

Digital Risk & Threat Monitoring

SecurityHQ's Digital Risk & Threat Monitoring identifies attacks, breached corporate material, credentials, intellectual property and brand infringement by harvesting data available on the visible, dark, and deep web.

Our Security Operations Centre together with DigitalShadows monitors the entire web to detect digital risks, alert, investigate and even take down offending content.

Key Features

Coverage

With tooling powered by Digital Shadows, the customer specific threat intelligence is then gathered by examining over 100,000,000 domains, including TOR, I2P, forums, social sites, paste sites, IRC traffic, cloud-based file sharing sites and other points of compromise across a multi-lingual and global environment.

Relevance

Our team analyses the data to Identify relevant threat actors & vectors targeting your organisation, correlate your vulnerable data with attack methodologies, and understand your digital footprint from your attacker's view. In short, we make the data relevant and actionable!

Take Down

Where possible, content which violates your identity is acted upon with a 'Take Down' of the content or site.

Benefits

- **24/7 Monitoring of your Digital Footprint**
- **Identify Threats:** Credentials, breach indicators and IOC's detection to neutralise the threat.
- **Protect your brand** by pursuing direct attacks to specific sectors and utilise campaign tracking.
- **VIP Targeting:** Your VIP's will be targeted, monitor exploits against them.
- **Actionable Intelligence:** Measure and track your company's digital risk and attack surface at any time.
- **Malware IOC's:** Target malware linked to specific industries. Block IP's on Firewalls. Block phishing URL's on proxy, and more.
- **Discover breaches before your adversaries:** Speed of response is essential to discover and respond to breached corporate data.
- **Digital Shadows:** Best available digital risk and threat platform. Leader in the Forrester Wave.

Monitor Deep Dark and Open Web



01.

Configure

Identify Key Assets

- Online Infrastructure
- Intellectual Property
- Company Domains



02.

Collect

Monitor for Exposure



03.

Contextualise

Threat Intelligence



04.

Mitigate

Take Action & Protect

- SearchLight Portal
- Automation and Orchestration
- Ticketing Platform or SIEM
- Threat Intelligence Platform
- GRC Platform

Why We Use Digital Shadows

Digital Shadows is the market leading Digital Risk solution that provides unrivalled coverage and expertise. The service includes access to ShadowSearch, a powerful and easy-to-use search engine, that combines structured technical data with content from the open, deep and dark web. The powerful syntax and configurable alerts enable you to quickly investigate security incidents and identify adversaries targeting your business, brand and reputation.

Included Modules

SecurityHQ configures, orchestrates, and provides access to our MSSP, to perform real-time monitoring and investigations against configured digital assets. The following modules are included.



SearchLight Core

- Employee Credentials
- Impersonating Domain
- Certificate Weaknesses
- Grey Labelled Platform

Pricing based on number of employees as end customer



Data Loss Detection

- Marked Documents

- Technical Data Loss
- Customer Data



Online Brand Security

- Mobile Apps
- Social Media

- Breaches



Attack Surface Reduction

- Vulnerabilities
- Open Ports

- Misconfigured Devices

Configuration

Once you have decided on your module/modules, SecurityHQ team consults with the client, to configure the monitored assets. Assets include domain names, VIP, credit card BIN'S and more.



Brand



Domain Name



Code Snippets and identification



Document Markings



Twitter Handles



Facebook Page



IP Ranges



Server Name and Format



BINs



DLP Identification



VIP Name



Instagram Page

Collect

Once configured, Digital Shadows SearchLight monitors and records mentions and hits against assets, by monitoring across open, deep and dark web



Technical Sources



Documents



Surface Web



Deep & Dark Web

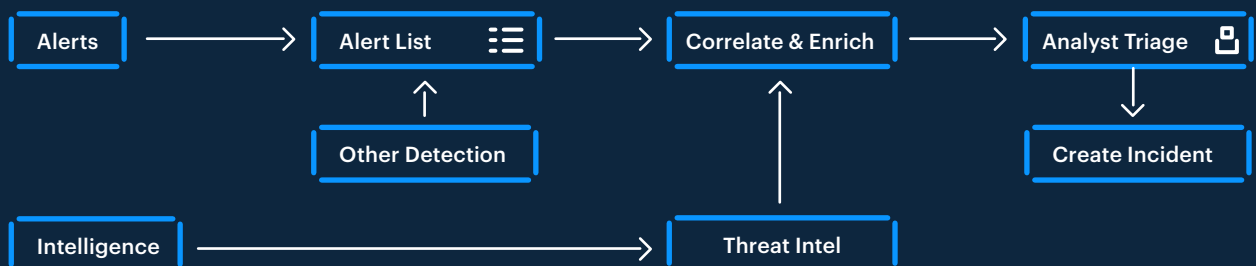
Monitor & Analyse

Using Digital Shadows SearchLight, detect and catagorise incidents and threats into a relative risk score, timeline and correlate the activity to threat intelligence, domain information and the matched assets

digital shadows

IBM Q Radar

Search Light



Intelligence Briefs

Our briefs provide technical indicators which customers may ingest into their own tools to build defensive tactics to block or monitor attackers. This includes IP addresses, hashes, vulnerabilities, domains, threat actor groups and malware, to provide threat analysts instant context into relevant threats. All intelligence is provided with a risk scoring, based on evidence, to enable prioritisation.

Service Features



Instant Visibility

Achieve immediate transparency of all your systems and processes.



Easily Integrated

Our services are simple to deploy and easy to integrate within your systems.



Low Maintenance

Once integrated, we do the work. Leave it to our professional team to manage your security.



Fast-track Investigations

Based on indexing customer URL's, domains, VIP's, IP's, and assets.



Weekly Meetings

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



Incident Management & Collaboration Platform

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



Direct Threat Monitoring

Focus on threats that are specific to your industry and business.



Global SOC's

Global SOC's ensure an all-encompassing world view of threats.



Certified Analysts

Powered by IBM QRadar, IBM Resilient and SecurityHQ.



Security Use Cases

Unlimited security use cases consulting and rule creation.



Effective Remediation

Don't just find the problem, remedy issues quickly and effectively to reduce future threats.



SLA Management

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

About Datrrix

Established over 25 years ago, digital transformation is the driving force behind the evolution of Datrrix services and solutions. Our professional and technical services teams adopt a consultative, client-centric approach that sees us design, build and manage superior solutions. Our critical networking, communications and cyber security solutions are the preferred choice for the nation's key institutions, as well as public and private sector organisations seeking to address the business challenges of compliance, performance, availability and affordability.

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

Reach us

enquiries@datrrix.co.uk | +44 (0)20 7749 0800

Follow us

f in t