Ziad Abdelgwad

Cybersecurity Specialist | SOC Engineer

Alexandria, Alexandria 21533   +201093392434   ziadalex2003@gmail.com   LinkedIn   GitHub

Summary

Cybersecurity professional with hands-on SOC experience and offensive security expertise. Skilled in SIEM deployment, threat detection engineering, and network security. Proficient in Elastic Stack, firewall configuration, malware analysis, and Active Directory security. Experienced in both defensive security operations and penetration testing methodologies.

Technical Skills

SIEM & Log Analysis

Elastic SIEM (ELK Stack)
Kibana (KQL & EQL)
Logstash
Winlogbeat
Fluent Bit
Windows Event Log Analysis
Custom Detection Engineering
UFW Log Ingestion

Network Security

Linux IPTables
Windows Defender Firewall
Uncomplicated Firewall (UFW)
WAF (Nginx with ModSecurity)
Wireshark
Snort
Cisco IOS Configuration
Nmap Scanning
Network Administration

System Administration

Active Directory Domain Services
Group Policy Management (GPO)
Domain Controller Hardening
Bash Scripting
Ubuntu Server
Linux Administration
Windows System Security

Security Operations

MITRE ATT&CK Framework
Static & Dynamic Malware Analysis
Process Injection Analysis
C2 Communication Analysis
IOC Extraction
Incident Response
Vulnerability Assessment
Penetration Testing

Programming & Development

Python Development
Java Programming
C++ Programming
Bash Scripting
MySQL Database
Cryptography Principles

Cloud & Infrastructure

AWS Cloud Security
Cloud Security Implementation
IDS/IPS Systems
Phishing Detection
Security Compliance

Experience

WE Innovate Cybersecurity Bootcamp August 2025 – Present

Intern

- Completed intensive hands-on training simulating real-world SOC environment
- Deployed and configured Elastic Stack (Elasticsearch, Kibana) with Fleet Server
- Built data pipelines for Windows/Linux log ingestion using Winlogbeat/Fluent Bit
- Developed detection rules using KQL/EQL for threat identification
- Conducted malware analysis of Ursnif/Gozi banking trojan
- Implemented Active Directory hardening with 20+ GPO security policies
- Configured Nginx WAF with ModSecurity and OWASP CRS rules

ABU QIR Fertilizers and Chemicals Industries Company July 2025

IT Network & Security Trainee

- Trained on enterprise network infrastructure and security systems
- Gained hands-on experience with industrial network security protocols
- Assisted in network monitoring and security operations
- Participated in IT infrastructure maintenance and troubleshooting

Alexandria Petroleum Company (APC) July 2025

IT Security Intern

- Implemented network security measures for enterprise infrastructure
- Managed database security and performed vulnerability assessments
- Troubleshot complex IT systems and network issues
- Deployed AWS cloud security solutions and compliance controls
- Monitored and responded to security incidents using SIEM tools

CIB Summer 2024

Cybersecurity Intern

• Completed intensive 8-week cybersecurity internship at Egypt's largest private bank
• Trained in digital transformation strategies and financial system security protocols
• Participated in workshops on data literacy and emerging workplace technologies

SARTA City August 2024 (Scheduled)

IT Infrastructure Intern

• Gained hands-on experience in network administration and IT operations
• Assisted in implementing security measures for smart city infrastructure
• Completed 120+ hours of professional training in enterprise IT systems

Education

Alexandria National University Alexandria, Egypt

Bachelor's Degree in Computer and Information Technology
January 2022 - January 2026
Major: Cyber Security

Projects

SOC & Security Operations

- Elastic SIEM Infrastructure: Deployed complete Elastic Stack with Fleet Server management
- Windows Log Pipeline: Built Logstash pipeline for Windows event log analysis
- Firewall Log Analytics: Configured Fluent Bit for UFW log ingestion with custom parsing
- Detection Engineering: Developed 7+ KQL/EQL rules for Windows threat detection

Network Security

- Campus Network Design: 500+ node simulation with Cisco Packet Tracer
- Domain Blocking Automation: Bash script for dynamic IPTables domain blocking
- NFS Server Configuration: Linux NFS server setup with persistent mounting

Application Security

- Phishing Detection Chrome Extension: XGBoost model with 94% accuracy
- E-commerce API Security: JWT Authentication with 2FA implementation
- SQL Injection Research: Vulnerability documentation and prevention methods
- Java Cryptographic System: AES-256 & RSA implementation

System Hardening & Analysis

- AD Hardening: Implemented 20+ GPOs for Active Directory security hardening
- Enterprise AD Design: Designed Windows AD structure for medium-sized organization
- WAF Implementation: Configured Nginx with ModSecurity and OWASP CRS rules
- Malware Analysis: Conducted static/dynamic analysis of Ursnif/Gozi banking trojan
- Password Attack Simulator: Tool for security testing and analysis
- Secure Document Vault: HMAC-based integrity verification system

Training & Courses

- Cisco CCNA (NTI Training Program)
- Cisco CyberOps Associate Training (NTI Academy)
- Network Security (NTI Certification Prep)
- Huawei HCIA-Security (NTI Training Program)
- IBM Cybersecurity Essentials (SkillsBuild Academy)
- Linux System Administration I & II (ITI Training Program)
- AWS Cloud Foundations (Canvas Platform)

Languages

Arabic: Native (C2)
English: Upper Intermediate (B2)