Peter Dohr

Rochester, NY | (585) 490-3052 | pdohr33@gmail.com | linkedin.com/in/peterdohr

CAREER Profile

Cybersecurity executive with 12+ years leading global security operations across financial services and SaaS environments. Known for building scalable SOC programs that cut risk and improve resilience by aligning strategy with business goals. Experienced in driving automation to reduce alert volume, delivering measurable ROI, and strengthening enterprise detection and response. Trusted partner to boards, regulators, and executives, demonstrating how SOC investments improve resilience, efficiency, and cost control. Holds CISSP, CISM, GIAC certifications, and a Master's in Information Assurance.

Core competencies include SOC strategy and operations, automation and SOAR, detection engineering, incident response, threat intelligence integration, breach and attack simulation, audit/regulatory engagement, budget management, and executive communication.

CAREER HIGHLIGHTS

- Automated SOC pipelines that resolved ~96% of alerts, freeing the equivalent of 14 FTEs (~$1.4M annually) for higher-value work in hunting and tuning.
- Cut $480K in annual spend by retiring duplicative sandboxing platforms while improving detection fidelity and operational efficiency.
- Increased analyst throughput 30% by introducing an AI-enabled case-note validator that reduced peer-review time 70% and streamlined SOC documentation.
- Reframed SOC metrics from volume-based (alerts closed) to outcome-based (MTTD, MTTR, risk coverage), enabling executives to see clear ROI and positioning the SOC as a business enabler.

PROFESSIONAL EXPERIENCE

Fidelity Investments - Boston Massachusetts (Remote)

Vice President, Security Operations Center | December 2022 - Present

Lead a global 24×7 SOC of 60+ spanning triage, detection engineering, threat hunting cyber development, insider threat, and incident management. Govern hybrid MDR/MSSP operations, SOC roadmap, metrics, and regulatory engagement.

- Automated alert handling through SOAR, achieving ~96% auto-closure and freeing ~14 FTEs (~$1.4M annual value) for proactive threat hunting and tuning.
- Governed MSSP/MDR partners, aligning SLAs and detection integration; ensured 24/7 coverage across enterprise
- Improved visibility into cloud and on-premise threats by deploying new use cases, enabling earlier detection of malicious activity.
- Elevated analyst retention and accelerated promotions by launching a skills matrix and formal mentor rotation program.
- Introduced AI-enabled case-note validator that cut review time 70% and boosted analyst throughput 30%.
- Accelerated audit and regulator response cycles with standardized evidence playbooks, reducing preparation time and improving confidence with SEC, ISO, and GDPR examiners.

Paychex – Rochester, New York

Enterprise Security Fusion Center Manager | November 2021 - December 2022

Directed a multidisciplinary fusion center spanning threat hunting, detection engineering, intelligence, adversary simulation, insider threat, DLP, and triage to protect 21,000 employees and 650,000+ clients. Oversaw MSSP/MDR partnerships, agile program delivery, and security roadmap execution.

- Improved detection coverage and reduced noise by creating a defense loop that tied intelligence, hunts, detections, and simulations directly to MITRE ATT&CK.
- Reduced cycle time and improved transparency by embedding Agile workflows (Jira, Confluence) into detection engineering and reporting.
- Reduced delays and improved signal quality by optimizing MDR/MSSP integration and tightening SLAs. ● Enhanced executive readiness through ransomware tabletop exercises that strengthened crisis coordination across business units.
- Enabled risk-based decision-making by delivering regular KPI/KRI reports to the CTO.

Enterprise Security Fusion Center: Threat Hunt Lead | March 2020 - November 2021

Built and led Paychex's first enterprise-wide threat hunting program from the ground up, designing strategy, detections, and playbooks while mentoring analysts. Generated adversary simulation telemetry in the absence of a red team to proactively identify and close detection gaps.

- Established the organization's hunt framework, aligned with MITRE ATT&CK, to proactively identify blind spots and close detection gaps.
- Emulated adversary behavior using BAS tools to create telemetry that drove new detections against threat actor tactics, techniques, and procedures (TTP's).
- Accelerated mean-time-to-detect by developing reusable hunt playbooks and reporting pipelines. ● Raised program maturity and built depth by mentoring junior hunters and analysts.

