

NATHANIEL W. HALL

Greater Chicago, Illinois • (860) 392-8538 • natewhall@gmail.com • www.linkedin.com/in/nathanielwhall

SUMMARY

Accomplished Information Security Director | Strategic Growth Leader: Extensive experience developing and implementing robust security strategies to safeguard organizational assets. Proven track record in risk management, compliance, and governance, and leading high-performing teams to respond effectively to security incidents. Adept at collaborating with cross-functional departments to align security initiatives with business goals while managing budgets and vendor relationships. Committed to staying at the forefront of emerging security trends and technologies to continuously strengthen the organization's defense mechanism.

EXPERIENCE

BOOZ ALLEN HAMILTON – Incident Response, Partnerships, M&A, Proactive Services **Chicago**
Incident Response Program Lead · Senior Manager..... April 2022 – December 2024

I leveraged my technical capabilities to cultivate new relationships with insurance brokers, insurance carriers, and law firms. I have also assisted insurance brokers with clients in preparing for and attaining cyber insurance coverage. Additionally, I focused on expanding existing partnerships through targeted account management and identifying new client opportunities.

- Defined and executed growth strategy for Booz Allen's DFIR Retainer Program, scaling client portfolio by 110% in one year and generating \$1.4M in new revenue.
- Contributed to a record-breaking \$44M in business unit revenue by expanding DFIR offerings and deepening relationships with insurers, law firms, and private equity partners.
- Advised brokers and insurance carriers on client preparedness and coverage alignment, positioning DFIR services as a value differentiator.
- Built strong partnerships with MDR vendors to enhance retainer value and integrate proactive services.
- Subject matter expert for webinars, articles, and speaking engagements.

WEST MONROE PARTNERS (divestiture) – Incident Response, SOC, MDR, M&A, Proactive Services **Chicago**
Cybersecurity Incident Response Commander & vCISO..... January 2021 – April 2022

As a subject matter expert, spearheaded incident response and proactive cybersecurity engagements, serving clients from both middle-market and Fortune 100 companies. I led high-stress incident response engagements, including multiple workstreams, to minimize service disruptions by recovering systems for medium—to large-sized businesses through effective risk mitigation.

- Led a team of incident response professionals, providing direction, mentorship, and support to ensure successful client outcomes.
- Designed and enforced policies and procedures to protect the organization's computing infrastructure, networks, and sensitive data from internal and external threats.
- Collaborated with IT, Legal, HR, and other departments to ensure security strategies aligned with the organization's business goals and operational needs.
- Championed pre- and post-incident process improvements, aligning with global regulatory standards.

ARETE INCIDENT RESPONSE – Incident Response, M&A, Proactive Services, SOC, MDR **Remote**
Incident Response Lead..... January 2020 – January 2021

Successfully led and leveraged the expertise of a team of technical experts within the Security Operations Center (SOC), digital forensics, and recovery teams to assess and establish the breadth of incident containment and recovery. Led all aspects of incident response engagement (end-to-end), including incident validation, monitoring, containment, eradication, log analysis, system forensic analysis, and reporting key milestones and metrics.

- Directed full-lifecycle IR engagements, including validation, containment, forensics, and reporting.
- Advised counsel and client executives on DFIR strategy and findings throughout engagement lifecycles.
- Led restoration team of 12 engineers across simultaneous engagements to minimize downtime and client disruption.
- Successfully led incident response activities, including triage, containment, and resolution, while minimizing organizational impact and ensuring business continuity.
- Led efforts to design and implement incident response playbooks, incorporating the latest industry standards, open-source technologies, and innovative solutions.
- Coordinated with technical teams and third-party vendors to ensure rapid triage, containment, and resolution of security incidents.
- Provided growth insights and client opportunities to the business development team.

PricewaterhouseCoopers LLP (PWC) – Proactive Services, GRC, Incident Response, Insider Threat **Boston**
Senior Associate: Incident Response & Threat Management..... April 2016 – December 2020

Supported organizations' infrastructure through the evolving Threat and Vulnerability Management Program by enhancing the end-to-end program and developing an industry best practices remediation roadmap for use across the organization's cybersecurity posture.

- Developed a robust insider risk management program for a large foreign national bank to assess and mitigate cybersecurity risk.
- Conducted risk assessments to help clients understand and quantify risk exposures and evaluate risk strategies. Created a future state of control objectives considering regulatory requirements (COBIT, ITIL, HIPAA, NIST, FFIEC, ISO, CIS) and industry best practices to supplement the initial state.
- Provide tactical and strategic leadership for cybersecurity functions, encompassing network security, cloud management, and vulnerability assessment and management.
- Enhanced threat and vulnerability management programs for large financial institutions.

ANALOG DEVICES, INC. – Security Operations Center (SOC), Governance, Risk, and Compliance **Boston**
Security Operations Analyst • Information Systems Security Group..... May 2015 – April 2016

- Developed a comprehensive insider threat program, collaborating with cross-functional teams including Cybersecurity, Physical Security, Legal, Human Resources, and Engineering.
- Reviewed HR employee termination reports for employee background information to support investigative procedures and assessed them through the organization's Insider Threat Program for security auditing purposes.
- Utilized Digital Guardian to assess security incidents throughout the organization. Escalated all security breaches to key stakeholders immediately per company processes and policies.
- Supported the buildout of the company's information security awareness culture, policy, and processes.

MILITARY SERVICE

U.S. MARINE CORPS, 2008-2012

Purple Heart, Combat Action Ribbon, Presidential Unit Citation, Good Conduct Medal

EDUCATION

NORTHEASTERN UNIVERSITY, Boston, Massachusetts
M.S., Information Assurance & Cybersecurity

FRAMINGHAM STATE UNIVERSITY, Framingham, Massachusetts
B.A., History, Minor in Criminology and Information Technology