CURRICULUM VITAE

FOR

# **Lance Gumede**

** mcse**   [](http://www.itil-officialsite.com/home/home.aspx)



sss

**Personal Details**

Surname: Gumede

Names: Lancelot Sibusiso Lethukuthula

Date of Birth: 02 Nov 1984

Nationality: South African

Gender: Male

Marital Status: Single

Drivers License: Code 10 (C1) + Own Transport

Hobbies: LAN Gaming, Sports, Music and Gym

Languages: English, Afrikaans, Zulu

Physical Address: 11 Waterfall Street

Southdown Estate

Alberton

Cell NO: **083 472 47 46**

Email: [lance.gumede@gmail.com](mailto:lance.gumede@gmail.com) or [Lance.Gumede@icloud.com](mailto:Lance.Gumede@icloud.com)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SECONDARY EDUCATION**

Name of School : **JOHN ROSS COLLEGE**

Highest Grade Passed : Matric

Year completed : 2004

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**TERTIARY EDUCATION**

Name of Institution : **VARSITY COLLEGE**

Course Name : Diploma: Information Technology

**McAfee:**

Certified McAfee Technical Professional Risk & Compliance

Certified McAfee Technical Professional Data Protection

Certified McAfee Technical Professional Network Defence

Certified McAfee Technical Professional Systems Security

Certified McAfee Technical Professional Web Email Security

Certified McAfee Service Provider Technical Support Endpoint

**EMC:**

RSA EnVision Administration & Event Source Integration

RSA Security Analytics Administration

RSA Security Analytics Analysis

**DQS:**

ISO 27001 Lead Implementer

**Foster-Melliar:**

Implementing Governance and Compliance (COBIT)

**Quintica:**

ITIL Foundation Certified

COBIT 5 Foundation

**IBM:**

QRadar SIEM 7.2 Foundation and Advanced

Security Intelligence Specialist Mastery Award

Guardium

**FNB:**

Banking 101

**SACS:**

CISSP bootcamp

**TORQUE IT:**

**Certified Cisco Network Associate:**

* Interconnecting Cisco Networking Devices Part 1
* Interconnecting Cisco Networking Devices Part 2

**Certified Novell Administrator**:

* Novell Open Enterprise Server for Netware

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DETAILED PROFESSIONAL EXPERIENCE**

Employer Name : **InfoGuardiun**

Position : **Senior Security Research Analyst**

Period : **1 July 2016 – Present**

**Duties and Responsibilities:**

* Lead and own the design and delivery of security solutions and services
* Provide detailed specifications for IT security solutions and support the development of security testing plans
* Work with the relevant stakeholders to ensure residual risk are adequately mitigated to the degree that meet the risk appetite of the business
* Contribute to formulation of policies and best practices for security management.
* Consult on policy guidance, interpretation and enforcement mechanisms.
* Undertake and facilitate risk and vulnerability assessment/workshops covering the more complex design solutions during various development phases to ensure technical vulnerabilities are identified and correctly managed, proposing solutions as required.
* Work with the relevant stakeholders in accurately assessing the likelihood and impact of technical vulnerabilities.
* Production and management of technical risk and vulnerability reports as per approved standards and processes.
* Providing support in security incidents and investigation as required
* Leading by an example inspire commitment, and a positive attitude from the team and encouraging innovative ideas.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DETAILED PROFESSIONAL EXPERIENCE**

Employer Name : **FNB**

Position : **Information Security Analyst**

Period : **4 November 2014 – 30 June 2016**

**Duties and Responsibilities:**

* Infrastructure service design and implementation
* Assist in providing oversight and enforcement of security directives, orders, standards, plans and procedure
* Review new system designs and major modifications for security prior to implementations
* Ensure all activities undertaken align with agreed service level and proactively seek ways to improve the provision of service to the wider organisation
* Corporate governance comply, understand and implement all steps within IT development and meet governance in terms of legislative and audit requirements
* Increase operational efficiency and suggest solutions to enhance cost effectiveness
* Analyse information security test results and report on recommendations to rectify any vulnerabilities identified and ensure compliance to security standard within the business unit and within the organisation
* Cultivate and manage objective working relationships with a variety of stakeholders, including end-users, SME’s, project managers and senior staff members by providing expert advice and consulting on all aspects of IT security
* Support with the planning, motivation and the management of the implementation of an appropriate security operational strategy for the organisation by ensuring that operating objectives and standards of performance are not only understood but owned by management and employees and ensure that appropriate standards of conduct are established and complied with.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DETAILED PROFESSIONAL EXPERIENCE**

