ThreatMon
Under Cyber Wings

DATASHEET

One Platform

for all intelligence needs.

www.threatmon.io

One Platform
for all intelligence needs.

Holistic Intelligence

ThreatMon Holistic Intelligence integrates actionable insights from both the Dark and Surface Web, providing a comprehensive defense against emerging threats.

Proactive Security

ThreatMon enables businesses to anticipate and counteract potential cyber threats before they can cause harm, ensuring robust protection through continuous monitoring and early detection.

Scalable for Your Business

ThreatMon's End-to-end Intelligence is priced according to the size of your business.

Effortless Operation

ThreatMon is easier to operate, a smart solution designed to boost the efficiency of your security professionals.

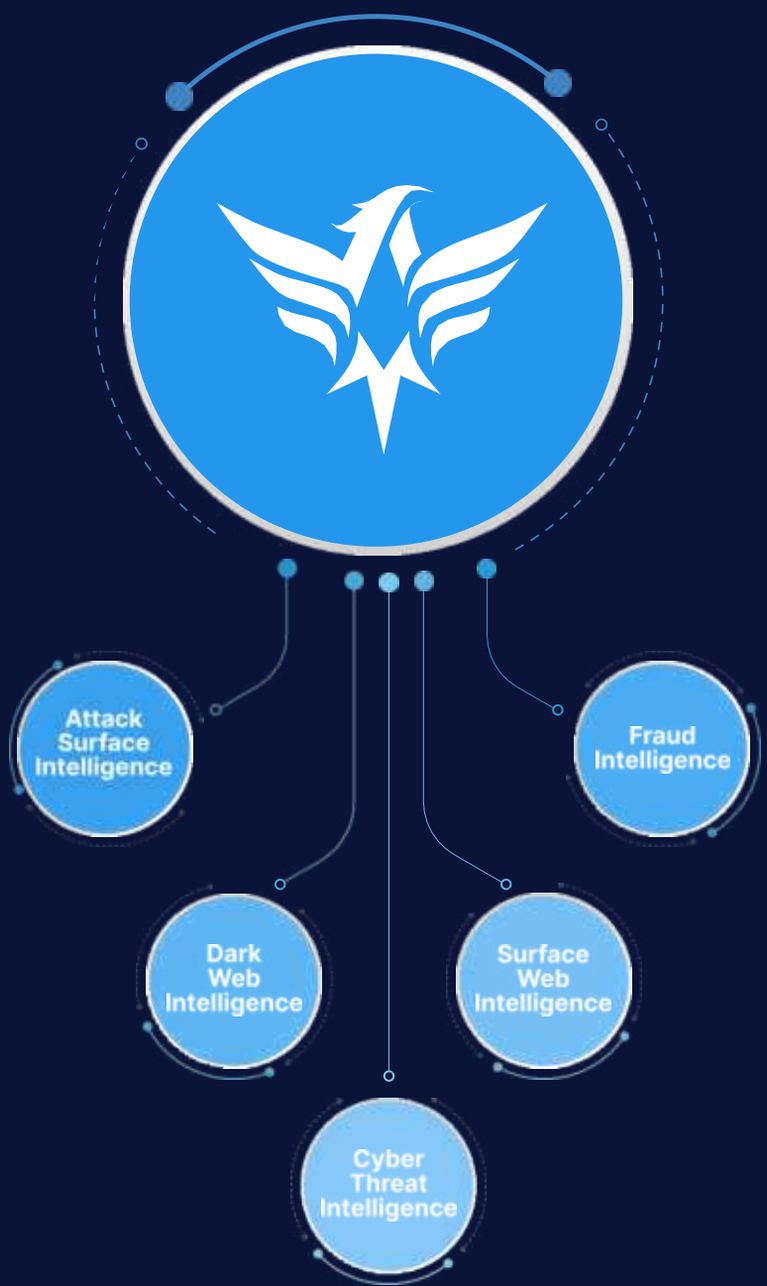
The ever-changing threat landscape evolves into a more fast-paced environment where threat actors collaborate the most, causing threats to emerge and harm much faster.

Today, it is proven that Businesses of all sizes may suffer from the agility of threat actors.

ThreatMon End-to-end Intelligence is designed to be your shield against threats lurking from the **Darfi Web**. It provides security by continuously gathering and contextualizing intelligence from the Dark and Surface Web, tracking indicators of threat actor activity to ensure a constant awareness of threats.

This Holistic approach enables a scaleable G democratized cybersecurity concept that brilliantly countermeasures threat actors. Furthermore, this smart solution improves your team's efficiency by facilitating routine security tasks, making your security team able to respond more in less time.

THREATMON
END-to-END INTELLIGENCE



Takedown Services

API G Integration

Threatmon AI

24/7 Analyst Support

ThreatMon End-to-End Intelligence consists of multiple modules that enable businesses to obtain collectively exhaustive threat intelligence.

Attacfi Surface Intelligence

See the weakest chain on your attack surface, from the threat actor's eye

Attack Surface Intelligence (ASI) is the first step to building your vigilant eye This module scans your external surface starting from your website detecting and mapping all your externally faced web assets.

The module delivers real-time intelligence from your external facing attack surface to alert you in case of vulnerabilities on your attack surface. Remember, this is how you are seen from the threat actors' eyes.

Asset Discovery G Monitoring

Detecting all external faced assets is key to maintaining awareness of them. Therefore, asset discovery is the most essential step in Attack Surface Intelligence. ThreatMon automatically detects & maps external assets. Once an asset is detected, it is continuously monitored.

Asset Discovery & Monitoring service,

- Discovers your external assets
- Thoroughly gathers and supplies critical information for remaining services
- Maintains continuous searches to increase awareness of external assets

Security Misconfiguration

Some vulnerabilities may occur due to human factors such as misconfigured assets. Security Misconfiguration continuously scans various potential vulnerabilities caused by misconfigurations.

