datacentrix

INTUITIVE THREAT HUNTING

Endpoint Detection and Response for the entire endpoint estate

Threat hunting

The security landscape is characterised by increasing multi-technique, multi-wave threats that are costing businesses greatly – both financially in terms of remediation, penalties and lost productivity, as well as in reputational damage. These financially motivated cyber criminals breach company networks, possibly residing undiscovered in the network for months.

Datacentrix partners with leading, global security specialists at the highest tier to deliver intuitive threat hunting solutions that equip businesses to easily hunt for threats at scale.

Key benefits

Automated, real-time and proactive threat hunting across the network delivers many advantages, the most prominent being the reduced time to respond to and remediate threats.

- Enjoy a highly visual, user-friendly interface
- Scope the attack by analysing endpoint metadata
- Switch to a real-time and proactive defence strategy
- Increase operational efficiencies
- Collect audit data
- Investigate, identify and remediate from a single pane of glass
- Reduce time and cost spent on investigation to resolution

Advanced managed security services and assessments

The combination of Datacentrix' team of security experts, leading threat hunting technology and comprehensive managed services, stops advanced threats and eliminates compliance issues. The monitoring and response services are delivered uninterrupted, across all platforms, including Windows, MAC, Linux, Virtual, iOS, Android, SaaS, Hybrid, on-premises and API.

Services are available on a consumption basis and as-a-service.

Managed detection and response services
to strengthen security programmes
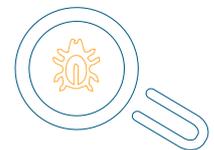
Active threat hunting
that proactively seeks out malicious activity

Incident response services
for the comprehensive resolution of security incidents

Advanced analysis
to solve the most complex security challenges

Cyber posture assessments
that support security hygiene by closing the gaps in threat detection

Compromise assessments
to uncover threats that are already active in the environment

Stop tomorrow's threats today

Next-generation antivirus and superior endpoint prevention
Multi-layer prevention instantly blocks sophisticated malware as well as file-less, and even master-boot-record-based ransomware that stops the threat before files can be encrypted.

Endpoint detection and response (EDR)
Automated threat detection and high-fidelity alerts mitigate security threats and prevent any harm. An advanced remediation toolbox expedites responses to any incident, no matter what the cause, and provides a complete investigation of the incident.

Unified view of malicious operations
The full attack scope is automatically correlated into a single threat package or malicious operation. This provides a unified view of the triggering event, the detection category, the root cause, affected endpoints, related processes, and connections between endpoints.

Artificial intelligence and machine learning
The EDR solution uses advanced behavioural analysis and machine learning techniques to recognise relationships between multiple events, determining whether they are part of a single attack.

Endpoint security analytics
Businesses that integrate threat hunting into the security function's overall workflow can establish a cybersecurity vantage point to challenges like audits, insider threats and validating indicator of compromise (IOCs).

- Gain access to every raw data point collected in real-time with the retention span ranging from 7 to 90 days.
- Query historical data, go back in time to answer questions on historical data, or replay events and achieve a unique level of security and insurance.

"

