

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 work in conjunction with the Compliance, Legal, Privacy, and Engineering functions to help teams do their best work.

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 worked with client engineering teams to design efficient software that meets security and privacy requirements. I have taken clients through first-time SOC 2, Type II audits, dealt with customer audit teams, and advised senior management on how best to ensure their business can both achieve its primary goals and comply with applicable regulatory requirements. I also co-wrote four whitepapers on forced data localization as it affects security, and more recently, one on Kubernetes and container security. I rejoined Leviathan in 2019 after spending time leading security programs as an FTE elsewhere. From 2014 until mid-2015, I worked as a Senior Security Consultant on Leviathan's Technical Services team. Languages spanned a wide array; compliance stacks included SOC 2, ISO 27001/2, HIPAA, HITRUST, CMS ARS, and PCI.

Policy Engineer

2019 - 2019

GitHub

I worked on 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 those fields' 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 to a range of clients, from small businesses to large corporations. Some highlights of past work: leading an international nonprofit's security

efforts, including both building a multi-regulated compliance program (FERPA, HIPAA, and FedRAMP) and implementing technical defensive tools; teaching at a Department of Defense information and network warfare (CNO) school; and two successful 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

Probably: an Irreverent History of the GDPR

August 10, 2018

DEF CON Crypto and Privacy Village - Las Vegas, NV

A humorous overview of the creation of the GDPR, what came before it, what it does, and why to embrace it.

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

Certified Information Security Manager (CISM)

February 6, 2020

Information Systems Audit and Control Association

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 Privacy Professional U.S. Private Sector (CIPP/US)

December 14, 2015

International Association of Privacy Professionals

Certified Information Systems Security Professional (CISSP)

July 20, 2012

International Information Systems Security Certification Consortium (ISC(2))