BYTES | Smarter together

Powered by SecurityHQ

MANAGED DETECTION & RESPONSE (MDR)

Powered by real-time log analytics, with security orchestration automation & response tooling, SecurityHQ's MDR service rapidly identifies & limits the impact of security threats.

Key Features

24/7 Threat Monitoring

Cybercrime is evolving, which means issues with solutions, including people, processes & technology, are prominent. SecurityHQ provides round-the-clock monitoring to detect, investigate, notify & respond to incidents & potential threats.

Incident Response, Orchestration & Automation

We support incident response using playbooks driven by advanced orchestration & automation systems (IBM Resilient). This process rapidly contextualises incidents with enriched data, orchestrates response workflows, & automates threat containment.

Advanced Security Analytics

SecurityHQ uses IBM QRadar to power our Threat Analytics & Correlation Engine. The scale & sophistication of QRadar is second to none.

Benefits

- **24/7 Detection of threats** powered by real-time analytics & IBM QRadar.
- **24/7 Incident response** supported by GCIH certified incident handlers.
- **Advanced Correlation & ML** to detect complex threats.
- **Incident Containment & Triage** Contain threats via incident playbooks & SOAR platform. Automate containment response to block threats.
- **Cloud Native:** Azure, AWS, Office365, Oracle Cloud & more.
- **Reduced Cost & Complexity** & up/ downscale effortlessly.
- **Improved Speed** of detection & response. SLA provides detection, analysis & notification within 15 minutes (critical events).
- **Feel empowered with 200+ Security Analysts** on demand.
- **Bespoke packages** & advanced modules.

Service Overview

01. Data Collection

- Syslog
- Cloud API
- Agentless Windows
- Apps & Database

02. Data Processing

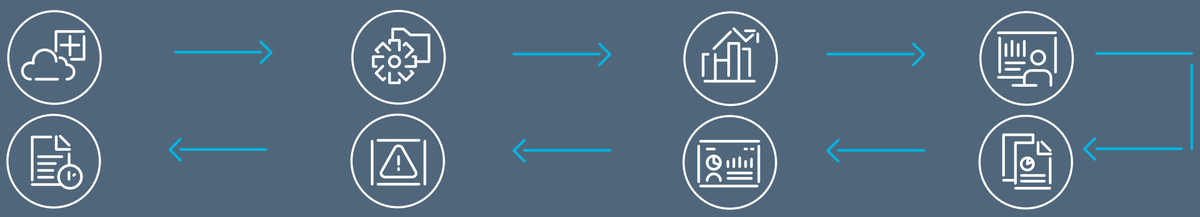
- QRadar SIEM analyses & correlates data
- Identifies risky user behaviour (UBA)
- Contextualise Intelligence

03. Advanced Analytics

- User behaviour analytics
- Business service risk profiling
- Anomaly + behavior algorithms

04. Analyst Detect & Respond

- 200 + SOC analysts detect, investigate and respond to anomalous activity
- 24/7 detection & response
- Eliminates false positives



08. Log Management & Compliance

- Secure log storage (1 yr)
- ISO 27001, PCI DSS, GDPR, NIST Compliance reporting

07. Threat Containment

- Mitigating risk with automatic containment
- Block malicious IPs
- Suspend rogue users
- Isolate infected machines

06. Incident Management & Analytics Platform

- Efficient incident management platform
- Orchestrate incident response, service request and SLA monitoring
- Improve quality and context for incident response

05. Business intelligence and reporting

- Data driven documents created using BI tooling
- Rich analytical reports to identify risk and enhance posture

Contact us at
tellmemore@bytes.co.uk

For more details visit
www.bytes.co.uk

Top 4 Customer Challenges

Incident Response Capability

The Problem

Security incidents do, and will, occur. Post detection, a rapid response is critical to contain and investigate rogue activity 24/7.

Solution

SecurityHQ provides Incident Response playbooks, supported with our IBM Resilient SOAR platform & Certified Incident Handlers to contain threats.

