SYGNIA

RECOGNIZED BY Gartner FORRESTER

SYGNIA MDR

DELIVERING BETTER DETECTION

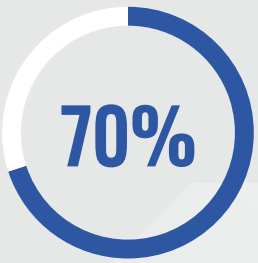
It is a surprise to absolutely no one that the world has changed drastically since the nail-biting days of worrying whether computers would survive the flip from 1999 to 2000.

In 1999, physical security monitoring was crucial to protecting crown jewels and detecting threats early. Since then, the traditional physical network perimeter has been dissolving, as organizations have pivoted from on-premises operations & data storage to the cloud.

The prolific growth of enterprise software tools such as CRMS, ERPs, email, business intelligence, marketing automation, content management, business process management, and supply chain management enable organizations to achieve skyrocketing levels of efficiency and productivity. Shifting from on-premises to cloud frees organizations and employees from the shackles of physical proximity, contributing to improved productivity and efficiency.

Great for business, not so great for security teams responsible for keeping those businesses up and running, while protecting both the organization and its clients. In fact, 70% of IT security professionals say the volume of security alerts has doubled in the past five years. Today, 56% of large companies handle over 1,000 security alerts daily.

To address this challenge, organizations are increasingly turning to MDR providers for help. MDR experts are ingesting tremendous amounts of data to detect threats to identify and contain malicious activity. Due to the sheer volume of data ingested for each client, most MDR's filter data prior to enrichment to manage data storage costs. This means that data which could be important to a future investigation may get filtered out.



70% of IT security professionals say the volume of security alerts has doubled in the past 5 years.

Today, 56% of large companies handle over 1,000 security alerts daily.

THE SYGNIA DIFFERENCE

Sygnia does it differently. Born on the battlegrounds of Incident Response, Sygnia MDR recognizes the value of having complete data.

Raw data is ingested in Velocity. Designed to meet the needs of incident responders, the Velocity platform is used by both Sygnia Incident Response and MDR.

After indexing, the raw data is enriched in Velocity, our purpose-built technology platform.

Data correlation is done after data enrichment. Because all indexed data is enriched, Sygnia security analysts are able to search all enrichment results & build powerful alerts based on the complete data set. Other MDR service providers enrich data only after an alert is triggered.

Step 1: Raw Data ingestion

Using Velocity, we collect vast amounts of information from a variety of sources, including network traffic, logs from security devices, servers, endpoints, applications, and cloud-based resources, as well as forensic artifacts from almost every operating system.

This data collection is essential for gaining a comprehensive understanding of the client environment and the complete scope of any attack. Velocity ingests more than 50 terabytes of data daily from hundreds of different data sources from logs and binary files. We support more than 100 binary file types and over 300 log types. Binary files are ingested via the Sygnia Pathfinder agent, and log data is typically ingested via Syslog, 3rd party collectors or APIs.

An average Sygnia MDR client has 10-15 data sources

With an average 2.1T of data ingested daily

Results in over 4T of enriched data daily

Step 2: Raw Data enrichment

An automated process enriches the raw data ingested into Velocity using multiple engines to provide context to the data. Enrichment actions include, but are not limited to:

- **Scanning for malware and malicious content using VirusTotal**
- **Binary and hash scanning searching for IoCs (Indicators of Compromise) using Opswat and MISP threat intelligence**
- **Convert IP's to geolocation using Dbip database**

Data correlation & deduplication is done after raw data enrichment, ensuring that data isn't lost in filtering prior to enrichment.

The enriched data is indexed in Sygnia's data lake, where the combined log and binary data sets can be queried using SQL. This enables Sygnia analysts to quickly create effective detection scenarios to gain a complete view of activity, and to perform real behavioral analysis when necessary. For example, firewall logs can be merged with binary data from a host device and logs from a cloud provider to create a complete timeline of activity for either a specific user host or a complete network.

Step 3: Detection Scenarios

Sygnia MDR uses three types of detection scenarios: Baseline, Custom and IR-based.

Baseline – Baseline detection scenarios address general risks and threats. They are based on open-source threat intelligence, including MITRE, NIST, and publicly available IoC. Most MDR's stop here.

Custom – Custom detection scenarios that are purpose-built for each customer's environment.

