

# Ibrahim A. Mahamane

(224) 434-6324 | [iamahamane@gmail.com](mailto:iamahamane@gmail.com) | [www.ibrahimmahamane.com](http://www.ibrahimmahamane.com)

---

Skilled information security professional with hands-on experience assessing key security threats and vulnerabilities, and implementing measures to monitor and protect organizational data and network. Problem solver with excellent written and verbal communication skills. Known for a strong work ethic and professional demeanor and exceptional Interpersonal skills.

## QUALIFICATIONS

---

- Network Monitoring, Intrusion Detection/Prevention Systems, Vulnerability Scanning (1+ year)
- Excellent communication skills with the ability to present value and overcome objections (5+ years)
- Experience with Splunk. Willing to learn other SIEM technologies;
- Experience performing security information risk assessments to identify system and network vulnerabilities.
- Ability to perform internal and external security and compliance monitoring activities.
- Understanding of common security standards and regulations including the ISO 27000 Series, HIPAA, PCI DSS, NIST SP 800-53, NIST Cybersecurity Framework, GDPR and HITRUST.

## EXPERIENCE/PROJECTS

---

### Security Analyst

*Performed the following tasks using Azure Sentinel(SIEM):*

- Used a custom PowerShell script to extract geolocation information from Windows Event Viewer metadata using a third-party API.
- Configured Log Analytics workspace to receive custom logs with the geolocation data.
- Extracted custom fields in Log Analytics workspace.
- Configured Sentinel workbook to display RDP brute force attack data on world map based on location and magnitude.

*Created a custom/proof of concept File Integrity Monitor <https://github.com/iamibie>:*

- Created an integrity baseline using the SHA-512 hashing algorithm.
- Continuously made comparisons between files and baseline, raised alert if file integrity is compromised.
- Examined alert to allow for further investigation of potential compromise.

*Performed the following Vulnerability Management tasks:*

- Installed and configured Nessus Essentials to perform credentialed vulnerability scans against Windows 10 Hosts
- Implemented vulnerability management function on sandbox networks (Discover, Prioritize, Assess, Report, Remediate, Verify).
- Conducted vulnerability assessment with Nessus and remediated vulnerabilities.
- Developed automated remediation process to proactively deal with vulnerabilities from Windows updates and other third-party software

### System Administrator

*Performed the following Active Directory Administration tasks:*

- Created and configured virtual machine running a Windows server 2019 on Oracle VM VirtualBox.
- Configured Windows DNS and DHCP services on Windows server 2019.
- Implemented Remote Access Server (RAS) features to support NAT and PAT.
- Implemented and configured Windows domain name services.
- Created PowerShell script to provision and maintain 500+ user accounts.
- Installed and configured Windows 10 desktop client.
- Configured Windows 10 desktop client to receive DHCP services from Domain Controller.
- Configured Windows 10 desktop client to access the internet via Domain Controller.

### DevOps Engineer

*Performed the following DevOps tasks:*

- Created highly available and scalable cloud infrastructure in AWS and Azure.
- Configured and maintained VPC, Security Groups, NACL, Route53 DNS hosted zones and CloudWatch on AWS.
- Created and managed IAM roles, users and groups according to security best practices.
- Used Terraform to automate infrastructure provisioning and maintain cloud infrastructure on AWS and Azure.

- Containerized and deployed applications using docker on cloud agnostic environments.
- Created Docker images from Dockerfile and pushed custom images to DockerHub.
- Used Docker-compose to run multi-container applications.
- Created and maintained custom scripts for process automation.
- Automated, test, build and deployment processes with Jenkins and GitHub.
- Configured Webhooks in GitHub to trigger automated builds in Jenkins.
- Resolved system/network issues and performed backups, upgrades and security patches.
- Configured and maintained SSL certificates for HTTPS using certbot.
- Developed web applications and REST API with JavaScript/NodeJS and Python/Flask.
- Created and Managed databases such as MYSQL and MONGODB.

### Capstone Project

- Via Capstone project, gained hands-on experience handling security incidents, including reviewing of raw log files, data correlation, and analysis.

## RELEVANT TRAINING

**Cybersecurity Engineering Program**, Flatiron School,

11/2021 – 03/2022

*Coursework includes 15 weeks of intensive classroom and lab-based training in security concepts including:*

- **Governance, Risk and Compliance (GRC)** - Compliance, Risk Management, BCP, Incident Response, Cyber Kill Chain.
- **Strategy and Analysis** - Strategic Planning, Leadership, Operational Design, Decision Making Cycle.
- **Threat Intelligence** - CTI Sources and Methods, Threat Actors, Social Engineering, CTI Diamond Model, Cyber Mission Analysis.
- **Logs and Detection** - SIEMs (**Splunk**), Normalization, Hunting, Alarms & Reports, Investigations, User and Process Monitoring
- **Networking** - OSI & TCP/IP Models, Routing, Protocols, Encapsulation, Framing, NAT Networks, VLANs
- **Network Security** - Wireshark, Port Forwarding, VPNs, Port Scanning, IDS / IPS, Firewalls, Vulnerability Management, MITM Attacks, DNS Security.
- **Systems** - VMs, x86/ARM Architecture, Linux, Windows, Memory, Storage, Python, Cloud
- **Systems Administration** - Windows, Unix/Linux.
- **Systems Security** - OWASP Secure Coding Practices, Input Validation, Buffer Overflows, Code Injection, Cloud Security Infrastructure.
- **Application Security** - OWASP Top 10, XSS, CORS, SQLi, DoS & DDoS, Vulnerability Scanning
- **Cryptography** - Stream & Block Ciphers, OpenSSL, Certificate Management, Symmetric & Asymmetric.

## OTHER PROFESSIONAL EXPERIENCE

**Legal Administrative/Paralegal Assistant** | *Joseph Greenwald and Laake, Rockville, MD*

09/2020 – 05/2021

- Assisted in drafting and filing legal documents including pleadings, discovery and memos.
- Supported case preparation for hearings, depositions, and trials by organizing discovery materials and exhibits.
- Served as notary and witness to will signings and trust executions.

**Executive Assistant to the President** | *Bay Atlantic University, Washington, DC*

09/2019 – 03/2020

- Managed the President's daily calendar, including scheduling appointments and meetings.
- Drafted memos and announcements, and disseminated information from the president to pertinent stakeholders.
- Assisted faculty and other department heads in organizing both on and off campus activities for students.

**Paralegal Intern** | *Cassano and Associates, Naperville, IL*

05/2019 – 09/2019

- Assisted senior paralegal with legal research and analysis.
- Transcribed, summarized and analyzed depositions to highlight pertinent information for the attorneys and paralegals.
- Occasionally covered for the secretary/ legal assistant; duties included, answering phone calls, performing new client intake, scheduling and coordinating meetings, interviews, and events.

## EDUCATION & CERTIFICATIONS

**CompTIA Security+**

May 2022

**Flatiron School** | Cybersecurity Engineering Program (Online) Certificate

March 2022

**North Central College** | Naperville, IL | BA in Political science & Philosophy

June 2019

**DuPaul University** | Chicago, IL | MS in Computer Science

*In Progress*