ThreatMinder

735 Battery Street San Francisco, CA 94111

(415) 636.9880

info@ThreatMinder.com

ThreatMinder Product Categories

Description and Use Cases

Product Descriptions

I) Investigation

II) Monitoring

1) ThreatMinder Sweep

2) ThreatMinder Radar

III) Use Case Examples

I Investigation

What Investigation Means:

- A specific focus on an item, person or instance
- A one-time data Sweep or ongoing Sweep of data related to Investigation
- Identifying an instance, item or person which needs additional on-line information to be:
    - Found
    - Vetted
    - Understood
- Typically Security, Criminal, Human Resources, and General Categories
- Core Focus is on the identified item
- May include some additional information not related to the company, organization or targeted asset

What Investigation Does:

- Create filters and keywords specific to the item under investigation
- Input optimizes crawlers, algorithms and data access partners specific to Investigation Target
- Focus is solely on Investigation Target
- Virtually guarantees that information on Investigative Target will be found, if available, across 400+ platforms from which data is pulled
- ThreatMinder Best Practices and Best Efforts will find all relevant and meaningful data related to the Investigative Target

I Investigation (continued)

What Investigation Does NOT do:

- Look outside the Investigative Target Definition
- Scour data related to general threats, geo-targeting, or other extraneous (to the investigation) posts, information or items
- Does NOT guarantee specific positive or non-benign results
- Does NOT guarantee anything will be found on the Investigative Target
- Does NOT guarantee additional target information is available online

When the Investigative Target is Found:

- The Target provides an online profile or post as needed
- Information provided by the investigator allows TM to directly correlate to the Investigative Target
- TM algorithms tied together multiple information pieces to find the Investigative Goal and Target

Why Investigative Target Information Wound not be Found:

- Nothing is posted online about the specific Investigative Target
- The Investigative Target is being referred to online with a separate, and unknowable, different name/slang/descriptor
- The Investigative Target is online in a separate part of the Internet which is unsearchable (Private or encrypted, for example)

NOTE: TM can find certain sites and information which have turned Offline and/or behind Authentication credentials (especially related to indexed sites, dark web, etc)

Investigation (continued)

Recommended Investigation Process:

- TM and Customer conduct a multi-pronged Investigation including:
  - Specific Target
  - Other people, products, groups known to traffic in the specific target or to be friends, acquaintances, colleagues of the target

Best Investigation Use Cases

Pre-Hire Enhanced Checks
Stolen Property/IP
Lost Property/IP
Missing Person
Information needing be corroborated
Attempting to find additional information on a Target (person, place, thing)
Security of Family Identities

II Monitoring

ThreatMinder Sweep - One-time Daily

What ThreatMinder Sweep One-Time Daily Monitoring Means:

- ThreatMinder will update online information related to the Target at least once per day
- Daily 'Sweep' of information across Web, Dark Web, Social Media
- Analyze results based on focus of Action and Target across Risk, Sentiment, Automated Confirmed Threats, Verified Confirmed Threats

What ThreatMinder Sweep Does:

- Create filters and algorithms specifically for overall monitoring of Target
- Crawls Web, Dark Web, Social Media on Daily basis (24 hours cycles)

What ThreatMinder Sweep Does NOT do:

- Does NOT provide Constant Monitoring of the Action Target
- Does NOT provide Near Real Time data updates

Best ThreatMinder Sweep Use Cases

Asynchronous Threat Monitoring
Non-Real Time Events
General Brand Monitoring
Anything NOT needing near real-time updates

II Monitoring (continued)

ThreatMinder Radar - Near Real Time Monitoring

What ThreatMinder Radar Near Real Time Monitoring Means:

- ThreatMinder will focus algorithms, crawlers and data access for ongoing, near-real time data radar
- ThreatMinder will update data on each specific Action Target in near real-time
- Data will be updated as available from each specific platform
- Different platforms update data in separate time intervals

What ThreatMinder Radar Does:

- Create filters and algorithms specifically for overall monitoring of Action Target
- Crawls Web, Dark Web, Social Media on a near real-time basis and reports results as available from each of the platforms monitored
- Performs ongoing 24/7 monitoring of data and platforms

What ThreatMinder Radar Does NOT do:

- ThreatMinder has no control over the timeframes for each platform being updated
- ThreatMinder never promises Real-Time data updates – all data is updated on a Best Efforts and SLA related to different platforms
- No guaranteed results related to information available or found
- No guarantee of finding every possible piece of information or posts online

II Monitoring (continued)

Best ThreatMinder Radar Use Cases

- Synchronous possible threats
- Anything needing updated information in near real-time
- Events
- Persons
- Locations
- Brands

III Use Case Examples

General Threats - Locations, People, Executives, Brands, Products, Events

ThreatMinder will focus on overall, and specified threats related to each of the above Use Cases

- Customer can provide additional information to augment Threat Monitoring
- Keywords, filters, slang, etc can be included to ensure algorithm focus and success
- ThreatMinder will scour related data specific to the Action Target which can create a Baseline for understanding the Action Target related to:
  - Sentiment
  - Risk
- General Threats will be categorized as found

III Use Case Examples (continued)

Disability Fraud, Code of Conduct, Local Crime, Theft, Fraud

ThreatMinder will focus on content and data related ONLY to the specific use case listed:

ThreatMinder does NOT:

- Focus on anything outside of this use case
- Analyze general threat information NOT related to the Use Case
- Guarantee results pursuant to the Use Case
- Guarantee to find every post or informational piece related to Use Case