Michael Roberts

Contact Information   (407) 733-5074
michaelrobertsucf@gmail.com

Resume Summary:

Experienced professional in application, network, and cloud security and architecture. With experience leading security initiatives for companies such as IBM, Northrop Gruman, NetApp, Chick-fil-A, Kinder Konsulting and Abbott Laboratories

Education

University of Central Florida, Orlando, FL
Master of Science in Digital Forensics, May 2021

University of Central Florida, Orlando, FL
Master of Business Administration (MBA), anticipated 2022

University of Central Florida, Orlando, FL
Bachelor: Information Technology, May 2019
Deans List 2017 & 2018

Infosec Institute
CISSP Training and examination
Passed exam 10/05/20

Certifications

ISC2 Associate - Member 774753
AWS Certified Solutions Architect
AWS Certified Cloud Practitioner

Experience

Security Engineer III   August 2019 - Present
Abbott Laboratories, Orlando, FL

- Design and implement a secure architecture for cloud based environments based on NIST, CIS, and FedRAMP requirements
- Drive security initiatives across multiple teams, such as a WAF/RASP implementation
- Write Python software for AWS infrastructure security assessment, Tenable.io vulnerability reporting, and automated access control reviews with SSO provider.
- Custom Implementation of Wazuh/Ossec and Suricata/Snort with many custom rules, out of the box features, and custom dashboards for SIEM (ELK) integration
- Evaluate the security posture of existing web applications and related cloud infrastructure.
- Perform security impact analysis to find flaws before they are introduced into production

Cyber Defense Team Lead   May 2016 - Present
University of Central Florida, Orlando, FL

- Lead a team of up to 14 engineers with a variety of roles, while ensuring yearly growth
- Act as the highest escalation for customer, management or engineering team security concerns
- Detect, re-mediate, prevent security risks throughout the business
- Use Metasploit, Nmap, Cobalt strike and other tools to perform network penetration testing.
- Use SIEM, EDR, and host native tools to detect and mitigate production threats
- Participated in team based competitions such as CCDC, CyberForce, and CPTC. Winning approximately 15 first or second place awards