

# Julian Cadavid

📍 3929 Maxine Street, Fort Myers, Florida, 33901    ✉ jcadacv@icloud.com    ☎ 7863148918

## EDUCATION

---

### Bachelors of Science in Cybersecurity and Information Assurance

09/2020 – 02/2022

*Western Governors University*

- WGU Cybersecurity Club Member
- The Order of the Sword & Shield National Honor Society

## CERTIFICATIONS AND SKILLS

---

CompTIA CySA+

CompTIA PenTest+

CompTIA Security+

CompTIA Network+

CompTIA Project+

CompTIA A+

Systems Security Certified Practitioner (SSCP)

ITIL®1 Foundation

## PROFESSIONAL EXPERIENCE

---

### SOC Analyst

04/2022 – present

*Binary Defense Systems*

- Evaluated/deconstructed malware to determine risk and understanding of the behavior and purpose of the malware sample to prevent future cyberattacks.
- Consolidated and conducted comprehensive analysis of threat data obtained from classified, proprietary and open source resources to provide indication and warnings of impending attacks against unclassified and classified networks.
- Perform analysis of SIEM events with an emphasis of white listing false positives to reduce alarm counts and increase true positive detections.
- Perform Cyber Threat Intelligence Research for new attack vectors and software vulnerabilities utilizing online tools including AbuselPDB, VirusTotal, Shodan, and IBM XForce.
- Escalate true positives and assist clients using ticketing system (Zendesk)

### Restaurant Manager

12/2015 – 04/2022

*Over Easy Cafe*

Sanibel, USA

Developed soft skills such as:

- Ability to deal with difficult situations in a friendly and positive manner in fast-paced environment
- Assisted entire team to achieve maximum efficiency during peak hours
- Able to multitask efficiently while paying close attention to detail

Manager: Trasi Sharp +1(239) 565-2263

### Operations & Technology Risk Management Intern

06/2021 – 08/2021

*The Depository Trust & Clearing Corporation*

Tampa, USA

- Developed a Sharepoint site for the Security Awareness training
- Helped train DTCC staff on phishing dangers through monthly newsletter contributions

## PROFESSIONAL SUMMARY

---

### How can I help your organization?

Cyber Security Analyst with proficient experience and good understanding of information technology. Developed skills in proactive network monitoring of SIEM platforms such as Splunk, Microsoft Sentinel, AlienVault/USM and LogRhythm, as well as a few others. I'm a curious person and enjoy tinkering with different technology to determine how to efficiently use it in a professional environment and contribute to my team.

## SKILLS

---

- AlienVault/USM
- Microsoft Sentinel
- Splunk
- Reverse Engineering
- Computer Forensics
- Malware Analysis
- Virtualization
- Packet Capture Analysis