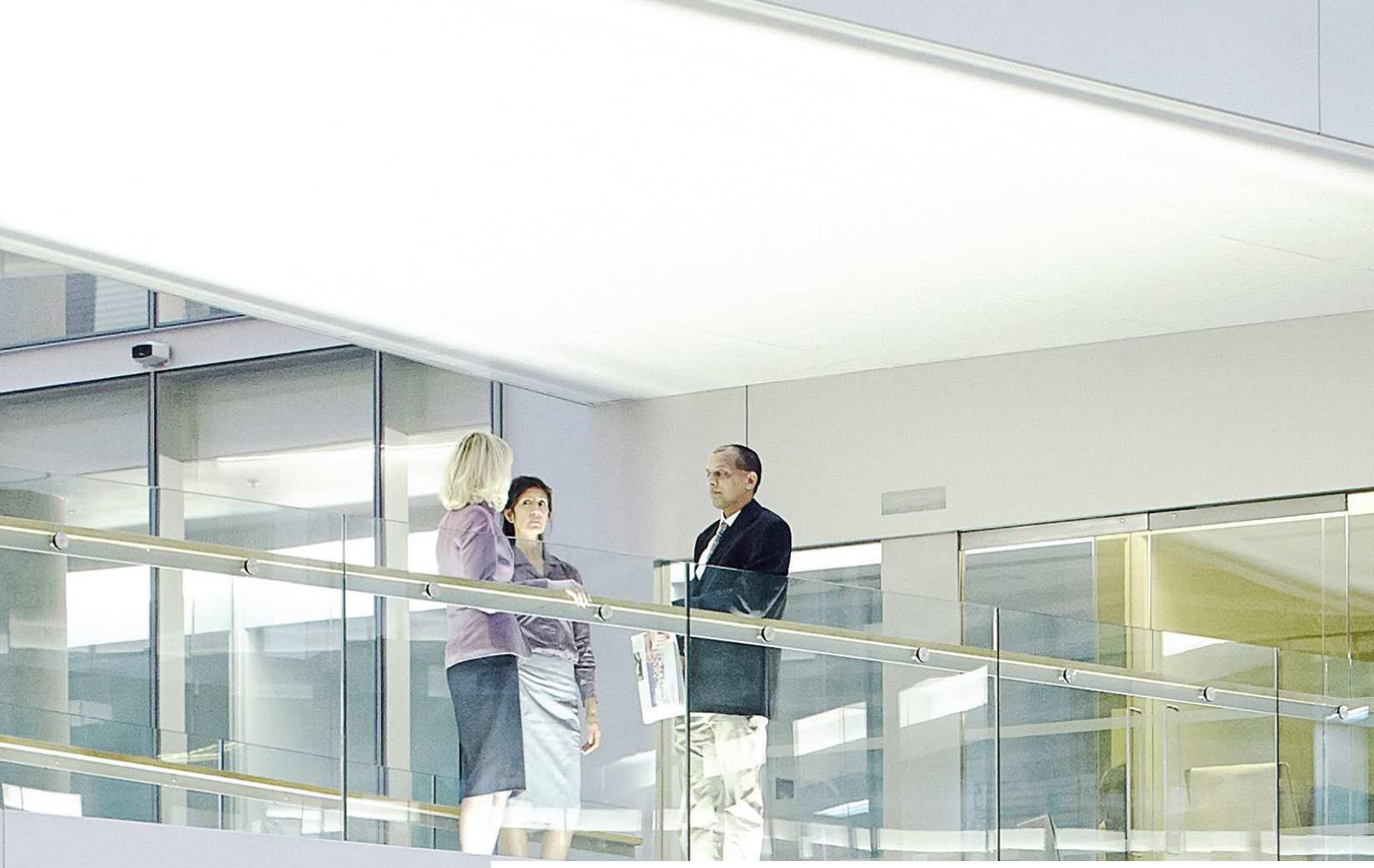
www.pwc.co.za

Cyber as a Service

Capability Overview

Cyber Africa

pwc



Contents

1 Context

2 The PwC Difference

3 Vulnerability Management as a Service

4 Access Governance as a Service

5 SIEM*Plus*

6 Deployment Architecture

7 Cyber Security and Privacy

8 Contact Us

1. Context

With the number of high profile security breaches and cyber-attacks growing each year, business is under enormous pressure to take proactive steps to minimize the chance of a cybersecurity breach and, when compromised, to slow the attackers' progress, and react quickly and efficiently to reduce the impact of the crime.

