datacentrix

Security
Operations Centre

24/7

100%

WWS

ZERO

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

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

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

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 an 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 24x7x365. Our service covers all devices, servers, applications, users and infrastructure.

Datacentrix categorises events into three primary categories: an event, an incident or a request. These are triggered by either telephonic, email or SIEM (security information and event management) alerts and follow an escalation process through tiers of support for both technical and non-technical escalations.

Governance methodologies: The established governance methodologies at Datacentrix primarily follow ITIL, COBIT and SAN's best security practices to ensure our operations can cater for multiple business verticals.

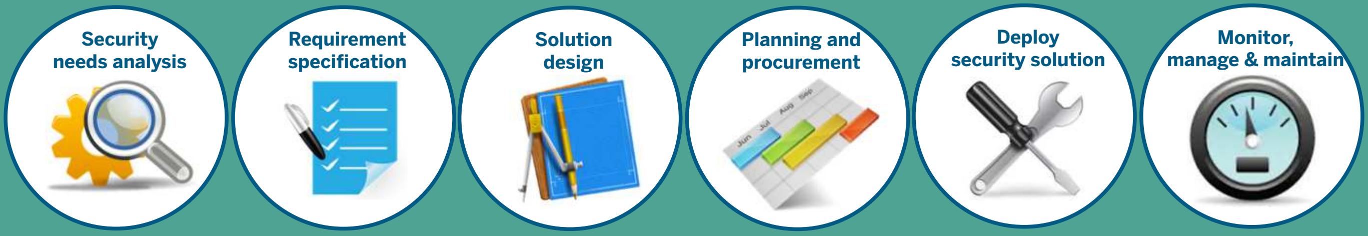
Analysts and responders: Our well-equipped team of analysts and responders form the base of our technical competence in the SOC and is available 24x7. The sole purpose of our analysts is to verify potential threats received by the firewalls and to handle events raised by the SIEM. They are responsible for the appropriate level of daily reporting and correspond directly with the management in our SOC.

Our response team deals with the day-to-day health checks and managed service items. The team is the next step in the escalation chain when an incident is critical. Our responders verify and handle incident escalations with our vendors.

Security specialists: The next escalation and capability step is to our security specialists who are dedicated within their field of expertise from firewalls to endpoints. We also have security compliance specialists with CISSP accreditations that assist with security governance and solution architecture.

Security operations and technical manager: Datacentrix customers have direct access to the security operations and technical manager. A dedicated security account manager is also assigned to each customer to ensure that all service eventualities are covered.

Datacentrix: Security operations engagement process



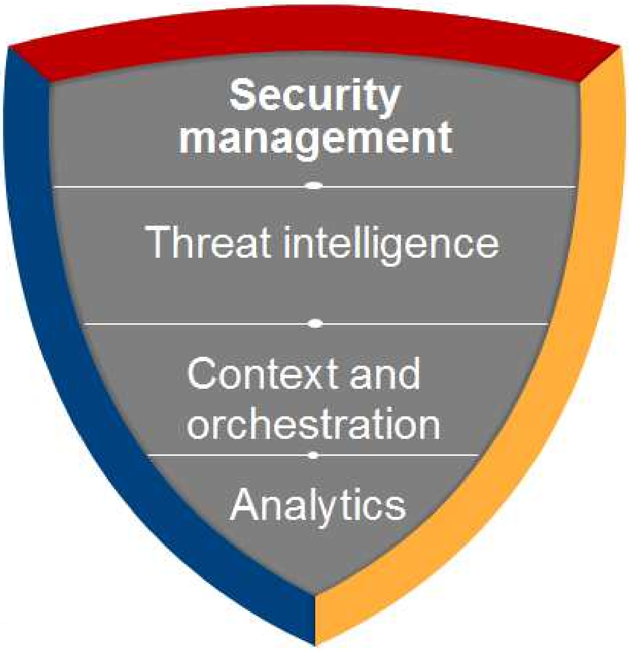
Software components

Our SOC and SIEM monitoring services comprise a blend of architectural components, resource capabilities and support structures.

The Datacentrix SOC monitoring solution involves a number of components. The enterprise security manager (ESM) and the advanced correlation engine (ACE) both reside at the Datacentrix SOC which is manned 24/7/365. The receiver resides onsite in a network segment closest to the customer's operational IT services.

Our SIEM backbone is built on McAfee SIEM to deliver the best-of-breed SECaas SOC services to your company. The SOC delivers expansive business value.

.



The Datacentrix SOC delivers business value:

- Ensures that you know when, where and how your valuable infrastructure is being used and by whom;
- Calculates baseline activity to know what is normal vs. abnormal;
- Rule-based and rule-less correlation detects known and unknown threats;
- Collects and correlates contextual information as intelligence for threat remediation;
- Continuously monitors and identifies threats, and automatically prioritises security events;
- A centralised threat dashboard provides comprehensive visibility and understanding of the threat landscape;
- Accelerates time to response using automated alerts and work flow;
- Correlates event information against threat feeds to enhance internal threat intelligence;
- Optimises threat investigations and forensics by leveraging an advanced indexing system; and
- Delivers actionable information in minutes through an integrated log and event collection, along with real time analytics.

Reporting and meetings

Real-time event escalation and reporting. This is a real-time event escalation service, where any specified event on the devices monitored can be reported on through a specific escalation procedure as specified by the customer.

Daily reports per device type monitored. This is a summary of the monitoring activities for the previous 24 hours, and includes any events escalated, if the contract specifies that events are to be reported.

Weekly reports per device type monitored. This is a summary of the monitoring activities for the previous 7 days, and includes any events escalated, if the contract specifies that events are to be reported. It can be scheduled for any day of the week.

Monthly reports. This report comes standard with any contract and any device monitored. It summarises the events of the past month and also includes current IT security trends and analysis of the environment monitored. It will also include a summary of events reported in the month, if the customer opted to have real-time security event reporting.

Ad hoc reports. These reports are customer-specific and are determined by the contract. The customer determines the frequency of reporting.

Customer meetings. Up to four hours are dedicated to customer meetings per month. More time can be allocated as necessitated by the customer.

INTELLIGENT

Real-time advanced analytics
Automated rule, risk/behavior and statistical correlation

Threat prioritisation
Turns billions of "so what" events into actionable information

ACTIONABLE

Active and customisable dashboards
Makes threat investigation and response easy

High performance data management engine
Fast response to data ingest, analytics and threat investigations

Ease of operation
Hundreds of out-of-the-box rules and reports plus a unified compliance framework

INTEGRATED

Comprehensive security
Broad data collection of devices, including cloud and VM support, plus McAfee Security Connected active integrations enable efficient and effective response

Frequently asked questions

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 with 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 the monitoring of data take up much bandwidth?
Very little bandwidth is used to monitor data. 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.

Wayne Olsen, security business unit manager at Datacentrix

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