Muhammet Matiyev

muhammet@matiyev.xyz | linkedin.com/in/matiyev | 0775170099

WORK EXPERIENCE

Cybersecurity Validation Analyst Intern — Feb 2024 – Present
Virtually Testing Foundation — L.A, California (remote)

- Implementing automated and continuous security controls validation using AttackIQ
- Implementing Breach and Attack Simulation (BAS) tools, aligned with MITRE ATT&CK, to automate threat-informed defense
- Deploying Services-Based BAS for efficient penetration testing
- Researching and analyzing emerging cyber threats, APTs and their TTPs
- Maintaining documentation of security validation procedures, findings, and mitigations

Ride Operator — June 2021 – Oct 2021
Santa Cruz Seaside Company — Santa Cruz, California

- Managed, monitored, and operated controls, for safety compliance
- Implemented emergency procedures
- Maintained documentation of incidents

Volunteer — June 2019 – Oct 2019
Tuna Foundation — Bucharest, Romania

- Volunteered at a food festival dedicated to supporting orphans, refugees, and people in need in Romania

PROJECTS (more on matiyev.xyz)

SOC-MOCK

- **Virtual Machine Forensics:** Set up a virtual environment, hardened a Windows VM, and deployed security tools (Sysmon, LimaCharlie EDR) to simulate a compromised system investigation
- **EDR Analysis for Threats:** Monitored and Analyzed EDR telemetry to identify adversary techniques like credential dumping attempts targeting the "lsass.exe" process
- **Automated Detection and Response Rules:** Created D&R rules in LimaCharlie to automate threat response (reporting, process termination) for suspicious activity
- **YARA for Malware Detection:** Implemented custom YARA rules for signature-based detection of the Sliver C2 framework and other potential malware

The Security Playground: Building Defenses and Launching Attacks

- **Network Security and Segmentation (pfSense/Security Onion):** Implemented pfSense Firewall for network segmentation, filtering malicious traffic, and enforcing security policies. Additionally, deployed Security Onion for continuous security monitoring, intrusion detection, and centralized log management.
- **Offensive Security Testing and Active Directory Simulation (Kali Linux/Windows Server):** Employed Kali Linux to exploit vulnerabilities and assess the lab's security posture. Configured a Windows Server as a domain controller to manage user accounts, enforce group policies, and simulate a real-world network. Windows Desktops joined the domain, allowing for user simulations and testing within the controlled environment.
- **SIEM Integration (Splunk/Universal Forwarder):** Installed and configured Splunk to function as a SIEM solution. Integrated Splunk Universal Forwarder on the Windows Server to forward logs for centralized analysis in Splunk.

EDUCATION AND CERTIFICATIONS

- **B.Eng. Chemical Engineering**, Babeş-Bolyai University, Romania — 2019 – 2023
- **Certified Cybersecurity Technician,** EC-Council, United States (remote) — Nov 2023

SKILLS

- **Monitoring** – Splunk SIEM, LimaCharlie EDR, Sysmon
- **Network Analysis** – Security Onion, Wireshark, tcpdump
- **Network Troubleshooting** – nmap, hping3
- **Network Security Administrative Controls** – Active Directory, pfSense Firewall
- **Cyber Threat Intelligence** – MITRE ATT&CK, D3FEND, Cyber Analytics Repository, ATT&CK Navigator
- **Penetration Testing** – Breach and Attack Simulation
- **Web Development** – HTML/CSS, JavaScript, React.js

LANGUAGES

English – **C1**
Russian – **C1**
Romanian – **B2**
Turkish – **C2**
Turkmen – **Native**