# Emmanuel Atala

emmanuel.atala@outlook.com | Emmanuel Atala | LinkedIn | (832) 883-2421 | US Citizen | Spring, Texas

**Education and Certifications:**

- MS Data Analytics – Data Science, Western Governors University – Enrolled.
- BS Cybersecurity and Information Assurance, Western Governors University – Graduated.
- CompTIA: A+, Network +, Security+, CySA+ and Pentest+. ISC2 SSCP, CCSP. Certificate of Cloud Security Knowledge v.4.

**Work History:**

*Detection Engineer, LevelBlue formerly AT&T Cybersecurity, Texas, 2022 - Current*

- Developed detections for different technologies, maintained malware sandboxes, and assisted with incident response activities.
- Used Jira to manage requests and epics for new detections or improvements to existing code.
- Used Bitbucket for version control and pull request review.
- Analyzed customer fleet data in Opensearch to develop new detections based on patterns.
- Published curated threat intelligence content using Alienvault OTX.
- Used regular expressions to match text patterns to enhance detections.
- Tested Tactics, Techniques, and Procedures in a sandbox environment to improve or develop new detections based on the results.

*SOC Analyst, AT&T Cybersecurity, Texas, February 2022 – December 2022*

- Provided detection and response services to over 200 customers as part of the AT&T Cybersecurity MSSP unit.
- Triaged alarms using USM Anywhere.
- Investigated anomalous activity and provided recommendations and best practices to customers.
- Escalated true positive events to team leaders and incident response teams.
- Trained new team members.
- Created threat briefings and simulations and presented to the team to stay up to date on new tactic techniques and procedures.

*IT Systems Administrator, U.S. Metals (via Addison Group), Houston, Texas, October 2021 – February 2022*

- Upgraded firmware and resolved topology issues on the Cisco Meraki network.
- Synced Proofpoint's TAP with Microsoft 365 to improve threat visibility on mailboxes and user accounts.
- Developed and maintained Crowdstrike's prevention, response, and update policies.
- Monitored and remediated alerts on user activity using Azure AD logs, Crowdstrike Falcon, Meraki IPS/IDS, and Proofpoint.

*IT Coordinator, Granite Construction (via Oxford Global Resources), The Woodlands, Texas, November 2018 – October 2021*

- Developed a PowerShell script to enable Microsoft Teams companywide to align with Microsoft's rollout schedule.
- Developed IT Help App using C# to improve user experience and increase usage of existing software like SCCM's Software Center and ServiceNow.
- Developed A self-service tool kit using C# and PowerShell, utilizing the Agile Methodology.
- Acted as a technical resource for IT Operations on different Cybersecurity initiatives like MFA, Knowbe4, and McAfee remediation on endpoints to improve the organization's security posture.
- Remediated compromised Microsoft 365 accounts.
- Acted as IT Operations liaison for CMMC compliance initiative.
- Developed a Power BI dashboard to track IT technicians' metrics on worked-on tickets.

*Desktop Support Analyst, The Woodlands United Methodist Church (via 3coast), The Woodlands, Texas, February 2018 – November 2018*

- Implemented password policy for regular and admin active directory accounts across the organization to follow industry standards.
- Developed a PowerShell script to capture the inventory of PCs joined to the Active Directory domain to create a process for asset management.
- Decommissioned shared Active Directory accounts to improve non-repudiation in the network environment.
- iOS device management using Apple Configurator.
- Hardware and software support of macOS devices.
- Managed and supported macOS devices using Profile Manager. Created profiles for each department that deployed customized apps and settings.
- Migrated users from local accounts in macOS devices to network accounts to prevent users from having privileged access to the operating system.
- Developed Group Policy to lock down kiosk PCs to prevent unauthorized access.

*IT Support Technician Level 2, ExxonMobil (via Experis), Spring, Texas, April 2017 – February 2018*

- Supported the upstream research lab's nonstandard IT environment.
- Developed an inventory and reporting tool using VBA in Microsoft Excel with Microsoft Access to track asset inventory.

*IT Support Technician, HPE (via BlackBox Network Services), Houston, Texas, July 2014 – March 2017*

- Provided IT support to server manufacturing facilities.