Three critical factors are core to maintaining a cyber-resilient organisation.

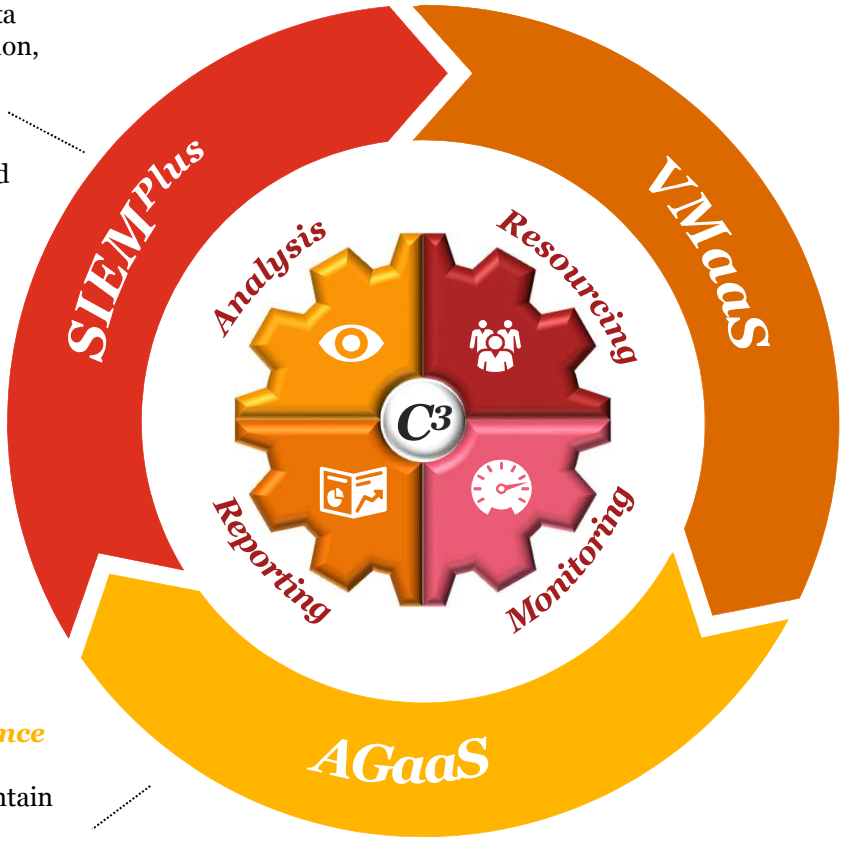
To maximise cyber-resilience, companies must identify and address system vulnerabilities, gain control over high risk accounts, and put in place robust event correlation, incident detection and response capabilities.

But the activities associated with these critical areas are both time and resource intensive – stretching already constrained internal security and operations teams, who would be better utilised consuming security intelligence data rather than generating and analysing it.

PwC's Cyber as a Service frees internal security teams to focus on protecting the business

SIEM Plus
Correlate and analyse real-time event data for incident detection, response and containment.

Integrate trend and threat intelligence data for incident classification and response prioritisation



Vulnerability Management as a Service
Identify and prioritise exposures associated with inherent system security vulnerabilities and infrastructure configuration errors

Access Governance as a Service
Establish and maintain accountability and manage exposures associated with user roles and privilege abuse

2. *The PwC Difference*

PwC is excited about the opportunity to partner with our clients to help them in the fight against Cyber-criminals and dishonest insiders

With PwC as the Managed Services Provider (MSSP), our clients' internal IT and Security teams are enabled to focus on the task of remediating vulnerabilities, maintaining effective access controls, and responding to indicators of compromise before the damage is done.

