Anomali Enterprise™

Anomali Enterprise Breach Analytics Platform

Data Sheet

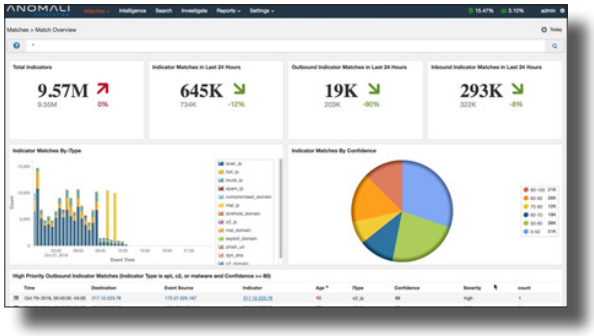
Making Threat Intelligence Work

Organizations looking to leverage threat intelligence quickly discover the data overload challenge. Between open source feeds, paid 3rd party feeds, ISAC/shared feeds, etc., they may suddenly have 10s of millions of IOCs to manage. This data can arrive in different formats and have different fields/information and often have duplicates and false positives.

Further, once you've gathered and normalized all this data you then want to triage billions of events on your network to identify potential matches. Not only is it necessary to look through today's events, but as new IOCs become known you need to search through historical data as well. Threat Intelligence is extremely temporal in nature, where IOCs related to a breach may not be shared until weeks or months after an initial compromise, requiring extensive retrospective analysis.

Anomali Enterprise provides immediate detection of IOCs across all your events, today and over the past 12 months. You gain actionable insight into active threats and how to respond.

Powerful Threat Hunting Engine



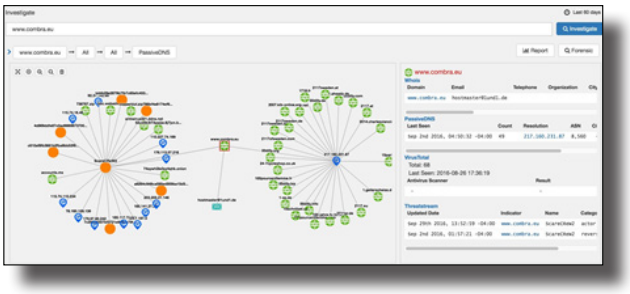
Built to work with your SIEM, Anomali Enterprise solves the data overload problem by automatically scouring internally collected log events for millions of threat indicators.

Matches are elevated and can be viewed directly within your existing SIEM console or be pushed into various other products to support SOC operations or existing workflows.

Rapid Indicator Expansion & Correlated Intelligence

Anomali arms analysts with the capabilities to efficiently and comprehensively investigate threats. An investigation may start when traffic to a malicious domain is discovered. Anomali lets analysts pivot through Whois and Passive DNS, and find associated threat indicators. From here Anomali allows the analyst to search all related IOCs across months of historical data to get a full picture of the threat. A robust API is also available for custom integrations.

- Pivot against internal log data
- IOCs mapped against the attack chain
- Automatic Domain Generation Algorithm (DGA) analysis
- Examine infiltration/exfiltration timelines
- Detect directionality of communications



365 Days of Searchable Data

Anomali Enterprise doesn't stop at matching the most recent events against threat data. It can efficiently identify IOC matches against up to 365 days of events. As new IOCs are discovered you can find any activity associated with the threat. This retrospective analysis is critical given attackers typically need months inside the network to carry out their plans. With Anomali Enterprise you can discover these existing threats even without keeping all historical event data online.

Analysts can perform searches across this data to enrich their investigations. Despite this large pool of data, Anomali Enterprise's remarkable scalability allows it to perform these searches quickly enabling analysts to work effectively and efficiently.

To find out more about Anomali Enterprise, contact info@anomali.com.

ANOMALI™

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com