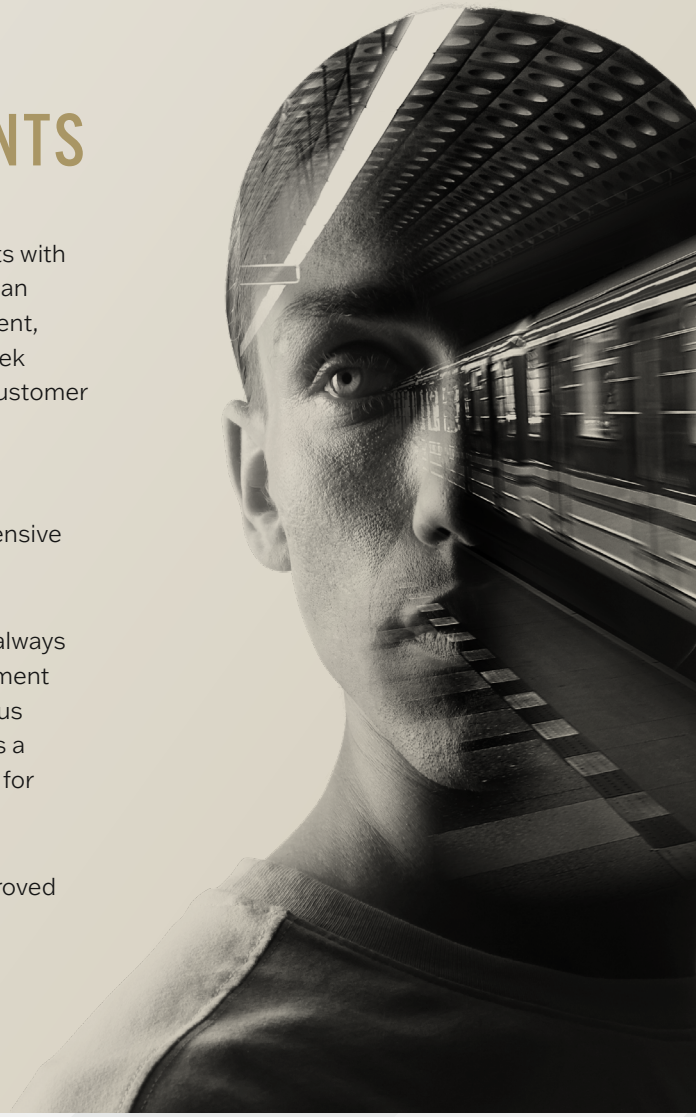
Custom detection rules are developed based on a thorough understanding of the client's business operations, environment, risk profile and relevant threats. A custom detection plan is created for each Sygnia MDR client. After identifying relevant risks and threats, likely adversary tactics are mapped to the MITRE ATT&CK framework. Next, we create a heat map of potential tactics at each phase of the attack lifecycle by risk level. Finally, we create a detection plan with custom detection rules by vector for each phase of the attack lifecycle, connecting risk factors with detection methods.

Additional custom detection scenarios are added as necessary due to new vulnerabilities, new threat groups, changes in policies, changes in the client's security stack, and/or changes to activities that take place in the client environments.

IR-based – Sygnia MDR clients benefit from detection scenarios based on the findings of our IR team in 3 ways:

1. For Sygnia IR clients, specific detection scenarios are created for post-breach monitoring to detect any attempt by the threat actor to return to the environment.
2. New IoCs identified by Sygnia IR teams are added to the Sygnia MISP server. The Sygnia MISP server is one of the enrichment engines used to enrich the raw data ingested into Velocity. All detection scenarios are automatically updated to reflect the latest IoC's.
3. When the Sygnia IR team passes incident knowledge to the MDR team, our cybersecurity engineers create new detection scenarios when necessary.

WHAT IT MEANS TO OUR CLIENTS



Better detection scenarios translate into laser-focus on real threats with significantly less noise- from an average of 4 billion events daily to an average of 6-7 incidents per week. By using Sygnia's Pathfinder agent, the Sygnia MDR team is able to investigate about 85 alerts per week without requiring client engagement. Most other MDR's require customer involvement to investigate all alerts.

The Pathfinder agent is a DFIR tool with collection and response capabilities which is deployed on all client endpoints for comprehensive visibility. This same agent is used in all Sygnia IR engagements.

This means two things for Sygnia MDR clients. First, while clients always have full visibility into Sygnia investigations, because their involvement is typically not needed, the client's security team is freed up to focus on activities. Second, the use of the Pathfinder agent also enables a seamless, real-time pivot from MDR to full-blown IR, with no delay for technology deployment.

Ultimately, Sygnia MDR clients benefit from reduced risk and improved operational efficiency.

Profile of a typical Sygnia MDR Client

2.1 T data ingested daily

85 alerts/week requiring MDR analyst investigation

6-7 incidents/week requiring client engagement

SYGNIA

Sygnia is a cyber consulting and incident response company, providing high-impact services to organizations worldwide. Sygnia works with its clients to quickly respond to threats and proactively enhance resilience. Our proven track record, commitment, and discretion have earned Sygnia the trust of security teams, senior executives, and management boards at leading organizations worldwide including Fortune 100 companies.
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