MUTISYA ERICK MUTHOKA

➲0715709468/0762798871 ➲ mutisyaerick12@gmail.com ➲ GitHub ➲ LinkedIn ➲Blog

Cyber Security Specialist

Executive Summary

A dedicated cybersecurity professional with a proven track record in implementing and configuring security solutions to mitigate technology risks. Proficient in deploying endpoint protection platforms, next-generation firewalls, and cloud security tools, I ensure comprehensive defense against cyber threats across diverse environments. My ability to assess, recommend, and implement tailored security solutions aligns with clients' risk profiles and business objectives, enhancing their resilience against evolving cyber threats.
Furthermore, I excel in crafting and implementing security policies, threat prevention measures, and intrusion detection capabilities. Leveraging industry-leading tools for effective risk mitigation and incident response, I collaborate closely with clients to develop robust security strategies that address regulatory compliance requirements and mitigate technology risks effectively. With a commitment to delivering tangible results and safeguarding clients' assets, I am eager to contribute my expertise as a Technology Risk Consultant, driving impactful solutions and enhancing organizational resilience in today's dynamic cybersecurity landscape.

Top skills & Competences

- **Red/Purple team operations**: Skilled in testing business resilience against known and unknown cybersecurity attacks and advanced persistent threats (APTs).
- **Vulnerability Assessments and Penetration Testing (VAPT)**: Vast experience in conducting security assessments for organizations. Key competencies in active directory assessments, web application and API testing, network assessment, firewall testing, and reviews of best practices and standards.
- **Threat Intelligence and advisories**: Experience in tracking cyberthreats and curating Indicators of compromises to help clients improve detection and response capabilities.
- **Incident Response**: I collaborate with incident response teams to investigate and mitigate security incidents, reducing the average incident response time considerably.
- **Cloud penetration testing skills**: Proficient in conducting cloud security assessments for firms with both hybrid and cloud-native applications/solutions. Performing configuration assessments in cloud workloads across multi-cloud environments.
- **Cybersecurity Audit skills**: conversant with industry standards and frameworks including CISA, CCM, ISO 2700(1-5), COBIT, NIST-CSF, and TOGAF training from the National Cyber Security Program.
- **Implementing and Configuring Security Solutions**: Proficient in deploying endpoint protection platforms, next-generation firewalls, and cloud security tools, ensuring comprehensive defense against cyber threats across diverse environments.
- **Developing and Implementing Security Policies and Measures**: Skilled in crafting and implementing security policies, threat prevention measures, and intrusion detection capabilities, leveraging industry-leading tools for effective risk mitigation and incident response.

➲ Certifications

November 2023	**Salt Technical Associate**	SALT Security

October 2023	**Ivanti Endpoint Manager - Administration**	Ivanti
September 2023	**Cato Certified Associate**	Cato Networks
August 2023	**Cloud and Network Security Analyst**	Cybershujaa
July 2023	**JAMF Certified Associate**	JAMF
July 2023	**Trellix Certified Architect-Endpoint Security (ENS)**	Trellix
April 2023	**Certified Cybersecurity**	ICS2
January 2022	**Mobile Application Security Foundation**	NowSecure

➲ Professional Experience

Cyber Security Engineer – Assurance Services ▪ CYBER1 Solutions - East and West Africa
March 2024 – Present

- Conducting comprehensive Vulnerability Assessments and Penetration Testing (VAPT) on client networks, applications, and security devices, from scoping to reporting.
- Installing and configuring Vulnerability Assessment, Penetration Testing, and SIEM solutions for clients, ensuring seamless integration and functionality.
- Staying updated on emerging vulnerabilities across networks, applications, and security devices for various clients, proactively addressing potential threats.
- Researching and maintaining proficiency in computer network exploitation, countermeasures, and evolving trends in network security, applying insights to enhance security measures.
- Evaluating clients' current security postures and proposing and implementing effective controls to mitigate risks and strengthen defenses.
- Testing and exploring new hacking methodologies, identifying vulnerabilities, and enhancing security measures accordingly.
- Providing cloud security assessments and managing cloud security services for clients, ensuring the protection of sensitive data in cloud environments.
- Training technical staff and software developers in secure software development practices, fostering a culture of security awareness and best practices.
- Assisting clients in achieving compliance with international (EU-GDPR, HIPAA) and local (Data Protection Act of Kenya, 2019) data protection regulations, securing both on-premises and cloud-based data to meet regulatory requirements.

Cyber Security Engineer - Technical Division ▪ CYBER1 Solutions - East and West Africa July 2023 – February 2024

- Installation and configuration of security solutions (eg EDR/XDR, MDM, ITSM, ITAM) to MSSP clients' sites
- Conducting Health checks for MSSP Clients on security solutions deployed on their environment.
- Conducting troubleshooting and knowledge transfer sessions with client's technical teams on various security solutions.
- Performing POCs, Demos, Presentations, on client sites for various security needs and solutions.
- Conducting discussions and execution of CYBER1 products and value-added service offerings with customers
- Proactively researching new threats, exploits and vulnerabilities and giving advisories to MSSP clients on findings.

Cybersecurity specialist (On-the-job training) ▪ eKRAAL Innovation Hub November 2021 – July 2022

Skills Gained.

- Security Operations Center (SOC) Setup: Proficient in establishing and managing a Security Operations Center, including incident management and response across all tiers.
- Red Team Operations and Vulnerability Assessments: Experience in staging red team operations, including penetration testing and social engineering, to assess vulnerabilities within enterprise setups.
- Digital and Mobile Forensics: Skilled in conducting digital and mobile forensics using tools such as Autopsy, FTK imager, Cellebrite SIFT, volatility, EXIF tool, and proficient in digital forensics report writing.
- Secure Software Development: Expertise in secure software development, including CI/CD security, cryptosystems, network security, and data protection.
- Incident Investigation and Malware Analysis: Proficient in conducting incident investigations, including malware analysis and reverse engineering.
- Security Awareness Training: Familiarity with designing and delivering security awareness training programs to educate employees on best practices and reduce security risks.

➲ Education

- Jan 2014 – June 2018: **Bsc Business Information Technology (BBIT) –** Jomo Kenyatta University of Agriculture and Technology **2nd Class Honors Upper Division**

➲ Honors & Achievements

Top Performing Learner: Recognized as the most outstanding learner at e-Kraal Innovation hub highlighting my exceptional dedication to excellence and outstanding achievements in mastering diverse areas of cybersecurity.

➲ Referees

Available upon request.