digi BUSINESSMONITORING

The all-in-one

Cyber Risk Management

platform from Digimune.

digimune.com

LIVE FREE

Businesses struggle with cyber security:

60% of SME's go out of business within 6 months of suffering a cyber attack.

Phishing, ransomware, malware and Business Email Compromise (BEC) result in significant financial losses and weeks of business interruption.

Mid-market, micro SME's and sole traders lack the time, expertise and budget to deploy best-in-class protection for their businesses.

digi BUSINESSMONITORING

Cyber Security for any business

An all-in-one cyber risk management designed to take the guesswork out of managing your company's digital risks.

- No agents to install, cloud-based SaaS platform.
- No technical knowledge required to get started, register in 2 minutes.

LIVE FREE

digi BUSINESSMONITORING

Use Cases

01

Discover Your Cyber Risk Profile:
All companies are at risk – especially those that think “a breach will never happen to us”.

02

Drastically Reduce Response Times:
Find out how hackers are targeting you so you can act faster.

03

Prevent Data Breaches:
Monitoring for leaked data, vulnerabilities and hacker activity combined with training and education.

04

Protect Revenue:
Protect your valuable contracts with government, banking, critical infrastructure or other large clients

Dark Web Monitor

Our **Dark Web Monitor** gathers leaked data records from over 350 websites cyber criminals use to trade data.

- Credentials
- Credit Cards
- ID information
- Addresses, phone numbers, mothers maiden names, etc.

digi BUSINESSMONITORING

Dark Web Monitoring detail

Languages

We have a presence in cyber criminal communities that operate in the following languages: *Russian, English, Turkish, German, Indonesian, Arabic, Danish, French, Malay, Polish, Portuguese, Spanish, Chinese, French, Italian, Vietnamese, Serbian, Bulgarian, Croatian, Malay, Greek.*

Records

Over 16 billion recovered data records, 30+ billion entities. Email addresses, passwords (hash/clear text), physical addresses, phone numbers, secondary identifiers (mothers maiden name, date of birth, answers to security).

Coverage

- Surface, Deep & Dark Web
- 393 monitored communities
- Over 3,000 breaches recovered.

LIVE FREE

digi BUSINESSMONITORING

Training

Our **Training** module provides a Cyber Security Score to every staff member and tells them how to improve their score. Our score is based on the following indicators:

- Training material completion
- Leaked data records
- Phishing simulation interaction

digi BUSINESSMONITORING

Training detail

Subjects

Good password practices, secure use of BYOD devices, incident reporting, secure use of cloud services, learning to spot phishing and more.

Tracking Score

Our training score is based on the user's risk profile and the completion of their training material. The user risk profile is derived from: awareness training knowledge, interaction with simulated phishing emails, amount of leaked data records.

Completion Tracking

All users have their completion rates tracked and made visible to the company administrator.

Staff Training Dashboard

Our **Staff Training Dashboard** provides a single view to all of the risk issues the employee needs to address.

- View training material
- Review records found in data breaches

Phishing Simulator

Our **Phishing Simulator** sends out our templated phishing emails to engage your staff in the cyber security education process.

- Monthly phishing emails
- New templates always being added

Phishing detail

Templates

Paypal payments, social network invitations, *Fedex delivery notifications, Office 365 login, Google Drive login*, many more.

Campaign

A fixed campaign runs for each business. Templates are sent monthly with new templates added over time. Start/pause campaign functionality.

Tracking

All users have their open and click rates tracked and fed back to the administrative user. Clicks also impact the user's training score.

Hack Monitor

Our **Hack Monitor** scans 100,000s of datapoints to look for indicators of your company being compromised.

- Phishing sites
- Hacker mentions
- Blacklist monitoring
- Breached companies

digi BUSINESSMONITORING

Hack Monitor detail

Coverage

Phishing sites, blacklists, data breaches, hacker mentions. Data feeds ingested as soon as possible from hourly to daily.

Alerting

Real time alerting via email when a match is found.

Further Detail

Further detail on alerts can be provided by our support team including. Screenshots out of hacker forums where the company was mentioned, alias of hacker involved, history of their activities.

LIVE FREE

Asset Monitor

Our **Asset Monitor** keeps track of your external facing assets and services.

- Domains
- IP addresses
- Staff email addresses

Vulnerability Monitor

Our **Vulnerability Monitor** scans your external infrastructure to look for weaknesses that hackers can exploit.

- Alerts ranked from very low to critical
- Remedial actions
- Discovery date
- CVE identification

digi BUSINESSMONITORING

Vulnerability Monitor detail

Coverage

Infrastructure vulnerabilities (web server, database, SSH, etc.) Misconfigured databases (Mongo DB, Elastic Search, etc.) Presence of Web Application Firewall Presence of malware on website.

Monitored Assets

Domains & their sub domains IP addresses.

Remediation

Full remediation instructions available in CVE descriptions.

digi BUSINESSMONITORING

Customer Support

Digimune offers **Customer Support** during office hours that include:

- Customer Onboarding
- Account Activation
- Product Configuration
- Any Product Related Enquiries

LIVE FREE

digimune
LIVE FREE

Contact
General enquiries: connect@digimunegroup.com
Support: support@digimunegroup.com
Claims: claims@digimunegroup.com
Sales: sales@digimunegroup.com