Ilgiz Khabibullin

213.266.3533 | ilgiz7725@gmail.com | github | linkedin | github.io

SKILLS AND TECHNOLOGIES

Cybersecurity Tools: Splunk Enterprise Security, IBM QRadar, SentinelOne, CrowdStrike Falcon, SOC Radar, Nmap, Fortinet, Proofpoint, Resilient, Jira, VirusTotal, AnyRun, MX Toolbox, Tenable.io, Nessus, Kali Linux, Armis, Elastic Stack, Sysmon, OSINT
Networking & Virtualization: Wireshark PCAP Analysis, DNS, Whois, Virtual Box, VMware, Web Application Firewall, Next Generation Firewall, TCP/IP, IDS/IPS, Fleet Server, Elastic Agent
Frameworks: OWASP, MITRE ATT&CK, Cyber Kill Chain, SANS, NIST Risk Management Framework
Technology: Google Suite & Google Docs, Microsoft Office Suite, Excel, GitHub, Microsoft Azure, Microsoft Sentinel
Soft skills: Critical thinking, problem solving, detail-oriented, team worker, discipline, leadership

EXPERIENCE

CyberNowLabs 4/2024 –Present
Cyber Security Support Engineer

- Perform vulnerability assessments and web application security testing with Tenable.io, Nessus, and Acunetix, while ensuring NIST Risk Framework compliance.
- Manage Fortinet NextGen Firewalls and configure VPNs, utilizing EDR/XDR tools like SentinelOne and CrowdStrike for advanced threat detection and response.
- Contribute to SOC shifts, engaging in real-world security operations and incident management with Jira.

U.S. Army National Guard 4/2021 – 4/2024
Transportation Specialist (E-4 Specialist)

- Protected classified materials during transport by following cybersecurity protocols and ensuring secure communications in mission-critical operations.

WestValleySoft 9/2018 – 9/2021
Quality Assurance Engineer

- Developed and executed test plans, collaborating with teams to identify vulnerabilities, conduct assessments, and implement security measures, ensuring product integrity and compliance.

EDUCATION

Advanced Software Quality Assurance Testing Course, Los Altos, CA
Basic Training and Advanced Individual Training (AIT)
Completed rigorous basic combat training followed by specialized training in transportation and logistics
Certified Defensive Security Analyst Course, Remote, USA

CERTIFICATIONS

CompTIA Security+
Google Cybersecurity Professional Certification
FEMA National Incident Management System (NIMS): ICS-100
Qualys Vulnerability Management
IBM QRadar Foundation

PROJECTS

- Built a SIEM system using Microsoft Azure and Microsoft Sentinel. Configured log analytics and automated alerts for proactive threat management.
- Platforms and Technology Used: Azure Virtual Machines, Microsoft Sentinel (SIEM), Log Analytics