CyberOps is the cloud-native Threat Management Platform we’ve developed to deliver our ThreatDetect™ Managed Detection and Response service.

As the interface between our 24/7 Cyber Security Operations Centre (CSOC) and your in-house team, CyberOps enables us to centrally monitor your environments and deliver the actionable information and automated actions you need to respond to incidents swiftly and effectively.

**Actionable intelligence**

Via this easy-to-use platform, receive:
- Notification of genuine security incidents
- Actionable mitigation guidance
- Automated actions to contain and disrupt threats

**How CyberOps supports the delivery of our MDR service**

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

- **Technology agnostic**
  CyberOps integrates with your existing detection tools as well as any additional technologies included with ThreatDetect.

- **Event enrichment**
  For enhanced detection accuracy and greater context, CyberOps enriches alerts with threat intelligence, including 19m+ IOCs.

- **Automated response actions**
  Incident response pipelines within CyberOps initiate rapid threat containment and disruption, automatically or at the click of a button.

- **Customisable dashboards**
  Dashboards present key security-related information and metrics, helping to improve situational awareness and measure performance improvements.

- **Seamless workflow integration**
  Support for a range of ITSM tools, including ServiceNow and Jira, enables incidents raised via CyberOps to be managed as part of wider IT and security operations.
Extended detection and response (XDR) via a single, technology-agnostic platform

By unifying visibility and supplying context-rich cases for analysis by SOC experts, CyberOps is key to our ThreatDetect MDR service - delivering the outcomes you need to respond to threats, 24/7.

**HOW IT WORKS**

01 **INGESTION**
CyberOps integrates with your underlying detection technology stack to ingest security event data from across your environments. This data is then analysed and enriched with threat intelligence to generate alerts.

02 **ANALYTICS**
Alerts are intelligently grouped by common attributes to create high-fidelity ‘cases’. Cases enhance contextual awareness by providing a more complete view of security incidents and reduce the need for alerts to be triaged individually.

03 **INVESTIGATION**
CyberOps presents cases to Redscan’s 24/7 Security Operations Centre experts for analysis. Cases which are validated as genuine incidents are raised for your security team with accompanying mitigation guidance.

04 **RESPONSE**
CyberOps’ Security Orchestration and Response (SOAR) capabilities accelerate incident response by automating threat containment and disruption in a variety of scenarios. Incident response experts from Kroll are on hand to provide optional remote and on-site support.

**SEAMLESS WORKFLOW INTEGRATION**

**ON-PREMISES AND CLOUD MONITORING**

Network Infrastructure

Endpoints

Applications

Cloud Infrastructure

---

Redscan is a trading name of Redscan Cyber Security Limited. All rights reserved 2021. Company number 09796638.