Grace Augustine

Abuja, Nigeria | gracienigma@gmail.com | +2348159342253| www.linkedin.com/in/cga2000/

PROFILE

Detail-oriented cybersecurity professional specializing in Security Operations Center (SOC) activities and adept at aligning security strategies with organizational goals. Proficient in leveraging advanced cybersecurity tools and techniques to detect, analyze, and respond to threats effectively, ensuring the protection of critical systems and data. Skilled in risk mitigation and incident response, with strong interpersonal abilities for seamless collaboration across cross-functional teams. Seeking a dynamic SOC Analyst role to enhance organizational security and contribute to building a resilient threat defense infrastructure.

SKILLS

- **Technical Skills:** Intrusion Detection & Prevention (IDS/IPS), Incident Response & Management, SIEM Tools (Splunk, QRadar, ArcSight), Endpoint Detection and Response (EDR), Network Security, Malware Analysis, Threat Hunting, Vulnerability Management, Threat Intelligence, Log Analysis, Cloud Security (AWS, Azure, Google Cloud), Programming & Scripting (Python, Bash, PowerShell)
- **Analytical Skills:** Critical Thinking, Problem-Solving, Attention to Detail, Risk Assessment, Pattern Recognition
- **Soft Skills**: Communication, Teamwork, Adaptability, Time Management, Continuous Learning
- **Frameworks & Standards**: NIST Framework, MITRE ATT&CK Framework, ISO 27001 Standards

WORK HISTORY

Freelance Cybersecurity Writer **January 2024-Present**

- Authored and published cybersecurity-focused technical articles, explaining key attack methods and mitigation strategies.
- Demonstrated deep technical knowledge by simplifying complex security concepts for a broad audience.

Some articles you'll find in my ***Portfolio*** include:

- **Why Cybersecurity?** - The article looks into why cybersecurity is critical in today's world, exploring the rising threats of cyberattacks, the impact on individuals and organizations, and the importance of staying one step ahead of hackers. It sheds light on the need for robust defenses, incident response, and the role of professionals in protecting digital assets.

- **A-Z of Tech** - The article provides an engaging and beginner-friendly breakdown of essential tech terms, from A to Z. Whether you're new to technology or want a quick refresher, it's a perfect resource to demystify jargon and expand your knowledge.

- **How Man-In-The-Middle (MITM) Attacks Work** – Explored how attackers intercept communications between two victims to steal sensitive information. The article discusses various tools used in MITM attacks (e.g., Wireshark, Ettercap) and outlines best practices such as strong password use, VPNs, and secure Wi-Fi.

- **Brute Force Attacks: How They Work and Prevention Methods –** A comprehensive guide on brute force attacks, explaining various types (simple, dictionary, hybrid, reverse brute force, credential stuffing) and effective defense mechanisms like strong passwords, lockout policies, and advanced threat detection.

DevMaster **April 2024 – Nov 2024**

Position: Cybersecurity Intern

Gained foundational cybersecurity expertise through an intensive one-year fellowship program, with a focus on real-world applications.

• Developed hands-on skills in network security, threat detection, incident response, and vulnerability management, aligning with SOC operations.

• Acquired exposure to key cybersecurity domains such as Cloud Security, Threat Intelligence, Digital Forensics, and Critical Infrastructure Security, enhancing versatility in detecting and addressing threats.

• Strengthened analytical and problem-solving skills critical for identifying and mitigating security incidents in fast-paced environments.

IBM Skillup Training **Jan 2024 – Oct 2024**

Position: Cybersecurity Trainee

- Acquired foundational cybersecurity knowledge through an intensive one-year fellowship program.
- Developed practical skills in network security, threat analysis, incident response, and vulnerability assessment.
- Gained exposure to various cybersecurity domains including Cloud Security, Critical Infrastructure Security, DevSecOps, Digital Forensics, and Threat Intelligence.
- Developed strong problem-solving and analytical skills essential for cybersecurity roles.

CERTIFICATION

ISC2 Certified in Cybersecurity (ISC)² **January 2025**

IBM SkillUp Cybersecurity Specialization **October 2024**

EDUCATION

BSc. International Relations, Obafemi Awolowo University **2024**

- *2:1, Second Class Honours, Upper Division*

PROJECTS

1. Threat Monitoring and Incident Escalation

- Monitored and analyzed security events using SIEM platforms like Splunk.
- Identified indicators of compromise (IOCs) and escalated incidents based on defined protocols.
- Collaborated with Tier 2 analysts to resolve high-priority incidents and improve detection rules.

2. Log Analysis and Anomaly Detection

- Conducted daily log reviews from firewalls, IDS/IPS, and endpoint security tools.
- Identified unusual patterns or traffic and generated reports for the SOC team.
- Suggested and implemented updates to detection rules based on findings.

3. Phishing Incident Investigation

- Investigated and responded to phishing emails reported by users.
- Analyzed email headers and attachments for malicious content or links.
- Contained threats by blocking malicious domains and educating users on phishing prevention.

LANGUAGES

English and Spanish

REFEREES

Available on request