Matthew J. Harmon

612-987-0115 | mjh@itys.net | OrcID 0000-003-1632-8927

Summary

Dynamic and seasoned ISIRT and CIRT investigator with a proven track record as both an individual contributor and manager. Known for exceptional problem-solving skills, in-depth research abilities, and strong collaborative leadership. Eager to take on a role where I can innovate and implement cutting-edge technology security solutions while building and leading a world-class security team.

Recent Projects

Automated Research Analysis June 2024 – Present

Natural Language Processing *Python, TensorFlow, OpenCV, NLTK, RegEx*

- Designed and developed centralized platform that integrates data from various asset types, by incorporating features for tracking, reporting, and real-time analytics which streamlined asset management processes
- Developed a system that accepts research papers containing indicators of compromise and tools, techniques, processes and outputs KQL
- Utilized NLTK and Spacy model for natural language processing, Beautiful Soup for page scraping, and PyTesseract for OCR.
- Achieved significant reduction in malware research analysis time, improved standardization of queries, and improved accuracy

Attack Surface Reduction and Management Jan 2023 – March 2024

Asset Management *Python, Flask, SQLite3, PostgreSQL*

- Built a tool for accounting and analyzing owned IP, Domain, and VPN network assets
- Implemented two models, a preloaded but static SQLite version and a continual updating version with PostgreSQL and PL/SQL.
- Deployed Attack Surface Management tool and regularly use it to identify software rapidly, test hosts for vulnerabilities, and account for assets

Industry Representation at Cyber Security Summit 2013 – March 2024

Advisory Board *Networking, representation, collaboration, parliamentarian*

- Built the reputation of a regional security conference through multiple committee participation and functional volunteer advisor.
- Implemented multiple out reach strategies, strategic partnerships, and technology solutions to run the conference online and in-person.
- Received the ”Founder Award” as well as ”Visionary Leadership” award.

Experience

Security Delivery Manager April 2020 – Present

Accenture *Minneapolis, MN*

- Serving as incident response manager for the Americas region, built infrastructure for global operations.
- Threat hunter across a global organization, engineering multi-cloud solutions, custom deployment system for forensic tools.
- Managed responses to incident alerts by prioritizing and investigating small and large-scale incidents and acting as a liaison to executive staff ensuring timely resolution and effective communication.

Co-Founder & Principal Consultant August 2010 – December 2019

IT Risk Limited *Minneapolis, MN*

- Founded a security consulting firm with a focus on risk assessments, audits, and red team exercises.
- Directed the creation of remediation strategies for audit issues and the formation of a security operations team.
- Launched a specialized division for small and medium businesses through collaboration with local not-for-profit organizations.

Publications

CSO Outlook Global
Taking control of IT Operations through the 20 Critical Security Controls *2015*

Mpls / St. Paul Business Journal Central Region
Cyber Experts Panel *2017*

ISO Focus+ Global
Plugging RFID Security Gaps *2010*

MITRE Corporation Global
Common Vulnerabilities and Enumeration (CVE 2001-0144) *2001*

International Organization for Standardization (ISO) Global
Liaison from ANSI to ISO and International Telecommunications Union (ITU) *1995-2010*

• Contributor to Software system infrastructure – Part 6: Security - ISO/IEC 24791-61

• Contributor to Information technology – Radio frequency identification for item management – Implementation guidelines – Part 4 Tag data security - ISO/IEC TR24729-4

• Contributor to Information technology — Smart transducer interface for sensors and actuators — Common functions, communication protocols - ISO/IEC 21450-1,2,4 IEEE 1451

Technical Skills

Programming Languages: Python, C, SQL, Lua, Go, Shell Scripting

Product Specific: Microsoft: PowerShell, KQL and Azure/Entra, MDX/Defender Advanced Hunting. Tanium, Ansible, Palo Alto, Proof Point, OpenLDAP, Splunk, Proejct Discovery Suite

Skills: Cyber security instruction, legal liaison, team management, internal audit, planning and mission focus, machine learning application, embedded hardware

Certifications

• Global Information Assurance Certification (GIAC) – GSEC #19748, GCIH #20483, GCIA #9570.

• International Information System Security Certification Consortium $(ISC)^2$ – CISSP #333906.

• Gaming Commission Class E License (2015).