

# Matthew J. Harmon

## EXPERIENCE SUMMARY

Matthew is a network and systems engineer, infrastructure architect and is a published security practitioner. He has instructed for the SANS Institute, authored courses, and taught at open-access colleges. Matthew teaches hands-on offensive and defensive computer security techniques, disaster recovery, and Linux. In addition, he spent fifteen years as a formal liaison building international standards, has taught and volunteered for the last decade while organizing and assisting with regional industry events. Matthew has excellent communication skills and the ability to communicate effectively with people from diverse backgrounds and all levels of an organization, with extensive experience across most industries and sectors.

## PROFESSIONAL EXPERIENCE ABSTRACT

### **CONFIDENTIAL, Global Technology** **April 2020 – Present** **Cyber Defense Infrastructure Architect**

- Assess the current state of operations, engage critical stakeholders on their units' pain points, identify gaps in controls, develop plans utilizing existing technology and relationships, and onboard new technology while training individual, organizational units on the latest technology.
- Build Greenfield specialized cloud system for high and extreme risk engagements.
- Lift organizational units to improved security posture while limiting interruption.
- Create new technology patterns that narrow and restrict weaknesses in publicly facing services.
- Manage audit, compliance, and information security controls.

### **IT Risk Limited** **August 2010 – 2019** **Principal Consultant**

- IT Risk Assessments, full-scope penetration testing and compliance audits, remediation assistance.
- Conduct incident response, investigation, forensic data acquisition, and security operations deployment.
- FBI InfraGard Minnesota Member and Casino Gaming Commission Registered

### **SANS Institute (Part Time / As needed, Independent Contractor)** **March 2008 – Present** **Instructor teaching Full Day, Week-Long & Local Mentor Format**

### **Saint Paul College** **January 2017 – May 2018** **Part Time Faculty - Computer Science**

- Advisory Committee for Cyber Security Associates of Applied Science Program (2014-2016)
- Teaching Computer Science and Cyber Security Assoc. in Applied Science as a Primary Instructor.

### **The MITRE Corporation** **March 2001 – February 2003** **INFOSEC Engineer/Scientist**

- Intrusion detection and threat analysis, exploit and vulnerability analysis, [Snort 1 RuleID sig 1324](#)
- MITRE CERT, CVE editor, NIPC article author, CVE 2001-0144 ([SSH1 CRC32 /bin/sh](#))
- My team assisted in creating the "MIDAS" intrusion detection, and threat analysis system used internally in the MITRE CERT and deployed worldwide in active warfare zones.

## VOLUNTEER SERVICES

### **Cyber Security Summit** **July 2013 – 2020** **Advisory Board & Technology Volunteer**

### **Security B-Sides MSP 2014-2017** **November 2013 – August 2017** **Lead Conference Organizer (Executive Director, 13-15)** **Infrastructure Support (Volunteer, 16-17)**

### **(ISC)<sup>2</sup> Twin Cities Chapter** **March 2012 – November 2014** **Founder & Elected Chapter President**

## **CERTIFICATIONS/LICENSES/DIPLOMA**

- GIAC (Global Information Assurance Certification):
  - Security Essentials (GSEC #19748)
  - Incident Handler (GCIH #20483)
  - Intrusion Analyst (GCIA #9570)
- (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP #333906)
- Aviatrix Certified Engineer (ACE) Multi-Cloud Networking Associate (ACE #2021-10689)
- Gaming Commission Class E License (2015)
- General Education Diploma (GED), Indian Hills Community College (1999)

## **NOTABLE TRAINING**

- SANS MGT 414, SANS+S Training Program for CISSP Certification
- SANS SEC 440, 20 Critical Security Controls
- ANSI #248 “Delegate to Diplomat: Representing the United States in International Activities”

## **Enrolled**

- University of the People, Computer Science, Bachelors of Science (Expected 2023)
- University of the People, (Declared) Master of Education (IB M.Ed. in Advanced Teaching, Expected 2024)

## **COURSES TAUGHT**

### **Saint Paul College Computer Science Department, Course Author & Primary Instructor:**

- CSCI [2461 70](#) & [71](#) Computer Networking 3 - Linux
- CSCI 2480 40 Network Security & Penetration Prevention
- CSCI 2482 40 Security Incident Handling, Response, and Disaster Recovery
- CSCI 2484 40 Ethical Hacking & Countermeasures

### **SANS Institute, Mentor & Community Instructor:**

- SANS SEC 401, “Security Essentials” (GSEC)
- SANS SEC 464, “Hacker Detection for Systems Administrators”
- SANS SEC 504, “Incident Handling and Hacking Techniques” (GCIH)

## **STANDARDS AND REGISTRATIONS**

- Contributor to ISO/IEC 24791-6, SC 31, Software system infrastructure – Part 6: Security
- Contributor to AIM Global, RFID Experts Group, REG 352 RFID – Guidelines on data access 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, and Transducer Electronic Data Sheet (TEDS) format

## **ELECTED AND DELEGATED POSITIONS**

- College **Professional Advisory Committee** member for:
  - [Sheridan College](#) Bachelor of Applied Information Sciences Information Systems Security (‘15-’19)
  - Saint Paul College Cyber Security Associates of Applied Science Program (2014-2016)
- Elected Board Member for Whittier Business Association, Delegated to Whittier Alliance At Large Board
- United States National Body Liaison from ANSI to ITU-T JCA-IoT (Internet of Things) (2007-2014)
- Liaison Officer from ISO/TC 122 (AutoID) to ISO/IEC JTC 1/SC 27 (IT Security) (2009-2014)
- Liaison Officer from ISO/TC 122 to ISO/TC 247 (Fraud countermeasures and controls) (2008-2014)
- Chair of ISO/IEC JTC 1/SC 31/US ADC 1/TG 7 “Security” (Security for Item Management) (2010-2013)
- Member ISO Technical Management Board (TMB) Privacy Steering Committee (2009-2012)
- ISO JTC1 / SC31 / WG4 / SG5 Security Ad Hoc Convener (2008-2012)