Trymore Hove
Cell: +2774 734 4351
Email: trymo036h@gmail.com
Johannesburg, South Africa

Trymore Hove – Availability : Immediately

Job Title: Cyber Security Engineer, Managed Security Services

Bio	An IT professional with excellent analytical, diagnostic, troubleshooting and superb interpersonal and communication skills gained through extensive training and working in challenging environments. I have more than 10 years solid working experience in Information Technology supporting Microsoft, Symantec NetBackup, EMC, Firewalls (Checkpoint, Fortigate and Palo Alto), IPS (Checkpoint/Fortigate), Checkpoint Cloud Security solutions (Sandblast Mobile, Network, CloudGuard SaaS/IaaS, Web proxy (ZScaler), Two factor authentication (Entrust IDG), Endpoint Security (McAfee), SIEM (McAfee), Vulnerability management (Qualys, Nessus & OpenVAS), Microsoft ATA, Cyberark, Cybereason and Cisco technologies in Financial institutions and banks An innovative problem solver who excels even in fast paced highly pressurized environments and am very committed my work thus always striving to go an extra mile to satisfy customer requests timeously. I am a fast learner who can adjust well in any challenging situation with absolute confidence
Certifications:	• CompTIA A+ • CompTIA N+ • CompTIA Security+ • ITIL ® Foundation v3 • Certified Information Security Manager (CISM) • EC-Council Certified Ethical Hacker (CEHv9) • ITIL ® Intermediate - Service Operation (SO) • ITIL ® Intermediate - Service Transition (ST) • Check Point Certified Security Expert R80 (CCSE) • Certified Check Point Security Administrator (CCSA) • Checkpoint SandBlast Network Administrator (CCSBA) • CloudGuard IaaS Public Cloud Administrator (CCVSA) • Checkpoint SandBlast Agent Administrator (CCSBA-AGENT) • CheckpointSandBlast Mobile Security Administrator (CCSBMSE) • Fortigate Network Security Expert (NSE1-7 – Partner training) • Microsoft Certified Solutions Expert Server 2012 (MCSE) • CCNA CyberSecurity Ops (Cisco Global Scholarship) • Cisco Certified Network Associate Routing & Switching (CCNA R&S)
Courses:	• Certified In The Governance of Enterprise IT (CGEIT – In progress – Exam May 2020) • Certified Information Systems Security Professional (CISSP – In Progress – Exam June 2020) • Certified Information Security Auditor (CISA – in progress – Exam July 2020)

Professional Experience

Performanta – Cyber Security Engineer

May 2019 – Present

- Threat hunting
- Threat modelling
- Design and ensure operations of IT security controls are in line with policies, processes, standards and procedures.
- Represent Information Security in the relevant business areas as well as various IT Architecture and or security committees and forums
- Analysis of known and emerging threats to determine risks against assets creation, maintenance, governance and communication of security policies and standards across Assurance that company assets are effectively managed and monitored to meet security requirements.
- Implementing Checkpoint threat prevention and threat extraction technologies
- Installing DLP technologies/policies to reduce the exfiltration of company sensitive information
- Installing, upgrading, maintaining, and administering perimeter security systems (firewalls and intrusion prevention and detection systems (Checkpoint R77.xx – R80.xx & Fortigate)
- Conducting vulnerability management and penetration testing exercises to assist clients reduce vulnerability attack surfaces
- Proactively monitor and control the identified production systems and networks to provide a secure environment and maximize systems availability.
- Correlating, analysing, and escalating information security related events and alarms using security event management tools and following best practices.
- Monitor and report on security data generated by the solution
- Providing expert advice and guidance on all aspects of IT security
- Participate in Checkpoint software upgrades and patch/security updates as recommended by the firewall vendors.
- Participate in all incident management and security governance activities
- Logging Checkpoint/Fortigate vendor requests for incidents and faults for further investigations
- Report on mitigating actions required to correct or remedy actions where necessary and inform CISO or Business Units of any significant changes and risk situations.
- Generating weekly/monthly firewall reports for customers
- Provide project related security consultations for customers
- Conduct customer firewall auditing exercises to improve security posture and performance.
- Conduct Disaster Recovery Plan / Business Continuity Planning activities
- Maintain current knowledge of the Information Systems security industry and emerging technologies

Reasons for leaving – Company currently retrenching

Syrex – Checkpoint Security Engineer

May 2018 – April 2019

- Performed day to day review of Checkpoint events/alarms
- Participated in tier 2 and tier 3 security operations support for all customers
- Participated in security compliance efforts for all onboarded customers
- Carried out audits and assisted to prevent, respond, and remediation of security incidents.
- Monitored, optimized, troubleshooted, documented, and otherwise pampered the network security environments for customers
- Initiated escalation procedures to counteract potential threats/vulnerabilities
- Maintained and deployed network infrastructure to support client security operations
- Evaluated new and emerging security products and technologies on the market
- Assisted in implementation of strategies for the threat analysis and vulnerability assessments

- Assist technical or support services staff with information systems capabilities assessment reviews and/or audits
- Designed, implemented and supported security-focused tools and services such as Checkpoint Firewalls, IPS and IDS solutions
- Worked with other security and technical staff to conduct network testing, documenting incident results and providing management with incident reporting and summary observations.
- Maintained required documentation and managed the security operations strategy plus compliance for the organization.