Employer Name : **Transnet SOC Limited**

Position : **Senior Information Security Analyst**

Period : 1 April 2014 – 31 October 2014

**Duties and Responsibilities:**

* Support communication of EISM information to the OD
* Represent the OD during EISM process & product evaluations
* Represent the OD and provide feedback at the bi-weekly Information Security Forum meetings
* Report unit concerns and considerations related to information security
* Provide input and feedback on current and future information security standards and initiatives
* Participate in the information security components of the Security Governance, Risk and Compliance council
* Receive security vulnerability reports for the OD’s information systems and disseminate such information to appropriate technical staff for resolution
* Provides EISM with regular status information such as critical server status and vulnerability management follow-up
* Provide advice to the OD’s by making reference to existing policies , standard and designs and facilitate the development of new material where required
* Assist in evangelising and implementing new information technologies and trends within the OD’s
* Review project proposal, RFC, RFIs and other project documentations and provide input with respect to information security requirements aligned with Transnetpolicies and standard, identifying gaps and working with the project team to close these gaps
* Liaise with the EIMS Risk function to ensure Information Security risk are adequately captured, controls identified and on-going basis mitigation actions are implemented
* Ensure that pre and post implementation security review of key technology implementations are performed
* Facilitate the rollout of the project security template to all projects in the OD
* Advise on security designs and facilitate the implementation thereof for all projects within the OD based on a risk assessment in accordance with the security template.
* Participate in and support establishment of incident response process, including incident reporting for the OD
* Maintain an effective information security awareness programme for the OD and in co-ordination with the EISM
* Promote security awareness and good security practises in the OD
* Attend information security awareness seminars and training presentations, seminars, workshops and events
* Disseminate information within the OD’s to raise awareness about information security issues
* Coordinate inventories of sensitive or critical information and information systems at the OD
* Coordinate risk assessment and participate disaster recovery and business continuity planning

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DETAILED PROFESSIONAL EXPERIENCE**

Employer Name : **SCS Africa @ Neotel**

Position : **Information Security Administrator**

Period : 1 June 2013 – 31 March 2014

**Duties and Responsibilities:**

Implement and maintain Information Security Policy on information security devices.

* Identify and classify IT and Information assets (Systems and Data) and the level of control and protection required.
* Responsible for securing the IT Systems that store, process, or transmit organizational information
* Make recommendation on all areas of IT which are exposed to risk and manage third party information security risk governance processes based on internal reviews and client requirements
* Ensure that IT Security policies and processes are defined, maintained and assessed for effectiveness and adequacy
* Implementation of new or revised IS policies / Procedure/ Guidelines and instructions as well as maintain and update risk registers
* Identify, import and assist with event source configuration of information technology assets.
* Document and implement processes and procedures required to successfully deal with the workflow of information security -incidents, -remediation and -reporting.
* Assist with Business Impact Analysis
* Perform Security Risk Analysis and risk management in conjunction with Availability and IT service Continuity Management.
* Designing security controls and develops security plans.
* Develop and document procedures for operating and maintaining security controls.
* Monitor and manage all relevant security breaches, handling security incidents, taking remedial action to prevent reoccurrences wherever possible.
* Continuous reduce the impact and volumes of all security incidents in conjunction with Problem Management by means of reporting and analyses.
* Promote education- and awareness- of security.
* Maintaining a set of security controls and documentation, as well as regular reviews and audits performed on all security controls and procedures.
* Ensure all relevant changes are assessed for impact from an information security aspect, including the Information Security Policy and security controls, Attend relevant CAB meetings.
* Perform security tests.
* Participate in any security reviews arising from security breaches and initiate remedial actions.
* Ensure that the confidentiality-, integrity- and availability- of the services are maintained at the levels agreed in the SLAs and that they conform to all relevant statutory requirements.
* Ensure that all access to services by external partners and suppliers are subject to contractual agreements and responsibilities.
* Designing and document network and security solutions as well as network and security components of business solutions.

