Alexander T. Karapetkov

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

Professional Summary

Detail-oriented and analytical cybersecurity professional with hands-on experience in monitoring, triaging, and responding to security events in fast-paced SOC environments. Skilled in leveraging SIEM tools, IDS/IPS systems, and log analysis to identify and escalate potential threats. Proficient in working with Windows, Unix, and Mac OS systems, with strong knowledge of network protocols, malware detection, packet analysis, and incident response. Committed to continuous improvement, teamwork, and maintaining awareness of the evolving threat landscape to support critical business operations and protect client infrastructure.

Education

Computer Science (B.S.) 2024

James Madison University Harrisonburg, VA

Technical Certifications

TCM Security SOC 101	Completed June 2025
Introduction to Splunk	Completed May 2025
Microsoft Power Up Program	Completed May 2025
CompTIA SecurityX/CASP+™ CE	Certified March 2025
CompTIA Security+™ CE	Certified December 2024

Skills

- **Cybersecurity:** Threat detection, Intrusion analysis, Incident response, Vulnerability assessment, Log analysis, Malware detection, Packet analysis, Network security monitoring, SSL decryption, Triage and escalation, Data loss prevention, Case management, Security event correlation, Security alert tuning
- **Tools & Technologies:** Splunk, Wireshark, TCPDump, Security Onion, Snort, Bro (Zeek), Kali Linux, Metasploit, Nmap, Nessus, IDA Pro, PEiD, PEview, Procmon, Web security gateways, Email security tools, SIEM platforms, HIDS/NIDS, Anti-virus software, DLP systems
- **Infrastructure & Systems:** Windows, Mac OS, Unix/Linux, Network devices (routers, switches, firewalls), GPO (Group Policy Objects), Active Directory, System and firewall logs, VPNs, TCP/IP protocols
- **Soft skills:** Excellent verbal and written communication, Analytical thinking, Attention to detail, Team collaboration, Customer service orientation, Problem-solving, Adaptability, Time management, Ability to work under pressure, Mentorship and guidance, Shift flexibility, Continuous learning mindset

Projects

TCM Security SOC 101 *Practical SOC Analyst Training* ..... June 2025

- ➔ Completed 80+ hours of hands-on labs simulating real-world Tier 1–2 SOC scenarios, including endpoint and network monitoring
- ➔ Performed phishing analysis, SIEM alert triage, log correlation, and incident response in a virtual lab environment
- ➔ Investigated security events using threat intelligence, digital forensics, and memory analysis techniques
- ➔ Developed proficiency in analyzing indicators of compromise (IOCs), escalating incidents, and documenting findings
- ➔ Aligned practical skills with SOC workflows, ticketing processes, and escalation paths

8-bit RISC-V ALU *Verilog* ..... April 2024

- ➔ Designed and implemented an 8-bit RISC-V Arithmetic Logic Unit (ALU) in Verilog, optimizing for efficiency and system integrity
- ➔ Developed modular designs with testbenches, ensuring thorough testing and validation to identify vulnerabilities in system components
- ➔ Enhanced skills in hardware description languages, digital circuit design, and debugging, with a focus on system security and reliability

Command Line Shell *C* ..... November 2023

- ➔ Developed a secure command-line shell in C, with features like process control, environment variable management, and secure input/output handling to mitigate vulnerabilities
- ➔ Applied system-level programming concepts to enhance security, focusing on process isolation and privilege boundaries
- ➔ Implemented best practices in input validation and environmental variable management to prevent exploitation

---

Professional Experience

Help Desk Technician at JMU ..... April 2023 - May 2024

- ➔ Provided technical support for hardware, software, and network issues, ensuring timely resolution and security
- ➔ Managed incidents in ServiceNow, prioritizing first-contact resolution to reduce risk and improve satisfaction
- ➔ Used tools like Nmap, Wireshark, Splunk, and Microsoft Defender to identify and resolve network and system issues
- ➔ Assisted in detecting and escalating security incidents, including phishing and unauthorized access
- ➔ Guided users through password resets, application support, and security best practices

Site Manager at JMU Recreation ..... August 2022 - May 2024

- ➔ Ensured safety, compliance with policies, and efficient programming of Intramural Sports, including conducting officials' training sessions, participants' pregame meetings, and performance evaluations
- ➔ Employed first-responder principles as needed (CPR, AED, Bloodborne)
- ➔ Oversaw the performance of staff members and communicated effectively with participants, ensuring smooth operations and compliance with safety protocols
- ➔ Acted as the first point of contact for any issues raised by participants, resolving disputes and facilitating effective solutions with strong call handling and customer service techniques