Defend Unlimited Threats with a Limited Budget

The Problem

SOC detection tools, and the analysts used to drive them, are costly. Building a defensive SOC capability inhouse is beyond the budget of most organisations.

Solution

Our SOC services provide world-class tools and skills, at a fraction of the price it would cost to build a Security Operation Centre inhouse.

Risk Reporting & Business Security Intelligence

The Problem

36% of breaches are the result of errors and/or misuse of systems. Risky assets, users and behaviour needs to be presented graphically and within a business context.

Solution

By visualising risky behaviour and misconfigurations, we target the threat at its source. Our customers receive detailed weekly reports with granular statistical analysis to illuminate risky behaviour, security posture issues and security incident metrics.

Complex & Evasive threat Detection

The Problem

Organisations struggle with the rapid identification of malicious behaviour. This identification requires a matured SIEM, with advanced correlation, anomaly and user behaviour analysis, together with continuous monitoring.

Solution

SecurityHQ applies advanced correlation & machine learning to expose patterns of illicit behaviour. SOC immediately investigates the extent of an event, and its context, to derive a complete analysis with mitigation and risk quantification.

Service Features

Threat Detection

24/7 monitoring and identification of threat, anomalies and policy violation with analyst driven investigations.

Weekly Meetings

Weekly security operations meetings, led by Senior Analysts, to illuminate risks, incidents and security posture enhancements.

SIEM Technology

Analytics powered by IBM QRadar, the world's most powerful SIEM with customer user access.

SLA Management

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

Log Management

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

Threat Intelligence

We ingest and correlate rich intel from IBM XForce, Virus Total, Domain Tools and more.

Global SOCs

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

Threat Response

24/7 threat containment and triage with incident management and orchestration powered by IBM Resilient.

Incident Management & Analytics Platform

Incident Management & collaboration platform for dashboarding, SLA Management, ticketing & customer ITSM integration.

Reporting

Daily, weekly and monthly reports with granular statistical graphing.

Business Intelligence Analytics & Visualisation

Business intelligence visualisations to present risks, posture issues and pattern user violations..

Security Use Cases

Unlimited security use case consulting and rule creation.

SOAR

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

Certified Analysts

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

How Does SecurityHQ Differ?

Founded over 15 years ago, SecurityHQ prides itself on its global reputation as an advanced MSSP, delivering superior engineering-led solutions to over 150 clients, around the world. We learn about what our clients do, speak their language, understand what systems/processes they have, and provide tailored solutions and improvements, backed by a team of professionals, to ensure complete resiliency against cyber threats.

Our mission is to provide world-class security operations to our clients and partners, to integrate processes seamlessly, and act as an extension of our user's own teams. The result is a bespoke service that seeks to address the users specific risks and challenges, that empowers their cyber safety.

Bespoke

Every customer is different. Your risks, industries, geolocations, regulatory requirements and processes demand a bespoke response. SecurityHQ customises your services, based on your requirements.

Business Intelligence

SecurityHQ relates all incidents to CIA impact against your systems, data and users.

Integrity & Transparency

SecurityHQ builds relationships on trust, built on a foundation of complete transparency in our operational delivery.

Incredible People

Our analysts are some of the most experienced and qualified in the industry.

Incident Management Platform

Collaboration is critical for effective security operations. SecurityHQ's Incident Management Platform is an arena for incident workflows, SLA management, data visualisation and documentary repository.

World's Best Technology

We only use Gartner Magic Quadrant technology, such as IBM QRadar, Resilient, X-Force.

Global Reach

SecurityHQ operates 6 Security Operation Centres globally and has unrivalled regional expertise with international oversight.

Personalised Service

Clients receive dedicated Service Managers and Senior Analysts who are available 24/7, every day of the year.

Have a question? We would love to hear from you.

Reach us

tellmemore@bytes.co.uk | 01372 418 500

bytes.co.uk/security

Follow us

f in 🐦