Managed Extended Detection and Response (XDR)

To keep up with new threats, businesses now require different combinations of detection and response capabilities. SecurityHQ offers XDR with multiple feature options, to ensure an enhanced security posture specific to your needs.

Threatscape

SecurityHQ

Managed Detection & Response (MDR) combines 24/7 Detection, 24/7 Response, SIEM Analytics, SHQ Response App, Designated Service Delivery Manager, with Security Data Analytics and Reporting.

With XDR, receive everything you get with MDR, plus the feature additions that work best for you.

Features include:

User Behaviour Analytics: Identify patterns of usage that indicate malicious or anomalous user behaviour. From launched apps, file access, to network activity, monitor who touched what, when and where an element was accessed, how it was made, and how often.

Network Flow Analytics: View and gain a comprehensive view of your entire network infrastructure, by examining sources, target ports, IP addresses and more.

Benefits

- Essential Cyber-Solutions and Improved SIEM Experience, Combined for Multi-Layer Protection.
- Advanced Threat Prevention & Detection with Comprehensive View of Risks via Real-Time Monitoring and Alerting.
- Compliance Standards Supported.
- Rapid Onboarding with Industry Experts.
- 24/7 Incident Response Supported by GCIH Certified Incident Handlers.
- Cost Saving - No Need to Build Internal SOC Capabilities or Maintain the Required Tools. We have it covered.

Endpoint Detection & Response: Continually monitor endpoints, gain full visibility of your whole IT environment, detect incidents, mediate alerts, stop breaches, and receive instant advice.

Contain-X Connector Threat Containment: IR Security Orchestration Automation and Response (SOAR) for accelerated enrichment, playbooks and threat containment.

Dark Web Monitoring: Monitor the dark, deep, and visible web to detect risks and alert, investigate and take down offensive content.

Bring Your own License: Whichever features work best for you, either apply SecurityHQ's own SentinelOne turnkey solution, or bring your own license and merge the package you want.

XDR Process

Hunt for Threats	Investigate Security Breaches	Collect and Organise Data	Improve Visibility	Speed up Detection and Repsonse Times

Not Sure What You Need? Discuss Feature Options with our Security Analysts.

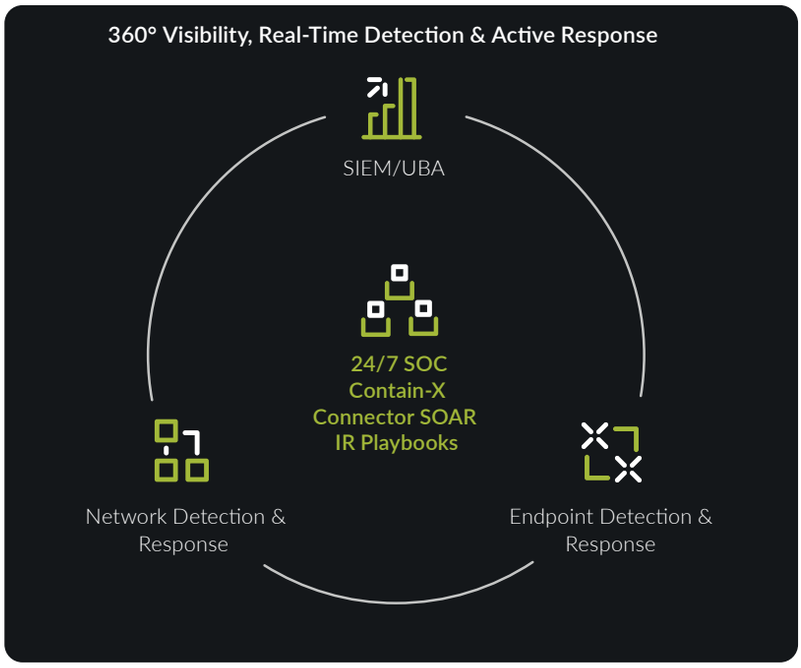
Threatscape

How XDR Works

Combined Network Detection and Response, Endpoint Detection and Response, SIEM, User Behaviour Analytics, and 24/7 SOC capabilities for real-time Detection and Active Response.

