device security, and digital infrastructure
- Conducted open-source intelligence research producing analytical reports on nation-state military capabilities and tactical methodologies

Red Team Operator / Consultant (Contract)

March 2022 — September 2022

Lime Security Consulting | Remote

- Led 8-person red team conducting adversary simulations against enterprise environments including financial services, critical infrastructure, healthcare, and technology sectors
- Designed and deployed command and control infrastructure using Cobalt Strike with custom malleable C2 profiles, Sliver, and bespoke frameworks while maintaining strict operational security
- Developed custom implants and payload stagers in C#, Rust, and Golang optimized for evasion of mature enterprise security stacks including CrowdStrike, SentinelOne, and Microsoft Defender
- Executed full-scope red team engagements across Active Directory environments, cloud platforms, ICS/SCADA systems, mobile applications, and air-gapped networks
- Conducted attack path analysis across multi-domain forest environments to identify and exploit trust relationships
- Collaborated with client security teams during purple team exercises to validate detection capabilities and improve SIEM alerting
- Built adversary emulation scenarios mapping to nation-state TTPs using MITRE ATT&CK framework and Caldera automation
- Authored detailed technical reports and executive summaries translating complex attack chains into actionable remediation guidance with risk-based prioritization
- Completed Barclays Red Team Challenge Delta, successfully testing security controls of global financial institution

Independent Security Research

2020 — Present | 20+ hours weekly

Remote

Vulnerability Research & Bug Bounty

- Discovered and responsibly disclosed 20+ vulnerabilities in font rendering libraries and graphics processing components affecting enterprise software vendors
- Developed custom fuzzing infrastructure targeting memory corruption vulnerabilities in widely-deployed parsing libraries
- Architected autonomous bug bounty system using Claude Code with MCP integrations implementing coordinator-solver architecture for automated vulnerability discovery, validation, and reporting

- Participated in HackerOne bug bounty programs identifying S3 bucket misconfigurations, API security issues, and authentication vulnerabilities
- Received formal recognition from Glenair Inc. (DOD contractor) and Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) for critical vulnerability discoveries

Threat Intelligence & Adversary Emulation

- Architected and deployed OpenCTI threat intelligence platform integrating commercial and open-source intelligence feeds for APT campaign tracking
- Produced finished intelligence products including threat assessments, campaign analysis reports, and adversary profiles aligned to priority intelligence requirements (PIRs)
- Built adversary emulation laboratory using multiple C2 frameworks for detection engineering and defensive playbook development
- Conducted cryptocurrency forensics investigations including international money laundering network analysis and cartel-tied exchange transaction tracing
- Developed mobile tactical operations center (TOC) architectures leveraging SATCOM for traffic analysis mitigation and attribution resistance

Continuous Development

- Completed HackTheBox ProLabs (Offshore, RastaLabs, Dante, CyberNatic, APTLABS) and 300+ standalone challenges

Event Manager / Subject Matter Expert *September 2020 — February 2021*

Kali Hacking Club (KHC) | *Remote*

- Served as subject matter expert for offensive security curriculum development supporting community of 7,000+ active members
- Created educational content covering penetration testing methodologies, Active Directory attack paths, and privilege escalation techniques

EDUCATION

Bachelor of Science, Cybersecurity (In Progress) — Lipscomb University, Nashville, TN | Expected Spring 2028

CERTIFICATIONS

Offensive Security Certified Professional (OSCP) — OffSec, 2025 | **Certified Red Team Operator (CRTO)** — Zero Point Security, 2022 | **Certified All-Source Intelligence Analyst** — McAfee Institute, 2024 | **Certified Cryptocurrency Forensic Investigator** — McAfee Institute, 2024

TECHNICAL PROJECTS

Terror-Strike Framework: Comprehensive penetration testing framework with 94 Python modules supporting multi-phase attack automation including network discovery, service enumeration, vulnerability identification, and exploitation

Autonomous Bug Bounty System: XBOW-style coordinator-solver architecture using Claude Code and MCP integrations for end-to-end vulnerability discovery, validation, and reporting automation with multi-agent orchestration

AirStrike: Distributed network scanning system enabling multi-node reconnaissance operations with orchestrated scanning modules

Adversary Emulation Laboratory: Multi-node virtualization cluster supporting red team tool development, malware analysis, and nation-state TTP research with isolated network segments for detection engineering

Threat Intelligence Platform: Production OpenCTI deployment integrated with MISP and commercial threat feeds for APT tracking, IOC management, and campaign analysis

ADDITIONAL

Languages: English (Native), Telugu (Native), Spanish (Conversational) | **Technical Diving:** Rescue Diver certified with Deep, Wreck, and Cave specializations | **Notable:** Youngest recipient of CRTO certification (age 17)