REDSCAN
A KROLL BUSINESS

Managed Detection and Response (MDR)

THREATDETECT™

Supplying the capabilities needed to rapidly identify and eliminate the latest cyber threats

Detect and respond to attacks sooner and more effectively

To minimise your organisation's cyber risk, the ability to quickly identify and respond to threats is essential. **ThreatDetect™** is an outcome-focused MDR service that supplies the people, technology and intelligence needed to hunt for threats and eliminate them before they cause damage and disruption.

Why proactive detection is needed

Even with the best preventative security controls in place, your organisation is not immune to breaches. Persistent attackers may eventually find a way to bypass your defences and, without suitable controls in place, could remain undetected for weeks, even months.

However, building a security operations centre (SOC) to identify and respond to threats 24/7 can take years and be extremely costly - requiring not only a range of technologies but a large team of experts to deploy, monitor and optimise them. ThreatDetect addresses these challenges by offering a quick-to-deploy turnkey detection and response capability for a cost-effective subscription.

KEY SERVICE FEATURES

- Experienced SOC experts, working as an extension of your team.
- Our **CyberOps™** Threat Management Platform for unified threat visibility, genuine incident alerting and automated response.
- Behavioural-based network and endpoint detection.
- The latest threat intelligence, including **16.5m+** indicators of compromise (IOCs).
- Hundreds of high-fidelity detections, aligned to the MITRE ATT&CK framework.
- Integrated insights from our red team to continually enhance threat coverage and visibility.
- Dedicated technical account management, regular reviews and service reports.

Business benefits

Broad threat visibility

Obtain unified visibility of security events across on-premises networks, systems, applications and cloud environments.

Continual detection of attacks

As threats evolve, ensure critical assets are protected against emerging threats as well as those that are currently known.

Eases the load on in-house teams

Reduce the workload on your team by outsourcing threat monitoring and analysis to our 24/7 SOC specialists.

Accelerates incident response

Benefit from high-quality remediation guidance and automated response actions to swiftly disrupt and eliminate threats.

Reduces time to maturity

Quickly elevate your security capabilities to a level once only achieved by large enterprises with extensive resources.

Facilitates compliance

Enhance your cyber resilience and demonstrate compliance with requirements of the GDPR, PCI DSS, ISO 27001 and more.

The visibility to detect. The context and actions to respond.

By centralising security visibility and providing context-rich alerts and automated response actions, **ThreatDetect** provides the support needed to respond swiftly and effectively to threats.

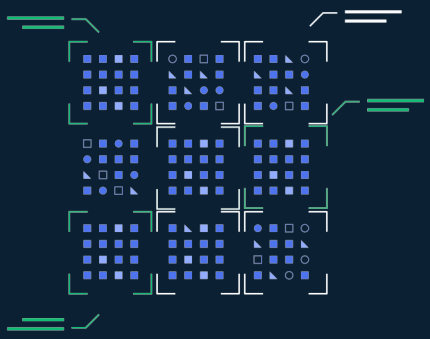
> **Thanks to Redscan we now have a solution that gives us the ability to monitor, isolate and eliminate threats across our IT infrastructure."**
>
> HEAD OF IT

1. Ingestion

Telemetry is collected from across your environment and ingested into our **CyberOps™** platform, where it is analysed and enriched with the latest threat intelligence.

2. Analytics

Detections are correlated and then grouped together by common attributes to create 'cases' – enhancing accuracy and reducing false positives.

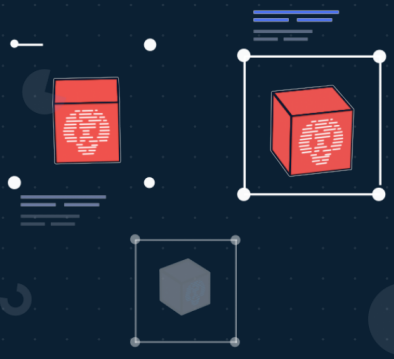


3. Investigation

Hi-fidelity cases are triaged by Redscan's 24/7 SOC experts, and those which require action are raised to your security team as prioritised incidents.

4. Response

Automated actions and detailed remediation guidance are supplied to swiftly disrupt, contain and eliminate threats before they can inflict damage and disruption.



WHY REDSCAN FOR MDR?

- A CREST-accredited UK-based SOC
- Recognised by Gartner and Bloor Research
- 'Great' Net Promoter Score (63)
- An agnostic approach to technology selection

REDSCAN
A KROLL BUSINESS

0800 107 6098 info@redscan.com www.redscan.com