Brendan Francis O'Connor

bfo@ussjoin.com https://ussjoin.com
406.545.0430

Experience

Staff Security Engineer 2022 -

Cedar

As a Staff Security Engineer, I am responsible for engaging in high-leverage work to improve security across Cedar to protect patients, medical providers, and our employees; I also help educate our engineers on secure programming practices, perform code reviews, and guide technical implementations of key client-required security features. My recent large-scale work has included rebuilding the corporate IAM and secrets management systems, compiling the first complete set of technical client contract requirements, and creating a trusted baseline and deployment tracker for our container build systems.

Senior Security Advisor 2014 - 2016, 2019 - 2022

Leviathan Security Group

I worked as a Senior Security Advisor in Leviathan's Risk and Advisory Services group, where I built security programs, advised teams on how best to meet compliance goals, and conducted large-scale architecture and security ecosystem assessments on codebases with more than ten years' engineering effort, more than 20 million end users, or both. I built SOC 2 Type II-compliant security programs and defended them during audits, and advised management at dozens of companies on HIPAA, FERPA, HITRUST, CMS ARS, ISO 27001/2/18, and PCI compliance. I also co-wrote four whitepapers on forced data localization as it affects security, and more recently, one on Kubernetes and container security.

Policy Engineer 2019 - 2019

GitHub

I as the primary technical resource for GitHub's public policy team, which advocates for laws, regulations, and judicial actions that protect the rights of software developers and promote open collaboration. As the team's first Policy Engineer, my role was to bridge the policy, security, and software development worlds to help ensure that GitHub could represent their concerns accurately in global policy discussions. I was primarily responsible for GitHub's policy efforts related to information security, supply chain protection, and international trade, and I represented GitHub Policy in broader Microsoft activities related to trade compliance.

Enterprise Security Platform Lead 2018 - 2019

RealSelf

As the head of the information security program at RealSelf, I directed the company's overall security, risk and compliance efforts. This involved close coordination with the RealSelf executive and engineering teams to align security priorities with our business goals and overall risk posture; I reported to the CTO and General Counsel. My work included developing and delivering security training, working with developers and SREs to design and implement security at all levels of our systems, building our ISO 27000-aligned information security management program, communicating with customers regarding security issues, leading security incident response efforts, working with our legal and privacy teams on vendor management, and managing our bug bounty program. I also worked on HIPAA, PCI, GDPR, and other regulatory issues to ensure that we were able to meet evolving obligations, and ultimately, that the trust our users placed in us was well-earned.

Chief Technical Officer / DSS 2010 -

Malice Afterthought, Inc.

Malice Afterthought provides information security consulting services. Some highlights of past work: I led an international nonprofit's security efforts, including both building a multi-regulated compliance program (FERPA, HIPAA, and FedRAMP) and implementing technical defensive tools; I taught at a Department of Defense information and network warfare (CNO) school; and I won and completed two DARPA Cyber Fast Track (CFT) contracts. Languages and tech stacks have included Ruby, Python, Perl, D3JS, UnityScript, Hadoop, Spark, and AWS, among many others.

Selected Presentations

Security by Consent; or, Peel's Principles of Security Operations October 18, 2016
SecTor - Toronto, ON, Canada
How to create and maintain a security operation within a larger organization that focuses on cooperation and consent, rather than coercion, based upon the 'policing by consent' model created in 1820s England.

Stalking a City for Fun and Frivolity August 3, 2013
DEF CON - Las Vegas, NV
Distributed sensor network data acquisition, filtering, and visualization, with several security applications. This presentation addressed the architecture and collection aspects of the CreepyDOL system, as well as the implications for global surveillance states and engineering as a profession.

CreepyDOL: Cheap, Distributed Stalking August 1, 2013
Black Hat USA - Las Vegas, NV
Distributed sensor network data acquisition, filtering, and visualization, with several security applications. This presentation addressed the architecture and collection aspects of the CreepyDOL system.

Education

Juris Doctor, Cum Laude September 2011 - May 2014
The University of Wisconsin - Madison

Master of Science in Engineering in Computer Science September 2005 - May 2009
The Johns Hopkins University

Bachelor of Science in Computer Science September 2004 - May 2008
The Johns Hopkins University

Certifications & Memberships

Attorney September 21, 2015
State Bar of Montana, Washington State Bar Association

Fellow of Information Privacy (FIP) June 6, 2023

Certified Information Privacy Technologist (CIPT) May 10, 2023

Certified Information Privacy Professional U.S. Private Sector (CIPP/US) December 14, 2015
International Association of Privacy Professionals

Certified Information Security Manager (CISM) February 6, 2020

Certified Information Systems Auditor (CISA) August 12, 2016
Information Systems Audit and Control Association

Certificate of Cloud Security Knowledge (CCSK) - v3 2016, v4 2022 February 20, 2016
Cloud Security Alliance

Certified Information Systems Security Professional (CISSP) July 20, 2012
International Information Systems Security Certification Consortium (ISC(2))