datacentrix

Security
Operations Centre

24/7

24 hours a day, 7 days a week. The Security Operations Centre monitors your security environment and systems every second of every day.

100%

100% redundancy is built into the Datacentrix SOC – servicing any and all professional security products available.

WWS

Worldwide security. Datacentrix maintains a consistent link into the worldwide security network for the most current information on threats.

ZERO

Zero day threats. Threats are minimised through specialised tools, managing threats before they become a reality.

Responding effectively and in a timely manner to information security threats requires the continuous and thorough analysis of an enormous number of ongoing events. Without an automated toolset to help find patterns, filter, clean and analyse all the data that forms the context of an attack, the task of protecting the organisation becomes exceedingly complex, time consuming, resource intensive and expensive.

Datacentrix provides an effective and efficient service that will monitor your network and security assets 24/7/365. Our service covers all devices, servers, applications, users and infrastructure components; managed centrally from our Security Operations Centre (SOC).

- The SOC service monitors all data centre resources using situational behavioural context (correlation) – physical and virtual – anywhere in your enterprise.
- You receive real-time alerts on security or system-impacting incidents.
- We perform forensic risk analysis and audits on your behalf and manage your security and event logs for historical analysis.

The Datacentrix SOC service is provided by a combination of people, processes and technologies that provide real-time situational awareness through the detection, containment, and remediation of IT threats.

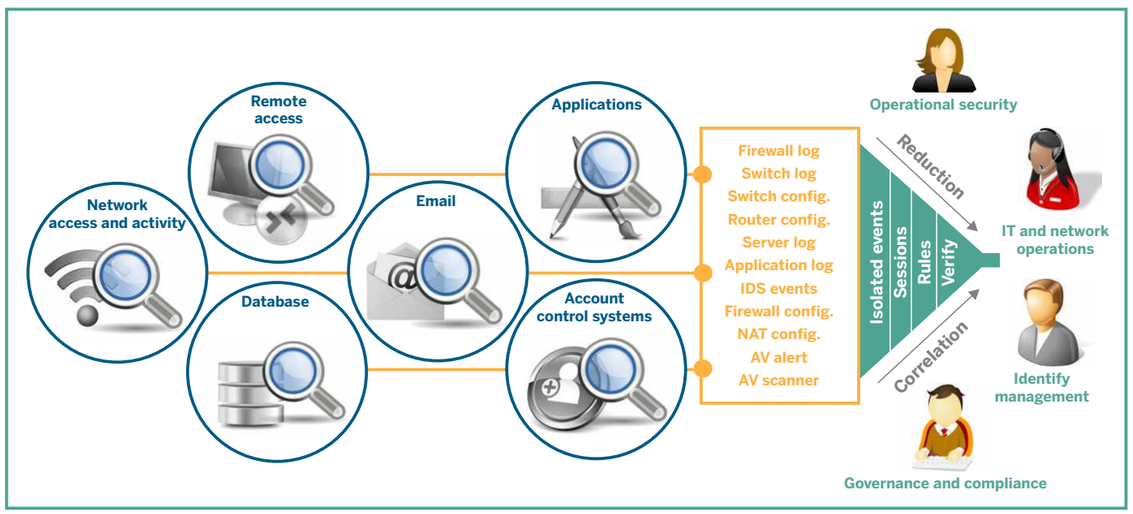
We manage security incidents on your behalf, ensuring that they are properly identified, analysed, communicated, processed and reported.

Our SOC integrates seamlessly into your security environment to ensure continuous operations. The Datacentrix SOC is staffed and fully functional around the clock, every day of the year.

The SOC facility is self-sufficient and operates from carrier-grade facilities that have redundant ISP connections, backup power generators and full redundancy.

An important objective of the Datacentrix security service is to assist customers in making astute investments in ICT security. The Datacentrix SOC offering is built in a way that allows customers to 'pick and choose' SOC modules, evaluate the benefits thereof and progressively add modules as and when required.

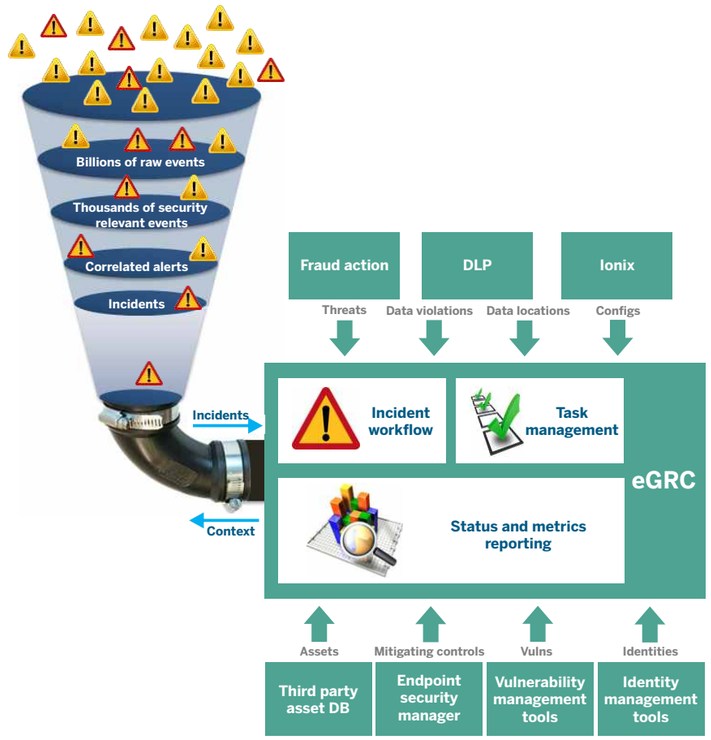
At the heart of the Datacentrix SOC service offering are the network intrusion prevention services (IPS) and network security monitoring, alerting, and analysis services.