Security Misconfiguration service is responsible for

- Continuously check for all potential misconfigurations on your attack surface may compromise your security

Vulnerability Management

Once your assets are detected, ThreatMon identifies what technologies your business uses. Then, continuously monitors for all relevant vulnerabilities in its broad library continuously updated by in-house security experts.

Vulnerability Management service is responsible for

- Identifies which technologies are connected with your attack surface
- ThreatMon continuously checks for vulnerabilities, cleverly tailoring its assessments to the specific technologies your business uses to evaluate their security.

Continuous Web Pentest

ThreatMon conducts pentests at regular intervals, identifying vulnerabilities and determining if they have been exploited, and then updates its assessments based on this information.

Fraud Intelligence

Don’t let Fraud slip in between you and your customer

Increasing your awareness of the entities that may be subjected to fraud is key to detecting certain threats and eventually building your impenetrable customer trust. How? Enriching Threat intelligence with Fraud Intelligence which is gathered in similar methods in various places which are vital for your business.

Fraud Intelligence monitors both the surface and dark web under five distinctive services to detect frauds that may harm your business without compromising your security. Below these five services are explained.

Social Media Monitoring

Social media is becoming integrated into both lives and businesses too. Detecting frauds such as impersonating accounts or suspicious posts targeting you is becoming more important. ThreatMon monitors social media platforms, Twitter, LinkedIn, Facebook, Instagram and Youtube

Reputation Monitoring

ThreatMon checks regularly to detect all black-listed; IP addresses, Mail servers, Websites, Domains, Company assets and Company-related malware activity.

Mobile App Monitoring

ThreatMon monitors the web to detect any rouge mobile application that may lead to fraud.

Phishing Monitoring

Despite their simplicity, phishing attacks remain one of the most preferred and efficient methods used by threat actors.

ThreatMon monitors continuously to detect any website and mail domain that is prone to be used in a phishing attack.

Credit Card Monitoring

ThreatMon operates through a system that tracks stolen credit card information available for sale on dark web black markets, from the BIN numbers. With this approach, you can proactively detect security vulnerabilities by monitoring stolen credit card details along with other sensitive data commonly traded on black markets.

Darfi Web Intelligence

Let's light the Dark Web up and find out what is targeting you

Do you know that many businesses detect a data breach only after days or weeks passed? What about data leaks, and stolen employee information? Potentially worse. But here is the good news! Cyber attacks leave traces on the Dark Web. Being aware of what is happening is key to establishing proactive cybersecurity.

Dark Web Intelligence scans all popular places on the dark web and brings all findings related to your business. Ensuring you'll know when your business is on the crosshair. ThreatMon categorizes Dark Web Intelligence under three services. Below, you can see the details.

$4.37
million
The Average Cost Of a Data Breach

280
days
The Average Time to Identify and Contain a Breach

2
million
Daily Users in TOR Browser

Botnet Monitoring

Devices infected with malware pose a real threat of data breach as compromised accounts or machines can be an entry point for attacks. ThreatMon scans all relevant places to track stolen access information, Employee, Customer, VIP and Business Related Info

Breach Monitoring

Data Breaches may be a nightmare for businesses. However, the real threat lies in being unaware of a data breach. ThreatMon Dark Web Intelligence tracks every inch of the dark web to detect employee, customer, and VIP-level data breaches

Hacfier Chatter Monitoring

The dark Web consists of various platforms including places that enable Hackers to communicate where generally critical information is shared and tried to be kept secret. ThreatMon tracks these places to find company related data.

Surface Web Intelligence

Not every threat lies in the Dark Web. Detect what is under your nose

Threats do not only emerge from the Dark Web. Sometimes misconfigured surface web assets such as code repositories and buckets may be enough to compromise your security.

ThreatMon provides a surface web scan to detect such threats while ensuring your end-to-end awareness

Misconfigured cloud storage is a leading cause of data breaches.

Code Repository Monitoring

This service searches and detects data about your business in all public code repositories.

Search Engine Monitoring

ThreatMon detects information that is publicly accessible from search engines.

Cyber Threat Intelligence

Keystone for ensuring end-to-end Intelligence: Familiar with cyber threat intelligence, with the latest technology

Centralized in the product, Cyber Threat Intelligence is the key to bringing all services together and contextualizing end-to-end intelligence. This service does not only offer intelligence on routine security operation center (SOC) tasks, instead, it delivers convenient features enabling you to optimize your sources in the fight against cyber threats.

Cyber Threat Intelligence is also responsible for monitoring the bulk part of the intelligence gathered in the ThreatMon platform. Some parts of this intelligence are further processed to be useful in the remaining modules. Below it is demonstrated how the Cyber Threat Intelligence module is categorized.

Threat Investigation

Threatmon Threat investigation module empowers you to detect various online threats, including those lurking in dark web forums, exposed data files, and IOCs. With its advanced search capabilities, you can also stay updated on relevant news, customize your threat hunting tactics, and access our API for seamless integration. Dive deep into the security status of domains and IP addresses, ensuring comprehensive protection.

Threat Feed

Choose your sources from the ThreatMon library to sustain the maintenance of your security needs. Besides reaching the latest IOCs, Threat Feed also allows automation with its seamless integration with your SIEM.

Threat Landscape

Besides, routine security operations, cyber threat intelligence is essential to understand where threat actors are shifting their operations and how best a business can protect itself.

Under this category, one can track

- Threat Actor / APT
- Ransomware Threats
- Vulnerabilities
- Data Breaches
- Dark Web Threats

ThreatMon

Under Cyber Wings

Kugen Singam
Cybersecurity Sales
kugen@ishantech.net
www.threatmon.io