Conduct and participate in internal security assessment, investigations and audits

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DETAILED PROFESSIONAL EXPERIENCE**

Employer Name : **Dimension Data @ Standard Bank**

Position : **Security Engineer**

Period : 1 September 2012 –31 May 2013

**Duties and Responsibilities:**

* Monitoring systems to ensure the Confidentiality, Integrity and Availability of information.
* Manage Anti-Virus agent installation/troubleshooting
* Documenting the Anti-Virus environment
* Resolve calls logged on the call management system
* Assist with and give input to service designs, redesign, planning and implementation.
* Provide daily download, test, and installation of virus definition files.
* Provide daily monitoring to ensure anti-virus / anti-malware protection is maintained.
* Coordinate scanning file/folder exclusions with other application owners.
* Enter change requests, attend the Change Control Board and attend the necessary Change Management Board meetings to obtain approval for changes and updates.
* Resolve incidents related to anti-virus.
* Coordinate with other support teams
* Provide compliance reports.
* Monitor information for available Antivirus Vendor patches and upgrades.
* Download, test and install Antivirus Vendor patches.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DETAILED PROFESSIONAL EXPERIENCE**

Employer Name : **T-SYSTEMS SA**

Position : **INFORMATION** **SECURITY ANALYST**

Period : 1 January 2009 – 31 Aug 2012

**Duties and Responsibilities:**

* Monitoring systems to ensure the Confidentiality, Integrity and Availability of information.
* Enter change requests, attend the Change Control Board and attend the necessary Change Management Board meetings to obtain approval for changes and updates.
* Coordinate with other support teams
* Provide compliance reports.
* Provide service improvement recommendations.
* Provide high level environment security audits.
* Monitor security solution system consoles
* Enhance security and risk mitigation
* Monitor IPS and IDS
* Provide fast, real-time network intrusion response
* Simplify security compliance
* Optimise IT and Network Operations through automated collection, analysis, alerting, auditing, reporting and secure storage of all logs
* Test and implement strategic security technologies
* Enterprise Malware Technologies: McAfee, Trend, Forefront, WSUS and Symantec
* Monitor and identify security events
* Escalate security alerts and incidents
* Perform maintenance tasks on security systems
* Identify unused rules on your IPS and firewall- Remove orphan rules
* Identify busy devices in order to facilitate capacity planning e.g.: VPN usage
* Vulnerability Assessment
* Highlight Risk and provide step by step for remediation procedures
* Highlight configurations errors on systems and network

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DETAILED PROFESSIONAL EXPERIENCE**

Employer Name : **M-IT & HP**

Position : **ON SITE ENGINEER**

Period : October 2008 - January 2009

**Duties and Responsibilities:**

* Represent HP during Anglo American Roll out project, ensure that each user is migrated to the new domain, ensure that radia ran efficiently, install every single user’s application from the APS server, and train to users how to login to Citrix server.
* Liaise with Hp project coordinators for obtaining site discovery documents, for obtaining new computer names and the users to be transformed.
* Feedback on project progress and number of users transformed a day.
* Set up test rigs for testing and making the relevant appointments with users.
* Test site readiness for Transformation.
* Re-imaging of assets.
* Ensure that assets have joined the Anglo Domain.
* Install software manually e.g. Minescape, Oracle, Sap, Hyperion, Active Pearl, Hummingbird, Interbase, Ultredit, Bentley etc.
* Deploy Hp assets (laptops, desktops, Workstations and thin clients).
* Copy user profile and data, copy of personal and archived data.
* Configure outlook, printers both local and network printers.
* End user Support after transformation.
* Technical Support after transformation
* Register assets on HP Alice tool.
* 1st Line and 2nd Line Support and Maintenance.
* Ensure SLA resolution times are met.
* Restoration of service.
* Customer interaction and communication.
* Incidents and events life cycle management.
* Service failure updates
* Meet SLA resolution times and focus on quick restoration of service, customer interaction and communication.
* Meet SLA resolution times and focus on quick restoration of service, customer interaction and communication.