Some of the factors that differentiate PwC from our peers include:

- Strong communication & project management skills
- Shared accountability and responsibility – we work with our clients to a collective goal
- An experienced team who listen and take account of what is needed, executing as required with a strong dose of pragmatism
- Driven to establish a long term partnership with our clients
- Determined to demonstrate value and justify our clients' investments in our services

3. Vulnerability Management as a Service (VMaaS) Overview

There are tens of thousands known vulnerabilities and each year the list grows larger. Our VMaaS service centres around the continuous identification, prioritisation and remediation tracking of security vulnerabilities and critical infrastructure configuration weaknesses. This allows our clients' IT and Security Teams to focus on timely remediation of those security weaknesses that pose the greatest risk to the business.

Our service consists of six main elements, grouped to address evolving security threats facing a business and reducing the risk of potential compromise.

1

Asset Discovery & Classification

Maintain a database representation of all IT assets in the environment.

Periodically refresh the asset database to ensure complete coverage

Classify assets based on criteria that enable a strategic, prioritised approach to vulnerability management

Periodically review classification to ensure accuracy of prioritisation

2

Threat Modelling

Based on an asset class, identify the top threats, and threat agents that class of assets is most sensitive to, linked to the attack vector most likely to be exploited by a would-be cyber-criminal.

Periodically update the model in line with the ever-changing threat landscape

3

Firewall Assurance

Provide a consolidated view of all Firewalls (and IPS') and their compliance to policy: Rule Set and Configuration

Optimise firewall Rule Sets and drive the remediation of shadowed and redundant rules

Facilitate change tracking of Firewall Rule Set changes

Provide workflow for firewall rule-set changes and rule-set certification

4

Network Assurance

Extend policy compliance to network devices including Routers, Switches, Load Balancers and Proxies

Maintain an up-to-date view of network topology based on current network configuration

Perform access path analysis to discover exposures and vulnerabilities associated with poor network configuration

5

Vulnerability Control

Execute continuous vulnerability scanning

Perform vulnerability analytics for context and prioritisation

Map vulnerabilities against Threat Intelligence sources to assist with prioritisation

Conduct virtual attack simulations to understand the exposures associated with identified vulnerabilities

6

Remediation Tracking

Drive and track remediation of vulnerabilities

Provide trend reports to gauge program effectiveness

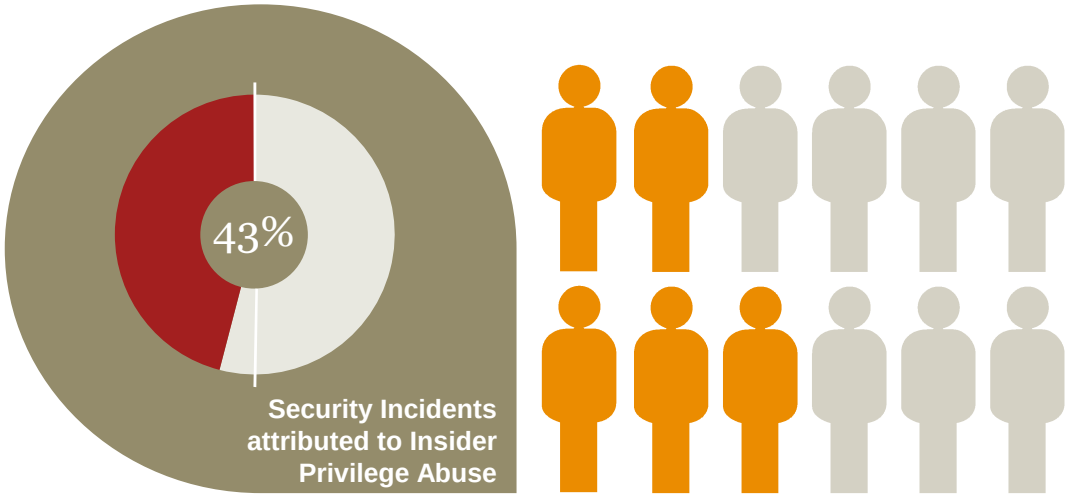
Provide advice on mechanisms to mitigate against exposures including:

- Detection of exploitation attempts
- Blocking access
- Patching
- Accepting the risk

Maintain a record of unmitigated exposures and rationale applied to risk acceptance

4. Access Governance as a Service (AGaaS) Overview

Access governance as a topic has grown in importance due to a growing awareness of, and sensitivity to, the risks associated with poorly managed user and administrator accounts and privileges. All types of organisations, in many industry sectors, are discovering that they need much greater visibility into who can access their key resources and how.



