Alexander T. Karapetkov

Email: *alexander.karapetkov@gmail.com* | LinkedIn: *https://www.linkedin.com/in/alex-karapetkov*
Github: *https://github.com/Alex-Karapetkov* | Portfolio: *https://alex-karapetkov.github.io/*
Mobile: (571) 242 - 9525 | Sterling, Virginia, 20166

Professional Summary

Computer Science graduate (B.S., 2024) with hands-on experience in cybersecurity, threat analysis, and incident response. Certified in CompTIA Security+, CASP+, and trained through TCM Security SOC 101 labs. Skilled in network monitoring, SIEM analysis, log correlation, endpoint forensics, and intrusion detection. Adept at translating technical analysis into actionable security recommendations. Seeking SOC Analyst or Cybersecurity Analyst roles leveraging both technical proficiency and problem-solving expertise.

Technical Skills

- **Cybersecurity & SOC:** Threat detection, Intrusion analysis, Incident response, Vulnerability assessment, Log analysis, Malware detection, Packet analysis, Network security monitoring, SSL decryption, Triage & escalation, Data loss prevention, Security alert tuning
- **Tools & Platforms:** Splunk, Security Onion, Wireshark, TCPDump, Snort, Zeek (Bro), Kali Linux, Metasploit, Nessus, Nmap, IDA Pro, Procmon, HIDS/NIDS, DLP systems
- **Systems & Networking:** Windows, Linux/Unix, Active Directory, VPNs, TCP/IP, Firewalls, Routers, Switches, GPO configuration
- **Programming & Scripting:** Python, Bash, PowerShell, SQL, Java, C, C#, HTML/CSS/JS
- **Soft Skills:** Analytical thinking, Problem-solving, Clear communication, Team collaboration, Time management, Adaptability, Mentorship, Customer service

Certifications and Training

CompTIA Security+ | CompTIA Advanced Security Practitioner (CASP+) | TCM Security SOC 101 Practical Training | Microsoft Power Platform Fundamentals (PL-900)

Relevant Projects

SOC Analyst Training – TCM Security SOC 101 ..... June 2025

- Completed 80+ hours of simulated Tier 1–2 SOC exercises including phishing analysis, SIEM alert triage, log correlation, and incident response.
- Investigated endpoints and network logs to identify Indicators of Compromise (IOCs), escalating high-risk events.
- Documented incidents and remediation actions, aligning with real-world SOC workflows and ticketing procedures.

Home Server Lab ..... July 2025

- Configured and managed a home SharePoint server farm with AD integration, emulating enterprise IT infrastructure for hands-on security and system administration experience.

➔ Implemented network segmentation, access controls, and monitoring scripts to strengthen environment security.

Command-Line Shell & Utilities | C, Ruby..... December 2023

➔ Built a custom Unix-like shell with support for process management, I/O redirection, and scripting, enhancing understanding of operating system security and system calls.
➔ Developed a terminal-based spreadsheet app with formula parsing and controlled execution, emphasizing safe code evaluation practices.

Python Threat Analysis Scripts ..... August 2025

➔ Automated log parsing, anomaly detection, and alerting for simulated network traffic.
➔ Validated detection efficacy through synthetic phishing, malware, and network scanning scenarios.

Professional Experience

Help Desk Technician at James Madison University ..... April 2023 - May 2024

➔ Resolved >90% of hardware, software, and network incidents on first contact, improving overall ticket resolution time.
➔ Managed and escalated incidents in ServiceNow, prioritizing critical issues and maintaining compliance with SLAs.
➔ Leveraged Nmap, Wireshark, and system logs to detect and remediate network vulnerabilities and configuration issues.
➔ Guided end users through secure password resets, system updates, and access requests, improving endpoint security posture.

Intramural Sports Site Manager at James Madison University ..... August 2022 - May 2024

➔ Directed daily operations and staff for intramural programs, ensuring compliance with safety and security protocols.
➔ Applied analytical and problem-solving skills to resolve conflicts and manage sensitive incidents efficiently.
➔ Conducted training sessions to improve team readiness, communication, and incident reporting.

Education

B.S. in Computer Science *James Madison University, 2024*

Selected Coursework**:** CS 240 Algorithms & Data Structures, CS 261 Computer Systems, CS 361 Advanced Systems, CS 330 Societal & Ethical Issues, CS 456 Computer Architecture

---