CALEB OUEDRAOGO

Information Technology Management / Cyber Security Analysis / Software Development
ouedraogocaleb2@gmail.com | **Philadelphia, PA** | https://www.linkedin.com/in/caleb-ouedraogo/

PROFESSIONAL PROFILE

I am an Information Technology Management graduate with an undergraduate background in Transportation and Logistics. Driven by a passion for technology, I transitioned to IT and now possess a solid understanding of IT principles and project management. My experience includes network engineering, cybersecurity analysis and penetration testing, with a focus on securing digital environments and mitigating threats. Currently, I am expanding my skills in full-stack software development to create innovative and efficient network solutions.

INFORMATION TECHNOLOGY COMPETENCIES

Systems: Linux/ Windows/ MacOS/ CISCO IOS
Databases: Relational and Non-relational Databases
Languages: SQL/ HTML/ CSS/ JavaScript/ Python
Software: MS Word/Excel/PowerPoint/Outlook/Azure/Sentinel/ AWS/ Wireshark/ SIEM/ SOAR/ DLP/ VirtualBox/ VMware/ Nmap/ Nessus/ OpenVAS/ Qualys/ Anti-Virus/ Git/ GitHub, etc.
Networking: DHCP, DNS, 802.11 LAN design, configuration, and troubleshooting/ Remote Desktop Assistance/ Network firewall/ Host firewall/ IDS/ IPS/ Network Packet Capture analysis/ EDR and Email Filtering Gateways, etc.

EDUCATION

Master of Science in Information Technology Management **Graduated**: June 2023
Western Governors University | Salt Lake City, UT (USA)

- Studies focused on IT Foundations, Network Infrastructure, Design, and Security.
- Courses included Project Management, Current and Emerging Technologies, IT sourcing and Development in a Global Economy, Managing Technology Operations and Innovation, Technical Communication, Financial Management for IT professionals, Power, Influence, and Leadership, etc.

Bachelor's degree in Transportation and Logistics **Graduated:** December 2017
Université Aube Nouvelle | Ouagadougou, BF-KAD (BURKINA FASO)

- Studies focused on Supply Chain Management, Distribution, Inventory Control, Logistics Technology, and Operations.
- Courses included Supply Chain Management and Information Systems, Logistics Process Management and Organization, Warehouse Management, Inventory Management, Production Management, Contract Management, and Transportation (Land, Rail, Maritime, and Air).

CERTIFICATIONS:

- **CompTIA PenTest+ Certification** (exam scheduled) August 2024
- **CompTIA CySA+ Certification** March 2024
- **NDG Linux Essentials Certificate** January 2024
- **Cisco Network Essentials Certificate** January 2024
- **Cisco Cyber Security Essentials Certificate** January 2024

ADDITIONAL BOOTCAMP TRAINING

- **Full Stack Software Development** (Part-Time) *LaunchCode,* June 2024 – February 2025
- **Cybersecurity Bootcamp** *PerScholas,* November 2023 – March 2024
- **SAS Visual Business Analytics** *SAS Institute,* September 2023 - November 2023
- **CompTIA Security+, Network+, and A+ Exams Preparation** *LinkedIn Learning / Udemy,* 2023

KEY ATTRIBUTES

- **Threat Detection:** Identify and analyze potential threats, using various tools and techniques.
- **Incident Response:** Respond to and mitigate cybersecurity incidents, minimizing potential damage.
- **Vulnerability Assessment:** Analyze systems for known vulnerabilities and recommend appropriate security patches or solutions.
- **Log Analysis:** Expertise in using log analyzers like Wireshark and tcpdump to interpret system and network logs for suspicious activities.
- **Threat and Vulnerability Management:** Understand how to utilize tools and techniques to assess an organization's cybersecurity posture.
- **Software and Systems Security:** Knowledge of secure software development and system configuration to maintain a secure environment.
- **Compliance and Assessment:** Familiarity with frameworks like NIST, ISO 27001, Cyber Kill Chain, MITRE ATT&CK, Diamond Model, Pyramid of Pain, and tools like Security Content Automation Protocol (SCAP) for compliance checks.
- **Security Operations and Monitoring:** Proficient in utilizing SIEM platforms, notably Splunk, for searching, monitoring, and analyzing machine-generated big data in real-time.
- **Networking:** In-depth understanding of network protocols, architectures, and tools, including Cisco devices, and Firewalls.
- **Analytical Thinking:** Ability to dissect complex security problems and derive logical solutions.
- **Critical Thinking:** Evaluate situations from multiple viewpoints to determine the best course of action.
- **Attention to Detail:** Recognize subtle changes or anomalies in large data sets or systems.
- **Continuous Learning:** Commitment to staying updated with the latest trends and advancements in Information Technology through self-directed learning and professional development opportunities.

