Michael Jackson

Security Engineer | Threat & Vulnerability | Offensive Security
Secret Security Clearance
Email: michael@takecntrl.tech | Ph: 618-491-4171 | LinkedIn: www.linkedin.com/in/takecntrl

Professional Summary

Hybrid Cybersecurity Professional with red-blue experience in adversary simulation, detection engineering, and secure infrastructure support. Proven ability to translate real-world attack telemetry into proactive defenses across classified DoD environments and enterprise networks. Skilled in tool-driven threat response, scripting automation, and compliance in high-stakes settings.

Education

Bachelor Degree in Applied Cybersecurity (BACS) – In Progress
SANS EDU | Remote

- SANS Bachelor’s Track (9 GIAC certifications, including GPEN, GRTP, GCIH, GXPN)

Associate of Applied Science – Information Technology & Cybersecurity
Ranken Technical College | St. Louis, MO

- Magna Cum Laude | President’s List

Professional Experience

Network Engineer III (Threat Detection Engineer) May 2022 – Jan 2024
Secure Data Technologies | O’Fallon, IL

- Led internal penetration testing and exploit validation engagements, performing structured reconnaissance, vulnerability exploitation, and privilege escalation to identify and verify critical weaknesses in production environments.
- Developed and tuned custom detection rules/SIEM content based on observed attacker TTPs from red team assessments, enhancing threat visibility and reducing false positives.
- Automated Active Directory, cloud, and network misconfiguration detection using Python and PowerShell, streamlining remediation across hundreds of assets.

Help Desk Specialist (Security Analyst) Feb 2024 – Jan 2025
BuddoBot | Scott Air Force Base, IL

- Performed compliance assessments and risk evaluations in classified DoD environments, remediating access control deficiencies and aligning systems with STIG/RMF requirements.
- Collaborated on internal security assessments, artifact collection, and audit preparation to ensure readiness for external reviews.

Network Controller (Cybersecurity Analyst) Jan 2025 – May 2025
DISA/Leidos | Scott Air Force Base, IL

- Executed vulnerability scanning and patch validation across secure enclaves, partnering with system owners to implement hardened configurations and mitigate identified risks.
- Monitored network traffic for anomalies, escalated verified incidents, and supported containment/remediation decisions to protect mission-critical assets.

Core Security Domains

Detection & Threat Engineering

- SIEM Content Development & Alert Tuning (Splunk, ELK, Graylog)
- Detection Rule Engineering (Snort, Sigma, Elastic)
- Log Pipeline Optimization & IOC Timeline Reporting

Endpoint & Network Defenses

- Endpoint Detection & Triage (CrowdStrike, SentinelOne, Velociraptor)
- Network Forensics & PCAP Analysis (Live TCP/IP trace, packet carving)
- Malware Propagation Analysis & Containment Strategy

Adversary Simulation & Red Team Support

- Scripted Threat Emulation & Payload Testing (custom Bash/Python modules)
- Virtualized Lab Design for Adversary Simulation

Tools & Platforms

- **EDR/SIEM:** CrowdStrike, SentinelOne, Velociraptor, Splunk, ELK, Graylog
- **Forensics:** Wireshark, Sysmon, PCAP analysis tools
- **Offensive/Recon:** Nmap, Metasploit, Burp Suite, Hydra, Gobuster
- **OSINT/Intel:** Shodan, Censys, VirusTotal, Any.run

Projects

Forge – Exploit Arsenal

Personal Project | 2025 – Present (Actively updating)

- Developed a comprehensive automated bash suite for harvesting, tagging, categorizing, and rapidly searching 400+ public CVEs and exploits.
- Enables quick exploit research, payload customization, and integration into red team engagements/freelance pentests.
- Features include modular tagging (e.g., by CVE, technique, target platform), fuzzy search, and export to various formats.
- GitHub: https://github.com/takecntrl/forge

Aura – Advanced Local LLM Fusion & Security Automation Framework

Personal Project | 2025 – Present (In Active Development)

- Architected a fully local, modular LLM-based automation system with persistent memory (vector database), multi-model orchestration (e.g., Dolphin3.0-Llama3.1-8B, TinyLlama), custom scripting pipelines, and event-driven behavior.
- Built core fusion and memory management components (Python/bash scripts, Chroma vector store for RAG) for reliable stateful processing and knowledge retrieval.
- Designed with security-focused capabilities in mind: integrates exploit harvesting/usage from personal tooling (e.g., Forge), automates network defense tasks (e.g., anomaly detection and response), and supports forensic leak tracing through log/telemetry analysis.
- Demonstrates advanced expertise in local LLM deployment, agentic automation, RAG systems, and chaining security tools for red/blue teaming workflows—currently focused on full integration and stability.
- Private project (no public repo or demo).