Steven **Collmann**

✉ stevcoll@gmail.com | ☎ (717) 638-8889 | Lancaster, PA | linkedin.com/in/stevecollmann

Work Experience

SIXGEN
Annapolis, MD

OFFENSIVE CYBER OPERATOR — *Nov 2020 – Present*

- Specialize in open source intelligence and analysis of data breaches
- Discovery of various critical level web vulnerabilities for large organizations
- Perform web application and network penetration testing for corporate clients
- Operate assessment tools such as Nessus, BurpSuite, SQLmap, and GoBuster
- Plan and execute targeted email phishing campaigns against high value targets
- Generate and obfuscate malicious payloads for Windows and Linux systems
- Engage in post-exploitation and privilege escalation efforts with red team
- Create detailed vulnerability and mitigation reports for organizations

Lancaster General Health
Lancaster, PA

CARDIAC MONITOR TECHNICIAN — *Feb 2019 – Sep 2019*

- Created dynamic EKG monitoring and quizzing application for training purposes
- Analyzed, documented, and reported patient cardiac rhythms in a rapid manner
- Interacted with floor patients in placing and maintaining wireless cardiac monitors
- Automated scanning and electronic documentation process to improve efficiency
- Performed training of new personnel in rhythm identification and analysis
- Troubleshot cardiac monitoring equipment to resolve artifacts and noise

ICF International
Aberdeen, MD

SENIOR SECURITY ENGINEER — *Jun 2010 – Sep 2017*

- Engineered proprietary, high-performance intrusion detection tools for 24/7 CERT
- Increased technical productivity of security analysts by several orders of magnitude
- Discovered several zero-day root level compromises, utilizing custom tools and tactics
- Performed DevOps between development team and DoD CSSP operations center
- Provided security consulting to incident handlers and cyber research associates
- Performed applied research on signature and anomaly based intrusion detection tools
- Co-authored public research papers and internal technical documents on cyber topics
- Participated in Information Assurance Certification and Accreditation Process (DIACAP)

Iron Mountains LLC
Morgantown, PA

SENIOR TECHNICAL CONSULTANT — *Dec 2012 – Feb 2014*

- Provided technical consulting and security engineering to chief technical officer
- Implemented enterprise wireless authentication solution for all endpoints
- Engineered and managed gateway security and antivirus products
- Directed operation of custom timekeeping and product engineering software
- Administered network intrusion detection tools and signature rulesets
- Managed physical security systems and automated building controls

Conestoga Christian School
Morgantown, PA

TECHNICAL CONSULTANT — *Jun 2005 – Dec 2012*

- Provided technical consulting, systems engineering, and network management services
- Saved client thousands per year through open source software and custom server builds
- Executed site-wide migration from legacy server platform to Windows 2012 Server
- Designed custom applications to track endpoint health and operational status
- Engineered enterprise-level wireless security solution for three campus buildings
- Performed network intrusion detection and analysis of potential insider threats

ITT Incorporated
Doha, Kuwait

REMEDY DEVELOPER — *Jan 2004 – Jan 2005*

- Developed and oversaw outage tracking system for Army regional communications
- Performed interface design, engineering, and workflow of Remedy applications
- Collaborated with development teams on integration of real-time network outage data
- Engineered first enterprise help desk application for Army in Iraq, Kuwait, and Afghanistan
- Assisted Army personnel with troubleshooting of terrestrial communications equipment
- Produced written and verbal technical briefings for Army BG and MG officers

Skills

Certifications:	A+, Network+, Security+, MCSD, MCP, GPEN, AWS Certified Developer
Languages:	Python, Perl, Ruby, C++, JavaScript, PHP, Go, Bash, PowerShell, VBScript
Databases:	MSSQL, MySQL, Oracle, SQLite, Splunk, PostgreSQL, Memcached, LevelDB
Cyber Offense:	MITRE ATT&CK, Kali, Metasploit, BurpSuite, Nessus, OSINT, Nmap, Wfuzz
Cyber Defense:	Snort, Bro, Tcpdump, Wireshark, SolarWinds, Splunk, ArcSight, ELK, SecurityOnion
Cloud Tech:	AWS EC2, S3, Lambda, ElastiCache, RDS, API Gateway, ELB, DigitalOcean
Systems:	Microsoft Windows, Linux, Unix, Ubuntu, Debian, CentOS, Solaris, VMware
Microsoft:	O365, AD, SQL, GPO, DNS, DHCP, LDAP, VPN, EFS, RADIUS, Kerberos
Medical:	EKG Interpretation, 12-Lead Interpretation, Basic Cardiology, Epic EMR, PPE
Soft Skills:	Creativity, Teamwork, Communication, Leadership, Adaptability, Collaboration

Projects

Facebook - Capture The Flag Platform (FBCTF) *PHP, HHVM, JavaScript, MySQL*
Significant contributions as a developer, performance engineer, and quality assurance tester *https://github.com/facebook/fbctf*

WraySec - Cyber Exercise Platform (CyExNg) *PHP, JavaScript, MySQL, AWS*
Comprehensive development, engineering, and quality assurance *https://wraysec.com/cyexng*

EKGMon - Cardiac Telemetry Platform *JavaScript, jQuery, HTML, CSS*
Sole developer of EKG training platform utilized in heart rhythm identification *https://ekgmon.com*

ICF - Network Security Tool Suite *Perl, Python, PostgreSQL, SQLite*
Sole developer, engineer, and quality assurance of a suite of intrusion detection tools *Private*

DoD - Cyber Range Development *MSF, C, Perl, Python, Ruby, PHP*
Development and engineering of large scale offensive scenario on DoD cloud range *Private*

Awards

2012	**2nd Place (World Finals)**, Team ICF	*Cyberlympics*
2012	**1st Place (North American Championship)**, Team ICF	*Cyberlympics*
2011	**1st Place (Maryland Cyber Challenge)**, Team ICF	*CyberMaryland*

Education

CHI Institute *Broomall, PA*
A.S. in Computer Programming *2000 – 2002*
GPA: 3.69