Mahmoud Mohamed Said Ahmed

**Mobile:** +201116060955

**E-mail:** mmsaeed509@gmail.com

**LinkedIn:** [linkedin.com/in/mahmoudmohamedsaid](https://www.linkedin.com/in/mahmoudmohamedsaid/)

**GitHub/GitLab:** [@mmsaeed509](https://github.com/mmsaeed509)

**Summary**

DevOps Engineer with expertise in cloud-native infrastructure (AWS, Kubernetes, Terraform) and cybersecurity. Proven track record of automating deployments, reducing downtime, and improving security posture. Creator of Exodia OS and contributor to open-source kernel modules. Skilled in building CI/CD pipelines, container orchestration, and penetration testing. Passionate about delivering scalable, secure, and automated systems.

**Military status** **(Completed)**

**Education**

Bachelor of Computers and Artificial Intelligence, Cairo University **(Class of 2023)**

**Projects:**

**Exodia OS** (Graduation Project – Excellent Grade)

* Built an **Arch-based** Linux distribution tailored for cybersecurity and penetration testing.
* Developed special editions including **Home** and **Acer Predator** with fan/RGB control.
* Adopted by cybersecurity enthusiasts with 500+ pre-installed tools.

# CI/CD Pipeline for VProfile App (GitOps, Kubernetes, Jenkins)

# Designed and deployed a multi-tier Java application with MySQL, Memcached, RabbitMQ, Tomcat, Nginx

# Implemented GitHub Actions workflows for development and production.

# Automated deployments on AWS EKS using Terraform + Helm

# Acer Predator Kernel Module & GUI (Linux PredatorSense)e

# Reverse-engineered Windows PredatorSense app to build a Linux kernel module (C).

# Developed a PyQt5 GUI App for the Kernel Module

# Open-sourced project adopted by the Linux Predator community

# Ransomware

* It’s a basic implementation of ransomware using Python, consisting of two programs: a server and a client
* The server is used to control the client (ransomware) and is hosted on the attacker's machine
* The client, which functions as the ransomware, connects to the server to encrypt/decrypt files

**Exodia OS Assistant (PyQt5 GUI App)**

* Built modular system assistant application for Exodia OS
* Designed custom UI with non-rectangular windows, dynamic buttons, and system integration features.
* Role Manager, which allows users to install, manage, and configure a role-based environment

# Experience:

**Cisco CyberOps Associate Trainee – NTI (1 month in Aug – Sept 2021)**

* Configured and monitored SOC environments, improving incident detection and response
* Gained hands-on experience in threat intelligence, packet analysis, and SIEM workflows.

**CCNA Training - FCAI (1 month in Aug - Sept 2020)**

* Hands-on labs with routing, switching, subnetting, and LAN/WAN protocols.
* Built and troubleshooted small-scale enterprise network simulations.

**Incident Response - CyberTalents (3 months in Jun - Aug 2021 )**

* Conducted digital forensics and reverse engineering exercises on malware samples
* Supported incident handling workflows, contributing to faster triage of forensic evidence.

# Skills:

# **Version Control & Linux:** Git, Git LFS, GitHub, GitLab, Debian/Arch/RHEL-based

# **Programming:** C/C++, Java, Python, Bash, PowerShell

# Containers & Orchestration: Docker, podman, OpenShift, Kubernetes

# CI-CD & IaC: Jenkins, GitHub Actions, GitLab CI, Terraform, Helm, Ansible, vagrant

# **Cloud**: AWS

# **Monitoring & Security**: Grafana, Incident Response, Penetration Testing

# **Certificates:**

# CyberSecurtiy: Incident Response, NTI CyberOps, PNPT

# DevOps: DevOps with Projects

# Networks: CCNA

# Programming: C With linux

# API: API and Web Service Introduction – Udemy

# Project Management: Complete Agile Scrum Master Certification Training – Udemy