LOGICALIS
Architects of Change
MEMBER OF THE **DATATEC** GROUP

South Africans need to boost their efforts in fighting cybercrime.

The Challenge

In the current South African landscape, many organisations will suffer a data security breach this year. It is crucial to assess whether you have the necessary resources to counter this threat and how swiftly you can respond.

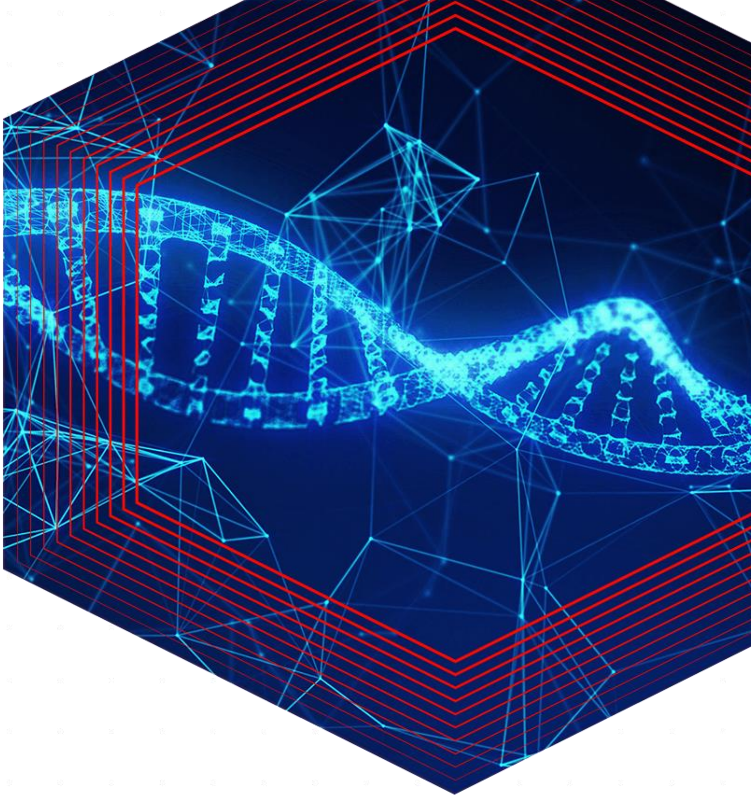
Safeguarding data

Protecting data is vital. Data privacy and security are fundamental components of modern security strategies.

Data acts as the fuel for business success, and when it is clean, secure, well-organised, and easily accessible, it builds trust within your organisation.

Supply and demand

The battle for talent poses another critical challenge in cybersecurity. The demand for cybersecurity skills and expertise far exceeds the available supply in South Africa, leaving many enterprises without the in-house resources to develop, execute, and refine their cybersecurity strategies.



Monitor, detect, respond

Failing to monitor systems, detect potential security incidents, and make rapid operational changes to counter detected threats leaves you vulnerable to attacks.

Additionally, the reputational damage resulting from a security breach further demonstrates the need for a new generation of cybersecurity measures.

As per INTERPOL’s African Cyberthreat Assessment Report 2022, a total of **230 million cyber threats** were detected in South Africa, out of which 219 million, or 95.21%, were e-mail-based attacks.

What’s worse is that the nation is already suffering from an alarming **100% increase** in mobile banking application fraud and is experiencing on average **577 malware attacks every hour.**

ITWeb Security Summit

LOGICALIS
Architects of Change
MEMBER OF THE DATATEC GROUP

A Security Operations Centre (SOC) can minimise the fallout of a data breach, but its business benefits go much further than that!

SOC Benefits:

Continuous safeguarding

Operating 24/7, security operations centres (SOCs) provide non-stop protection throughout the year. This constant surveillance is vital for early detection of any abnormal activities. Cyber-attacks do not adhere to a strict schedule of Monday to Friday, 9 to 5.

Rapid and efficient incident response

By maintaining constant vigilance, SOC team members significantly reduce the time it takes to detect a compromise from the moment it initially occurs. If any suspicious activity is identified, SOC analysts conduct thorough investigations to confirm whether it is indeed an attack before taking steps to contain it.

Reduced breach and operational costs

Through their proactive approach, SOC teams help decrease the impact of a breach on an organisation, thereby mitigating potential costs associated with data loss, legal actions, and damage to the business's reputation.

The longer a cyber attacker remains undetected within a network, the greater the potential damage they can cause to the company. Furthermore, SOC teams aim to minimise downtime and disruption to business operations during an attack, effectively preventing financial losses.

In terms of operational efficiency, a centralised SOC team can lead to reduced capital expenditure (Capex) and operational expenditure (Opex). By consolidating security expertise within a streamlined team, it avoids multiple groups or departments duplicating efforts when addressing the same cybersecurity incidents.

Proactive threat prevention

SOCs go beyond incident detection by actively conducting analysis and threat hunting, which helps prevent attacks from occurring in the first place. With increased visibility and control over security systems, SOCs enable organisations to stay ahead of potential attackers and proactively address issues.

Security expertise

A SOC consists of a diverse team, including a SOC manager, incident responders, security analysts, security engineers, threat hunters, forensic investigators, and compliance auditors.

Each team member brings a unique skill set that, combined with the expertise of others, plays a crucial role in detecting, remediating, analysing, and learning from threats.

They possess in-depth knowledge of proven technologies for threat detection and prevention, such as SIEM, behavioral threat analytics, AI and machine learning, and cloud access security brokers, as well as the most advanced threat detection techniques.

LOGICALIS
Architects of Change
MEMBER OF THE DATATEC GROUP

Every organisation needs a reality check that forces it to ask:

How many security functions are we capable of doing in-house effectively?

Communication and collaboration

SOC teams excel in communication and collaboration, both within their own team and across the organisation. They conduct security awareness training programmes to educate employees, contractors, clients, and other stakeholders about potential threats.

SOC members also share security insights with C-level executives, management, business leaders, and department heads, enabling company leaders to assess potential risks and determine whether to accept them or adopt new policies and controls to mitigate them.

Compliance

SOC monitoring capabilities play a crucial role in ensuring enterprise compliance, particularly with regulations that require specific security monitoring functions and mechanisms, such as GDPR and POPPIA.

Enhanced business reputation

Having a SOC demonstrates a company's commitment to data security and privacy, which builds confidence in employees, clients, customers, and third-party stakeholders.

A company that prioritises the security and privacy of its data earns a stronger reputation, potentially leading to increased recommendations from existing clients and attracting new ones.

> “ ”
>
> We generate about 170,000,000 events a month. There is no way our internal security team would be able to review that amount of data without using partners and their threat intelligence to help identify potential threats
>
> **Ray Thorpe**, Global CISO, ESW

How can Logicalis assist?

1. **Zero Trust Workshop**, including setting of goals, identifying blockers and exploring available solutions.
2. **SOC Tour** and detailed managed service presentation.
3. **Security Assessment and/or Audit Readiness Workshop**.
4. **10% discount** Security Services for one year on projects signed before end July 2023.
5. More information on the Logicalis Security portfolio.

Contact: info@za.logicalis.com