Receive 360-degree visibility that is constantly evolving and adapting to your hybrid, multi-cloud, IT environment, across your logs, Endpoint, and network, to increase speed of detection and remediation of both known and unknown threats.

A key discriminator within our XDR service offerings are our expert incident analysts who manage incident response using playbooks driven by advanced orchestration and automation systems. This process contextualises incidents with enriched data, coordinates response workflows, and automates threat containment.



Integration of the Following Value-Added Service Components:

- Machine Learning
- Security Orchestration & Response
- Mitre ATT&CK Tagging
- Access to Over 260 Trained and IBM Certified Analysts and Engineers
- Incident Management Platform
- Security Business Intelligence Reporting
- User Behavioural Analytics
- Commercial Grade Threat Intelligence
- SecurityHQ Response Mobile App
- Extensive Integration with over 500 Log Source Types
- Over 1,500 Preconfigured Use Cases

Threatscape

Service Features

SecurityHQ Response App

The power of the SOC in the user's hands, interaction, and collaboration has never been easier. Now available on Android and IOS, XDR features are convenient, easy to use, and save valuable time.

Designated Service Delivery Manager

Weekly security operation meetings, led by Senior Analysts, to illumuate risks, incidents, and security posture enhancements.

24/7 Threat Detection

24/7 monitoring and identification of threats, anomalies and policy violations with analyst-driven investigations.

24/7 Threat Response

24/7 Threat Containment and Triage with Incident Management and Orchestration.

SIEM Analytics

Powered by the most Powerful SIEM, with customer user access.

Data Analytics & Reporting

Daily, weekly and monthly reports with granular statistical graphing. Business intelligence visualisations to present risks, posture issues and pattern user violations.

SLA Management

15-minute response for critical incidents, with real-time SLA dashboards.

SOAR

Security Orchestration Automation & Response for accelerated enrichment, playbooks and threat containment.

Log Management

1-year log archiving, with extended log archiving available on request.

Security Use Cases

Unlimited security use case consulting and rule creation.

Global SOCs

Global SOCs based in the UK, Middle East, Americas, India, and Australia ensure a global view.

Certified Analysts

Powered by IBM QRadar, IBM Resilient and our Incident Management & Analytics Platform.

Common Customer Challenges and How We Solve Them

A lack of **Visibility** and awareness.	By visualising risky behaviour and misconfigurations, target the threat at its source, for **Complete Visibility & Peace of Mind.**
Cost and **Risk Reduction.**	Likelihood of a breach is reduced & 24/7 Detect & Response delivered at a fraction of the cost of DIY.
Peace of mind... **Assurance.**	The Capacity and Capability to deliver bespoke services at scale, via combined threat intelligence and human expertise.
A need for **Rapid Response.**	Incident Response playbooks, SOAR platform, and Certified Incident Handlers to contain threats and watch your back!
A **Partner** to depend on.	A partnership that works as an Extension of Your Team, to expose patterns of illicit behaviour and reduce risks.

How Does SecurityHQ Differ?

SecurityHQ is a Global MSSP, that detects, and responds to threats, instantly. As your security partner, we alert and act on threats for you. Gain access to an army of analysts that work with you, as an extension of your team, 24/7, 365 days a year. Receive tailored advice and full visibility to ensure peace of mind, with our Global Security Operation Centres, and utilize our award-winning security solutions, knowledge, people, and process capabilities, to accelerate business and reduce risk and overall security costs.

Threatscape

Why Choose Threatscape

We are the trusted security partner of enterprise clients who rely on us to secure critical IT assets in over 100 countries around the world. We are one of very few dedicated cyber security companies with a separate Microsoft Security Practice, and our expertise in this space is re¬flected in our status as a Microsoft Security Gold Partner and the Global Microsoft Security & Compliance Partner of the Year 2020/21.

Contact us

Email Address
info@threatscape.com

Call Us
Dublin: 01 901 7000
London: 0203 653 0000