Vulnerability Assessment: Penetration Test Engineer II | June 2019 - March 2020

Performed advanced penetration testing and security assessments of enterprise applications, infrastructure, and cloud environments. Provided actionable remediation guidance to reduce vulnerabilities and improve resilience.Perform both manual and automated penetration tests of internal systems and web applications.

- Performed red team engagements and penetration testing of enterprise applications to uncover high-risk weaknesses and support proactive remediation.
- Delivered executive-level reporting and technical remediation plans that accelerated patching cycles and reduced exploit exposure windows.
- Built and refined repeatable penetration testing methodologies, enabling consistent coverage and scaling assessments across the enterprise.
- Strengthened application security posture by embedding secure design principles into development cycles.

Security Investigations Unit: Engineer II (Promoted from Engineer I) | Oct 2015 – Jun 2019

Promoted to lead complex investigations into insider threats, malware, and anomalous activity after strong performance in initial triage and forensic analysis. Partnered with HR, Legal, and Compliance on sensitive cases, while using investigation outcomes to strengthen SOC content and shorten response times.

- Advanced from Engineer I to Engineer II within two years, reflecting proven ability to manage high-impact investigations and deliver executive-ready findings.
- Conducted endpoint, log, and network forensic analysis to uncover root causes of compromise and insider misuse across hybrid enterprise environments.
- Delivered executive-ready investigation reports and regulatory evidence packages; refined SOC workflows to accelerate compliance response times.
- Developed new detection rules and investigation playbooks from case findings, reducing

mean-time-to-respond (MTTR) and informing SOC tuning.

MIT Lincoln Laboratory – Lexington, Massachusetts

Information System Security Officer | June 2014 - October 2015

Served as ISSO for classified research environments, holding and maintaining an active DoD Top Secret security clearance. Ensured compliance with DoD, NIST, and FISMA standards while balancing hands-on security engineering with policy implementation and regulatory liaison responsibilities.

- Conducted system risk assessments, security control validation, and vulnerability remediation to maintain Authority to Operate (ATO) for classified networks.
- Authored and maintained security documentation (SSPM) used in DoD and government audits. ● Collaborated with program managers, researchers, and system admins to integrate security controls into high-performance computing and specialized R&D systems.
- Engaged with DoD accrediting authorities and regulators to address findings, achieve certifications, and sustain compliance across sensitive environments.

BitSight Technologies – Cambridge, Massachusetts

Technical Researcher | November 2013 - April 2014

Supported BitSight's global security ratings platform by performing reconnaissance, vulnerability analysis, and organizational profiling using OSINT techniques.

- Conducted OSINT-driven reconnaissance of public entities to identify exposures and inform security posture scoring.
- Performed internal network vulnerability scans with QualysGuard, reviewed reports, and provided recommendations to strengthen defenses.
- Built organizational profiles for companies worldwide, mapping external IP ranges, physical addresses, and key contacts for use in BitSight's security ratings product.
- Collaborated with product teams to improve data accuracy and expand coverage of the platform.

EDUCATION SUMMARY

Northeastern University, Boston, MA

- Master of Science in Information Assurance (MSIA), May 2015

Niagara University, Lewiston, NY

- Bachelor of Science in Criminal Justice, Minor in Computer Science, Summa cum Laude, May 2013

CERTIFICATIONS AND AWARDS

- CISSP - Certified Information Systems Security Professional - ISC2, 2025
- CISM - Certified Information Security Manager - ISACA, 2025
- GNFA - GIAC Certified Network Forensic Analyst - GIAC, 2021
- GREM - GIAC Certified Reverse Engineering Malware - GIAC, 2018
- GCFA - GIAC Certified Forensic Analyst - GIAC, 2017
- GCIH - GIAC Certified Incident Handler - GIAC, 2016
- Security+ - CompTIA, 2015
- Eagle Scout - Boy Scouts of America, 2009