**Christopher J. Alonso**

Aventura, FL | [christopheralonso1@gmail.com](mailto:christopheralonso1@gmail.com) | <http://christopherja.rocks>

**WORK EXPERIENCE**

**IBM**

*Cyber Security Remediation & Innovation Engineer* March 2021 - Present

* Provided full remediation documentation (steps,pocs,etc) in response to security incidents that occurred throughout the IBM ecosystem.
* Implemented full stack web application to allow other teams within IBM to report and request assistance from our internal organization.
* Created tool to detect specific malware IOCs in memory and alert if server seems to be compromised. Specifically tailored for praying mantis suite of IIS Server Attacks.
* Wrote blog posts on behalf of team to inform other organizations of specific attacks executed in the wild in various systems.

**ConquestCyber (United Data Technologies Branch)**

*Senior Cyber Threat Hunter/Backend Dev* March 2020 – March 2021

* Ran attacks on virtual azure environment to analyze log data and craft alerts for the SIEM, using tools such as cobalt strike, and self-written tools. This was to ensure that our sentinel platform had the latest alerts and most up to date IOC’s
* Used python to solve issue of generating alerts from elastic database and streamline them into the SOAR platform for automation and response.
* Onboarded data using custom programs written by myself to ingest data from AWS cloud to Azure sentinel cloud siem and across Gov cloud environments.
* Implemented Azure Devops System to have azure sentinel SIEM providing end to end pipelines and deployment system for new alerts and playbooks.

**HealthChannels**

*Cyber Security Analyst* October 2019 – March 2020

* Successfully created windows machine security standard by automating task of hardening windows devices before being shipped out to remote employees.
* Completely built Splunk SIEM solution from the ground up, ingesting data from multiple sources allowing a view into organization network security as well as cloud usage statistics.
* Developed custom Splunk application which ingested data from google alert center and pushed it directly to a Splunk cloud instance via HEC.
* Lowered risk of PHI exfiltration by creating cloud custom solution for remote employees in which all amazon workspaces are ephemeral saving no data on disk after disconnect.
* Secured company on an incident by incident basis swiftly responding to all security incidents across many attack vectors such as phishing and malware containment.

**United Data Technologies**

*Cyber Security Engineer/Python Dev* March 2019 – October 2019

* Monitored network traffic via ELK SIEM and provided timely reports to clients on commonly occurring events and network traffic as well as steps for remediation.
* Wrote Python based web application to facilitate the transfer of data from various applications throughout the company allowing multiple systems to work as a single integrated unit.
* Built Demisto SOAR solution from scratch and wrote python programs to automate incident analysis and response reducing workload for team members and lowering number of analysts needed on SOC team on any given shift.
* Engineered end to end L1 SOC workflow starting with all alerts for ELK SIEM based on mitre attack framework along with playbooks tailored to each alert automatically occurring in the Demisto soar solution. Procuring an automation standard and freeing up analysts to perform other tasks such as threat hunting, forensics etc.

**SKILLS, ACTIVITIES, INTERESTS & CERTIFICATIONS**

**Certifications:**

* Offensive Security MacOS Researcher (OSMR)
* Offensive Security Certified Expert (OSCE3)
* Offensive Security Web Exploitation Expert (OSWE)
* Offensive Security Experience Penetration Tester (OSEP)
* Offensive Security Exploit Developer (OSED)
* Offensive Security Certified Expert (OSCE Old)
* Offensive Security Certified Professional (OSCP)
* CRTE
* Red Hat Certified Engineer (RHCE)
* Microsoft Azure Administrator (AZ-103)
* Microsoft Azure Security Engineer (AZ-500)
* Microsoft O365 Security Administrator (MS-500)
* Security+

**Programming:** Golang, Python, C, PHP, Bash, PowerShell, Docker, Linux,

**GitHub:** [*https://github.com/latortuga71*](https://github.com/latortuga71)

**Cobalt.io Pen tester** [*https://www.cobalt.io/*](https://www.cobalt.io/)