MATTHEW J. HARMON

Minneapolis, MN • 612-987-0115 • resume@mjh.email

matthewjharmon.com

iD 0000-0003-1632-8927

- Cyber Incident Responder, Infrastructure Architect, Author, Teacher, Lead by Example
- Computer Science (Cyber Security) Instructor and Course Author (Off. Sec, Def. Sec, UNIX)
- SANS Instructor for SEC 401 (Security Essentials) and SEC 504 (Incident Response)

PROFESSIONAL EXPERIENCE

CONFIDENTIAL / Information Security, Global
(04/2020)-Present

- Led incident response operations across a global organization.
- Built hyper accountable, non attributable, infrastructure for high risk global operations creating a multi-cloud solution enabling new business opportunities.
- Improved tracking of false positives and known accepted behaviors.

IT RISK LIMITED / Co-Founder and Principal Consultant, Minneapolis
(08/2010)-(12/2019)

- Built a security consulting firm performing risk assessments, audits, and red team activities.
- Led remediation assistance treatments for audit findings, and security operations team building.
- Built secondary "small and medium business" division bringing cost effective enterprise security measures to small a medium sized organizations by partnering with local not-for-profits.

Q.E.D. SYSTEMS / CTO, Worldwide
(08/1998)-(07/2010)

- Built technology services and implemented control measures for a remote enterprise.
- Led development of standards within ANSI, ISO, and the ITU:
    - Participant in ISO JTC 1 / SC 27 (IT Security), Participant in SC 31 / WG 7 (Security),
    - Liaison Officer from ISO/TC 122 to ISO/TC 247 (Fraud countermeasures and controls),
    - Chair of ISO/IEC JTC 1/SC 31/US ADC 1/TG 7 "Security" (Security for Item Management).

The MITRE Corporation / INFOSEC Engineer/Scientist, East Coast
(03/2001)-(02/2003)

- Intrusion detection and threat analysis, exploit and vulnerability analysis:
    - CVE 2001-0144 & Snort 1 RuleID sig 1324. SSH1 CRC32 /bin/sh vulnerability.
- Team created the "MIDAS" intrusion detection, and threat analysis system used internally in MITREs CERT and deployed worldwide in active warfare zones.

VOLUNTEER EXPERIENCE

CYBER SECURITY SUMMIT / Advisory Board, Central Region
(07/2013)-2020

- Advisory board member and technology lead,
- Awarded for Visionary Leadership "The Morries."

SECURITY B-SIDES MSP / Advisory Board, Minneapolis / Saint Paul
(11/2013)-(08/2017)

- Event organizer and volunteer providing leadership and technology services for the event.

(ISC)² TWIN CITIES CHAPTER / Co-Founder & President, Minnesota
(03/2012)-(11/2014)

- Elected chapter president organizing providing monthly education to local security professionals.

MEDIA

- Expert panel with Minneapolis / Saint Paul Business Journal on Cyber Security (10/2017)
- Interviewed by KSTP for television reports on Breaches (2016-2018)
- Interviewed by KSTP for a television report on ATM Skimming (05/2015)
- Interviewed for Tech Pro (by the Tech Republic) article on Penetration Testing (2015)
- Interviewed for Tech Pro (by the Tech Republic) article on Risk Assessments (2014)
- Interviewed by WCCO for a TV spot on Security B-Sides MSP 2014 (2014)

PUBLISHED

- Published in CSO Outlook "Taking control of IT Operations through the 20 CSC" (06/2015)
- Published in ISO Focus+ "Plugging RFID Security Gaps" (04/2010)
- Contributor to CVE 2001-0144 and Snort 1 RuleID sig 1324 (2001)
- Contributor to ISO/IEC 24791-6, SC 31, Software system infrastructure – Part 6: Security
- Contributor to ISO/IEC TR24729-4, Information technology – Radio frequency identification for item management – Implementation guidelines – Part 4: Tag data security
- Contributor to ISO/IEC 21450-{1,2,4} IEEE 1451.{1,2,4}, Information technology — Smart transducer interface for sensors and actuators — Common functions, communication protocols

CERTIFICATIONS & LICENSES

- GIAC (Global Information Assurance Certification):

    - Security Essentials (GSEC #19748)

    - Incident Handler (GCIH #20483)

    - Intrusion Analyst (GCIA #9570)

- (ISC)^2 Certified Information Systems Security Professional (CISSP #333906)

- Aviatrix Certified Engineer (ACE) Multi-Cloud Networking Associate (ACE #2021-10689)

- Gaming Commission Class E License (2015)