Considering we operate in an era where sentiments regarding cyber security are not "if" but rather "when" you get hacked, Datacentrix has assisted us in becoming more proactive and responsive regarding this. The advanced managed security solution we have implemented has provided us with a constant flow of information and insight that allows us to proactively make decisions regarding our security posture and any associated risks. It has further allowed us to have a clearer plan regarding our security strategy road map so that we are maximising the benefits from our security investments. **Global travel services provider**
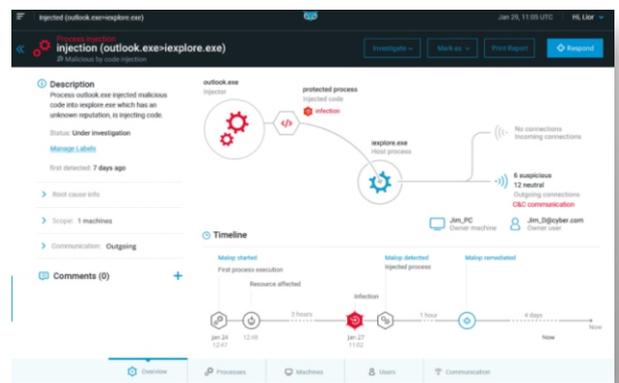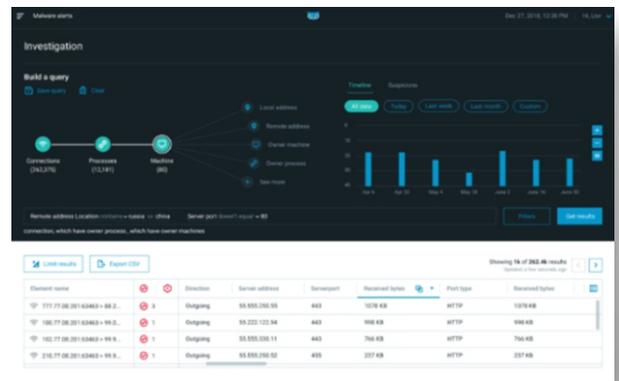
DON'T LEAVE YOUR PROTECTION TO CHANCE

Contact us for a free proof of concept worth R100 per endpoint*

Experience the functionality and ease of use of the data breach assessment and endpoint detection and response solution.

The full version of the solution is utilised during the proof of concept, which takes approximately two to three weeks to complete.

About Datacentrix

Datacentrix enables digitalisation success. The company's specialist teams leverage the combined power of information and communications technologies to advise, connect, transform, improve and future-proof business, supporting customers throughout their digital journey.

Datacentrix offers expert advisory services and deep technical expertise across a mature offering, providing proven execution capability that is endorsed by the world's foremost technology partners. With a strong African footprint, the company is recognised for its agility, in-depth industry knowledge, ethical practices and strong overall performance.

Empowerment and compliance
Datacentrix is a Level One (AAA) B-BBEE Contributor, with 135 percent procurement recognition.

The company and its subsidiaries hold ISO 27001 – Information Security Management System (ISMS); ISO 9001:2015 – Quality Management System; ISO 14001:2015 – Environmental Management System; and OHSAS 18001:2007 – Occupational Health and Safety Management System certifications.

The ISO 27001 certification is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes. It provides a set of standardised requirements for establishing, implementing, operating, monitoring, maintaining and improving information systems management.

Contact
Wayne Olsen, Security Business Unit Manager
wolsen@datacentrix.co.za
087 741 5000

GAUTENG

Corporate office
Corporate Park North
238 Roan Crescent
Old Pretoria Road,
Midrand, 1685
Tel: +27 (0)87 741 5000

Logistics Centre
26 Landsmark Avenue
Kosmosdal
Extension 11
Samrand, Midrand
Tel: +27 (0)12 657 5000

COASTAL

Cape Town office
18 Oxbow Crescent
The Estuaries
Century City
Cape Town, 7441
Tel: +27 (0)21 529 0700

Durban office
Ground Floor, 6 The Terrace
Westway Office Park
Westville
Durban
Tel: +27 (0)31 389 0500

Port Elizabeth office
Southern Life Gardens
Ground Floor, Block B
70 2nd Avenue
Newton Park, Port Elizabeth
Tel: +27 (0)41 391 0200

East London office
8-10 Winkley Street
Chesswood Office Park
1st Floor, Block B, Berea
East London
Tel: +27 (0)43 705 8000

MIDDLE EAST

Dubai office
Unit number F12
DMCC Business Centre
Level 13 AG Tower
Dubai, United Arab Emirates
Tel: +971 (0)565 761 1980

Doha office
Office number 501
Regus Business Centre, Al Muntazah Trading Centre
5th Floor, Building nr 1, Office nr 8, Hiteen Street
Muntazah, Doha, Qatar
Tel: +974 4007 9638

www.datacentrix.co.za