Jeremy McHugh, D.Sc.

AI Security Researcher | Engineering Leader | D.Sc. Cybersecurity

Pittsburgh, PA
https://mchugh.ai

EXPERIENCE

Preamble, Inc., Pittsburgh, PA — *CEO & Cofounder*

March 2023 - PRESENT

September 2020 - March 2023 – *CTO*

- Led AI security initiatives developing usage policies and frameworks for LLM safeguards
- Designed threat models and evaluation systems to assess cyber-relevant capabilities of AI models
- Discovered prompt injection vulnerabilities in GPT-3 Davinci and developed patented mitigation methods
- Contributed to NIST AI RMF and OWASP LLM standards
- Collaborated with ML engineers to develop systems balancing security research with misuse prevention
- Built and led technical team of 15 across AI research, product development, and policy implementation
- Advised and sponsored the first AI hacking competition (HackAPrompt - 600K+ attempts), developing datasets
- Raised VC funding and managed Air Force contracts

Westinghouse Electric, Pittsburgh, PA — Lead Threat and Vulnerability Analyst

June 2019 - April 2021

- Led global vulnerability management program across enterprise infrastructure, conducting threat modeling and risk assessments
- Developed threat intelligence procedures and detection capabilities, implementing monitoring systems
- Collaborated with cross-functional teams to translate technical cybersecurity risks into business impact assessments for our board of directors

NTT Security, Pittsburgh, PA — Threat Detection Analyst

October 2017 - May 2019

- Provided managed security services in Security Operations Center (SOC), conducting threat hunting

SKILLS

Vulnerability Research

Exploit Development

Threat Modeling

AI Safeguard Development

Penetration Testing

Malware Analysis

LLM Security Research

Policy Development

Team Leadership

Cross-functional Collaboration

Model Fine-Tuning

CERTIFICATIONS

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

GIAC Penetration Tester (GPEN)

GIAC Web Application Penetration Tester (GWAPT)

GIAC Certified Incident Handler (GCIH)

EC Council Certified Ethical Hacker (CEH v9)

EC Council Certified Network

- Applied threat intelligence, malware analysis, and machine learning techniques to identify actionable security events
  - Developed and documented threat detection methodologies for

diverse client environments

Raytheon, Tucson, AZ — Information Assurance Specialist Intern

September 2017 - October 2017

- Conducted security assessments to identify and mitigate vulnerabilities in defense systems
- Monitored for insider threats and ensured compliance with regulatory security requirements

US Air Force, Tucson, AZ — *IT Specialist (Active Duty Service)*

October 2013 - October 2017

- Implemented cybersecurity principles and hardening procedures for IT systems per NIST and DISA guidelines • Conducted vulnerability scans as a member of a Cyber Protection Team (CPT) and remediated security gaps

EDUCATION

Marymount University, *Doctor of Science (D.Sc.), Cybersecurity*

2020 - 2023

Dissertation on Defensive AI

Sans Technology Institute, *Graduate Certificate, Penetration Testing & Ethical Hacking* 2016 - 2018

Western Governors University, *Master's Degree, Cybersecurity and Information Assurance* 2015 - 2016

Pennsylvania State University, *Bachelor's Degree, Telecommunications*

2008 - 2012

Penn State Ice Hockey Club

Community College Of The Air Force, *Associate's Degree, Information Systems Technology*

2014 - 2015

EC Council Computer Hacking Forensic Investigator (CHFI)

Cisco Certified Network Associate Cyber Ops (CCNA Cyber Ops)

CompTIA Security+ ce

CompTIA A+ ce

Patents

Mitigation For Prompt Injection In AI Models Capable of Accepting Text Input

(Pending) Generative AI System

Awards

US Air Force Distinguished Graduate

US Air Force Basic Training Honor Graduate

Cisco Global Cybersecurity Scholarship

Defense Architect (CNDA)

Splunk Certified User