ADAM NURUDINI

SOC MANAGER & SENIOR SECURITY ENGINEER

PROFILE

Results-oriented information security professional with over 7 years of experience in managing information security risks and delivering information security solutions to meet organizational goals. Strong hands-on technical background in IT Security and solid understanding of the security technologies, proccesses, tools and best practices.

HIGHLIGHTS

- Over 7 years experience in VAPT (red team).
- Experienced in Infrastructure, Web, Mobile and API security testing to identify vulnerabilities.
- Knowledgeable in SOC advancements such as XDR, NDR, EDR and SOAR.
- Experienced in using offensive security tools like Burpsuite, MobSF, Acunetix, Metasploit and Nmap.
- SOC automation development and cloud operations (e. g. AWS & Azure) experience.
- Thorough knowledge of SIEM technologies, like Rapid7 InsightIDR, IBM Qradar and Microsoft Sentinel.
- Experienced in Bug bounty and responsible disclosures.

CORE COMPETENCES

- Vulnerability Assessment & Penetration testing
- Coordinating an Incident Response
- SOC analyst/manager
- Code review and software composition analysis (SCA)
- Web Development
- Malware analysis
- Bug Bounty/ Responsible disclosure
- Leadership and Managerial skills
- Network Security Engineering
- Passionate about Blockchain, Smart Contract & Crypto
- Experienced and good VAPT report writing skills.

EDUCATION & CERTIFICATIONS

BACHELOR OF SCIENCE

Information Communication Technology

Ghana Institute of Management and Public Administration

2017 – 2021 – Accra Ghana

CompTIA Inc - Certification.

CompTIA Advanced Security Practitioner (CASP)

January 2016 – Accra Ghana

EC-Council Inc - Certification

Certified Ethical Hacker (CEH)

April 2015 – Accra Ghana

PECB - Certification

ISO/IEC 27032 Lead Cybersecurity Manager

CONTACT INFORMATION

+233(544)-53-4444 | adam.nurudini@gmail.com | Accra, Ghana.
LinkedIn Profile: https://www.linkedin.com/in/adamnurudini/

PROFESSIONAL EXPERIENCE

SECURITY OPERATIONS CENTRE MANAGER (HEAD)

Consolidated Bank Ghana | Accra-Ghana | January 2022 - Current

Oversees hiring, training and evaluating SOC staff. Assesses and reviews incident and compliance reports. Reports on SOC activities to business executives. Manage relationship with external security vendors such as MSSPs to ensure service delivery meets SLAs and work closely to improve their efficiency.

- Hired and trained junior and senior SOC analysts.
- Recorded zero data breach.
- Managed the bank ISO27001 certification project.
- Developed processes and playbooks for the SOC.
- Led team to perform VAPT on all internal applications.
- Designed and implemented security infrastructure for a new government bank (Development Bank Ghana).
- Managed the bank's PCIDSS certification project.
- Implemented Imperva cloud and on-premises web application firewall WAF solutions.
- Implemented database activity monitoring solution.
- Implemented a Security Operation Centre (SOC)
- Deployed a cloud-based security awareness and phishing simulation solution Knowbe4 (PhishER & PAB Alert).
- Built out long-term security strategies, initiatives, and new capabilities to ensure the bank meets its objectives.
- Assisted and mentored Analysts and SecOps Engineers.
- Ensured a high level of technical proficiency and training for multiple cybersecurity teams.

SENIOR SECURITY ENGINEER – Detection & Response

Consolidated Bank Ghana | Accra | July 2019 – January 2022

- Deployed a cloud based SIEM & XDR (Rapid7 insightIDR).
- Performed security assessment (VAPT) 200+ applications.
- Reviewed 200+ applications source codes with Checkmarx
- Performed bank wide automated Phishing simulations
- Implemented an automated cloud and on-premises vulnerability scanning Rapid7 InsightVM (nexpose)
- Implemented CyberArk Privileged access monitoring tool.
- Implemented Darktrace enterprise Immune system for Network detection and Response.
- Implemented a cloud-based security orchestration platform.
- Implemented Palo Alto and FortiGate Firewalls.
- Managed Office365 Security Console as Security Admin.
- Triaged and prioritized detected security incidents.
- Reviewed and finetuned SIEM rules and Events sources.
- Managed over 3500 endpoints and over 800 servers.
- Configured and troubleshooted security infrastructure.
- Dark web monitoring and external threats hunting.
- Security automation and writing Yara and SIEM rules.

