INTUITIVE THREAT HUNTING

Endpoint Detection and Response for the entire endpoint estate

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.

- South Africa has the highest probability of data breach occurrence in 2020, globally
- South Africa has the lowest deployment of automated threat hunting technology for 2020, globally
- 45% of all attacks in South Africa are malicious
- The average dwell time in South Africa is 150+ days
- The average time to containment is 40 to 60 days
- The average incident response cost is in excess of R20 million per incident, excluding business impact, share price, brand, etc.

Source: Ponemon Institute Research, 2018 Cost of a data breach study

Key benefits of threat hunting

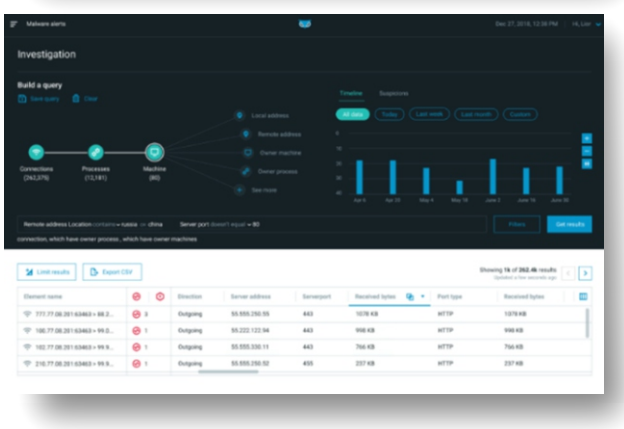
Automated, real-time and proactive threat hunting across the network delivers many advantages, the most prominent being the reduced time to respond to and remediate threats.

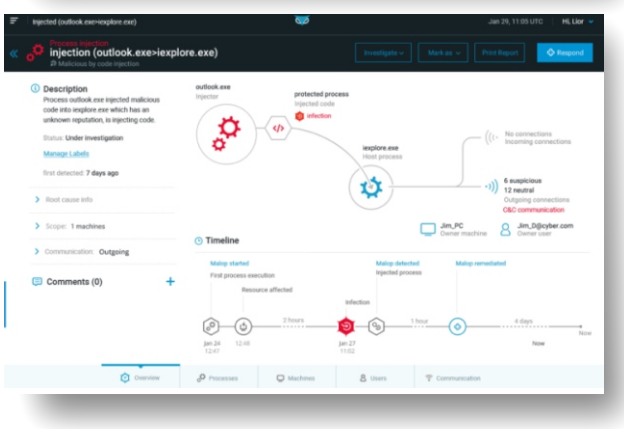
- Enjoy a highly visual, user-friendly interface
- Scope the attack by analysing endpoint metadata
- Switch to a real-time and proactive defence strategy
- Increase operational efficiencies
- Collect audit data
- Investigate, identify and remediate from a single pane of glass
- Reduce time and cost spent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

Customer reference

Cybereason is easy to deploy and run, we are not just using Cybereason as the Bank's EDR solution, there are so many more uses for this tool, from file searches, creating firewall rules based on the connections between servers, checking where AD service accounts are being used, and so much more.
Jaco De Beer, Chief Information Security Officer (CISO) at Bidvest Bank Limited

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.

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.

Consider going hands-off while Datacentrix delivers:

Managed detection and response services
to strengthen your security programme

Active threat hunting
that proactively seeks out malicious activity

Advanced analysis
to solve the most complex security challenges

Incident response services
for the comprehensive resolution of security incidents

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

Customer reference

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.
Herby Seedat, Chief Information Officer at BidTravel

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. * Terms and conditions apply

Click here and we will contact you >>

ABOUT DATACENTRIX

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

Datacentrix offers 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. Find out more at www.datacentrix.co.za.

Empowerment
The company is a Level One (AAA) B-BBEE Contributor, with 135 percent procurement recognition.

The significance of ISO 27001 compliance
Datacentrix holds a PECB Management System Certificate in ISO/IEC 27001:2013. The 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. ISO 27001:2013 provides a set of standardised requirements for an information security management system. The standard adopts a process-based approach for establishing, implementing, operating, monitoring, maintaining and improving information systems management.