SecurityHQ | pylones*

Managed Detection and 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 280+ Security Analysts** on demand.
- **Bespoke packages** & advanced modules.

Service Overview

01. Data Collection

- Business Assets Profiling: High, Medium, Low
- Integration: Event Collector(s) and IP-Sec site-to-site VPN
- Log collection: Cloud API, Agentless Windows, Apps & Database

02. Data Processing & Event Analytics

- Data Enrichment: Business and Threat Intel Context
- Data Retention: SecurityHQ Tier-3 Certified SOC
- Correlation Analytics: Real-time enriched events correlation for threat detection

03. Behavioral Analytics (ML & AI)

- Machine-Learning and AI: User Behavior Analytics
- Risk Profiling: User and Business
- Advanced Threats: Un-known Insider Threat Detection

04. Detection & Investigation

- 280+ SOC (L1-L4) analysts: 24/7 SOC Monitoring
- SOC Actions: Detect >Triage > Investigate > Respond

05. Proactive Threat Hunting

- Detect APT's & Zero-day: Threat Advisories, ML and manually spotting identity & protocol anomalies
- Use-cases improvement: Incorporate discovered signature/signatureless IOCs into use-cases

06. Incident Management

- SecurityHQ Platform: Security Posture, Risk Level and Asset Management
- On-Demand Access: 280+ Analysts, Interact with the SOC
- Automation: Orchestrate Incident Response, Service Request and SLA Monitoring

07. IR SOAR Playbooks

- Focus on complex threats: Automate response to repeated/targeted attacks.
- Automated kill-switch: Disrupt a malware outbreak
- Playbook Actions:
  - Block Malicious IPs
  - Suspend Rogue Users
  - Isolate Infected Machines

08. Security Data Analytics

- Powerful Business Reporting: Weekly and Executive Reporting using Qlik BI
- Digital Risk: Rich Analytical Reports to Identify Risk and Enhance Posture
- Proactive Threat Advisories

09. Weekly SecOps Workshops

- SOC meeting: Weekly with SDM & L3 Analyst
- Digital Risk: Rich Analytical Reports to Identify Risk and Enhance Posture
- Service Evolution: Establish a consultative-led approach for maturing security posture

10. Security Compliance

- Business Assets Profiling: High, Forensics: Secure Log Storage (Min. 1-Year)
- Regularity & Compliance: ISO 27001, PCI DSS, GDPR, NIST Compliance Reporting

Contact us at
info@pylones.gr

For more details visit
www.pylones.gr

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.

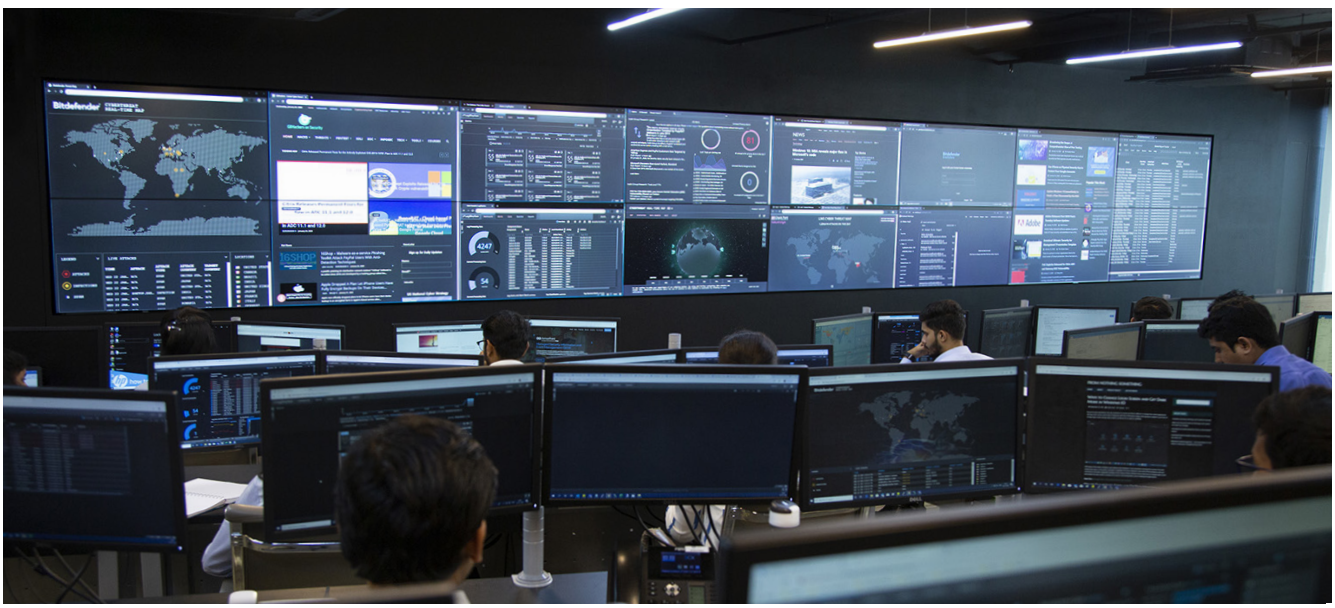
Complex & Evasive threat Detection

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.

Threat Response

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

Weekly Meetings

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

Incident Management & Analytics Platform

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

SIEM Technology

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

Reporting

Daily, weekly and monthly reports with granular statistical graphing.

SLA Management

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

Business Intelligence Analytics & Visualisation

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

Log Management

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

Security Use Cases

Unlimited security use case consulting and rule creation.

Threat Intelligence

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

SOAR

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

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

Challenges	Our Solutions
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?

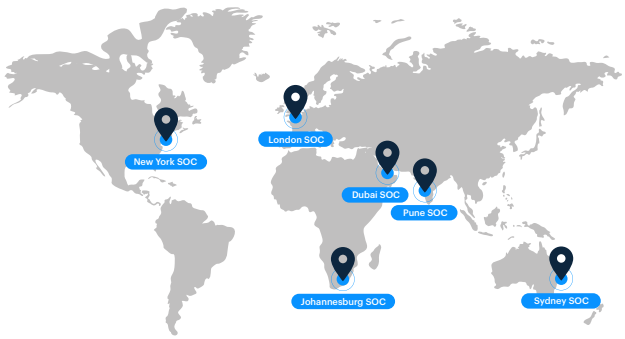
SecurityHQ is a Global MSSP, that detects, and responds to threats, instantly. As your security partner, we alert and act on threats for you. Gain access to an army of analysts that work with you, as an extension of your team, 24/7, 365 days a year. Receive tailored advice and full visibility to ensure 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.

About Pylones

Pylones Hellas is a leading company in the Greek ITC market. Since its establishment in 1997, Pylones has strategically focused on meeting the needs of modernizing private sector infrastructure. Moving steadily and carefully, the company succeeded in forming one of the largest Information Technology, Communications and Security Systems Integrators in Greece. Having completed two decades of successful operation with constant evolution, Pylones today has the required knowledge and experience to provide its customers with integrated technology solutions with high added value.

Have a question?

We would love to hear from you.



Pylones

phone +30 210 7483700

email info@pylones.gr

website www.pylones.gr

SecurityHQ