Ben Virgilio

Cybersecurity Manager (Program lead, security engineering) | GCPN, GPCS, GDSA, GMON
New York, NY | ben@benvirgilio.com | linkedin.com/in/benvirgilio | benvirgilio.com | github.com/nebriv

I build security that enables the mission instead of getting in its way: high-impact, low-friction, and measurable. Over 14+ years I've built and run enterprise security programs, and today I lead security engineering for a 2,000+-staff research and educational institution across detection, response, identity, and vendor governance. What I'm proudest of is that, rather than buying a packaged MSSP, my team and I built our own security operations platform out of open-source and community tooling: a production SOAR, 500+ detection rules, recurring threat hunting, 25-feed threat-intel distribution, and centralized logging across 15+ sources, all on a Zero Trust identity foundation, with AI and LLMs put to real work rather than used as a talking point.

EXPERIENCE

American Museum of Natural History | New York, NY
Cybersecurity Manager | May 2022 – Present
Senior Security Engineer | Aug 2017 – May 2022
Security Engineer | Feb 2016 – Aug 2017

- **Program & Team Leadership.** Lead cybersecurity engineering for a 2,000+-staff research and educational institution, maturing the program into a security and detection engineering practice with 24/7/365 coverage across a complex hybrid environment. Built and lead the team across hiring, performance, and on-call; own the institutional security budget end-to-end on a deliberately lean, open-source-first strategy; and serve as the institution's primary cybersecurity subject-matter expert.
- **Detection & Response.** Own detection engineering and incident response on an in-house security operations platform – built on open-source and community tooling rather than a packaged MSSP – spanning a production SOAR (8 playbooks; MTTA cut from hours to minutes), 500+ MITRE ATT&CK-mapped detection rules, a recurring threat-hunting program, threat-intel automation ingesting 25+ feeds into 6 enforcement points, and centralized logging across 15+ sources, plus a KPI metrics dashboard and LLM-assisted incident enrichment. Validate coverage continuously against tabletop and external red-team exercises.
- **Identity, Cloud & Edge Architecture.** Built and run the institution's Zero Trust identity foundation – certificate-based 802.1x EAP-TLS, SSO, IAM, MFA with FIDO2 hardware tokens, and risk-tiered Conditional Access that tightens automatically for users who fail phishing simulations – alongside a revamped security-awareness program. Codified change-management governance for the production cloud and edge (WAF, DNS, tunnels) infrastructure-as-code pipelines where none existed, and led an institution-wide PKI/TLS modernization across hundreds of certificates.
- **Hands-On Engineering & Infrastructure.** Stay deep in the stack across security, networking, and systems: consolidated 12 legacy firewalls into a multi-context high-availability cluster, introduced cloud firewalls, and secured an NSF-funded Science DMZ for high-volume research data transfer; run Linux server administration, Intune/Entra, and AWS and Azure operations; and shipped 60+ internal repositories – Python tooling, IOC automation, incident investigation – many on CI/CD pipelines. Still drop to low-level network diagnosis when speed matters, recently root-causing a recurring cloud-provider VPN disconnect by correlating rekey events, then building a monitor for it.
- **Risk, Governance & Executive Reporting.** Own the program's business-facing surface: framework alignment (NIST CSF and CIS Controls, with PCI DSS, FERPA, and NIST 800-53 engagement), the risk register and third-party/vendor risk, data loss prevention, a vulnerability-management cadence restructured across

3 remediation teams, and external partnerships – incident-response retainer, cyber-insurance reviews, recurring penetration testing, and external auditors. Produce the executive briefings, root-cause writeups, and risk narratives that roll up through the CIO to the board, and grow the team through SANS training and CTFs, including a 1st-place finish at SANS NetWars Core 2025.

Stroz Friedberg | New York, NY

Analyst → Associate | Jun 2014 – Feb 2016

- **Security Assessments.** Conducted client reviews that identified technical vulnerabilities alongside systemic issues rooted in organizational politics and culture.
- **Penetration Testing.** Executed engagements on wireless, physical infrastructure, servers, and web apps with tools such as Metasploit, BurpSuite, and Responder; showed how individual vulnerabilities chained together to escalate from unprivileged access to domain admin roles.
- **Executive Reporting.** Presented technical findings to C-suite, translating complex vulnerabilities into specific, prioritized recommendations; worked with client technical teams to tailor remediation to their environment.
- **IR Engagement Support.** Supported major incident response engagements, using offensive security experience to map likely attack vectors and vulnerabilities for the responders.
- **Zero-Day Research.** Reverse engineered zero-day vulnerabilities identified during assessments and reported findings to the relevant vendors for mitigation.
- **Active Directory Assessment Toolkit.** Developed internal scripts to assess client Active Directory environments for vulnerabilities, producing rapid, repeatable readings on system health and surfacing broader infrastructure issues. Auto-generated reporting data cut the time needed to prepare final client reports.
- **Portable Log Analytics.** Contributed to the creation, deployment, and implementation of a portable log analytics system used in forensic and incident response investigations.

Senator Patrick Leahy Center for Digital Investigation | Burlington, VT

Lead Network Administrator | Sep 2013 – Jun 2014

- **Network Administration.** Managed and maintained the research and isolated forensics networks, ensuring data integrity for active case files.
- **Research Support.** Provided insights and resources to LCDI research projects and oversaw internal web resources for employees.

