Matthew J. Harmon

Security Manager, Threat Hunter, Lead Incident Responder

Minneapolis, MN resume@mjh.email +1 (612) 987 0115 https://matthewjharmon.com

Professional Summary

Cybersecurity executive with 20+ years of experience leading global incident response, threat hunting, and infrastructure architecture across enterprise and multi-cloud environments. Specializes in TTP-driven detection, forensic analysis, and post-incident recovery, with deep expertise in building resilient, fault-tolerant systems for high-risk operations and remote workforces. Architect of custom threat ingestion pipelines using NLP, TensorFlow, and OpenCV to accelerate hunt cycles and improve detection fidelity. Contributor to international standards through ISO, ITU, and ANSI, shaping protocols for AIDC and RFID security. Longtime SANS instructor and community organizer, known for developing immersive labs, mentoring professionals, and advancing collaborative security practices.

Core Competencies

- **Threat Hunting Leadership & Strategy:** Tools, Techniques and Procedures (TTP)-driven detection
- **Incident Response & DFIR Methodology:** Coordination, playbook writing, dwell-time reduction
- **Offensive Security & Red/Blue Collaboration:** Threat simulation, control testing, purple teaming
- **Cloud & Infrastructure Security:** Multi-cloud architecture, identity and access management (IAM)
- **Toolchain Development & Automation:** Custom scripting, tooling frameworks, pipeline integration
- **Global Standards Engagement:** ISO/IEC, ITU, ANSI liaison; committee chair

Technical Proficiencies

- **EDR & Forensics:** ELK Stack IDS, Snort (sig. author), Volatility, FTK, F-Response
- **SIEM & Threat Intelligence:** Splunk, Microsoft XDR/Sentinel, CrowdStrike, OpenVAS, Qualys
- **Networking & Firewalls:** Palo Alto, iptables/pf/OPNsense, Check Point FW-1, Cisco PIX/ASA
- **Cloud & Infrastructure:** AWS (+GovCloud), Azure, GCP, Terraform, Ansible, PostgreSQL, SQLite
- **Frameworks & Methodologies:** MITRE ATT&CK, OSSTMM, NIST CSF, SP 800 series, PCI-DSS, HIPAA

Community Leadership

- GCVE-BCP-02, *Practical Guide to Vulnerability Handling and Disclosure*, 2025. (link)
- Lead Organizer, Security B-Sides MSP (2013–2017): Created a multi-year security conference engaging the local community in a no-cost educational event in partnership with The Nerdery and Target Corporation.
- Founder & President, $(ISC)^2$ Twin Cities Chapter (2012–2014) including the creation of monthly presentations on a variety of timely security topics.

Teaching

- SANS Instructor for SEC 401 (GSEC), 464, 504 (GCIH) from 2008–2020.
- Primary Instructor for CSCI 2461 & 2462 from 2018–2020 teaching offensive and defensive computer security and Linux.

Professional Experience

Accenture — CIRT Manager of the Americas

Mar 2020–Present

- Led proactive, TTP-driven threat hunts across global environments, reducing attacker dwell time from industry average to under 1 hour.
- Supported and mentored a global team, performed malware analysis, and OSINT data gathering.
- Developed and executed incident-response and threat-hunting strategies.
- Developed a custom threat ingestion tool leveraging NLP, TensorFlow, and OpenCV to automate IOC parsing and ATT&CK mapping—accelerating hunt cycle time by 40 percent.
- Architected and built a multi-cloud infrastructure for high-risk work and remote workstations.

IT Risk Limited, LLC — President, Principal Consultant

Aug 2010–Dec 2019

- Founded and led a consulting firm focused on I.T. risk and red and blue-team activities.
- Led security engagements and advised executive leadership on cyber strategy.
- Directed team development, hiring, and performance management.
- Directed client acquisition through strategic sales engagements and live technical demos, resulting in a 3x increase in contract conversions.
- Led and resolved multiple high-impact disaster recovery scenarios, restoring critical infrastructure within SLA and minimizing business disruption.

Q.E.D. Systems — CTO, CISO
Aug 2003–2010

- Chairman ISO JTC1 / SC31 / US TAG 7 (Technical Group, Security for Item Management).
- Formal Liaison and Participant in ISO JTC 1 / SC 27 (IT Security); Participant in SC 31 / WG 7 (Security).
- Member ISO Technical Management Board (TMB) Privacy Steering Committee.
- Spearheaded development of AIDC security standards across ISO, ITU, and ANSI—establishing global protocols for secure item management.
- United States National Body liaison to ITU-T JCA-NID (Joint Coordinated Activity—Network Identifiers).
- Contributor to ISO/IEC TR 24729-4, *Information technology—Radio frequency identification for item management*, *Implementation guidelines—Part 4: Tag data security*.
- Contributor to ISO 24791-6 (Software system infrastructure—Part 6: Security).
- Contributor to AIM Global REG 352 (RFID — Guidelines on data access security).
- Authored "RFID Security Gaps" in ISO Focus+ (Apr 2010), influencing revisions to international RFID security guidelines.

The MITRE Corporation — InfoSec Engineer and Scientist
Mar 2001–Feb 2003

- Co-designed and implemented MIDAS, an early SIEM platform integrating threat analytics—laying groundwork for modern intrusion detection systems.
- Discovered and documented SSH1 CRC32 overflow vulnerability (CVE-2001-0144); authored Snort signature (RuleID 1324) adopted in national defense networks.

Early Contract Experience

- MCI WorldCom: Nov 2000–Feb 2001; LAN Tech
- Breakwater Security Associates: Aug 2000–Oct 2000; Security Consultant
- Playback Media, Inc.: Mar 2000–Aug 2000; Network Security Engineer
- Ulysses Telemedia Networks, Inc.: Aug 1999–Oct 1999; Systems Integration Engineer
- Norstan Communications: Jun 1999–Aug 1999; HP-UX Systems Administrator
- Secure Computing Corporation: Apr 1999–Jun 1999; Solaris Systems Administrator
- Pacific Tradewinds: Jan 1996–May 1999; Systems Administrator

Certifications

- $(ISC)^2$ CISSP #333906
- GIAC GSEC #19748, GCIH #20483, GCIA #9570
- Casino Gaming Commission Class E License (2015)

Publications and Presentations

- "Taking Control of IT Operations through the 20 Critical Security Controls", *CSO Outlook*, 2015. (link)
- "Plugging RFID Security Gaps", *ISO Focus+*, Apr 2010. (link)
- Interviewed by KSTP TV on ATM-skimming (May 2015) and breach response (2016–2017).
- Interviewed by Tech Pro on data centers and risk management.
- Presentation Archive available on GitHub.

Career Highlights

- Ran an early ISP in the 90's "GNU Networks" based on this new "Linux" free operating system.
- Since the pandemic began, I've taken the lead in hosting multiple weekly mentoring sessions.
- Certified Weather Spotter by the National Weather Service (2024).
- Volunteer for the Minneapolis CERT and Minnesota Medical Reserve Corps (2018–2024).
- Founders Award by the Minnesota Cyber Security Summit for contributions to the continued success of the event.
- Nominated for the Nobel Peace Prize. (Minneapolis)