

KYLE FOLLANSBEE

**willing to relocate*

EDUCATION

University of South Florida

Master of Science in Cybersecurity; Cyber Intelligence

Cumulative GPA: 4.0 / 4.0

Relevant Coursework: Cryptography, Digital Forensics, Professional/Technical Communication, Information Security and Risk Management, Business Continuity and Disaster Recovery, and Intrusion Detection.

Tampa, FL

December 2021

University of Florida

Bachelor of Science in Journalism; Investigative

Highlight: Most published staff writer during Summer 2014 for the largest student-run newspaper in the US

Gainesville, FL

May 2015

CompTIA

Cybersecurity Analyst (CySA+) CSO-002

Valid December 2021–December 2024

PROJECT & RESEARCH EXPERIENCE

Microsoft Azure Sentinel (SIEM)

Assembled an Azure Sentinel and connected it to a live virtual computer that served as a honeypot. Observed Event Viewer Logs in VM via Security Center (Microsoft Defender for Cloud). Reviewed real-time international attacks (RDP Brute Force). Extracted custom fields from log data. Utilized a custom PowerShell script to compile attacker's geolocation and plot on a map.

February 2022

Ubuntu VirtualBox Cryptography Lab

Deployed virtual environments using an Ubuntu v20.04 image to explore; secret-key cryptography concepts, writing programs that encrypted/decrypted different messages in length and content, padding, initialization vectors (IV), keyed hashes using HMAC-MD5/HMAC-SHA256/HMAC-SHA1, obtaining an X.509 certificate, generating a certificate signing request (CSR), signing and verifying a file using the Elliptic Curve Cryptography (ECC) scheme, Public Key Infrastructure (PKI), and Management of Certificate Authority with Blockchain.

October 2021

Issue Analysis Research on Cyberbiosecurity: A Priority for US Healthcare Security

Led a group of colleagues to research, source, and publish a 17-page paper utilizing techniques, i.e., Chronologies and Timelines, Structured Self-Critique, Key Assumptions Check, Starbursting, Mind Maps, and Reversing Assumptions to analyze how cyberattacks on the healthcare industry can directly endanger the wellbeing of American patients.

July 2021

Issue Analysis Research on the National Security Threat Presented by Deepfakes

Researched, sourced, and published a six-page report indicating that deepfake creation technologies, e.g., reactive neural network training and generative adversarial networks (GANs) are outpacing detection technologies and will threaten US national security by impacting democracy, weakening citizen trust, and influencing socioeconomic institutions.

November 2020

Front-end Development

As a freelance developer, I minimized coding time by utilizing JavaScript libraries (React), Bootstrap, and preprocessors (Haml/Sass). Maintained budget-friendly solutions by taking free online courses to learn new languages, e.g., Python. Earned friendly, personable reputation leading to 20% increase of clients in five months.

June 2019 - December 2019

PROFESSIONAL EXPERIENCE

Sumter County Sheriff's Office

Network Administrator

Wildwood, FL

January 2020 - present

- Supported 100+ internal users via domain integration, Group Policy configuration, and DNS/DHCP implementation
- Configured Symantec Endpoint Protection, local Firewalls, site-to-site VPNs for new WFH protocols
- Responded to malware incidents by containing and recovering data; reduced avg. monthly events from 2 to 0
- Resolved a variety of T.1-3, LAN, and WAN networking issues by working closely with vendors and end-point users
- Active Directory Administration on Windows Server; provision/deprovisioning user accounts via PowerShell or GUI
- Enforced internal threat compliance by hosting network security, data storage, and software usage workshops

TOOLS & SKILLS

Offensive Security: Kali Linux, Metasploit, nikto, Nmap, Snort, Splunk, Volatility Framework, Wireshark

Cloud/Virtualization: Microsoft Azure Sentinel, SolarWinds Virtualization Manager, VirtualBox, VMware

Programming: Bootstrap, Docker, ES6 (JavaScript), Git, Haml (HTML5), jQuery, Node.js, Python, React, Sass (CSS3)

Operating Systems: Linux, macOS / X, TailsOS, and Windows 11 / 10 / 7

Technical: Active Directory, Firewalls, LAN/WAN setup, SSL/TLS management, TCP/UDP, Cryptographic Schemes

Languages: English (native), Spanish (beginner)

LICENSES

US Amateur Radio, General Class

Callsign: KF0LLY

August 2020