

# NATHANIEL W. HALL

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

## SUMMARY

**Digital Forensics & Incident Response Executive | Strategic Growth Leader:** Senior cybersecurity executive with over a decade of experience in Cybersecurity and Incident Response (DFIR) across insurance, private equity, and Fortune 100 clients. Proven ability to drive revenue, scale incident response programs, and build elite technical teams. Adept at advising stakeholders through high-stakes cyber crises while aligning services with strategic business goals. Speaker, collaborator, and thought leader trusted by legal counsel, insurers, and enterprise executives.

## EXPERIENCE

PONDURANCE – Incident Response, Threat Intelligence, Proactive Services **Chicago**  
**Incident Response, Legal & Insurance · Technical Director** ..... April 2025 – Current

Cybersecurity Incident Response Technical Director focused on threat intelligence-driven responses, proactive service delivery, and aligning with strategic partners. Skilled at translating complex threat activity into actionable outcomes and working closely with legal and insurance partners to streamline response, reporting, and the maturity of programs.

- Advised brokerage and insurance stakeholders on cyber risk posture, coverage applicability, and technical preparedness, positioning DFIR capabilities as a critical component of enterprise resilience and incident readiness.
- Advised senior management on technology strategy, vendor evaluation, and critical project initiatives to support organizational and security objectives.
- Contributed to incident response workflows by assisting with digital evidence collection, analytical triage, and remediation planning, documenting findings, and driving post-incident learning.
- Designed and refined threat intelligence collection, analysis, and dissemination workflows in partnership with IR and SOC teams to support detection, response, and strategic decision-making.

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

Leveraged my technical capabilities to cultivate new relationships with insurance brokers, insurance carriers, and law firms. I have also assisted insurance brokers and their clients in preparing for and obtaining 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.

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 across multiple workstreams to minimize service disruptions by recovering systems for medium— to large-sized businesses through effective risk mitigation.

- Led and developed a high-performing incident response team, providing strategic direction, technical mentorship, and operational oversight to drive successful client outcomes consistently.
- Conducted due diligence for private equity firms, advising on cyber risks tied to mergers and acquisitions.
- 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 business disruption.
- Coordinated with technical teams and third-party vendors to ensure rapid triage, containment, and resolution of security incidents.

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 and industry best practices, to supplement the initial state.
- Provided tactical and strategic leadership for cybersecurity functions, encompassing network security, cloud management, and vulnerability assessment and management.

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.
- Utilized Digital Guardian and EDR to assess security incidents throughout the organization. Escalated all security incidents 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**