Mojalefa L. Letsoara

Cybersecurity Analyst | SOC, Incident Response & Threat Detection
letsoaramojalefa8@outlook.com | +27 78 909 9643 | Phuthaditjhaba, Free State | LinkedIn | GitHub

Professional Profile

Cybersecurity Analyst with 3+ years of combined technical support experience across TFS Group and Q-lit Radio Station. Currently providing Windows-based IT support while building hands-on security operations capability through independent SOC investigations covering SIEM alert triage, phishing and malware analysis, identity-based attacks, network security monitoring, and full incident response lifecycles. Holds CompTIA Security+ and CySA+, Microsoft SC-200, SC-900 and AZ-900, with practical experience across Microsoft Sentinel, Splunk, Wazuh, Azure, KQL, Sysmon, Zeek and Suricata. Seeking a Cybersecurity Analyst or SOC Analyst role where technical support experience, security investigation skills and structured documentation can support a live security team.

Core Technical Skills

SIEM & Security Monitoring: Microsoft Sentinel, Splunk, Wazuh, alert triage, security monitoring, event correlation, log analysis, alert escalation
Incident Response & Detection: incident investigation, incident response, threat detection, IOC analysis, threat hunting, MITRE ATT&CK, KQL detection rules
Threat & Malware Analysis: phishing analysis, malware analysis, ransomware investigation, VirusTotal, MalwareBazaar, Hybrid Analysis, URLScan, Cisco Talos, PhishTool, YARA
Identity & Access: Active Directory, MFA, risk-based authentication, account takeover analysis, NIST SP 800-63
Endpoint & Network Security: Windows, Sysmon, auditd, IDS/IPS, Zeek, Suricata, endpoint security, antivirus deployment
Cloud & Infrastructure: Microsoft Azure, Log Analytics, Azure Monitor Agent, data collection rules, Bicep IaC, hub-andspoke networking, Linux
Frameworks, Models & Standards: NIST Cybersecurity Framework (CSF) familiarity, NIST SP 800-61 Incident Response, MITRE ATT&CK, Cyber Kill Chain, Diamond Model, Tactics Techniques & Procedures (TTPs), CVE/CVSS, GDPR, HIPAA and PCI DSS awareness
Documentation: incident reports, technical writing, security findings, communication with technical and non-technical audiences

Training and Certifications

- CompTIA Security+, issued June 2026
- CompTIA CySA+, issued June 2026
- Microsoft Certified: Security Operations Analyst Associate (SC-200), issued July 2026
- Microsoft Certified: Security, Compliance and Identity Fundamentals (SC-900), issued March 2026
- Microsoft Certified: Azure Fundamentals (AZ-900), issued March 2026
- Microsoft Certified: Azure Administrator Associate (AZ-104), exam booked for 20 October 2026
- Microsoft Certified: Cloud and AI Security Engineer Associate (SC-500), exam booked for 21 October 2026

Practical Projects

Stonegate SOC: Sentinel IR Simulation 2026

- Set up a Microsoft Sentinel environment for a fictional retail and logistics client, including a Log Analytics workspace, Azure Monitor Agent and data collection rules across a Windows Server 2022 build.
- Wrote a KQL detection rule for MITRE ATT&CK T1110 (brute force) and worked through 18 simulated incidents from triage to closure.

Conti Ransomware Investigation (TryHackMe, Splunk) 2026

- Investigated a simulated Exchange server compromise across more than 28,000 events in Splunk, correlating security events across Windows Security, Sysmon and IIS logs to reconstruct the attack chain.
- Identified a trojanised system binary, a backdoor account and a web shell installed through chained CVEs, and produced a formal SOC investigation report mapped to MITRE ATT&CK.

Phishing Email Triage Lab 2026

- Investigated six synthetic phishing emails end to end: raw header analysis, PhishTool triage, and enrichment through Cisco Talos, VirusTotal and URLScan, benchmarked against a legitimate control sample.
- Applied a weighted risk-scoring model to reach an analyst verdict on each case and wrote YARA rules for the phishing patterns identified.

File & Hash Threat Intelligence Analysis 2026 ● Ran a structured malware triage across four live samples using VirusTotal, MalwareBazaar and Hybrid Analysis: static file inspection, SHA256 hashing and dynamic sandbox execution.

- Confirmed a BlackMoon trojan, an IcedID banking trojan masquerading as a legitimate Windows binary, a doubleextension social engineering payload and an Akira ransomware sample, mapping each to MITRE ATT&CK.

Enterprise Hybrid SOC Lab (Stoneage Logistics scenario) 2026, ongoing

- Built a hybrid Azure environment using Bicep IaC: hub-and-spoke network, a domain-joined Windows 11 endpoint with Sysmon, a Linux server with auditd, and Zeek/Suricata network monitoring feeding a SIEM stack of Wazuh, Microsoft Sentinel and Splunk, each verified with real data flowing.
- Network, identity, endpoint and multi-SIEM phases are complete, along with a Darktrace integration design; detection engineering, threat hunting and incident response are the phases still in progress.

Legacy Account Recovery (ATO) Case Study Dec 2025 - Jan 2026

- Analysed how weak account recovery mechanisms, such as security questions, enable Account Takeover attacks, using the 2013 iCloud breach as a real-world case study.
- Mapped the full attack chain to MITRE ATT&CK (T1078, Valid Accounts) and NIST SP 800-63 guidance, and proposed defensive controls including MFA enforcement and risk-based authentication.

Professional Experience

IT Support Technician, TFS Group, Phuthaditjhaba May 2025 - Present

- Provide technical support for users across Windows-based environments, resolving hardware, software, connectivity and system issues.
- Support antivirus deployment and endpoint security best practices across user devices.
- Applied proper incident response discipline to a suspected security event, ruling out compromise through investigation before tracing the true cause to a Layer 2 network loop on a branch switch.
- Maintain documentation and provide user support while ensuring minimal disruption to business operations.

Volunteer Cybersecurity Analyst, Blue Team Training, Hacking Hub (Volunteer) Oct 2025 - Present

- Take part in structured Blue Team training covering threat detection, incident response, SIEM operations and malware analysis, consistently documenting findings for the community.
- First community member outside the founder to complete the Immersive Labs learning pathway.

Radio Host & Technical Support, Q-lit Radio Station (Freelance) Feb 2020 - Feb 2022

University of the Free State Qwa Qwa Campus

- Provided technical support and troubleshooting for Windows workstations, software applications and studio infrastructure, diagnosing hardware, OS and application issues to restore services quickly.
- Installed, configured and maintained software, and performed system maintenance, upgrades and repairs to improve reliability.

Education

- National Senior Certificate (Matric), 2018
- Bachelor of Arts, Sesotho and History, University of the Free State, 2020 - 2025 (not completed)
- Diploma in Information Technology, Richfield Graduate Institute of Technology, conditional acceptance received, registration planned for 2027

Additional Information

- Driver's Licence: Code C1