ANOMALI MATCH™

Enhancing your MISP Implementation

REAL-TIME FORENSICS

Every day, new threats are being discovered, which adds to the list of millions of known Indicators of Compromise (IOCs). This presents organizations with three primary challenges:

- The Malware Information Sharing Platform (MISP) excels at facilitating the sharing of technical data about an incident within a community, but it does not provide deep enrichment and a validated context. Analysts often spend more time doing additional research about each incident that occurs.
- As new threats surface, organizations need to be able to determine if the attackers have already targeted or breached their network. This means being able to look over historical data, going back a year, or multiple years, to identify indications of compromise.
- Operationalizing threat data into actionable intelligence can be a difficult task for any security team. Sifting through millions of IOCs to find what is relevant to the company can be compared to finding a needle in a haystack. Furthermore, the current security solutions are not designed around scaling to the volume of data required for the visibility of the emerging threats within a network.

ENRICHING MISP

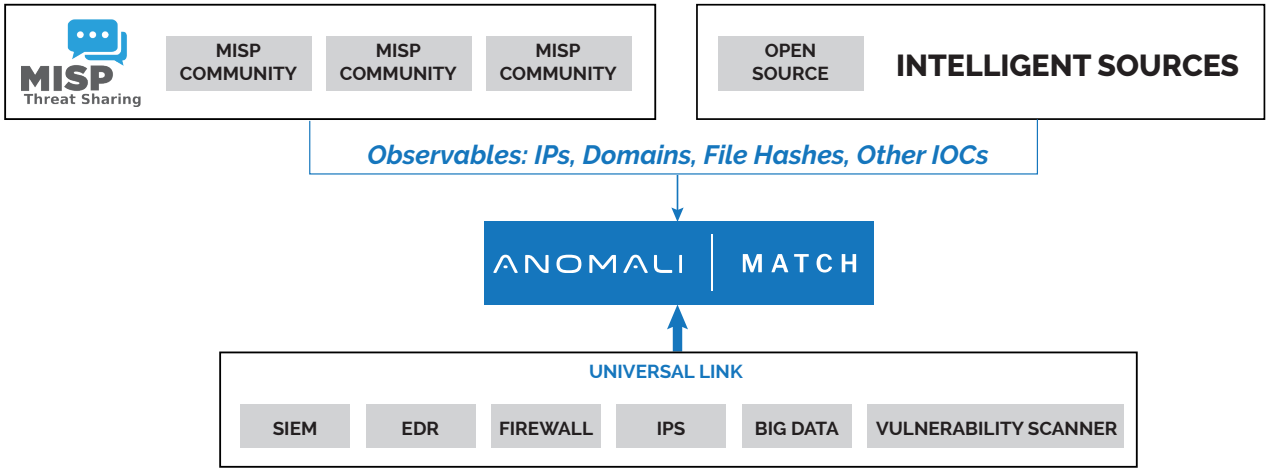
Anomali Match multiplies the value of MISP information by automatically expanding, scoring, and enriching the MISP and technical data. This frees analysts from the need to research and enrich threat intelligence data manually, and it allows for a better understanding of the malicious activity within the network. Seamless integrations allow organizations to select shared data in order to push to existing security solutions like SIEM, orchestration platforms, EDR, firewalls, and IDS/IPS.

DETECTING NEW AND EXISTING THREATS

Anomali developed the Real-Time Forensics (RTF) technology to conduct searches over vast quantities of historical data, in seconds, instead of hours/days. RTF is the foundation of Anomali Match, providing security teams with instant visibility across all the historical data.

STAYING ONE STEP AHEAD

Anomali Match is purpose-built to conduct intelligence matching, and it is capable of processing millions of IOCs and billions of internal log entries. It operationalizes threat data and automatically shows security teams what is relevant to them, and which threat data are actionable intelligence. By positively identifying the "indicators of interest," the intelligence can be fed directly to the endpoints and firewalls, for blocking.



CASE STUDY: RETROSPECTIVE ANALYSIS FOR THREAT ANALYST

BUSINESS CHALLENGE:

A new cyber threat is announced, and its details are released and shared within MISP. Tina, a Threat Intel Analyst, is asked if their organization currently has (or has had) any activity associated with the threat actors, with the Indicators of Compromise (IOCs,) or with the methods associated with it. The challenge, with questions like this, is that most tools are not designed to perform the required historical analysis. Most tools require around fifteen minutes, just to query the database. During the wait time, Tina simply has to make a decision to ignore incoming alerts.

SOLUTION:

Anomali's detection capability enhances MISP by combining its intelligence with Tina's historical network traffic. Tina can uncover evidence of potential compromises and breaches by looking back at the historical data. The high-performance processing of Anomali's Match engine allows Tina to turn millions of data points into actionable threat intelligence, and to focus on the higher priority threats to the organization.

CUSTOMER BENEFIT:

Tina no longer ignores alerts, because of the long wait-times of search queries to other tools, and she focuses her attention on the highest fidelity alerts. By pinpointing malicious activity related to known threats, in a matter of seconds, versus minutes or hours, it allows her to answer:

- whether or not her organization is being attacked?
- who is attacking them? and
- have the attacks been successful?

CASE STUDY: STREAMLINE INTELLIGENCE FOR THREAT ANALYST

BUSINESS CHALLENGE:

Tina, a Threat Intel Analyst is working with hundreds of millions of IOCs stored within its organization's massive security data lakes. Handling this large volume of data makes it difficult to undertake the respective analytic steps in a timely manner, and to detect and solve the threats.

SOLUTION:

Anomali aggregates intelligence from MISP and uses a machine-learning algorithm to automatically reduce false positives, to remove duplicates, and to apply confidence scores to the IOCs. Tina can then further enrich the intelligence by carrying out investigations, by creating new associations, and by leveraging third-party sources, all from within a single pane of glass.

CUSTOMER BENEFIT:

Tina can work more efficiently than ever before, while addressing more threats. The time it takes to analyze a threat has been reduced from hours, to a few minutes. This time adds up, while investigating many malicious IOCs every week.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®