New York, New York

Ben Virgilio

ben@benvirgilio.com
https://benvirgilio.com

Experience

American Museum of Natural History

New York, New York

Cybersecurity Manager — May 2022 - Present
Senior Security Engineer — August 2017 - May 2022
Security Engineer — February 2016 - August 2017

Led the growth of a small cyber security program at a globally recognized Museum and research institution. Accomplishments include the development of a risk driven vulnerability management program, incident response procedures, compliance and alignment with numerous security frameworks and the migration of aging network security infrastructure. Balancing security fundamentals with research and education requirements.

Responsibilities

- Monitor, triage, and respond to security incidents using an array of in-house and off the shelf tools
- Produce and implement Strategic Security Plans
- Maintain and audit network security access control (Cisco Catalyst ACLs and Cisco Firepower/ASAs) and monitoring devices (Security Onion/Surricata/Zeek)

Projects

- Supported the deployment of an NSF Grant Funded (Award #1827153) Science DMZ network, a high-speed network designed to support the transfer and management of high- volume scientific research data. Responsible for the development and implementation of low impact highly effective security measures
- Overhauled and deployed network access control including the use of certificate based 802.1x authentication

Stroz Friedberg

New York, New York

Associate — January 2015 - February 2016
Analyst — June 2014 - January 2015

Responsibilities

- Assess network infrastructure and design, Active Directory security and account management processes, and overall patch management procedures
- Execute penetration tests using Metasploit Framework, BurpSuite, Responder and other industry recognized tools
- Interview clients to understand security culture, risks and concerns and develop wholistic recommendations designed to support existing initiatives
- Supported incident response engagements leveraging penetration testing methodology to guide triaging.

Projects

- Developed internal tooling to support incident response investigations and security assessments

Senator Patrick Leahy Center for Digital Investigation

Burlington, Vermont

Lead Network Administrator — September 2013 - June 2014

Responsible for the upkeep and functionality of both the research and isolated forensics networks and computing environments.

Education

Burlington, VT **Champlain College** **2010 | 2014**

Bachelor of Science Degree in Computer Networking and Information Security
With Minor in Computer and Digital Forensics

Project Highlights

Most of my work can be found on my github account https://github.com/nebriv/, but there are a few projects I wanted to highlight.

- **This Resume!** (https://github.com/nebriv/resume/)
  While all resumes are a bit of project, I heeded many a peers advice and built out this resume using LaTeX. I then took it a bit further and developed a little Github action workflow to automatically build a PDF. This allows for multiple different versions of content, and should provide a good history.
- **VTOLVR-Mods** (https://vtolvr-mods.com)
  Developed python backend to allowing mod creators to upload their mod packages to a central location accessible by the modloader platform. Backend site utilizes a RESTful API, numerous integrations with Steam, Discord and others, as well as full administration and moderation utilizes.

Skills)

- **Cisco Products** ASA, AnyConnect, Identity Services Engine (ISE), Umbrella, DuoSecurity
- **Scripting/Programming Languages** Python, PHP, Powershell
- **Microsoft E5/A5 Solutions** Defender for X, Entra, Sentinel, Purview
- **Microsoft Azure**
- **Amazon Web Services (AWS)**
- **Operating Systems** Windows Server, RHEL/CentOS, Debian/Ubuntu
- **Vulnerability Scanners** Acunetix, Tenable.io/Nessus, Qualys, BurpSuite, Metasploit, sqlMap

Certifications

- **CompTIA Security+ Certified** July 2013 – July 2016
- **GIAC Continuous Monitoring** September 2017 – Present
- **GIAC Defensible Security Architecture** October 2021 – Present
- **GIAC Public Cloud Security October** 2022 – Present