Security monitoring alerting and analysis provides early warning for attempted intrusions and cyber-attacks, as well as alerts to management that facilitate appropriate countermeasures.

Security incident and event management (SIEM)
Our SIEM system provides customers with security monitoring for all network and security devices.
In addition, SOC services provide:

- Automated and human monitoring of information systems in real time
- Prevention, detection and management of cyber-attacks and IT security incidents
- Incident verification against worldwide baseline samples
- Network discovery and vulnerability assessment
- Governance, risk and compliance (GRC)
- Website assessment and monitoring
- Application and database scanners
- Unified threat management (UTM)
- Log management systems
- Enterprise antivirus
- Penetration testing
- Intrusion systems
- Firewalls



How do SOC services work?
SOC services work by using a security information and event management (SIEM) system that monitors all devices (including firewalls and intrusion prevention systems).

How does the monitoring occur?
A connection is made between Datacentrix' SOC and a remote collector within your firewall-secured network that allows security information to be sent to Datacentrix where full-time analysts monitor and analyse the information.

Is there contact with the analysts?
The analysts will only notify you if any irregular activity indicates that your network is under attack or if you request assistance in analysing or documenting security events.

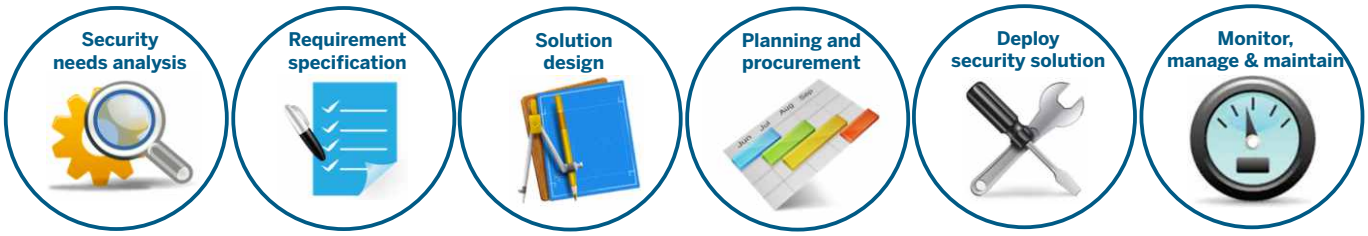
Would Datacentrix be "punching" a hole into my primary defence to conduct the monitoring?
No - the only connection is the one made to the remote controller (securely via your firewall) that allows for syslog information to be monitored.

Does Datacentrix view customer data during the monitoring process?
No - Datacentrix only monitors the external network. The customer is responsible for monitoring their internal network.

Does the monitoring of data take up much bandwidth?
Very little bandwidth is used. A customer should notice very little, if any, change in their bandwidth utilisation.

Are there report generation capabilities?
Reports can be provided daily, weekly and monthly to provide timely, historical insight to the amount and type of activity on your external network.

Datacentrix: Security operations engagement process



Datacentrix SOC: Technologies employed

Tools and description
The SOC is based on an industry leading Security Incident and Event Management (SIEM) tool called Security Analytics.
An orchestration layer integrates people, processes and technology, optimising investments. This agile framework enables analysts to detect and respond to security incidents and data breaches more efficiently and also provides: ➤ Centralised incident management aggregates and connects systems and processes; ➤ Integrated context during incident response; ➤ Industry best practices for incident response and breach management; and ➤ Tracking and reporting on key performance indicators to SOC stakeholders.
GRC modules allow you to build an efficient, collaborative enterprise governance, risk, and compliance (GRC) program across IT, finance, operations, and legal domains, helping you to manage risks, demonstrate compliance, and automate business processes.

Technology Partners

RSA

About Datacentrix

Datacentrix is a complete ICT systems integrator, providing solutions and services across the full information value chain to its customers. The company uses leading technologies to drive customer business strategies, unlocking efficiencies and empowering meaningful business insight.

Our most valuable assets are captured in the minds and spirit of our people. Every person at Datacentrix is a critical part of our service delivery model and our strategy for generating sustainable value for our customers and stakeholders.

We value partnerships and go the distance to establish trusting, lasting customer and stakeholder relations. Our longstanding affiliations and accreditations with our technology partners enable direct access to technology using the shortest channels.

It's our passion for excellence that drives our innovative and flexible solution design. Datacentrix' value-driven strategy and proven execution capability reinforce its position as one of the top ICT players in the local market.

Corporate office
Corporate Park North
238 Roan Crescent, 1685
Old Pretoria Road, Midrand

Tel: +27 (0)87 741 5000

Logistic centre
26 Landmarks Avenue
Kosmosdal, Extension 11
Samrand, Midrand

Tel: +27 (0)12 657 5000

Cape Town office
18 Oxbow Crescent
The Estuaries
Century City, 7441

Tel: +27 (0)21 529 0700

Port Elizabeth office
175 Cape Road
Mill Park
Port Elizabeth

Tel: +27 (0)41 391 0200

East London office
8-10 Winkley Street,
Chesswood Office Park
Block B, Berea, East London

Tel: +27 (0)43 705 8000

Durban office
Ground Floor, 6 The Terrace
Westway Office Park
Westville, Durban

Tel: +27 (0)87 741 9000

www.datacentrix.co.za