Felix Guerrero Jr.

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

Summary

Security Engineer / Threat Hunter with over **10 years of experience** in threat detection and incident response, specializing in the identification of nation-state threat actors through authentication log analysis, architecting and building security solutions including a centralized threat indicator platform, and implementing detection methodologies for external threats and insider abuse.

Professional Highlights:

- Developed centralize threat intelligence to store indicators in modern format (STIX v2.1).
- Deployed AWS serverless pipeline tracking 100+ C2 indicators. ***Blog on Serverless Lambda***
- Created C2 analytics dashboard for threat intelligence ***Access Sight: C2 Tracker***
- Developed Fetch tool for M365/Azure enumeration with Python. ***Blog on Fetch***
- Designed 45+ identity management detections. ***Detections List***

Professional Experience

Bank of America, Dallas, TX, USA

AVP -> Vice President: Threat Hunt - Cloud Lead SEPT 2020 – CURRENT

- Led identification of nation-state threat actors through authentication log analysis using Splunk, Python, and CrowdStrike. Designed and developed a centralized threat indicator platform to store and categorize indicators. Created 85+ detection rules through cross-team collaboration, generating alerts to mitigate threats across Azure/M365 and AWS infrastructure. Executed threat-hunt hypotheses revealing insider threats and nation-state actor infiltration attempts.

BlackBerry, Dallas, TX, USA

Security Consultant OCT 2019 – MAY 2020

- Led offensive security team exploiting Active Directory and enterprise networks.

Salesforce, Herndon, VA, USA

Senior Incident Response Analyst FEB 2018 – JUNE 2019

- Led / supported technical efforts on critical government and corporate investigations, including insider threats, data exposure, and corporate-wide compromises. Developed time-saving scripts to automate data extraction during high-severity incidents. Mentored junior analysts on incident management and data analysis.

Education

Towson University, Towson, Maryland, USA

Bachelor of Science in Information Technology JUN 2016