GREGORY FUENTES

linkedin.com/in/gregory-fuentes | Fort Worth, Texas 76108 | 682.225.3270 | gregoryfuentes80@gmail.com

PROFESSIONAL SUMMARY

Passionate about information security with a focus on cloud security and security engineering. Eager to transition to cloud security, I bring expertise in application security, cloud security, network security, and incident response duties, along with a background in software development. Given my experience, I am well-equipped to contribute effectively to defensive information security goals and objectives.

EDUCATION

Seattle Pacific University Seattle, WA
Bachelor of Science in Computer Science, June 2018

EXPERIENCE

Senior Application Security Engineer Dallas/Fort Worth, TX
Luminator, June 2024 – *Present*

- Contribute to ISO 27001 by creating 20 Corporate Policies for security and compliance
- Implemented Semgrep and TruffleHog into 30 CICD pipelines for Software engineering teams
- Lead AppSec/DevSecOps Security assessments along with Software engineering teams
- Developed IR program with tools such as KAPE and PowerShell Hunter and implemented SOAR workflows such as automating a Terminated Users workflow
- Managed and maintained 1314 device migration into CrowdStrike
- Perform Vuln management/assessments across On-Prem/Cloud (Azure) infrastructure using tools such as PingCastle, Amass, ScubaGear, Prowler, etc …

Security Consultant Dallas/Fort Worth, TX
NetSPI, May 2022 – *May 2024*

- Contribute to Microburst Azure tool and converting Bash Android scripts to Python for Mobile Hacking service line
- Administered 30 Web/Code-Assisted Pen Tests using Burp Suite, Postman, and other tools
- Managed secure code review utilizing SAST/DAST scanning tools such as Semgrep, Contrast, AppInspector, Fortify, Cloc, and Checkmarx
- Created and deployed Jenkins Declarative Pipelines for scanning imported code builds with different tools integrated with Gitlab

Security Consultant Dallas/Fort Worth, TX
Coalfire, September 2021 – May 2022

- Advised clients on technical security and compliance activities
- Performed Web based Application and API Penetration Testing using Burp Suite, Postman, and other tools
- Drafted compliance reports and security policies according to the NIST framework
- Skilled in the understanding of Network and Internet protocols including OSI model

Cyber Test Exploitation Engineer Associate Dallas/Fort Worth, TX

Lockheed Martin, November 2019 – August 2021

- Developed Splunk queries, macros, and dashboards to accomplish proper threat detection and monitoring in On-prem and Cloud environments (AWS)
- Directed 20 Web/Network Pen Tests using Burp Suite, Nmap, Metasploit, Postman, and other tools
- Supervised Virtual machine maintenance such as snapshots and logging using VMware ESXi
- Lead Cloud security assessments/config reviews specifically aimed at IAM access permissions
- Contributed to Python development to support bugs and add new features in the Enterprise Purple Team Reporting Framework
- Generated Bash script that helped with Host analysis of Linux machines for Incident Response duties
- Performed detailed Host analysis on systems and servers as part of IR responsibilities
- Gained knowledge in security fundamentals and common vulnerabilities (e.g. OWASP Top Ten)
- Performed Vulnerability Management with Qualys, Nmap, and other tools

Software Developer Intern/Associate Software Developer Bellevue, WA

T-Mobile, June 2018 – October 2019

- Azure Cloud Management on real-time data processing pipelines
- Created and deployed Enterprise applications with Docker
- Performed Java based software dev. surrounding data engineering with Spring Boot/Kafka

BLOG / GITHUB / Certifications

- Blog for Infosec Walkthroughs and Projects (https://gregoryfuentes80.gitbook.io/gfuen-infosec-blog/-cloudblog/)
- The following is content from my Cloud Blog ○
    - AWS Detecting Unauthorized IAM use with Athena and CloudTrail
    - AWS How to Apply Service Control Policies in AWS Organizations
    - AWS Detecting Ransomware on S3 using Athena and CloudTrail
    - Azure How to Setup and secure access in Azure Blob storage
    - AWS How to make IAM and Resource Policies for S3 Access
    - AWS CloudGoat Walkthrough
    - Azure Penetration Testing Azure Book Walkthrough
    - AWS FLAWS Walkthrough
    - Kubernetes Goat Walkthrough
    - AWS Setting up Emails for GuardDuty Findings using SNS
- Main Repo (https://github.com/Gfuen)
- Terraform Projects (https://github.com/Gfuen/TerraformProjects)
- Python AWS Lambda Project (https://github.com/Gfuen/LambdaSendSplunk)
- Python Wazuh EDR Deployment Proejct (https://github.com/Gfuen/WazuhAuto)
- Python AWS EC2 Incident Response Project (https://github.com/Gfuen/AWSServerIsolate)
- Open-Source Contribution (https://github.com/RhinoSecurityLabs/pacu) and (https://github.com/NetSPI/MicroBurst)
- Certifications
    - AWS Security Specialty, AWS Certified Cloud Practitioner, Certified Information System Security Professional (CISSP), Azure Fundamentals