We have formulated a cloud-enabled managed service offering for Access Governance, enabling our clients to quickly gain and maintain visibility over user access risk.

Common Challenges Encountered

Privileges exceed access levels that were originally approved/provisioned

No single authoritative identity repository for employees/non-employees

Access review practices are manual and reviewers have insufficient context of user access needs

Time lines to revoke access are excessive

Access profile cloning occurs inappropriately

Role/rule-based access is used inconsistently

Segregation of duties are poorly enforced

AGaaS Benefits

A clear record of "who has access to what" in the business – for employees, contractors and 3rd parties

Continuous identification of dormant and orphaned accounts

Streamlined and managed access certification and re-certification

Prioritisation of areas of greatest access risk e.g. privilege creep or toxic role combinations

Evidence to demonstrate compliance and effective oversight in respect to data protection and access governance

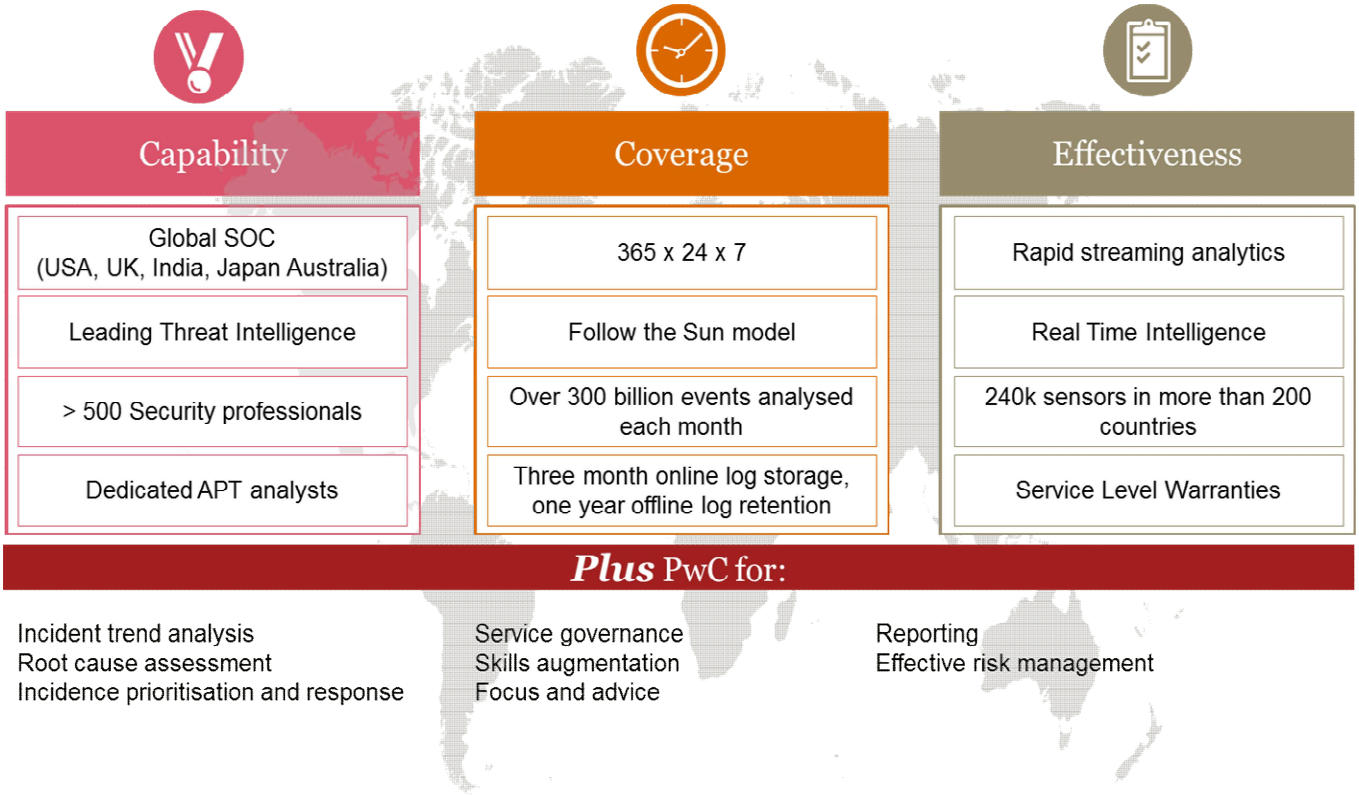
5. SIEM*Plus*

SIEM technology promises event correlation, log centralization with consolidation, console reduction and finally the ability for less trained engineers to be a first step in the defense of a company's high value targets.

