

Elmaddin Azizli

Fort Collins, CO 80525 | elmeddin.azizov007@gmail.com | (720) 993-8989 | </in/elmaddin-azizli>

Dedicated Cyber Security Analyst skilled in analyzing security alerts with SIEM tools like Splunk and enhancing network security through Wireshark investigations, achieving a 10% reduction in unauthorized access. Proficient in vulnerability assessments and malware analysis, embodying adaptability, critical-thinking, and problem-solving, firmly focused on continuous process optimization and excellence.

EDUCATION

Colorado State University (CSU) PhD in Computer Science	Fort Collins, CO Exp. Dec. 2029
University of Central Florida (UCF) Master of Science in Cybersecurity , GPA: 3.4	Orlando, FL May 2024
Clarusway Practical Cybersecurity Program	Remote Nov. 2023
University of Central Florida (UCF) Bachelor of Science in Information Technology , GPA: 3.3 Honors: Dean's List – Fall 2020, Fall 2021, Fall 2022, Fall 2023, President's Honor Roll – Spring 2022	Orlando, FL May 2022

WORK EXPERIENCE

Cybersecurity Instructor – Western Caspian University	October 2024 – January 2025
<ul style="list-style-type: none">Delivered comprehensive lectures on Information Security, covering security fundamentals, threat management, and data protection to 16 undergraduate students.Developed and implemented hands-on activities, case studies, and real-world scenarios to enhance students' practical understanding of cybersecurity principles.Designed course materials aligned with industry standards, including NIST, OWASP, and ISO 27001 frameworks, ensuring relevance and applicability.Evaluated student progress through assessments and projects, providing detailed feedback to foster student growth and improve learning outcomes.	
Cybersecurity Analyst – Duskbeacon	June 2023 – January 2024
<ul style="list-style-type: none">Monitored Duskbeacon's Multi-platform Honeypot, handling 230 potential security breaches on average per month.Analyzed 5+ alert types through Splunk and QRadar SIEM solutions and identified security anomalies for investigation.Triaged incidents employing a diverse set of tools (SIEM, Firewall, EDR, Email Security Appliances), investigated and resolved issues, and escalated triaged alarms to L2 analysts when necessary via the Jira ticketing system.Implemented identity and access management protocols for more than 500 user profiles, resulting in a 10% decrease in unauthorized access incidents within 4 months.Created monthly reports highlighting findings from over 3 security tools and illustrated visual representations of security breaches within the environment.Examined over 150 PCAP files monthly using Wireshark to isolate anomalous traffic, scrutinized details of 60+ compromised hosts, and documented Indicators of Compromise, resulting in a 10% reduction in security breaches within a year.Reviewed existing policies and guidelines to align with the National Institutes of Technology (NIST 800) Risk Framework standards.	

PROJECTS

Shellcode Loader	Sep 2023 – Oct 2023
<ul style="list-style-type: none">Implemented a C++ shellcode loader using dynamically resolved Windows API functions for discreet memory allocation and execution, successfully evading detection in 90% of test scenarios.Utilized Windows Cryptography API to decrypt AES-encrypted shellcode just before execution, enhancing concealment.Leveraged Havoc C2 for presumed command and control activities post-exploitation.Developed a YARA rule to identify the shellcode loader by targeting strings related to cryptographic and memory manipulation API calls.	

Vulnerability Scanning

Jan 2023 – Feb 2023

- Installed and configured Nessus Essentials to perform credentialed vulnerability scans against Windows 10 Hosts using VMware.
- Implemented Vulnerability Management Function on sandbox networks: Discover, Prioritize, Assess, Report, Remediate, Verify.
- Conducted vulnerability assessments with Nessus; remediated vulnerabilities.
- Developed automated remediation process to preemptively deal with vulnerabilities stemming from Windows updates and third-party software.

SKILLS

Technical Skills

SOC Experience: Log Analysis, Packet Detection Analysis, Online Sandbox (FlareVM) | **SIEM:** Splunk Enterprise Security, IBM QRadar | **EDR:** CrowdStrike | **Ticketing:** ServiceNow, Jira, TheHive | **Kali Linux Tools:** Nmap, Burp Suite, Metasploit, Meterpreter | **Vulnerability Analysis:** Nessus, Qualys, OpenVAS | **Networking:** IDS/IPS, Wireshark, TCP/IP & OSI Layers, LAN, DNS, VPN, Whois, URLVoid, Phishing Analysis | **Virtualization:** VMware, VirtualBox | **Firewall:** FortiGate, Iptables, Eve-NG | **OSINT:** OSINT Framework, Google Dork, Exploit-dB, TheHarvester, Shodan.io, VirusTotal, Any.Run | **Malware Analysis:** Yara | **Security Frameworks/Standards:** NIST-800, MITRE ATT&CK, Cyber Kill Chain, OWASP 10, | **Programming Languages:** Python, JavaScript, SQL, C, C++, Java, HTML, CSS

Soft Skills

Adaptability | Analytical Thinking | Dedication | Organized | Persistency | Problem-Solving | Time Management | Customer Service

CERTIFICATIONS & ACHIEVEMENTS

- Security+ ce Certification / CompTIA, 2023
- SOC Level 1 / TryHackMe, 2023
- Cyber Defense / TryHackMe, 2023
- Practical Ethical Hacking / TCM Security, 2023