Nik (Nikki) Gray
📞 | ✉️ Available upon request
🔗 LinkedIn: https://www.linkedin.com/in/nik-g-8a246170
🐙 GitHub: https://github.com/NikGunRay
📍 Oklahoma City, OK

Professional Summary
Cybersecurity professional with 11+ years in cybersecurity sales, technical advisory, and strategy. Actively transitioning into engineering and security analyst roles with hands-on experience in email security, threat detection, vulnerability management, and multi-tenant MSP environments. Known for rapidly upskilling in evolving cybersecurity domains through labs, certifications, and project work. Passionate about continuous learning and driven by a deep curiosity for how threats evolve and how to stop them.

Core Skills & Tools

- **Security Tools:** Nmap, Wireshark, Burp Suite, Splunk, Suricata, Hashcalc, Regedit, Resmon, ipconfig, netstat
- **Platforms & Environments:** Linux (Ubuntu), Windows Server 2019, Thunderbird (EML analysis), Active Directory
- **Cloud & Email Security:** DMARC, SPF, DKIM, Check Point Harmony Email & Collaboration
- **Cybersecurity Fundamentals:** Web protocols (HTTP/HTTPS), DNS, Firewalls, Network traffic, SOC operations
- **TryHackMe Portfolio:** Hands-on experience in modules such as Linux, Windows, Web Exploitation, Packet Analysis, Phishing Investigations
- **Version Control & Projects:** Git, GitHub, Markdown, Cybersecurity Portfolio Projects, Technical Project Reporting (README documentation)
- **Certifications:** CompTIA Security+, UniverCP Training (Check Point), TryHackMe Pre-Security Certification

Recent Projects & Labs
GitHub Cybersecurity Portfolio – github.com/NikGunRay

- **Greenholt Phish Investigation:** Full email header and EML file analysis in Thunderbird. Extracted headers, traced IP, verified SPF/DMARC, and analyzed attachment via SHA256.
- **Linux & Windows Fundamentals Labs (TryHackMe):**
  - Commands: whoami, ls, grep, find, nano, chmod, resmon, msinfo32, regedit
  - Concepts: File permissions, background processes, shell operators, UAC, Task Scheduler, Registry Editor
- **Packet Analysis & Web Exploitation:** Used Wireshark and Burp Suite to capture and dissect network traffic, analyze requests, and identify potential vulnerabilities in HTTP communication.
- **Project Reporting:** Created structured markdown documentation (README files) for each project to summarize objectives, tools used, and findings.

Professional Experience

Senior Sales Director, Cybersecurity | *Veriti*
Feb 2023 – July 2024

- Closed $677K in sales in 6 months with a $4.1M pipeline
- Led technical demos and supported security tool configuration
- Consulted clients on risk exposure, including CVEs and CVSS score interpretation

Director of Strategic Accounts, Cybersecurity | *HUMAN Security*
Oct 2021 – Feb 2023

- Integrated security advisement into enterprise accounts
- Partnered with Snowflake, AWS, and GCP
- Supported security renewal strategy for bot mitigation and fraud prevention by helping customers understand active CVEs in their environments and interpreting CVSS scores to inform urgency and remediation timelines

Account Executive | *Check Point Software Technologies*
Apr 2019 – Oct 2021

- Partnered directly with Check Point's R&D team to proof technical documentation and deliver customer feedback, bridging product development with real-world use cases
- Facilitated calls between global customers and R&D—an uncommon level of collaboration that reflected high trust from both internal and external stakeholders
- Frequently supported team-wide quota achievement after surpassing personal quarterly targets
- Closed Check Point's first IoT deal
- Maintained 95%+ renewal rates
- Provided security insights and licensing support

Education & Certifications

- **B.S. Human Sciences**, Oklahoma State University
- **CompTIA Security+**, Active through 2027
- **Check Point UniverCP**, Hands-on technical training
- **TryHackMe Pre-Security**, Certificate of Completion