Lee 'Simba' Mtoti (972-275-6072)
Irving, TX

Background Notes:

- AWS & ECSA certified Information Security professional with over 15+ years of experience in vulnerability management, Assessment & Remediation practices.
- Solid experience in vulnerability scanning tools such as IBM Appscan & Nessus, configuring and troubleshooting vulnerabilities.
- Developed applications & tools for searching and visualizing fully aggregated, cross-linked and standardized Vulnerability Databases based on CVE and other standards (CPE, CWE, CAPEC, OVAL, WASC and CVSS**).**
- Expert knowledge of vulnerability frameworks such as CVSS, OWASP, vast experience in web application/ internet security assessment.
- Extensive experience working in a cloud environment, handled vulnerability & security testing for AWS cloud services, Developed AWS Public Cloud migration architectures**,** automated pipelines, and reusable services, Led multiple cloud security projects as Portfolio Security SME in cross functional IT projects.
- Solid experience working in a CI/CD Devops environment, setting up configuration management systems, speeding up Devops processes creating automated pipelines using Jenkins, Ansible, and CloudFormation.
- Proficient in penetration testing (white box, black box and gray box) for known, unpatched vulnerabilities, and exploiting those vulnerabilities to determine the risk and ensure they are not false positives.
- Well versed with python/ Perl scripting & automation.
- Architected and deploy Splunk environment on premise for log correlation.
- Created Splunk dashboard for visualization logs

Software/Hardware Tools and Skills:

- **Programming Languages**: Assembly (NASM, Borland TASM), C++, Perl, VB, VBA, VBScript, JavaScript, Java, R, Python
- **Full Stack**: Applications, Databases, OS-Windows, Linux, Arch Linux, IP networks
- **Commercial Sast/Dast Tools**: Fortify SCA (Static Code Analyzer), Ounce labs (Static Code Analysis), Web Inspect, QAInspect, RAPID7 AppSpider (NTOSpider), **IBM Appscan, Nessus**, Canvas, SAINT, WhiteHat, SonarCube, Veracode
- **Compliance**: Sarbanes-Oxley (SOX) section 404, HIPAA, VISA CISP/PCI; Security and Privacy Policy Development, NIST SP 800-53A
- **Data Science**: Data mining, munging, Web scraping, analysis, machine learning and modeling.
- **Data Science Tools**: R, RStudio, Shiny, Python, Plotly Dash, Highcharter, Weka, Tableau, Octave, Matlab.

Education:

- Data Mining for Advanced Analytics Graduate Certificate – UC San Diego, San Diego, CA **Aug 2018 – Aug 2019**
- Graduate Business Analytics Certificate - SMU COX, Dallas, TX **Jan 2019 – May 2019**
- Advanced Computer Security Certificate - Stanford University, Stanford, CA
- Master of Science: Project Management (Information Security Management) - Northeastern University, Boston, MA
- Master of Science: Computer, Information and Network Security - DePaul University (CTI), Chicago, IL
- Master of Science: Distributed Systems - DePaul University (CTI), Chicago, IL
- BBA: Information Systems - University of Wisconsin-Madison, Madison, WI
- BBA: Operations and Information Management - University of Wisconsin-Madison, Madison, WI

Certifications:

- **AWS Associate: Solutions Architect, Sys Ops Administrator, Developer**
- **AWS Professional: Solutions Architect, DevOps Engineer**
- WCSD: WhiteHat Certified Secure Developer
- CEH: Certified Ethical Hacker
- **ECSA: Certified Security Analyst**
- **LPT: Licensed Penetration Tester**
- **CCNA: Cisco Certified Network Associate; Cisco Certified Network Associate - Security**
- **CASS: Certified Application Security Specialist**

- **CIPP/US: Certified Information Privacy Professional/ United States**
- Machine Learning (Stanford Coursera course) – verified
- Exploratory Data Analysis (Udacity Data Analysis with R) – verified
- Intro to Data Science (Udacity) – Verified
- Data Analysis and Statistical Inference (Duke Coursera course) - verified
- Data Science Specialization (Johns Hopkins University) – 9/10 course completed verified

Personal Project: https://kill3rbee.shinyapps.io/vFeedCard/

- This CVE Analytics Visualization and Reporting Dashboard(CARD) Shiny App is for searching and visualizing a fully aggregated, cross-linked and standardized Vulnerability Database based on CVE and other standards

Interview Project: https://kill3rbee.shinyapps.io/vFarmers/

- This Shiny App is for searching and visualizing Agricultural cropping season, insurance premiums, payouts for farmers across Ghana

Professional Experience:

