

Michael Cochran

mclarkfyru@gmail.com | (443) 900-7903 | 7452 School Avenue, Dundalk, MD 21222

OBJECTIVES

Pivoting 9 years of elite federal cyber operations and specialized systems engineering into private sector innovation. Aiming to apply a proven track record of autonomous systems engineering, breakthrough AI efficiency research, and proprietary tool development to architect scalable, high-performance solutions in a commercial environment.

SKILLS & AI RESEARCH

- **Core Programming:** Senior Python Development, Senior Rust Development, C, C++, Assembly x86, and Golang.
- **Aptitude:** Exceptional aptitude for rapid skill acquisition; fully prepared to master any additional languages or technologies on demand.
- **Cyber Operations:** Advanced Penetration Testing, Digital Network Exploitation, Target Digital Network Analysis, Target Analyst Reporting, and Title 10 Offensive Cyber Operations.
- **AI & Independent Engineering Research:** Prototyping "Sentinel," an advanced AI project tailored for defense applications, utilizing Rust to architect a high-performance framework.
- **Tokenization Breakthrough (Coding Focus):** Developed a proprietary tokenization methodology specifically for source code, resulting in a 3.2x increase in LLM efficiency and context density during programming tasks.
- **SaaS Development:** Developing "ronin-sites.pro," a scalable SaaS platform utilizing Python, FastAPI, and Vue.js to build cost-effective, reliable infrastructure.

EXPERIENCE

Senior Systems Engineer | MaxisIQ

(September 23, 2024 – Present)

- Worked on mission critical systems enabling USCYBERCOM's ability to conduct Title 10 Operations.
- Created custom python software to conduct systems survey using minimal third party support that supports protocol connections like SSH and Kerberos domain authentication.
- Designed software plans to conduct automation of server service repairs upon recognizing a degraded service state.

Senior Software Engineer | Two Six Technologies

(September 9, 2022 – September 23, 2024)

- Worked on integrations to mission critical software aligned to the Joint Cyber Warfighting Architecture while supporting a user interface that allows for external integration support.
- Experienced in converting custom, proprietary query language by removing the abstraction layer on top of SQL to allow for yaml to SQL syntax queries with an offline json representation of the actual database.
- Experienced in creating software that conducts data extrapolation with custom regex parsing and data sanitization.

United States Army Systems Developer | USCYBERCOM J38 Joint Mission Operations Center Enterprise

(June 6, 2020 – September 9, 2022)

- Critical factor in standing up organization for synchronizing existing Joint Mission Operations Centers utilizing USCYBERCOM Offensive Cyber Operations authorities.
- Conducted development work in support of Cyber National Mission Force and USCYBERCOM J9 for a large scale project.
- Created Application Programming Interfaces between project components.
- Created Test Cases in conjunction with the usage of a CI/CD pipeline.
- Led documentation efforts in conjunction with best Python Documentation Practice.
- Conducted data modeling and validation for API rest implementations.
- Programmed the automation of network protocols for project use.
- Utilized Gitlab to work with a large team that were in charge of different equities.
- Contributed in the usage of Docker Images to pivot project to utilize containers.

Offensive Cyber Operator | Combat Mission Team

(February 6, 2017 – June 6, 2020)

- Certified as a USCYBERCOM Title 10 Offensive Cyber Operator.
- Conducted over 100 missions in direct alignment of USCYBERCOM's countering violent extremist organizations directive.
- Initiated and led automation efforts of operator techniques and technologies using Python programming.
- Automation efforts included: File IO, Network IO, Command Line Interfaces, User error protection, Linux/Unix OS interactions, and Verbose Logging.

Digital Network Exploitation Analyst | National Mission Team

(July 5, 2014 – February 6, 2017)

- Conducted mapping and analysis of networks of interest through intelligence sources.
- Correlation of targets of interest while performing analysis.
- Accurate reporting to the Intelligence Community while adhering to proper procedures.