SYGNIA

RECOGNIZED BY Gartner FORRESTER

THREAT INTELLIGENCE EXPOSURE MONITORING DATASHEET

Early detection is crucial to impactful risk reduction. Detecting internal risks is hard enough. Identifying external risks is even harder.

Focusing on the most relevant external risks, Sygnia Threat Intelligence Exposure Monitoring (TIEM) scours the open and dark web for data leaks, impersonations and asset exposures. Unlike other services that provide findings only, Sygnia TIEM also provides clear actionable recommendations to keep you secure.

KEY BENEFITS

- **Reduce cyber risk**
  - **Reduce attack surface through better attack surface management**
  - **Early detection of data leaks**
  - **Early detection of in-progress attacks**
- **Improve operational efficiency of security teams**

ABOUT SYGNIA

Sygnia is a global leader in cyber incident response and cyber response readiness. Sygnia combines human expertise and purpose-built technology to beat attackers and keep organizations secure continuously. Our experience responding to some of the most complex cyber-attacks informs our cyber readiness services. We help clients at each phase of their cyber security journey:

Know: Gain a clear picture of where they stand and what they need to do to improve your security posture.

Prepare: Help clients prepare for the unexpected with a holistic plan.

Simulate: Test client defenses, strategies, and executive decision-making against targeted attack.

Detect: Identify and eliminate threats with the expertise and technology to enhance visibility and rapidly contain attacks.

Respond & Recover: Always ready to respond, working tirelessly to help clients resolve and recover with minimal business impact.

THE SYGNIA THREAT INTELLIGENCE EXPOSURE MONITORING DIFFERENCE

ANALYSIS BY SECURITY EXPERTS

Human interpretation of threat intelligence findings provides better understanding and contextualization using Sygnia knowledge of attacks and attacker TTPs provides impactful risk reduction.

BROAD VISIBILITY

We use a wide variety of tools, sources and methods for the broadest view of external exposures.

RAPID TRANSITION TO IR

In case malicious activity is found, rapidly take IR action with a trusted global leader in Incident Response.

ACTIONABLE RECOMMENDATIONS

Reports include both findings and actionable recommendations, improving operational efficiency by telling you what to do now to reduce risk.

CUSTOMIZABLE

Service is customizable to meet your organization's unique needs.

FAST & EASY ONBOARDING

Onboarding is fast and easy. We can start with just a domain name.

MONITORING ACROSS 3 CATEGORIES OF EXPOSURES

Data Leaks and Malicious Mentions

Look for externally leaked credentials, leaked confidential files, client data

- > Leaked Credentials
- > Data Leaks
- > Confidential File Exposure
- > Malicious Mentions
- > VIP Monitoring
- > Third Party Risk

Impersonations

including look-alike domains impersonating legitimate organizations and social media accounts impersonating legitimate brands or individuals

- > Look-alike Domains
- > Social Media Impersonations
- > Malicious Files Related to Client
- > Phishing Files and Pages

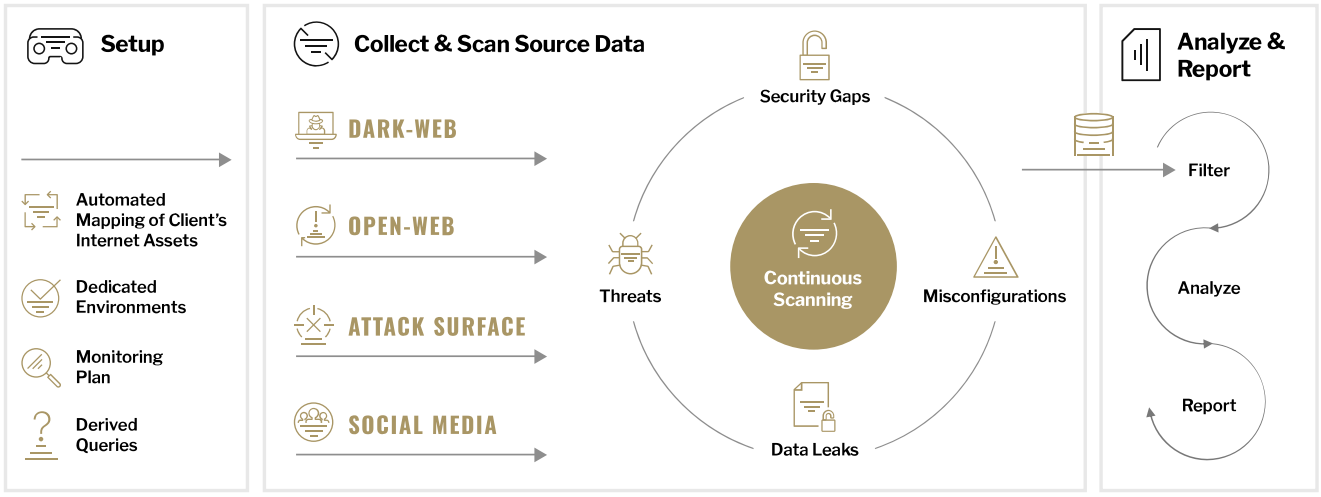
Internet-exposed assets

including ports, web interfaces and other assets such as mail and certificate security gaps and blacklisted mail servers.

- > Assets Mapping
- > Exposed Ports
- > Assets Alerts

HOW IT WORKS

Sygnia Threat Intelligence Exposure Monitoring consists of 3 phases: Setup, Collect and Scan, and Analyze and Report.



1. Setup:

- Identify and map internal assets for automated, ongoing monitoring.
- Build dedicated environment to monitor identified assets
- Create an ongoing monitoring plan
- Generate derived queries

2. Collect and scan data from various source types

- Open web, looking at public and commercial portals and repositories
- Dark web, look at a range of dark forums, channels, chatters and marketplaces
- Scan the attack surface for internet-exposed assets
- Social media, across channels such as Telegram, X and Facebook

3. Analyze and report

Service delivery can range both in terms of delivery frequency and coverage period.
Project delivery options:

Project Type	Delivery
One-Time Standard	**One-time report** Covering previous 12 months
Annual Program	**Monthly report** Covering new alerts since previous report
Custom	**One-time or Periodic report** Addressing specific, tailored requirements

SYGNIA

Sygnia is the foremost global cyber readiness and response team, applying creative approaches and battle-tested solutions to help organizations beat attackers and stay secure. Sygnia is a trusted advisor and service provider of technology and security teams, executives and boards of leading organizations worldwide.
Learn more at Sygnia.co.

A TEMASEK COMPANY AND MEMBER OF THE ISTARI COLLECTIVE

TEMASEK ISTARI

24/7
INCIDENT RESPONSE COVERAGE
Suspicious of an incident? Call +1-877-686-8680 now. Learn more at www.sygnia.co