

CODY MARTIN

Mobile: (843) 801-9007

<https://www.codymartin.com>

Email: codymartin00@gmail.com

<https://substack.com/profile/50250573-cody-martin>

Information Security and Cybersecurity professional with experience in Fortune 200 consulting. Experienced in communicating organizational risk to technical and business stakeholders for strategic business decision-making. Also experienced in presenting tools in public forums and providing instruction on new research. Skilled at attacking a wide range of environments including Active Directory, Linux, and Azure Active Directory as well as developing offensive and operations-based applications in C# and Python. Responsibly published multiple vulnerabilities after working closely with affected software and hardware vendors. Specialized experience in offensive cloud security within large enterprise environments.

CORE COMPETENCIES:

Mentoring, Cloud Security, Penetration Testing, Vulnerability Research, Risk Identification & Assessment, Technical Writing, Python, C#, Application Development, Product Management, Agile Product Development

INDUSTRY CERTIFICATIONS:

- Altered Security Certified Azure Web Application Security Professional (**CAWASP**) (2022)
- Pentester Academy Cloud Security Professional (**PACSP**) (2022)
- Altered Security Certified Az AD Red Team Professional (**CARTP**) (2021)
- Altered Security Certified Red Team Professional (**CRTP**) (2021)
- Offensive Security Certified Professional (**OSCP**) (2019)

PROFESSIONAL EXPERIENCE:

Black Lantern Security (BLSOPS LLC) Charleston, SC February 2020 – Present

Senior Red Team Operator

- Mentor junior level staff on specialized areas of knowledge and the offensive lifecycle
- Perform and take ownership of Penetration Tests and Red Team exercises against enterprise environments from kickoff to delivery
- Create and deliver reports on vulnerabilities discovered, risk management, and cybersecurity maturity following the NIST SP-800 Series and a modified version of the Cybersecurity Maturity Model to client stakeholders including technical and executive audiences
- Provide recommendations and remediation support for discovered issues
- Develop and manage multiple public/private offensive and operations-based applications
- Publish articles on new vulnerabilities discovered (CVEs) during client assessments and tool development
- Present at Information Security conferences including BSides Augusta and BSides Greenville

Ingalls Shipbuilding Mobile, AL May 2018 – October 2018

Intern Software Developer

- Developed custom application for business operations using C# and JavaScript
- Increased the speed of product development by coordinating team resources more effectively
- Performed code reviews regularly
- Delivered the product on time and meeting all customer requirements

Continental Aerospace Mobile, AL August 2016 – May 2018

Intern Software Developer

- Developed multiple custom applications for external and internal corporate functions using C# and JavaScript
- Managed front-end and server-side application development
- Performed code reviews regularly
- Worked with the client to ascertain product functional requirements
- Delivered fully functioning products to client on time that met all outlined requirements

EDUCATIONAL ACHIEVEMENTS:

University of South Alabama **Mobile, AL** **2013 – 2019**

Bachelor of Science in Computer Science (BSCS) (3.6 GPA)

- Areas of study included offensive cyber security, compiler design, secure software development, information assurance, static code analysis using abstract interpretation and formal methods
- NSF CyberCorp Scholar for Service Recipient (SFS) (2019)
- Cum Laude
- Presented robotics automation research at ACM Mid-Southeast Conference (2017)
- Treasurer for USA ACM (4 years)
- Officer with Upsilon Pi Epsilon (2018-Present)

Bachelor of Science in Mathematics (BS) (3.6 GPA)

- Areas of study included cryptography, number theory, general topology, graph theory, and applied statistics
- Mathematics Departmental Scholarship recipient (Multiple)
- Presented novel proofs of the hemi-compactness property of certain topological spaces at USA Summer Undergraduate Research Fellowship (2018)
- Presented work contributed to pi-base, a general topology proof and counter example database, at the USA/USM/SELU Research Mini-Conference (2018)
- Treasurer for USA Math & Stat Club

PROJECTS:

GitHub – [Offensive-Azure](#) (Public) **Online** **April 2022- Present**

Product Owner, Developer

- Microsoft Cloud offensive toolkit written in Python 3
- Utilizes Continuous Integration / Continuous Delivery (CI/CD) pipelines to maintain code consistency and security
- Actively managed with the use of the Scrum framework and product management best practices

GitHub – [Enter The Matrix](#) (ETM) (Public) **Online** **July 2021 – Present**

Product Owner, Developer

- Threat modeling and attack narrative building application built with NIST SP-800-30v1 in mind
- Generates attack graphs and threat trees based on engagement scenarios
- Ties in with the MITRE ATT&CK framework for Enterprise/Mobile/ICS
- Generates “living” Threat Matrices used by defenders
- Presented at BSides Augusta (2021) and BSides Greenville (2021)
- Built with C# and JavaScript
- Actively managed with the use of the Scrum framework and product management best practices

PUBLICATIONS:

- [Privileged Directory Traversal in Brocade Fabric OS](#) (August 2022) (CVEs) (BLSOPS LLC)
- [Introducing Offensive-Azure](#) (March 2022) (Tool) (BLSOPS LLC)
- [Privileged Read and Weak Default Credentials in Brocade Fabric OS](#) (February 2022) (CVEs) (BLSOPS LLC)
- [A Better Way to Threat Matrix](#) (October 2021) (Tool) (BSides Augusta)
- [A Better Way to Threat Matrix](#) (October 2021) (Tool) (BSides Greenville)
- [Threat Matrices](#) (July 2021) (Blog) (BLSOPS LLC)
- [Tripp Lite Stored XSS](#) (June 2021) (CVEs) (BLSOPS LLC)
- [Enter The Matrix](#) (October 2020) (Tool) (BLSOPS LLC)
- [Cisco Unified IP Conference Station 7937G](#) (April 2020) (CVEs) (BLSOPS LLC)