LOGICALIS
Architects of Change
MEMBER OF THE DATATEC GROUP

Security Operations Centre (SOC)

The Challenge

The threat landscape in South Africa is rapidly evolving and many organisations will suffer data security breaches this year.

Do you have the necessary resources to counter this threat and how swiftly can you respond?

Safeguarding data

Failure to protect your organisation's data can result in serious legal, operational and brand damage. It is becoming a top priority to ensure that your data is clean, secured and easily accessible.

Skills and Expertise

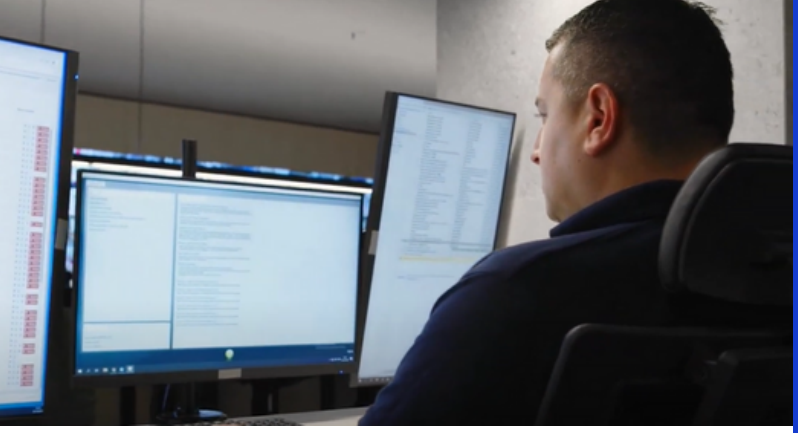
The demand for cybersecurity skills in South Africa far exceeds the available supply. This leaves many organisations without the in-house expertise to implement their cybersecurity strategies.

Increasing threats

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 email 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



A Security Operations Centre (SOC) has many benefits:

24/7/365 protection

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 seldom take place during work hours.

Rapid incident response

SOC teams drastically reduce the time it takes to detect breaches and threats. Suspicious activity is identified and SOC analysts investigate before rapid steps are taken to contain the potential threat.

Reduce operational costs

Breaches are very expensive and SOC teams can help prevent or mitigate losses from data breaches, legal consequences or reputational damage.

Undetected cyber threats can cause significant damage, but SOC teams can prevent disruptions and protect against financial losses.

Proactive threat prevention

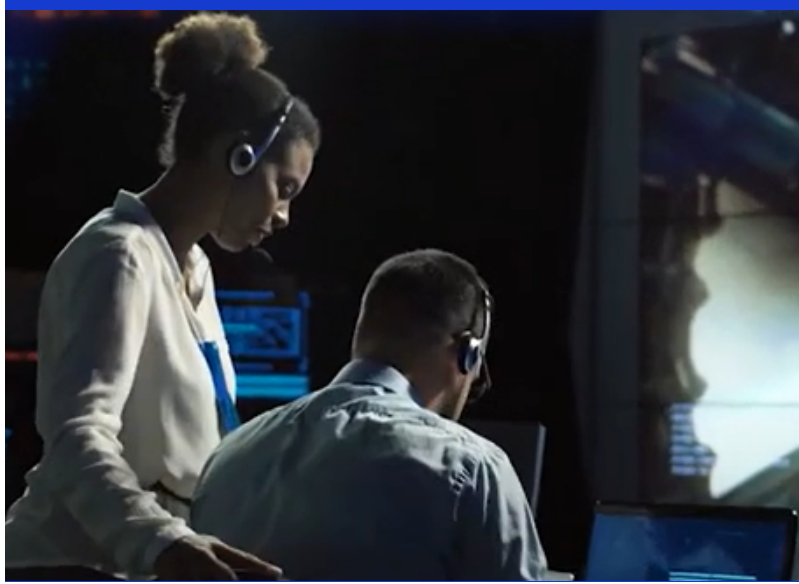
SOCs go beyond incident detection by actively analysing and hunting for threats. With increased visibility and control over security systems, SOCs enable your organisation to stay ahead of potential attackers and address issues before they become disasters.

Security expertise

Our SOC team consists of a diverse range of experts, including a SOC manager, incident responders, analysts, engineers, threat hunters, investigators and compliance auditors.

Each team member brings a unique skill set that plays a crucial role in detecting, remediating, analysing and adapting to threats.

They have in-depth knowledge of proven technologies such as SIEM, behavioural threat analytics, AI & machine learning, and many more of the latest threat detection techniques.



How many security functions can you manage in-house?

"Our team handles a significant volume of approximately 300 million monthly events, which is a substantial number. To effectively identify potential threats, the SOC team employs security tools such as UEBA, SIEM, SOAR, and threat intelligence tools to correlate these events."

Kagiso Mokgofa, Logicalis SOC Manager

Sharing insights

SOC teams can educate and train employees, contractors and other stakeholders in cybersecurity best practices. They also share their insights with management, which helps with informed policies and decisions.

How can Logicalis help you?

LOGICALIS
Architects of Change
MEMBER OF THE DATATEC GROUP

- Zero Trust Workshops
- SOC Tour
- Security Assessment
- Security Portfolio Overview
- Audit Readiness Workshops
- SOC Managed Service

www.za.logicalis.com

info@za.logicalis.com