UMass Amherst, Administration & Finance | Amherst, MA

Security Consultant | Jan 2012 – Aug 2013

- **Permissions & Data Discovery.** Conducted NTFS permissions audits, located sensitive data using Identity Finder, and built vulnerability remediation plans via the Qualys platform.
- **Printer Hardening.** Hardened multi-function printer configurations and shipped automated tools for continuous assessment and remediation.

TECHNICAL SKILLS

Security & Risk: Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), Endpoint and Extended Detection & Response (EDR/XDR), Detection Engineering, Threat Hunting, Incident Response, Vulnerability Management, Data Loss Prevention (DLP), Threat Intelligence (STIX/TAXII), MITRE ATT&CK, Zero Trust, Identity and Access Management (IAM), Third-Party Risk Management (TPRM)

Compliance & Frameworks: NIST Cybersecurity Framework (CSF), NIST SP 800-53, CIS Controls, PCI DSS, FERPA

Cloud & Platforms: Microsoft Sentinel, Defender (Endpoint, Cloud Apps, Identity, Office 365), Entra ID, Conditional Access, Purview, Azure (Functions, Logic Apps, OpenAI, AI Foundry, Container Apps, Log Analytics, Firewall); AWS (Landing Zone Accelerator, IAM Identity Center, Organizations, Control Tower, EC2, VPC, Lambda, Route 53, S3, CloudTrail, Athena, KMS); Cloudflare (Zero Trust, WAF, Workers, Tunnels)

Engineering & Automation: Python, PowerShell, Kusto Query Language (KQL), Bash; Terraform (remote-state), AWS CDK, GitOps CI/CD, DevSecOps, Podman quadlets, systemd-managed containers, Docker Compose; LLM integration (Azure OpenAI, AI Foundry, agentic workflows)

Network & Identity: Cisco (firewalls, VPN, Identity Services Engine, Umbrella); 802.1x EAP-TLS; Multi-Factor Authentication (MFA), FIDO2 hardware tokens; Privileged Identity Management (PIM); Security Assertion Markup Language (SAML), OAuth, Microsoft Graph

Operating Systems & Assessment: RHEL, Rocky Linux, Oracle Linux, CentOS, Debian, Ubuntu; Windows Server, Active Directory; macOS; BurpSuite, Metasploit, Responder, sqlmap, Tenable.io / Nessus, Qualys, Acunetix; mobile application assessment; open-source security tooling

CERTIFICATIONS

GIAC Cloud Penetration Tester (GCPN) | Mar 2026 – Present

GIAC Public Cloud Security (GPCS) | Oct 2022 – Present

GIAC Defensible Security Architecture (GDSA) | Oct 2021 – Present

GIAC Continuous Monitoring (GMON) | Sep 2017 – Present

AWARDS

SANS NetWars Core 2025, 1st Place (Team) | 2025

SANS SEC588 Class Coin (top student, Cloud Penetration Testing) | Dec 2025

EDUCATION

Champlain College | Burlington, VT

B.S., Computer Networking & Information Security; Minor in Computer & Digital Forensics | 2010 – 2014

PROJECTS

This Resume & Tracker | github.com/nebriv/resume

The résumé you're reading and the system around it. It's authored in LaTeX and built by a GitHub Actions pipeline that produces a tailored PDF for every branch, and it's backed by a small Cloudflare Worker that attributes opens and in-PDF link clicks so I can actually tell who's reading. Stack: LaTeX, GitHub Actions, Cloudflare Workers, D1.

VTOLVR-Mods | vtolvr-mods.com

A community platform for the VTOL VR flight sim. A Python backend and RESTful API let mod creators publish packages that the in-game loader pulls down, with Steam and Discord integrations and a full administration and moderation stack. It's grown into real infrastructure that a community actually depends on. Stack: Python, REST, Steam, Discord.

Home Lab | Self-hosted infrastructure

My production-grade playground. k3s runs on Proxmox behind a Traefik ingress; TrueNAS backs Nextcloud and Immich; Raspberry Pi nodes pick up distributed workloads; OPNsense segments IoT, media, and compute onto separate VLANs; and CrowdSec watches the whole estate across k3s, TrueNAS, and pfSense. It's where I prove out deployment patterns and security tooling before any of it gets near production at work.

hikesafe-web | github.com/nebriv/hikesafe-web

A hiking safety and trip-planning tool that pulls scattered outdoor data sources into one place, so you can prepare for a trail without juggling ten browser tabs. It came out of the time I spend in the mountains.

AudioBook-Generator | github.com/nebriv/AudioBook-Generator

A generative audio pipeline that turns text into narrated audiobooks with modern text-to-speech, a fun way to make long reading consumable on a commute or a trail.

AllTrails-DataExporter | github.com/nebriv/AllTrails-DataExporter

A utility for getting your own AllTrails activity history back out into open, portable formats, because your outdoor data should belong to you, not a single app.

VTOLVR-TacviewLogger | github.com/nebriv/VTOLVR-TacviewLogger

A telemetry logger for VTOL VR that emits Tacview-compatible debrief files, so a squadron can fly an engagement and then replay and pick it apart afterward.