AlexandriaSegovia

W: AlexandriaSegovia.com
E: Alexandria.Segovia@gmail.com

EDUCATION

Georgia Institute of Technology
Master of Science in Cybersecurity – Dec 2022

Florida International University
Bachelor of Science in Electrical Engineering (July 2020) / GPA 3.4

Bachelor of Science in Internet of Things Engineering (May 2019) / GPA 3.6

HONORS

FIU Worlds Ahead and Cum Laude Graduate
Dean's List (2018-2020)

SKILLS

Competency with C, C++, JavaScript, HTML, CSS
Experience with Wireless Communication Protocols (I2C, ZigBee, Z-Wave, etc)
Experience with Embedded Systems, various microcontrollers and microprocessors, sensors, digital hardware, analog and digital circuits, logic design
Competency with AutoCAD, MATLAB, MS Visual Studio
Linux and Unix OS, Kali Linux, Ethical Hacking
Windows OS and Server & Systems Administration
Windows Active Directory and Group Policy
Tenable Nessus
Namicsoft Reporting Software
Nipper and Paws Studio
CIS Assessor
Burp Suite
RapidFire Tools
Security Monitoring and Escalation

PROFESSIONAL EXPERIENCE

CYBERSECURITY CONSULTANT, UNITED DATA TECHNOLOGIES | MAY 2019 - PRESENT

Supporting member of a team of cyber security consultants performing vulnerability assessments and management, penetration testing, and CISO supporting tasks and analytics. Responsibilities include:

- Determining the most effective way to protect computers, networks, software, data and information systems against any possible attacks.
- Performing vulnerability testing, risk analyses and security assessments.
- Performing and reporting various scopes of Risk Assessments and (GLBA, PCI, IT, Security, HIPAA, Infrastructure, etc)
- Testing security solutions using industry standard analysis criteria
- Documenting and updating security processes, investigating possible security exceptions, and maintained and modified security metrics. Automating reporting processes.
- Responsible for investigating cyber security breaches or suspicious activities
- Developing and implementing C-Level reporting structures
- Advising incident responders in the steps to take to investigate and resolve computer security incidents. Conducting forensic investigations following security incidents.
- Monitoring and analyze security information and event management SIEM for remediation of security issues. Monitoring and analyzing network traffic, Intrusion Detection Systems (IDS), security events and logs.

SERVICE DESK ASSOCIATE, GE DIGITAL | FEBRUARY 2018 - MARCH 2019

Responsible for solutioning the IT needs of over 300,000 GE employees globally, tasked to provide front-line customer support, work with specialized teams to resolve application-specific issues, and resolve network outages in order to maintain maximum up time and service reliability.

- Assisting multiple end user issues simultaneously, both by chat and phone. Working in a high-volume and fast paced environment. Delivering excellent customer support to contribute in raising the customer satisfaction ratings by over 100%.
- Providing over 80% first contact resolution rates in user issues. Prioritizing and managing several open issues at one time.
- Researching and resolving network outages, escalating outages to appropriate response teams. Working with specialized teams to resolve issues within business-specific applications such as Oracle, Salesforce, etc.
- Involved in several piloting programs to assist in creating and proofing new technical processes for the Service Desk.
- Mentor and guide for new employees during training periods. Playing an active role in the development of new employees and their experience.
- Identifying and creating solutions to be added to the GE Digital Knowledge Base. Identify and suggest possible improvements on process, procedures and or systems.

SOLUTIONS ENGINEER, INFOSIGHT, INC. | NOVEMBER 2014 - JANUARY 2018

Highly engaged with a strong team to deliver managed IT security and infrastructure needs to customers, including small and medium businesses.

- Conducting social engineering tests to include designing and capturing phishing emails and responses, physical security testing, and targeted phone calls to determine customer reaction and provide further security training.
- Monitoring SIEM reports and conducting threat analyses to protect client networks and prevent any possible attacks.
- Handling customer requests within an SLA period in a timely and efficient manner, providing excellent customer service and communication.
- Customizing company internal portals in various languages such as HTML, CSS, PHP, etc. as well as recreating company website to include incorporating marketing tools for lead generation to benefit sales.
- Managing group policy and active directory for multiple customers. Administrating several Windows environments and servers.
- Creating and writing company policies and procedures regarding security measures, writing technical process documents in order to preserve company information.