


Nijat Alammadov

nijat.ammadov@gmail.com ❖ (+994) 50-291-45-71 ❖ Baku, Azerbaijan ❖  [Nijat Alammadov](#)

WORK EXPERIENCE

Azer Turk Bank OJSC

Jun 2024 – Present

Leading Security Engineer

Baku, AZ

- Designed and executed a comprehensive cybersecurity architecture, integrating advanced solutions such as SIEM, XDR/EDR, UBA, FIM, and vulnerability scanners for proactive vulnerability management, establishing a robust multi-layered defense framework..
- Conducted comprehensive penetration testing assessments to evaluate the security posture of critical systems and applications, identifying vulnerabilities and exploit paths. Developed and executed targeted test plans, delivering detailed reports with actionable remediation strategies to enhance overall security resilience..
- Oversaw incident response protocols and crafted detailed, scenario-based playbooks to streamline the handling of security incidents. Provided expert guidance and support to L1 analysts, enhancing their effectiveness in threat detection and escalation processes..
- Enhanced the integration of security tools with SIEM systems, tailoring correlation rules, alerts, and dashboards within QRadar to optimize threat detection, improve incident response times, and facilitate real-time monitoring.
- Implemented comprehensive Data Loss Prevention (DLP) strategies and conducted thorough security audits while generating insightful threat intelligence reports. Fostered a security-conscious culture through tailored training programs, equipping employees to recognize and respond to potential security threats effectively.

Pasha Bank OJSC

Jun 2022 – Jun 2024

SOC Analyst

Baku, AZ

- Tickets on the Jira ticketing system are handled and resolved within the Service Level Agreement on a 24x7 rotating schedule.
- Proactive SOC/NOC monitoring, investigation, mitigation of security incidents, and technical analysis of various security breaches and potential system compromises are conducted.
- Potential, successful, and unsuccessful intrusion attempts and compromises are recognized through thorough reviews and analyses of relevant event detail and summary information.
- Malicious artifacts, phishing emails, suspicious domains, and IP addresses are investigated using online tools. Proper solutions based on accurate analysis are recommended.
- Security monitoring and alerting systems are managed and maintained. Incidents from QRadar SIEM are tracked and analyzed. A variety of network and host-based security appliance logs (SIEM, Firewalls, NIDS, HIDS, DLP, Sys Logs, etc.) are analyzed to determine the appropriate remediation actions and escalation paths for each incident.
- Detailed investigation and response activities are performed for potential security incidents. Documentation related to security incidents, including incident reports and procedures for responding to incidents, is created and maintained.

Prosol CJSC

Dec 2021 – Apr 2022

SOC Analyst Intern

Baku, Azerbaijan

- Weekly “capture-the-flag” projects are undertaken to assist in answering key questions about security tools and incident response.
- Assistance is provided in maintaining and monitoring the existing security infrastructure, evaluating emerging technology, and implementing new systems to uphold the confidentiality, integrity, and availability of information assets, all while maintaining operational and process documentation as necessary.
- Cybersecurity best practices are incorporated from the start of a product’s ideation through collaboration with design teams.
- Different open source/vendor based products (such as IBM QRadar SIEM (All in one appliance), ELK Stack), Wazuh, TheHive/Cortex) are deployed.
- Incidents on XDR system are analyzed and investigated.

Certifications

- **Certified Red Team Operator(CRTO)**
- **eLearnSecurity Certified Professional Penetration Tester (eCPPTv2)**
- **eLearnSecurity Junior Penetration Tester v2 (eJPTv2)**
- **CompTIA Security+**
- **Blue Team Level 1(Security Blue Team)**
- **TestDaF-Zertifikat(TestDaf-Institut)**
- **IELTS**

EDUCATION

Khazar University

BS Computer Engineering

Sept 2018 – Jun 2022

Baku, AZ

- Graduated with Honor diploma

SKILLS & COMPETENCIES

- **Cyber Defense:** SIEM, IBM QRadar, Elasticsearch (ELK), Wazuh, TheHive/Cortex, Wireshark, IDS/IPS, Firewall, XDR, Yara, Authentication Methods, Incident Management, Phishing Analysis, Incident Handling, Endpoint Protection.
- **Penetration Testing & Vulnerability Assessment:** OWASP Top 10, XSS, SQL Injection, nmap, OpenVAS Metasploit, Linux, Windows, Privilege Escalation
- **DevSecOps:** SAST, DAST, Linux, Docker, Vulnerability Management, AWS
- **Digital Forensics & Incident Response:** FTK Imager, AutoPSY, Stegonagraphy
- **Programming & Scripting:** Python, Powershell, JavaScript, SQL, HTML/CSS(SASS), Bootstrap, OOP, C#, Unity
- **Networking:** TCP/IP, OSI, DHCP, DNS, Network Essentials, Routing, VLAN, IPv4, Subnetting, Wireless Networking (LAN)
- **Help Desk:** PC Hardware Building, Diagnosing and Troubleshooting, Microsoft Office, Windows 10, Linux Distributions, Virtualization.
- **Soft Skills:** Responsibility, Active Listening, Leadership, Time Management, Communication, Critical thinking

Achievements

- **Azerbaijan Robotics Olympic 3rd Place(Lego EV3 Sumo)**
 - Developed and engineered LEGO EV3 robots for both Sumo and Line Follower challenges, showcasing a hands-on application of robotics and programming skills.
 - Demonstrated expertise in hardware integration by skillfully combining various components to create custom LEGO EV3 robots. Successfully incorporated and programmed a functional color sensor, enabling precise color and light detection capabilities.
 - Proficiently formulated intricate algorithms within the LEGO EV3 Mindstorms Student Edition, orchestrating seamless robot movements and actions. Translated conceptual designs into operational code, resulting in precise and effective robot responses.

Languages

- **Azerbaijani** - Native or Bilingual Proficiency
- **Turkish** - Native or Bilingual Proficiency
- **English** - Professional working proficiency
- **Deutsch** - Professional working proficiency