SENIOR SECURITY CONSULTANT

Netwatch Technologies | Accra Ghana | July 2018 - July 2019

- Led incidence response services clients.
- Led the security team in VAPT engagements.

January 2020 – Accra Ghana

PECB - Certification
ISO/IEC 27001 Lead Implementer
January 2020 – Accra Ghana

Axelos - Certification
ITIL v3- Foundation Certificate in IT service management
September 2015 – Accra Ghana

CISCO - Certification
Cisco Certified Network Associate
January 2014 – Gurgaon New Delhi - India

Network Bulls – Training Certificate
Cisco Certified Network Professional (CCNP)
May 2014 - Gurgaon, New Delhi - India

FortiGate NSE – Certifications
NSE 1, NSE 2 & NSE 3 Network Security Associate
July 2022 - Accra – Ghana

Just Line Malaysia – Training Certificate
Practical Computer Forensic Auditing and Fraud Investigation
October 2015 - Singapore

CyberArk – Training Certificate
CyberArk Pas System Administration
November 2020 - Accra – Ghana

In Progress Training and Certifications
Certified Information Systems Security Professional CISSP
SC-200 Microsoft Security Operations Analyst

ACTIVITIES AND HONORS

- Speaker - ISACA, Philosophy of information security workshop, Accra Golden Tulip.
- Trainer - GIMPA School of Technology Cyber Security workshop.
- Speaker - OWASP Ghana Chapter Meetup / Conference. University of Ghana Legon.
- Student Association President - GIMPA School of Technology.
- Black Hat Europe 2018 Scholarship.
- Speaker & Host - OWASP Ghana Chapter Meetup / Conference. GIMPA.
- Black Hat Asia 2018, Singapore conference attendee.
- Speaker - Mobex Africa ICT Expo – Cyber security conference, Accra Mall.
- Speaker - ISACA Identity & Data Protection Risks in a Highly Digitized World.
- Attendee - Hack in The Box GSEC Singapore conference.
- Speaker - Mobex Africa ICT Expo – Cyber security conference, Accra Kempinski Hotel.
- Led the security team in Ransomware attack response.
- Led the team in API and Mobile application Security assessment projects.
- Assisted in driving secure coding and infrastructure security training through presentations and classes for clients.
- Assisted in driving security awareness to the end users through presentations and classes.
- Led social engineering attacks on multiple client engagements.
- Designed and managed red team attack infrastructure in AWS and Google cloud hosting Gcloud (GCP).
- Led the team in clients cloud infrastructure security audit.

INFORMATION SECURITY OFFICER
ToppCore Security | Accra Ghana | January 2015 – July 2018

- Performed penetration tests on web-based applications, networks, mobile apps and computer systems
- Conducted physical security assessments of servers, systems and network devices.
- Employed social engineering to uncover security holes (e.g., Poor user security practices or password policies).
- Reviewed and defined requirements for security solutions.
- Developed internal web applications.
- Designed and implemented office network infrastructure.
- Use DAST tools with IAST capabilities to test and find application vulnerabilities within DevOps pipelines.
- Improved startups application and infrastructure security

TECHNICAL PROFICIENCIES

Platforms:	UNIX/Linux, Windows, Linux (Red Hat, Centos), Mac OS, VMware ESXi, HyperV
Programming Languages	Bash Shell Scripting, HTML, Java, PHP, MySQL, Python, Yara, Regex, Solidity, Go or Golang
Security tools and solutions	Burpsuite, Metasploit, Acunetix, Netsparker, Nessus, FortiGate, Nmap, Netcat, CheckMarx, Inspeckage, Core Impact, HPE WebInspect, NiperStudio, PawsStudio, AlienVault, Darktrace, kali Linux, MobSF, Microsoft Sentinel, Imperva WAF & DAM, Cisco ISE, Palo Alto, Docker, Azure pipelines, CI/CD, Cloudfalre, Incapsula, ELK, PostgreSQL Database, SonarLint, DeFi, Cryptocurrency, Solana, Etherscan, Ethereum
Testing Standards:	OWASP, SANS SWAT, NIST, OSSTMM, PCIDSS, ISO27001, ISO27032, Agile, CIS
Web CMS:	Drupal, WordPress, Joomla, Magento

VOLUNTEERING

- AfricaHackon Ghana chapter: Mentoring security enthusiast.
- Gimpa school of Technology: Leadership & mentoring students
- OWASP Ghana Chapter: Training Infosec community

INTEREST

Reading, Mentoring, attending conferences, Training, motivating people, bug bounty, blogging, Capture the flag (CTF) and research