TAKOOR Shashiduth

INFORMATION SECURITY ANALYST

📞 (+230) 5928-0406 | ✉ shashiduth.takoor@gmail.com | ⌨ github.com/s-takoor | 🔗 linkedin.com/in/shashiduth-takoor

SUMMARY

Information Security (InfoSec) Analyst with 6+ years of hands-on experience in cybersecurity, specialising in both defensive and offensive security. Proven track record as a cybersecurity consultant, delivering expertise across diverse locations such as Mauritius, Madagascar, Djibouti, and the Kingdom of Saudi Arabia.

WORK EXPERIENCE

Checkout Ltd.   *Ebene, Mauritius*
ANALYST I, INFOSEC ANALYST   *Mar. 2023 - Present*

- Spearheaded the integration of Wiz, Cloud Security Posture Management (CSPM) solution into development workflows, enhancing detection of vulnerabilities, secrets, and misconfigurations in Infrastructure as Code (IaC) templates, containers and VM images.
- Optimised incident response through the integration of Wiz with Slack and Jira, orchestrating real-time alerting and automated issue resolution. Jira issues are dynamically generated based on severity, swiftly dispatched to stakeholders on a Jira Board, adhering to defined SLAs for remediation, minimising response time and human intervention.
- Collaborated with the workplace technology team to set up OKTA Single Sign-on (SSO) and Wiz Role-based Access Control (RBAC), simplifying access management through automated provisioning and deprovisioning.
- Revamped monthly patching by transitionin to a more efficient process. Previously, vulnerabilities were manually extracted from Qualys VMDR, shared them via Email and Slack. Now, with access to Wiz, teams can quickly identify resources requiring OS patching.
- Conducted comprehensive security assessments, including API testing, mobile SDK testing, and segmentation testing, to identify vulnerabilities and recommend remediation strategies.
- Assisted with the review of findings from HackerOne bug bounty and vulnerability disclosure program.
- Configured option profiles for authenticated vulnerability scans targeting network devices such as firewalls, switches, and routers for our data centres, enhancing our overall security posture and regulatory adherence.
- Collaborated with cross-functional teams to ensure compliance with industry standards and regulations such as Payment Card Industry Data Security Standard (PCI DSS) and System and Organisation Controls (SOC2).

Checkout Ltd.   *Ebene, Mauritius*
ASSOCIATE, INFOSEC ANALYST   *Mar. 2022 - Mar. 2023*

- Leveraging Wiz to uncover vulnerabilities, misconfigurations, threats and unnecessary permissions across cloud resources.
- Conducted PCI ASV assessments using Qualys, ensuring compliance with PCI DSS standards.
- Assisted in deploying endpoint protection solution such as Cylance and SentinelOne organisation-wide.
- Manage cloud applications traffic via Netskope Cloud Access Security Broker (CASB) and integration with Garrison Ultra Remote Browser Isolation (RBI).
- Monitoring and analysing security events leveraging on LogRhythm SIEM and Microsoft Azure Sentinel SIEM and SOAR.
- Automated monthly security reporting by utilising the Wiz API and Python to extract data points, formatting with LaTeX, and generate PDF reports shared organisation-wide via Confluence.

Mauritius Network Services (MNS) Ltd.   *Ebene, Mauritius*
INFORMATION SECURITY OFFICER   *Sep. 2020 - Feb. 2022*

- Implemented Wazuh, an open source security platform, to enhance security monitoring capabilities. Proficiently monitored and analysed security events, ensuring proactive threat detection and response.

- Incident handling and incident response, swiftly mitigating security incidents to minimise potential risks.
- Reviewed and enhanced existing information security policies and procedures to align with industry best practices such as ISO 27001.
- Conducted security assessments, identifying vulnerabilities and offering strategic remediation strategies for stakeholders' optimal security posture. Activities include vulnerability scan and offline configuration audits leveraging on Tenable Nessus, web and mobile pentesting.

Ernst & Young (EY)
INFORMATION SECURITY OFFICER

Ebene, Mauritius
Oct. 2019 - Sep. 2020

- Conducted comprehensive security assessments, identifying vulnerabilities and delivering actionable remediation strategies. Activities encompassed vulnerability assessments, penetration testing, as well as web and mobile application security testing.
- Contributed expertise as consultant conducting cyber maturity assessment in the Middle East. Activities included facilitating workshops with stakeholders, evaluating existing controls, policies, and procedures, and providing recommendations to enhance compliance with the ISO 27001 standard.

Birger.
SECURITY OPERATION ANALYST

Phoenix, Mauritius
Apr. 2017 - Sep. 2019

- Real-Time security monitoring and analysis of security events through Symantec Managed Security Services (MSS) and IBM QRadar SIEM to swiftly detect potential threats.
- Promptly addressing security incidents, from initial detection to resolution, ensuring minimal impact and efficient mitigation.
- Produced comprehensive security reports tailored for diverse stakeholders, providing valuable insights and actionable recommendations.
- Conducted security assessments for stakeholders in the East African region, employing industry-standard methodologies such as Open Web Application Security Project (OWASP). These assessments encompassed vulnerability assessments and penetration testing aimed at identifying and remediating vulnerabilities, misconfigurations and potential security risks.
- Ensured compliance with international standards such as ISO 27001 and NIST, aligning security practices with industry best practices and regulatory requirements.

EDUCATION

Open University of Mauritius (OUM)
B.S. IN COMPUTER SCIENCE

Reduit, Mauritius
Jul. 2020 - Jul. 2023

- Coursework: Algorithms, Blockchain, Computer Architecture, Cybersecurity and Digital Forensics, Data Structures & Complexities, Object-oriented Programming, Python
- Thesis and Final Year Project: Blockchain-Based Voting DApp

SKILLS

- Vulnerability Assessment and Penetration Testing (VA/PT)
- Incident Handling and Incident Response (IH/IR)
- Security Auditing and Compliance
- Security Information and Event Management (SIEM)
- Threat and Vulnerability Management
- Cloud Security (AWS)
- Security Documentation, Metrics, and Reporting