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst Trainee November 2023 – March 2024
Per Scholas | Philadelphia, PA (USA)

- Conducted vulnerability assessments using tools like Nessus, OpenVAS, and Qualys to detect potential security vulnerabilities in systems, networks, and applications, ensuring network integrity and reliability.
- Participated in simulated incident response scenarios, demonstrating the ability to investigate and mitigate security incidents effectively, thereby protecting network infrastructure.
- Monitored security alerts and notifications produced by SIEM tools like Splunk, analyzed logs and network traffic for suspicious activity, and escalated incidents to maintain network security.
- Generated reports, summaries, and presentations to communicate cybersecurity risks, network vulnerabilities, incidents, and recommendations to management, stakeholders, and other relevant parties.
- Assisted with compliance evaluations, audits, and examinations to assess the effectiveness of established network security controls and recognized areas needing improvement.
- Configured routers and switches to optimize network performance, ensuring efficient data flow and robust connectivity across the network.
- Designed and implemented network solutions, including LAN, WAN, and wireless configurations, to meet organizational needs.
- Performed regular network maintenance and updates to ensure optimal performance and minimal downtime.
- Utilized network monitoring tools to proactively identify and resolve issues before they impact users.

Amazon Fulfillment Center Associate Part-Time) August 2022 – Current
Amazon | West Deptford, NJ (USA)

- Assisted in the training of new hires.
- Collaborated with team members to meet daily production goals.

- Demonstrated a commitment to maintaining a safe working environment, participating in safety initiatives and protocols.
- Operated forklifts and other equipment to move and organize goods within the warehouse, showcasing adaptability and quick learning.
- Strong attention to detail in operations, emphasizing task accuracy and precision.

PROJECTS

Honeypot Project: Azure Sentinel Map with Live Worldwide Cyber Attacks

The project demonstrated the global scale and distribution of cyber-attacks using Azure Sentinel and a purposely vulnerable VM, emphasizing the critical importance of network security and system hardening when deploying systems on the internet.

- Created an Azure account with an active subscription specifically for this project.
- Deployed a Windows 10 Pro Virtual Machine (VM) and configured it to be highly visible on the internet, allowing all incoming traffic to ensure it is easily discoverable by potential attackers.
- Established a Log Analytics Workspace and configured Data Collection Rules to gather and monitor logs from the VM, successfully connecting the VM to the Log Analytics Workspace.
- Set up Azure Sentinel to visualize the collected data, configuring a Sentinel map with longitude and latitude data to display the geographic locations of cyber events.
- Accessed the VM via Remote Desktop and executed a custom PowerShell script to collect IP addresses from failed login attempts recorded in the VM's event viewer. These IP addresses were forwarded to a third-party API to determine their geolocation, and the resulting data was stored in a file on the VM. This log file was subsequently collected and ingested into the Log Analytics Workspace for visualization in Azure Sentinel.
- Within 30 minutes of the VM's creation, over 1,000 failed login attempts were recorded from around the globe, with attack origins including the United States, Russia, South Korea, Netherlands, Morocco, Brazil, and Turkey.

This underscored the global reach and rapid onset of cyber-attacks, illustrating the necessity of robust network security measures and proactive monitoring using SIEM tools like Azure Sentinel or Splunk.

Active Directory Environment Project using VirtualBox

This project demonstrated the setup and management of an Active Directory environment in a virtualized setting, highlighting essential network engineering skills.

- Installed VirtualBox on a Mac machine for the project.
- Deployed and configured a Windows Server 2019 on VirtualBox to serve as a Domain Controller. The server was set up with two Network Interface Cards (NICs) - one for the internal network and another for internet access.
- Implemented Active Directory Domain Services (AD DS) on the server, creating a domain to establish a structured and secure network environment.
- Configured Remote Access Service (RAS) and Network Address Translation (NAT) on the server to enable client internet access through the server.
- Set up Dynamic Host Configuration Protocol (DHCP) on the server to automate IP address assignment for clients on the network.
- Executed a custom PowerShell script to create 1000 user accounts on the server. Each account was assigned a username using the first letter of its user's first name followed by its last name, and a password.
- Installed and configured a Windows 10 Pro client on VirtualBox, joined to the domain, allowing all 1000 users to access the client using their credentials.

This explained the practical application of network engineering principles in setting up and managing a comprehensive Active Directory environment within a virtualized infrastructure.