Onalenna Ketshabile

onalennaketshabile.vercel.app

+27-68-269-9551 | onalennaketshabile@gmail.com | linkedin.com/in/onalenna-ketshabile | github.com/Onalenna-Ketshabile

Summary

I am a dedicated cybersecurity professional with a strong foundation in both software development and cloud computing. I specialize in protecting systems, analyzing vulnerabilities, and implementing proactive security measures. With experience in security operations and hands-on practice in real-world scenarios, I continuously seek to grow my skills and contribute to creating secure, resilient environments. I'm passionate about solving complex problems and delivering impactful solutions.

Education

University of Johannesburg Johannesburg, South Africa
BSc Honors in Computer Science (NQF 8) *Feb 2024 - Present*

- Specialization: Cyber Security
- Course Work: Information Security, Ethical & Legal Aspects of IT, Computer Forensics, Information Security in the WWW, Network Information Security, New Systems Development Paradigms, Information Security Risk Analysis

University of Johannesburg Johannesburg, South Africa
BSc in Information Technology (NQF 7) *Feb 2020 - Feb 2023*

- Final Average: 76%
- Specialization: Computer Science and Informatics (Software Development)
- Course Work: Informatics, Computer Science, Mathematics (Calculus, Applied Math, Linear Algebra, Discrete Math, Abstract Math)
- Awards: Artificial Intelligence in the 4IR (SLP), Top 10 Performers in Informatics for the first semester of 2020 and 2021, Top 10 Overall Performers for the first semester of 2020
- Verify Completion.

Experience

Cyber Security Analyst April 2024 – Present
IGuardSA *Johannesburg, South Africa*

- Provide 24/7 security monitoring and support for clients, ensuring robust defense against potential threats and continuous system vigilance.
- Conduct in-depth investigations using QRadar (IBM SIEM Tool), Reaqta, Kaspersky, Defender, and other antivirus solutions to identify and mitigate threats across client environments.
- Analyze and respond to suspicious email activities, including phishing and spoofing, using Microsoft Defender, Mimecast, and Checkpoint, reducing email-based threats significantly.
- Deploy and manage advanced security controls to protect against phishing, malware, and emerging cyber threats.
- Monitor alerts from IDS/IPS and infrastructure tools like IBM QRadar SIEM and Paessler PRTG to ensure proactive threat detection and system health.
- Prepare detailed weekly and monthly reports on security incidents, observed trends, and the effectiveness of incident response measures, providing actionable insights to stakeholders.
- Escalate unresolved incidents for deeper investigation, ensuring timely resolutions and improved client trust.

Network Support Engineer October 2023 – March 2024
Cell C *Johannesburg, South Africa*

- Optimized a daily reporting script in Python, improving data completeness and integrating automated screenshot-to-Excel functionality for streamlined reporting.
- Resolved complex subscriber issues related to network-level messages and calls using Linux tools, enhancing user experience.
- Supported critical projects such as WiFi Calling and SMSC, generating detailed KPI reports to drive operational efficiency.
- Monitored and maintained Ubuntu Linux nodes, performing upgrades, cleanups, and certificate renewals to ensure system stability.
- Diagnosed and resolved network issues using TCP dumps and Wireshark analysis, minimizing downtime.

- Developed thorough documentation on system health, bug tracking, and daily operations to improve team efficiency and knowledge sharing.

IT Intern April 2023 – March 2024

Atos Pty Ltd *Johannesburg, South Africa*

- Provided IT support to internal staff, assisting with technical issues, password resets, and laptop setups, ensuring smooth operations.
- Delivered network support as a contractor to Cell C, maintaining network environments and supporting high availability for key systems.
- Participated in training programs to enhance technical skills, applying knowledge to improve service delivery.