Reasons for leaving – Contract ended

Information Security Architects (ISA), Security Specialist

August 2017 – April 2018

- Maintained and administered perimeter security systems (firewalls and intrusion prevention and detection systems (Checkpoint, Cisco, HP, Dell Sonic Wall)
- Maintained and managed Anti-Virus Infrastructures for customers (Symantec Endpoint, F-Secure, Kaspersky, McAfee)
- Proactively monitored and controlled the identified production systems and networks to provide a secure environment and maximize systems availability.
- Correlated, analysed, and escalated information security related events and alarms using security event management tools and following best practices.
- Monitored and reported on security data generated by the security solution
- Researched on security incident response trends such as: vulnerabilities, exploits, risks and their countermeasures; incident response processes and tools.
- Provided expert advice and guidance on all aspects of IT security
- Performed timely software upgrades and patch/security update as recommended by the firewall vendors.
- Conduct customer firewall auditing exercises to improve security posture and performance.
- Conduct Disaster Recovery Plan / Business Continuity Planning activities

Reasons for leaving – Seeking growth

Dimension Data - Security Engineer L2

June 2013 – July 2017

- Web proxy management (ZScaler)
- Vulnerability management (Qualys)
- Two factor authentications (Entrust IDG)
- Provided Risk Advisory advice to the customer
- Endpoint Security (McAfee) solution management
- Microsoft ATA security device solutions management
- Managed and updated Standard Operating Procedures (SOPs)
- Performed daily, weekly and monthly tasks as per customer requirements
- Resolved all calls allocated as per SLA in the call management system
- Analysed, troubleshooted and investigated security-related, information systems anomalies based on security platform reporting, network traffic, log files, host-based and automated security alerts.

- Managing and maintaining Firewalls (Checkpoint/ASA), IPS/IDS technologies
- Provided daily report to the insight of Security solution environment health.
- Assisted with the development of security tool requirements, trials, and evaluations, as well as security operations procedures and processes
- Represented Security solution in project discussions, workshops and were necessary as requested.
- Created and maintained documentation on Security solution processes, policies, procedures and diagrams, ensuring they are accurate and current.
- Conduct customer firewall auditing exercises to improve security posture and performance.
- Conduct Disaster Recovery Plan / Business Continuity Planning activities
- Disk Staging
- Designed backup policies
- Media and Device Management
- Catalogue Consistency Checks
- Provided support for Symantec NetBackup technologies
- Implemented Intelligent Disaster Recovery processes
- Implemented and Configured different types of tape robotic libraries
- Devised backup strategies as per customer requirements
- Implemented backups in clustered environments
- Installed and maintained Symantec / Veritas storage devices
- Installed patches on Windows Master, Media and Ops Center Reporting servers
- Monitored daily, weekly and monthly full/differential backups via NetBackup Console GUI/ Ops Center/ Java Console
- Interacted with difference functional areas in IT to resolve/plan system events
- Conduct customer firewall auditing exercises to improve security posture and performance.
- Conduct Disaster Recovery Plan / Business Continuity Planning activities

Reasons for leaving – Wanted to further my Checkpoint knowledge

Pink Elephant SA – Network Support Administrator - Team Lead

January 2009 – May 2013

- Handled network related projects
- Conducted remote troubleshooting
- Checkpoint & Cisco ASA firewall administration
- Managed all network security related incidents
- Managed and maintained the network cabling infrastructure
- Generated daily, weekly and monthly management reports
- Configured, managed and maintained internet connectivity
- Installed, configured and troubleshooted Secure Remote Access (APN, VPN)
- Incident Management, Change Management and Problem Management resolution
- Configured and implemented Routing and Switching – LAN, WAN, VLANs and Routing protocols, Wireless LANs, VoIP solutions and IPT solutions.
- Installed, configured, troubleshooted and operated Cisco network equipment and infrastructure
- Maintained and administered perimeter security systems such as firewalls and IPS/IDS solutions

Reasons for leaving – Was offered a permanent role

References available on request