The journey from installation to insight, when deploying a SIEM technology, is far from straightforward

While SIEM does this well when properly installed, maintained and staffed, this proves to be a task that consumes significant human resources, demands substantial care and tuning, and returns a great deal of data that offers little in the way of real, useable security intelligence, unless further contextualised against the backdrop of prevailing cyber-threats and the organisation's sensitivity to such threats.

Our approach is a combination of cloud services for SIEM and Threat Intelligence, coupled to a centralised coordination, tuning, trend analysis, reporting and incident response and recovery capability.

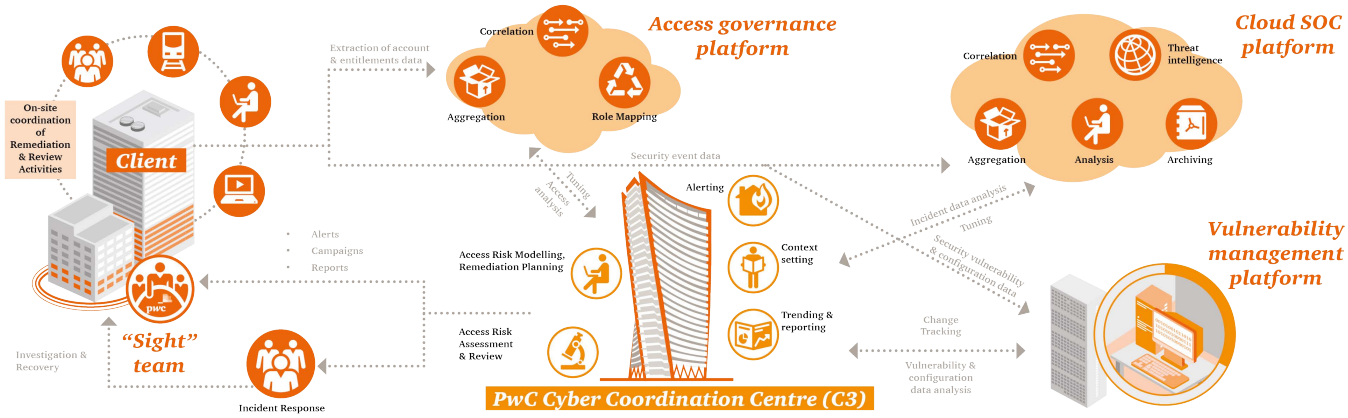


6. Deployment Architecture

PwC's Managed Services are deployed and delivered in a 3-tier model. Central to the service is the C3 (The Cyber Coordination Centre) where the bulk of security analysis and report preparation takes place.

Unlike traditional security managed services however, our model also ensures a strong on-site presence. Our SIGHT Team, are the "eyes and ears" on the ground, building relationships with our clients' operational, risk and security teams, and gaining a solid understanding of the priorities, realities, limitations and capabilities of the organisation. This ensures that security recommendations and reports processed by the C3 receive the correct emphasis and are actioned timeously.

Last and vital for rapid capability deployment and time to effectiveness are our various platforms for Access Governance, Secure Operations Centre and Vulnerability Management. To this end we have partnered with best-in-class providers in each category – firm in our belief that corporate security programs should be about leveraging technologies rather than about deploying them.