Apprentice February 2023 – March 2024

Accenture (in collaboration with the University of Johannesburg) *Johannesburg, South Africa*

- Enhanced Python and JavaScript skills by automating processes, building scripts, and developing interactive web applications.
- Gained hands-on experience in machine learning, focusing on data preprocessing and model implementation using Python libraries.
- Designed and developed responsive web pages with HTML, CSS, and JavaScript, ensuring user-friendly interfaces.
- Participated in Agile workflows, contributing to daily stand-ups, peer reviews, and maintaining high code quality.

Projects

Hosting a Static Website on AWS S3 (GitHub Link)

- Configured an S3 bucket for static website hosting, creating custom index and error pages.
- Secured the bucket with IAM policies to ensure appropriate access control.
- Tools and Services: AWS S3, IAM Policies, Static Website Hosting.

AWS EC2 Instance with Secure SSH Access (GitHub Link)

- Deployed an AWS EC2 instance with secure SSH access by configuring key pairs and security groups.
- Hardened security by disabling password-based authentication and implementing `fail2ban` for brute-force protection.
- Tools and Services: AWS EC2, Security Groups, Fail2Ban.

Internet Speed Test Using Python (GitHub Link)

- Developed a program to measure internet download and upload speeds using Python.
- Integrated Speedtest API for accurate and reliable speed testing.
- Tools and Services: Python, Speedtest API, Command Prompt.

Password Strength Checker Using Python (GitHub Link)

- Designed a tool to assess password strength using regex and security heuristics.
- Provided actionable feedback to enhance password robustness.
- Tools and Services: Python, Regex, Command Prompt.

Certifications

AWS Certified Cloud Practitioner Verify Certification

- Core concepts of AWS cloud, including services, security, pricing models, and cloud architecture basics.

CompTIA Security+ Verify Certification

- Comprehensive understanding of network security, threat management, identity management, and risk mitigation. Emphasizes best practices in security policies and procedures.

CompTIA Network+ Verify Certification

- In-depth knowledge of network infrastructure, operations, security, and troubleshooting for both wired and wireless networks. Emphasizes key protocols.

(ISC)^2 Certified in Cyber Security Verify Certification

- Foundational knowledge in security principles, risk management, network security, access control, and incident response.

Other Cloud-Related Certifications

- **AZ-500: Microsoft Certified: Azure Security Engineer Associate**
- Verify Certification
- **SC-400: Microsoft Certified: Information Protection and Compliance Administrator Associate**
- Verify Certification
- **SC-200: Microsoft Certified: Security Operations Analyst Associate**
- Verify Certification
- **SC-900: Microsoft Certified: Security, Compliance, and Identity Fundamentals**
- Verify Certification
- **AZ-900: Microsoft Certified: Azure Fundamentals**
- Verify Certification

Skills

Technical Skills

- **SIEM & SOAR:** QRadar, Microsoft Sentinel, IBM SOAR.
- **Endpoint Protection:** Microsoft Defender XDR, Trellix, Kaspersky, Azure Defender, ReaQta.
- **Email Security:** Microsoft 365 Defender, Mimecast.
- **Network Monitoring:** Wireshark, BetterCap, QRadar Flows.
- **Systems:** Windows, Linux.
- **Cloud Security:** AWS (EC2, S3, IAM, Lambda, VPC, CloudTrail, CloudWatch, AWS WAF, GuardDuty, RDS), Azure.
- **Web Development:** React, Node.js, JavaScript, SQL, API Development.
- **Scripting & Automation:** Python, JavaScript, PowerShell, Bash.

Soft Skills

- Communication Skills.
- Problem-Solving.
- Attention to Detail.
- Adaptability and Quick Learning.
- Collaboration and Teamwork.
- Ethical Judgment.
- Perseverance and Resilience.
- Curiosity and Research Skills.

Hands-On Practice & Bug Bounty

Hands-On Practice

- Active participation on platforms like LetsDefend, TryHackMe, and HackTheBox.
- Focused on building practical cybersecurity skills through simulated environments and challenges.

Bug Bounty

- Freelance bug bounty hunter on HackerOne, working toward identifying and reporting security vulnerabilities.
- Gaining experience in vulnerability assessment and developing a deeper understanding of security flaws.