Ilgiz Khabibullin

213-266-3533
ilgiz7725@gmail.com
github.com/zigl1
linkedin.com/in/ilgizqa

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

Project: SIEM with Microsoft Azure and Microsoft Sentinel, Personal Project
- 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

EXPERIENCE

Company: CyberNowLabs   4/15/2024 - Present
Title: Cyber Security Support Engineer (Intern)
- Conduct log and SIEM alert analysis using Splunk Enterprise Security and IBM QRadar, simulating cyber-attacks with Nmap and analyzing network traffic with Wireshark in Kali Linux to enhance threat response strategies.
- 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.

Company: U.S. Army National Guard   04/29/2021-04/29/2024
Title: Transportation Specialist (E-4 Specialist)
- Protected classified materials during transport by following cybersecurity protocols and ensuring secure communications in mission-critical operations.

Company: WestValleySoft   09/02/2018–09/01/2021
Title: Quality Assurance Engineer
- Developed and executed comprehensive test plans, collaborating with development and security teams to identify vulnerabilities, conduct security assessments, and implement security measures, ensuring product integrity, compliance with best practices, and faster time-to-market.

SKILLS AND TECHNOLOGIES

Cybersecurity Tools: IBM QRadar, Splunk, Crowdstrike, SentinelOne, Acunetix, Fortigate, Kali Linux, Wireshark, Nmap, Tenable/Nessus, Proofpoint, Jira, VirusTotal, AnyRun, MX Toolbox, Armis, OSINT