ALI H. NAQVI

Phone: (516) 413-9952 | **Email:** Anaqvi1694@gmail.com

Experienced information security professional seeking a role in cybersecurity operations with a focus on identifying and remediating security vulnerabilities to reduce cyber risk and ensure business continuity. Skilled in leading IT risk assessments, security monitoring, compliance, and process improvement. Collaborative, analytical, and adaptable individual eager to contribute to a dynamic organization.

EDUCATION

JOHN JAY COLLEGE (School of Criminal Justice) - M.S. in Digital Forensics & Cybersecurity **Received July 2022**

BARUCH COLLEGE (Zicklin School of Business) - B.B.A. in Accounting & CIS **Received May 2019**

CERTIFICATIONS, TOOLS, & FRAMEWORKS

- CompTIA Security+
- CompTIA Network+
- Archer & AuditBoard
- Microsoft Azure DevOps
- ServiceNow & Jira
- Windows & Linux
- NIST, CIS, & ISO27K
- MITRE & OWASP
- HTML & CSS
- SQL & DBMS

SECURITY ACTIVITIES

- Obtained Qualys VM certifications and configured the tool to discover assets on the network, created asset tags, and grouped them based on OS, SW/HW, and location. Scheduled and performed external and authenticated scans to detect vulnerabilities and prioritized them using CVSS and QDS. Applied automated patching to remediate vulnerabilities and designed dynamic dashboards.
- Securely acquired forensic images of several compromised assets using FTK Imager and completed Chain of Custody forms. Utilized Autopsy to review key artifacts (Registry, Prefetch, ShimCache, Shellbags, LinkFiles, etc.) and issued reports with detailed steps.
- Configured Splunk to obtain logs for OS, applications, servers, and network devices (IDS/IPS) with forwarders and collectors. Used Splunk queries to search, analyze, and visualize logs to triage incidents following the cyber kill chain for indicators of compromise.
- Conducted network forensics with Wireshark to analyze packet captures for IOCs of malware strains such as Emotet and TrickBot.
- Investigated phishing emails (header, body, URLs, attachments, etc.) with BEC tools including PhishTool, AnyRun, and CyberChef.
- Curated CTI data from OSINT platforms (OpenCTI, MISP, and NVD) for intel on threat actors, TTPs, and suggested course actions.
- Review Cybersecurity news, attend industry events, and participate in forums to regularly learn about the latest threats and trends.

WORK EXPERIENCE

BLACKROCK INC. — June 2022 – December 2022

Information Technology Audit Associate **New York, NY**

- Tested IT controls covering system build, infrastructure resiliency, logical access, change management, information security, data lineage, cryptography, production monitoring, asset management, and disaster recovery for compliance with regulations and policies.
- Reviewed vendor due diligence tasks to verify SLA metrics, patch management, external audit results, and security assessments.
- Analyzed internal application and infrastructure vulnerability reports for critical security issues and execution of remediation plans.
- Presented Senior Management with quantitative and qualitative risk assessment reports detailing inherent, detective, and control risks.
- Verified successful and timely implementation of corrective action plans as part of the risk mitigation strategy for audit observations.
- Created flowcharts illustrating end to end business processes integrated with control mappings to identify higher risk areas for testing.
- Managed communication channels with stakeholders for walkthroughs, evidence gathering, status updates, and issue verification.

SS&C TECHNOLOGIES INC. — November 2017 – April 2021

Information Technology Audit Associate **New York, NY**

- Led audits and delegated duties to junior staff; tasks involved gathering audit evidence, reviewing work papers, and finalizing audit reports to assess compliance with security baselines for business applications, database servers, and supporting IT infrastructure.
- Presented technical audit summary reports to Management using simple terminology, summarizing the broader context and implications of the various types of risks (financial, legal, reputational, etc.) affecting the business and critical technology functions.
- Participated in the Agile application development process to ensure timely completion of quality assurance activities, user stories, acceptance criteria testing, automated code testing, vulnerability scans, business process documents, and Management approvals.
- Leveraged excel analytics to standardize datasets and automate control testing to reduce manual efforts and identify control failures.
- Consolidated audit data and built dynamic dashboards to summarize team KPIs for planning and performance optimization.
- Verified corporate policies such as SDLC, IAM, BCP/DR, data classification, and user training against industry standards.
- Triaged security incidents and audit findings for root cause analysis and coordinated corrective action plans with stakeholders.
- Partnered with cross functional departments to support corporate control objectives and strengthen comradery between the teams.