eSENTIRE

Managed Detection and Response

Cloud adoption, business applications and remote users continue to expand at exponential rates. Your cybersecurity team is fighting a losing battle to keep pace with your business requirements and growing attack surface. While traditional security controls and MSSPs were once effective, they are no match for the growing speed and sophistication of modern threats.

How it works

We support your cyber program with a combination of cutting-edge machine learning XDR technology, threat hunting expertise and security operations leadership to mitigate your business risk, enable security at scale and drive your cyber program forward.

Multi-Signal MDR

At eSentire we believe a multi-signal approach is paramount to protecting your complete attack surface. We ingest network, endpoint, log, cloud, insider and vulnerability data to enable complete attack surface visibility, and drive deeper investigations, in order to strengthen the speed and completeness of our response capability. We correlate indicators of compromise and early detections between multiple signals, and our 24/7 SOC Analysts and Elite Threat Hunters quickly investigate, contain, and enforce response actions against advanced persistent threats that bypass traditional security measures.

- Network - Defend brute force attacks, active intrusions and unauthorised scans
- Endpoint - Protect assets from ransomware, trojans, rootkits and more
- Log - Intelligence and visibility across AWS, O365, GCP, DevOps and more

- Cloud - Configuration escalations, policy & posture management
- Insider Threat - Detects malicious insider behaviour leveraging Machine Learning models

Whether your environment is in the cloud, on-premises or somewhere in between we have the visibility to see what other MDR providers will miss.

Multi-Signal Ingestion

Gain full threat visibility, deep correlation and investigation capabilities, strengthening our time to contain and complete response.

24/7 Threat Hunting

Zero-Trust approach to hunt elusive attackers. Proactive and automated blocks of malicious intent plus 24/7 Elite Threat Hunting support.

Atlas XDR Cloud Platform

Rapid detection and automated threat disruption at scale. Delivers Security Network Effects to harden your defences with every detection globally.

Rapid, Robust Response

Minimise attacker dwell time with Mean Time to Contain of 15 minutes. We disrupt, isolate and contain threats before they impact your business operations.

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organisations in 75+ countries, across 35 industries, from known and unknown cyber threats. Team eSentire's mission is to hunt, investigate and stop cyber threats before they become business disrupting events.

Contact Brigantia

Suite 2.1, Hurstwood Business Centre, York Road, Thirsk, YO7 3BX

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com