Thumbiko Nyasulu

Cybersecurity Analyst | Detection & Response

+353858429584 • thumbikonyasulu@ymail.com • Linkedin • Github • Portfolio

PROFILE

Cybersecurity Analyst with hands-on experience in SOC monitoring, threat detection, log analysis, incident triage, vulnerability management, and forensic investigation across cloud and on-prem environments. Skilled in Microsoft Sentinel, Splunk, and QRadar, with strong knowledge of attacker techniques aligned to MITRE ATT&CK. Adept at improving detection fidelity, hardening endpoints, analysing network traffic, and developing scripts to automate operational workflows. Security+ and CySA+ certified, with proven ability to communicate technical insights, reduce risk exposure, and support enterprise security operations under pressure.

PROJECTS

Azure SOC Honeynet Project

- Designed and deployed a honeynet environment integrated with Microsoft Sentinel to simulate attack scenarios.
- Analysed attacker activity through NSG logs, firewall logs, VNet traffic, and threat intelligence feeds.
- Implemented identity and policy hardening to improve cloud security posture.

IBM QRadar SIEM Implementation & Threat Detection

- Deployed and configured QRadar SIEM in a lab SOC environment.
- Investigated security events using AQL queries.
- Built custom parsing and correlation rules to improve detection accuracy.

Splunk Enterprise SIEM Monitoring & Dashboarding

- Set up Universal Forwarders for scalable log ingestion.
- Created SPL dashboards, alerts, and threat-hunting queries.
- Built real-time reporting for SOC investigations.

WORK EXPERIENCE

Atos • **South Dublin, Dundrum** **02/2025 - Present**

IT Service Desk Analyst

- Strengthen endpoint security by implementing MFA and VPN troubleshooting, reducing user access risks by 20%.
- Contribute to compliance reporting by tracking security-related incidents in ServiceNow
- Support automation initiatives using PowerShell and API integrations
- Use Active Directory, Microsoft 365, and Exchange to manage user accounts.
- Basic experience supporting macOS and iOS devices

Amazon Web Services (AWS) • **Dublin, Tallaght** **02/2024 - 01/2025**

IT Hardware Technician

- Resolved 50+ weekly hardware and infrastructure issues, maintaining 99.9% uptime.
- Assisted with multi-site network configuration and monitoring, ensuring seamless connectivity.
- Conducted system updates, patching, and vulnerability mitigation across environments.

Surecom • **Dublin, Rathcoole** **01/2022 - 01/2023**

IT Security Support Analyst

- Conducted vulnerability scans with Nessus and Nmap, remediating critical risks.

- Collaborated with IT and management teams to maintain ISO27001 and GDPR compliance.
- Monitored security alerts and logs, performing initial triage and threat analysis.
- Implemented endpoint protection measures including antivirus deployment, patch management, and access controls.
- Performed network traffic analysis using Wireshark and firewall logs to identify suspicious behaviour

EDUCATION

Bachelor of Science, Computer Science

Technological University of Dublin • Grange Gorman, Dublin

CERTIFICATIONS

CompTIA Security+
CompTIA CYSA+
AWS Academy Graduate – Cloud Foundations
DevOps Fundamentals LinkedIn Learning

SKILLS

Automation & Scripting: PowerShell, Python, Kusto Query Language

Security Tools: Nessus, Nmap, Wireshark, Metasploit, Kali Linux, IDS/IPS fundamentals, firewall log analysis, Exposure to Microsoft Defender, CrowdStrike Falcon

Security & Monitoring: SIEM (Microsoft Sentinel, Splunk, QRadar), Log Analysis, Threat Detection, Vulnerability Management, Incident Response, Abuse Prevention, Endpoint Hardening, Security Policies, Compliance (ISO27001, GDPR)

Network: LAN/WAN fundamentals, VLANs, VPN, DNS, DHCP, PKI