Cybersecurity and Privacy

PwC can help you see the big picture

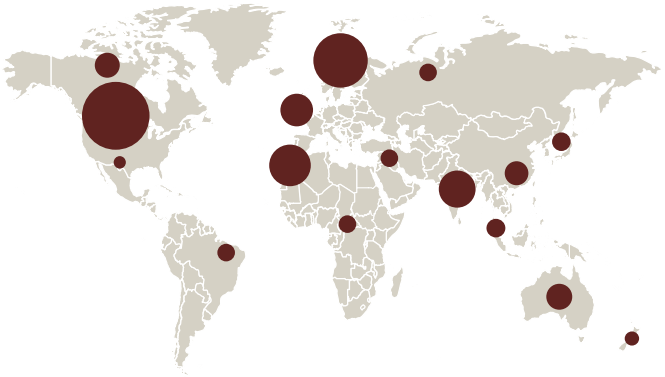
PwC's Cybersecurity and Privacy practice helps clients think more broadly about cybersecurity and privacy and move boldly toward new possibilities. PwC sees cybersecurity and privacy as a tool to not only protect business value but also create it. We offer an end-to-end portfolio of services to support any technology leader at any point, including strategy and transformation, implementation and operations, incident readiness and response, and privacy and consumer protection.

pwc

Seeing the big picture

About PwC's Cybersecurity and Privacy practice

PwC's global team of 3,300+ practitioners include specialized consultants, former law enforcement agents, cyber-forensic investigators, intelligence analysts, technologists, attorneys and industry leaders in cybersecurity and privacy. Our team has deep experience helping global businesses across industries strategically assess, design, deploy and improve cybersecurity programs. Learn more at pwc.com/cybersecurityandprivacy



Diverse Network of Resources

PwC has deep experience helping organizations strategically assess, design, deploy and improve cybersecurity programs. We also have a long history of building trusted relationships with business leaders at all levels.

Experience

Our tactical knowledge gleaned from decades of projects across industries, geographies and technologies informs our services.

Global analytics and cybersecurity impact centers

Our Impact Centers give companies and organizations from around the world access to experts and experience from across the PwC global network to help companies deal with the challenges of keeping pace in this era of digital disruption and to successfully transform for the future.

Certified Incident Response Capabilities

The National Security Agency (NSA) awarded PwC its Certified Incident Response Assistance (CIRA) accreditation and the first professional services firm in the UK to receive accreditation by Cyber Incident Response (IR) scheme run by CESG – the information assurance arm of GCHQ - and the Centre for the Protection of National Infrastructure (CPNI).

CyberArk named PwC 2017 Americas Partner Excellence Award Winner

SailPoint named PwC its 2016 Global Advisory Firm of the Year

HPE named PwC its Global Alliance Advisory Partner of the Year 2017 – Intelligent Edge Solutions

PwC rated as a Leader in **ALM**: ALM Vanguard Cybersecurity Consulting 2017Analyst Report

Notes

Contact us

Johannesburg

Kris Budnik
Partner lead for Cyber Africa
Mobile: +27 (82) 600 7311
Email: kris.budnik@pwc.com

Busi Mathe
Partner
Risk Assurance Cyber Security and Privacy
Mobile: +27 (82) 210 3121
Email: busisiwe.mathe@pwc.com

Simone Santana
Associate Director
Business Development - Cyber Africa
Mobile: +27 (83) 200 5009
Email: simone.santana@pwc.com

Durban

Junaid Amra
Partner
Forensic Technology & Cyber Afirca
Mobile: +27 (82) 953 9325
Email: junaid.amra@pwc.com

Cape Town

Johan Andries Pretorius
Associate Director
Risk Assurance & Cyber Security
Mobile: +27 (84) 503 5050
Email: johan.a.pretorius@pwc.com

Nigeria

Wunmi Adetokunbo-Ajayi
Partner | Digital Risk and Cyber Security
Mobile: +234 (0) 7051265583
Email: wunmi.adetokunbo-ajayi@pwc.com

Namibia

Linda Hatupopi
Cyber Security & IT Risk Assurance
Mobile: +246 811 29 7738
Email: linda.hatupopi@pwc.com

Mauritius

Vikas Sharma
Associate Director
Mobile: +230 54973395
Email: v.sharma@pwc.com

Kenya

Edward Kerich
Partner/ Director
Mobile: +254 (735) 812029
Email: edward.kerich@pwc.com

Alex Muriuki
Advisory Technology
Mobile: +254702004050
Email: alex.muriuki@pwc.com