

# SAMSON LETSOALO

## JUNIOR CONSULTANT

### CONTACT



060 525 0674



mslets6040@gmail.com



13 Cypress Noordwyk Midrand

### SKILLS

- Excellent Verbal and written communication skills
- Computer skills (MS office, MS word, excel and PowerPoint.)
- Team player
- Problem solving and decision making skills
- Critical thinking skills
- Time Management
- Analytical and Interpersonal skills
- Flexible and initiative
- Strong understanding of networking protocols and security concepts
- Proficient in security tools and technologies, such as SIEM (Security Information and Event Management) systems, IDS/IPS (Intrusion Detection and Prevention Systems), and vulnerability assessment tools
- Familiarity with operating systems, including Windows, Linux, and macOS
- Knowledge of programming languages, such as Python and PowerShell

### LANGUAGES

- English
- Northern Sesotho
- Sepedi

### AWARDS/ CERTIFICATES

- (ISC)<sup>+</sup> Candidate  
10/2022
- Microsoft Certified: Security Operations Analyst Associate 01/2023 to 01/2039
- Microsoft Certified: Azure Fundamentals  
12/2022
- Microsoft Certified: Azure Network Engineer Associate  
02/2023 to 02/2024
- Microsoft Certified: Cybersecurity Architect Expert  
02/2023 to 02/2024
- Certified in Cybersecurity (CC)  
02/2023 to 02/2026
- Certified SOC Analyst Foundation  
24/04/2023

### PROFILE

Mathematical Science graduate with possess hands on knowledge. I am a confident person who works well under pressure. My combination of self-discipline and interpersonal skills allows me to work independently or as part of a team. I am highly dedicated and pairing ambition and drive alongside a sense of humor and positive "can-do" attitude. Highly motivated and detail-oriented individual seeking an entry-level position as a SOC Analyst. Aiming to apply technical expertise, analytical skills, and training experience on letsdefend.io to detect and mitigate cybersecurity threats and contribute to the overall security posture of an organization.

### WORK EXPERIENCE

#### Junior Consultant

2022 - Present

RIC Consulting

- At RIC Consulting, I worked as a Qlik support and IT support specialist. In the Qlik support role, I was responsible for providing technical assistance to users of Qlik products, troubleshooting issues, and ensuring the smooth operation of the software.
- I assisted with the installation, configuration, and customization of Qlik applications, and collaborated with the development team to identify and resolve bugs.
- In the IT support role, I was responsible for providing technical assistance to employees of RIC Consulting, troubleshooting issues with hardware and software, and ensuring the smooth operation of the company's computer systems.
- I assisted with the installation, configuration, and maintenance of hardware and software, and provided training to employees on the proper use of various applications.
- Throughout my time at RIC Consulting, I demonstrated excellent communication skills, an ability to troubleshoot complex technical issues, and a strong attention to detail.
- I also worked well both independently and as part of a team, and consistently met or exceeded performance expectations

#### Training

2022 - Present

letsdefend.io

1. Threat Hunting: LetsDefend.io allowed me to participate in real-world threat hunting scenarios. I gain hands-on experience in proactively searching for indicators of compromise (IOCs), identifying suspicious activities, and detecting potential threats within network environments.
2. Incident Response: The platform provided practical experience in incident response methodologies. I learnt how to investigate security incidents, collect and analyze relevant data, and take appropriate actions to contain and mitigate the impact of incidents.
3. Malware Analysis: LetsDefend.io offered me opportunities to analyze and dissect real-world malware samples. This experience will enable me to understand the inner workings of malware, identify its behavior, and develop effective strategies for detection and remediation.
4. SIEM Utilization: The platform utilizes Security Information and Event Management (SIEM) systems. I learnt how to leverage SIEM technologies to monitor and analyze security events, correlate logs from multiple sources, and identify potential security incidents or anomalies.
5. Log Analysis: By working with LetsDefend.io, I gained experience in analyzing and interpreting log files generated by various systems and devices. This skill is crucial for identifying security events, tracking user activities, and uncovering potential threats or vulnerabilities.
6. Forensic Analysis: The platform offered modules or exercises focused on forensic analysis. This experience taught me how to collect, preserve, and analyse digital evidence in a forensically sound manner, supporting incident investigations and legal proceedings if required.

REFERENCES

NAME : Tshegofatso Lucia Mmakola  
OCCUPATION: Junior Cloud Engineer and Support  
TELL :071 495 5057  
Email: tshegofatsolucia96@gmail.com

NAME : Karyn Knight  
OCCUPATION: Senior Qlik Support  
TELL : 083 227 9381  
Email: Karyn.e.khight@gmail.com

NAME : Mr Baloyi  
OCCUPATION: Lecture  
TELL : 072 813 5708

Security Analyst Home LAB 1:  
Performed the following tasks:  
Installed and configured Nessus Essentials to perform credentialed vulnerability scans against Windows 10 Hosts  
Implemented Vulnerability Management Function on sandbox networks:  
Discover, Prioritize, Assess, Report, Remediate, Verify  
Conducted vulnerability assessments with Nessus; remediated vulnerabilities  
Developed automated remediation process to pre-emptively deal with vulnerabilities stemming from Windows updates and third-party software.

System Administrator Home Lab 2  
Performed the following tasks:  
Active Directory Administration on Server 2019:  
PowerShell: Automated provision, maintaining, and deprovisioning user accounts.  
Implementation and management of Group Policy Objects  
Security Group maintenance and administration  
Backup administrator using Windows native backup utilities.  
Implementation and maintenance of Windows DNS and DHCP services  
Configuration of Windows File Servers with implementation of quotas and NTFS permissions

Security Analyst Home LAB 2:  
Performed the following tasks:  
GitHub: [github.com/jtech.io](https://github.com/jtech.io) (For Penetration Test Reports and Python Projects)  
YouTube: [youtube.com/jtech.io](https://youtube.com/jtech.io)  
Developed of content for, as well as performed the following tasks:  
Implemented Vulnerability Management Function on sandbox nextworks:  
Discover, Prioritize, Assess, Report, Remediate, Verify  
Conducted vulnerability assessments with Nessus; remediated vulnerabilities  
Performed penetration tests on VulnHub and HackTheBox using the high-level assessment methodology described by NIST 800-115. (See [github.com/jtech.io](https://github.com/jtech.io) for full reports)  
Experience using nmap in conjunction with bash and python scripting to automate the fingerprinting phases of security assessments and pen tests. (See [github.com/jtech.io](https://github.com/jtech.io) for script samples.

EDUCATION

Bachelor of Science (Mathematical Science)

- University of Limpopo2021
- Introduction to Database Systems
  - Operating Systems
  - Artificial Intelligence
  - Computer Networks
  - Time Series Analysis
  - Design and Analysis of Experiments
  - Applied Linear regression
  - Sampling Theory

National Senior Certificate  
Harry Oppenheimer Agricultural High School

2016-2018