Ali H. Naqvi

(516) 413-9952 | a.naqvi1223@gmail.com

Professional Summary

Technical and strategic cybersecurity leader with 7+ years securing enterprise environments across sports, technology, and finance. Proven track record in building and scaling enterprise security programs, combining hands-on technical execution (SIEM, EDR, IAM, cloud security, Zero Trust) with strategic risk management and executive buy-in. Architected and deployed the first cybersecurity program for the Memphis Grizzlies, achieving near-real-time detection and response, enterprise-wide visibility, and measurable risk reduction. Adept at aligning security operations with business priorities and delivering outcomes that protect critical assets and enable growth.

Core Competencies

- **Security Ops & Threat Mgmt:** Incident Response Leadership, Managed Security Services, SOCaaS, SIEM (Rapid7) SOAR (InsightConnect), EDR (SentinelOne, Microsoft Defender), Threat Hunting (MITRE ATT&CK)
- **Risk & Vulnerability Mgmt:** Rapid7 InsightVM, Surface Command, Penetration Testing, Patch Management, Risk Assessments, Root Cause Analysis, CVSS Scoring
- **Cloud & Infrastructure Security:** Entra ID/AD, Defender for Cloud (CSPM), Key Vault, Conditional Access, Ubiquiti and FortiGate Firewalls, VLAN Segmentation, VPN (Cloudflare WARP, FortiClient), IDS/IPS
- **IAM & Zero Trust:** Zero Trust Architecture, Conditional Access, Federated Access, RBAC, Passkey (FIDO2), Privilege Access Management (Delinea), Just-in-Time Access (Azure PIM)
- **Governance & Compliance:** Policy Development, Data Governance, DLP (Microsoft Purview), AI Security, Secure SDLC, Audit & Compliance Readiness (NIST CSF, CIS, SOX, PCI, HIPAA)
- **Leadership & Reporting**: MSSP Oversight, Team Mentorship, Executive Dashboards, KPI Tracking, Risk Reduction
- **Certifications:** CISSP, CompTIA CySA+, Security+, Network+

Relevant Experience

MEMPHIS GRIZZLIES, LLC. — Memphis, TN

Cybersecurity Program Lead — *July 2023 – Present*

Program Leadership & Strategy:

- Implemented the organization's first mature enterprise security architecture, integrating 100+ on-prem and virtual servers, 2,500+ multi-OS endpoints (Windows, MacOS, Linux), and Azure/AWS into a unified security architecture.
- Optimize $1M+ cybersecurity budget and co-lead a 12-member IT team across cybersecurity, help desk, networking, and infrastructure, driving strategic execution and delivering a 30% cost savings while maximizing ROI.
- Provide regular briefings to executive leadership, aligning cybersecurity risk posture with business priorities and enabling informed, strategic decision-making at the highest levels.

Security Operations:

- Streamline Incident Response and Vulnerability Management workflows in partnership with the MSSP, leveraging Rapid7 InsightIDR/InsightVM, SentinelOne, and ServiceDesk automation to cut MTTD to under 1 minute, MTTR to under 5 minutes, and accelerate remediation of critical vulnerabilities.
- Lead deployment of Cloudflare VPN + ZTNA, replacing legacy Forticlient VPN incorporating device posture checks, WAF, DDoS protection improving access reliability and reducing VPN support tickets by 80%.
- Support the Network team in standing up Ubiquiti NGFW, including rule vetting, IPS/IDS configuration and testing, VLAN isolation, and log ingestion, minimizing attack surface, lateral movement risk, and enhancing visibility.

Governance & Compliance:

- Publish and maintain a suite of IT governance policies, including Identity & Access Management, Patch & Change Management, Security Awareness, and Acceptable Use, resulting in consistent policy adoption.
- Stand up the organization's first centralized asset inventory, enhancing enterprise-wide visibility by cataloging assets by business unit, asset owner, asset criticality, and data sensitivity.
- Govern the organization's AI enablement strategy, publishing the first AI Governance Policy, launching an internal AI Lab, and enabling secure AI use-cases using Microsoft CoPilot, Azure Foundry, and GitHub Enterprise.

Risk & Data Protection:

- Launch data governance and DLP initiatives, scanning all cloud and on-prem environments for sensitive data, classifying data utilizing standardized security labels, and enforcing data loss prevention policies.
- Establish the penetration testing and remediation program to proactively identify and close exploitable vulnerabilities.
- Lead the full incident response lifecycle, including development of the organization's IR Plan, execution of BIAs, BCPs, and enterprise-wide tabletop exercises.

Collaboration & Influence:

- Manage external collaboration with the NBA League Office and peer clubs to implement a 350+ cybersecurity control framework, influencing league-wide standards and promoting consistent adoption and policy improvements.
- Support deployment of a player health/performance analytics platform with HIPAA-aligned safeguards, encrypted data pipelines, and role-based access controls.
- Champion a culture of security through targeted training campaigns, including emerging threat topics such as deepfakes, vishing, and AI-driven attacks.

BLACKROCK, INC. — New York, NY

Sr. Associate Governance, Risk, & Compliance (GRC) — *June 2022 – December 2022*

- Conducted technical risk assessments of enterprise platforms, addressing critical and high-risk findings tied to data leakage, vulnerability exposure, and production monitoring gaps.
- Reviewed secure SDLC practices, including SAST, DAST, and source code analysis integrations into CI/CD pipelines reducing production vulnerabilities and strengthening shift-left security posture.
- Partnered with cross-functional stakeholders to develop secure architecture diagrams and control flowcharts, proactively identifying systemic risks and embedding security-by-design into application projects.
- Leveraged Archer GRC to document and track control gaps and monitor remediation progress, ensuring centralized governance and risk assessment readiness across all risk domains.
- Facilitated end-to-end audit readiness and evidence collection, standardizing workflows with structured playbooks, improving documentation efficiency, and reducing audit preparation time.
- Delivered executive-facing risk reports that improved issue prioritization and team accountability, accelerating remediation timelines and enhancing leadership visibility into enterprise risk posture.

SS&C TECHNOLOGIES, INC. — New York, NY

Sr. Associate Information Technology Audit — *November 2017 – April 2021*

- Promoted from Intern to Associate (2018) to Senior Associate (2019) for exceptional performance and leadership.
- Executed 12+ IT audits, annually, covering cybersecurity, secdevops, access management, and data privacy across several global offices, ensuring compliance with SOX, NIST, and GDPR, upholding audit quality and consistency.
- Led and mentored a team of analysts optimizing department capacity, resource allocation, and workflow execution to streamline audit operations and enhance overall team efficiency.
- Developed automation scripts to standardize control testing, cutting audit time by 60+ hours per engagement.
- Built Power BI dashboards consolidating over 50,000 compliance-related data points from vulnerability scans, audit findings, and risk assessments.
- Partnered with internal risk, compliance, and engineering teams to define control ownership, streamline evidence workflows, and align technical audit procedures with business risk priorities.
- Identified control gap trends across recurring audit engagements and collaborated with leadership to recommend process improvements and policy updates.

Education

John Jay College, School of Criminal Justice — New York, NY

M.S Cybersecurity & Digital Forensics — *Received May, 2022*

Baruch College, Zicklin School of Business — New York, NY

B.B.A Accounting & Information Systems — *Received August, 2018*