

Security Analyst Intern Security Analyst Intern Security Analyst Intern - CyberNow Labs Centreville, VA Work Experience Security Analyst Intern CyberNow Labs - Fairfax, VA January 2019 to Present

Perform analysis of log files via QRadar SIEM solution      Process development/improvement

Liaise with the Company's SOC to respond to emerging incidents in a timely manner; triage details and provide support to both the SOC and Business Managers      Assist in performing periodic access reviews / inactivity reviews      Analyze and review escalated cases until closure. This includes investigating and recommending appropriate corrective actions for cyber security incidents

Perform post mortem analysis on logs, traffic flows, and other activities to identify malicious activity

Perform vulnerability scanning Nessus IT Help Desk UMIZ LLC - Fairfax, VA June 2016 to December 2018      Installing and configuring computer hardware, software, systems, networks, printers and scanners      Responding in a timely manner to service issues and requests      Providing technical support across the company      Repairing and replacing equipment as necessary

Oracle BI Developer Central Bank of Azerbaijan - Baku, AZ January 2014 to February 2016      Collaborating with business analysts and developers to produce software designs      Transforming software designs and specifications into high functioning code in the appropriate language

Junior Oracle Database Administrator Baku Insurance - Baku, AZ August 2012 to December 2013 Maintaining database by identifying and solving database requirements; supporting users

Education Bachelor in Information Technology and Systems Engineering Azerbaijan State Oil Academy - Baku, AZ MBA Azerbaijan State Economic University - Baku, AZ Master of Science in Information Technology Virginia International University - Fairfax, VA

Skills Metasploit, Nessus, Nmap, Siem, Splunk, Wireshark, Css, Security, Database administration, Database, Sql server, Mysql, Oracle, Sql, Active directory, Tcp, Tcp/ip, Vmware, Networking, Android studio, Information Security, Cyber Security, Linux, Network Security

Additional Information Core Competencies      ? Security: IBM's Security QRadar SIEM, FireEye Redline, Splunk fundamentals, AnyRun, VirusTotal, Phishing Analysis, Threat Analysis, Security Onion,      ? Vulnerability Management: Nmap, Nessus, Metasploit Framework, Kali Linux,      ? Networking: Wireshark, TCP view packet analysis, TCP/IP      ? Experience: SQL, HTML, CSS, Javascript,      Android Studio      ? Operating Systems: Windows, Linux

Fedora/Ubuntu, iOS, VmWare, Active Directory ? Languages: Fluent in English, Russian, Azerbaijani, Turkish ? Oracle applications, OBI, SQL server, MySQL, Toad ? Oracle Database 10g/11g database administration skills, ODI and ETL development ? Actively pursuing Security+ and CEH certifications

Name: Blake Allison

Email: [hectorgonzalez@example.org](mailto:hectorgonzalez@example.org)

Phone: +1-457-677-9966