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 development of the cybersecurity program at a globally recognized research and educational institution. Established layered defenses with a focus on enhanced visibility and rapid detection, adopting new and well established technologies and methodologies. Prioritized strategic, impactful security measures that both safeguarded and supported the institution'sprimary focus on research and education. These foundational security initiatives empowered the museum to safely extend its global reach and influence.

Responsibilities

- Formulate and oversee the institution's cybersecurity strategy, ensuring a balance between security measures and the organization's core focus on research and education.
- Continuously assess potential security risks and implement measures to mitigate vulnerabilities across on-premises infrastructure, cloud platforms, and vendor solutions.
- Architect and deploy a multi-tiered security approach, incorporating both traditional defenses like network-based IDS and advanced deceptive measures. This strategy aims to enhance detection speed, increase system-wide visibility, and proactively identify potential breaches in their earliest stages.
- Lead the institution's response to cybersecurity incidents, coordinating rapid detection, containment, and remediation efforts.
- Influence the selection, deployment, and effective use of security technologies and tools in alignment with the institution's objectives.
- Assist the CISO in the development, review, and refinement of cybersecurity policies and procedures. Ensure alignment with relevant regulations and security frameworks, and facilitate security audits, liaising with auditors as required.
- Engage with senior management, departments, and external industry entities, facilitating effective communication and collaboration on security matters. Participate in the Information Sharing and Analysis Center (ISAC) specific to educational institutions.

Notable 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.
- Spearheaded the integration of 802.1x EAP-TLS authentication, complemented by the implementation of Single Sign-On (SSO), advanced Identity and Access Management (IAM), and Azure Conditional Access. Further fortified user access controls through the deployment of DuoSecurity's Multi-Factor Authentication (MFA) and FIDO2 tokens, driving the institution's move toward a holistic, risk based, zero-trust framework.
- Authored over 60 internal code repositories in GitLab, comprised of tools for operations, incident investigation, IOC automation, SIEM mailbox monitoring, data redaction, and more. Leveraging CI/CD for risk-reduced deployment of detection and prevention strategies.
- Transitioned legacy ASA firewalls to a more agile and robust multi-context high-availability cluster. Additionally, introduced cloud-based firewalls, facilitating the secure migration of essential business processes to cloud infrastructures, offering scalability and adaptability to emerging threats.
- Developed an in-house security operations system using open-source platforms and cloud solutions,

bolstering threat monitoring and incident handling. Implemented Defender Advanced Hunting rules tailored for sophisticated phishing campaigns, and other industry specific threats. Enhanced detection and response strategies by integrating the Mitre ATT&CK framework, ensuring a robust understanding of adversary tactics.

- Led the evolution of the institution's centralized logging capabilities by implementing an ELK stack. Directed the integration of diverse log sources, including servers, network hardware, cloud services, and more. Developed unit testing for specific log capture capabilities to valid capabilities across system upgrades and changes. Strategically developed alerts based on data collected from previous penetration tests, bolstering detection and proactive response to potential attack vectors.
- Developed a tailored cybersecurity training curriculum, complemented by controlled phishing tests to gauge and enhance employee threat awareness. This initiative led to heightened user vigilance, evidenced by the successful detection and reporting of sophisticated phishing campaigns.
- Transitioned from Spirion to Microsoft's DLP solution to enhance data security measures, deployed on premise data scanners. Collaborated with appointed departmental data custodians to review and address findings, streamlining data protection and compliance efforts. Developed sensitive data labels for users to flag their data in accordance with institutional data security policies.

Stroz Friedberg

New York, New York

Associate — January 2015 - February 2016

Analyst — June 2014 - January 2015

Responsibilities

- Conducted comprehensive security assessments, emphasizing a holistic approach that not only identified technical vulnerabilities but also systemic issues rooted in organizational politics and culture.
- Executed penetration tests on wireless, physical infrastructure, servers, and web apps with tools such as Metasploit, BurpSuite, and Responder. Highlighted how vulnerabilities were chained together to escalate from unprivileged access to domain admin roles.
- Presented technical findings to C-suite, translating complex vulnerabilities into actionable insights. Collaborated with client technical teams to prioritize and tailor solutions, ensuring recommendations fit their unique environment and needs.
- Supported major incident response engagements, leveraging offensive security experience to provide detailed roadmaps of potential attack vectors and vulnerabilities.
- Engaged in reverse engineering of zero-day vulnerabilities identified during assessments, subsequently reporting findings to relevant vendors for mitigation.

Notable Projects

- Developed internal scripts to assess client Active Directory environments for vulnerabilities. These scripts facilitated rapid, accurate, and repeatable insights into the health of the client's systems, predicting broader infrastructural challenges. Automatically generated actionable reporting data, significantly enhancing the efficiency of final client report preparations.
- Supported the creation, deployment, and implementation of a portable log analytics system, streamlining forensic and incident response investigations.

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/)
  Constructed this resume using LaTeX, integrating it with a custom-built GitHub action workflow for automated PDF generation. This implementation ensures efficient versioning and flexibility for content variations.
- **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 mod loader platform. Site features include a RESTful API, numerous integrations with Steam, Discord and others, as well as full administration and moderation utilizes.
- **Home Lab/Home Automation**
  Deployed internal proxmox hypervisor to run home lab resources including standard network requirements (DNS/IDS/etc), along with Home Assistant and other home automation utilies. Multiple VLANs separate IOT/media/computer systems, bridged with an OPNSense router out to commodity ISP. Home lab provides a sandbox to deployment various configurations and software stacks to learn and test against. This setup also provides a sandbox environment for testing and learning, with VPN integrations to various cloud providers for added flexibility.

Skills/Proficiencies

- **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** Azure Firewall, Sentinel, Container Apps, Logic Apps, Log Analytics, Virtual Machines and Networking
- **Amazon Web Services (AWS)** IAM Identity Center, EC2, VPC, Lambda, Route 53, S3
- **Operating Systems** Windows Server, RHEL/CentOS, Debian/Ubuntu
- **Vulnerability Scanners** Acunetix, Tenable.io/Nessus, Qualys, BurpSuite, Metasploit, Responder, sqlMap, and many more open source security tools as they are released

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