Verizon, Irving, TX **Aug 2017 – Present**

Senior Principal, Security Engineering - Cyber Risk, Privacy & Compliance

- Architected and developed data exploratory analysis, validation, accuracy and reporting tool used on an internal data repository used by Legal, Finance and other portfolios to make data driven decisions.
- **Developed an application/tool for searching and visualizing fully aggregated, cross-linked and standardized Vulnerability Database based on CVE and other standards (CPE, CWE, CAPEC, OVAL, and CVSS). This application can be used to triage application specific issue determined by the business risks associated with the application in conjunction with the security requirements.**
- Responsible for mapping GDPR and the new California Privacy policy into achievable Privacy by Design and Privacy by default and derive engineering requirements which can be implemented to meet Verizon regulatory and contractual responsibilities under the laws.
- **Responsible for communicating, education and employee awareness of security issues to include State/Federal mandates in support of federal law and corporate compliance (EEC Privacy Regulations, FCC, PCI, GDPR, CCPA, etc.).**

Distinguished Member of Technical Staff, Application Security **Jan 2013 – Aug 2017**

- **Responsible for standardizing Enterprise VPC Security and Network design, Cloud Migration strategies, increasing SecDevOps automated processes across entire portfolio of > 100 legacy applications, toolchain integration, micro-servicing architecture and standards for breaking apart a monolithic applications, standard architectures, templates, and automated pipelines using Jenkins, Ansible, and CloudFormation**.
- **Designed and developed an application that determined cloud risk baseline, amount of rework an application would require to make it cloud native for all portfolio applications (400+) planned to migrate to AWS**
- **Selected as instructor by Cloud Program Office to teach an AWS Solution Architect Group Sessions**
- **Worked with different business portfolios to ensure that new products adhere to establish standards, policies and guidelines to reduce security risks, and recommend remediation approaches.**
- Provided architectural and technical guidance to support information system and infrastructure design, improvements, and planning while identifying security architecture issues, and provided security solutions for gaps.
- **Developed AWS Public Cloud migration architectures, automated pipelines, and reusable services.**
- Migration of Legacy and Greenfield Enterprise applications in a lift and shift, transformational, and re-platform approaches using developed automated pipelines**.**
- **Lead DevOps Toolchain Clearing House & Governance Team to standardize and automate Onboarding, Integration, Customization requests, Escalations, App Stack Standards, and Environment Management**.
- **Lead multiple cloud security projects as Portfolio Security SME on cross-team IT projects in regards to network security, platform security, application security, access and authentication to our enterprise environment.**

Distinguished Member of Technical Staff, IT Security **Nov 2008 – Jan 2013**

- Performed portfolio specific penetration testing (white box, black box and gray box) of applications and systems.
- **Performed portfolio specific web application assessments on large e-commerce site and corporate intranets for different business unit within Verizon.**
- **Developed security practices for Source Code Review, Manual Code Review, Manual Malicious Code Review and Web Application Custom Error Handling.**
- Created training to assist developers understand how to identify threats and countermeasures for their application using Threat Modeling.

NecUnified, Irving, TX **Mar 2007 – Sep 2008**

Security Consultant – Cyber Security Solution

- **Performed penetration testing (white box, black box and gray box) for known, unpatched vulnerabilities, and exploiting those vulnerabilities to determine the risk and ensure they are not false positives**.
- **Performed web application assessments on large e-commerce site and corporate intranets for large organizations.**
- Developed homegrown tools to assist in our daily work of pen testing.
- **Provide detailed written reports communicating security risks, their business implications and recommended remediation approaches**.

TransUnion LLC, Chicago, IL **Mar 2006 – Feb 2007**

Senior Security Consultant

- Lead TransUnion's first PCI framework certification, development and implementation effort on IT infrastructure.
- **Performed IT controls evaluation for TransUnion's Sarbanes-Oxley 404 compliance effort.**
- Performed TransUnion's key vendors and processing agents audits is USA and Canada.
- **Performed web applications assessment and recommend solutions.**
- **Implemented Threat Modeling to support security by design for Web Applications.**

ReddShell Corporation, Denver, CO (Acquired by Trustwave) **May 2005 – Mar 2006**

Senior Security Engineer

- **Architect, design and implement Web application vulnerability assessment tools for client security environments**
- **Develop supporting documentation and delivery of all Web application vulnerability assessments from development through testing and production.**
- **Scanned, reviewed and remediated web application vulnerabilities using QAInspect and WebInspect.**
- **Created, Managed Test Plans, Test Cases that had not passed QA within Mercury TestDirector (Quality Center) before Staging (testing applications coming out of QA) for all web applications.**
- **Performed internal audits and assessments to meet government and industry compliance (SOX and Visa CISP/PCI).**
- **Proof of concept evaluation, architecting, engineering, and implementing security and QA solutions for client IT infrastructures.**

CNA, Chicago, IL **Jan 2003- May 2005**

System Software Engineer

- Gathered business requirements and implemented Active Directory group policy management.
- **Performed asset management of all hardware, operating systems and software in the enterprise (except UNIX).**
- Architected, designed, supported, and maintained Microsoft SMS 2003 software distribution, hardware and software inventory environment for the enterprise including wise packaging, QA, and production.
- **Identified and resolved enterprise wide issues associated with name resolution, network availability/performance, domain authentication, replication, and security vulnerabilities.**
- **Identified and performed GAP analysis and remediation for CNA's first SOX framework development effort and implementation on IT infrastructure worldwide.**
- Worked with developers to review and recommended fixes for defects that did not meet policy or compliance requirements.