Felix Guerrero Jr.

Email: FelixGuerrero12@gmail.com **Mobile Phone:** (443) 666 4032
Website: DetectionsForCatchingBaddies **Certifications:** **OSCP**, **OSCE**, **RHCSA**, **RTO**, AWS **CCP** / **SCS**, CEH

Summary

Security Engineer with 9 years of experience in threat detection and incident response, developing creative solutions to capture offensive operations.
Professional Highlights:

- Deployed AWS serverless pipeline tracking 100+ C2 indicators. ***Blog on Serverless Lambda for Threat Intelligence***
- Developed C2 analytics dashboard for an threat intelligence servers tracker publicly available. ***Access Sight: Threat Intelligence C2 Tracker***
- Developed Fetch tool for M365/Azure/Microsoft Graph enumeration. ***Blog on Fetch - Azure Enumeration Web App***
- Designed 45+ identity management detections for Splunk, Crowdstrike EAM, and LogScale. ***Detections List***

Professional Experience

Bank of America, Dallas, TX, USA

Vice President: Threat Hunt Sept 2020 – Current

- Spearheaded cloud threat hunt initiatives, identifying security risks within the corporate Azure/M365 and AWS infrastructure.
- Generated 85+ alerts identifying four threat groups using TTPs, mitigating threats related to process execution and network communications.
- Developed and executed 10+ threat hunt hypotheses, revealing internal policy abuse and corporate fraud.

BlackBerry, Dallas, TX, USA

Security Consultant Oct 2019 – May 2020

Salesforce, Herndon, VA, USA

Senior Incident Response Analyst Feb 2018 – June 2019

- Led security investigations, resolving major cases involving insider threats and data exposures.
- Automated data extraction scripts, cutting response times by 40 percent.
- Mentored 8+ junior analysts in incident management and data analysis, boosting team efficiency.

MKA Cyber, Fairfax, VA, USA

Lead Security Analyst Dec 2016 – Jan 2018

- Led client-facing technical projects, creating Python scripts to automate the collection of indicators of compromise, reducing data gathering time by 40
- Developed Splunk SIEM dashboards, enhancing real-time security analytics.

Education

Towson University, Towson, Maryland, USA

Bachelor of Science in Information Technology Jun 2016