Anomali Enterprise

Real-Time Forensics

Every day new threats are discovered, adding to the list of millions of known Indicators of Compromise (IOCs). This presents organizations with two challenges:

- Evaluating newly identified threats to identify an existing breach
- Checking millions of IOCs daily to identify newly launched attacks

The first challenge is especially critical. As new threats become known, organizations need to know if attackers have already targeted and breached their networks. This means being able to look over historical data going back 6 months or longer to identify potential breaches. The second challenge, checking millions of IOCs daily for new matches, addresses the need for organizations to maintain visibility into emerging threats to the network.

32% of organizations able to access data from **3 months ago**

4% of organizations are able to access data from **1 year ago**

2017 Ponemon Survey

Detecting New Threats

To determine if their organization was breached, security teams must take new threat intelligence and find any matches against recorded network activity over months or even years. Anomali developed the Real-Time Forensics (RTF) technology to complete searches over vast quantities of historical data in seconds instead of hours/days. RTF is the foundation of Anomali Enterprise, providing security teams instant visibility across all historical data.

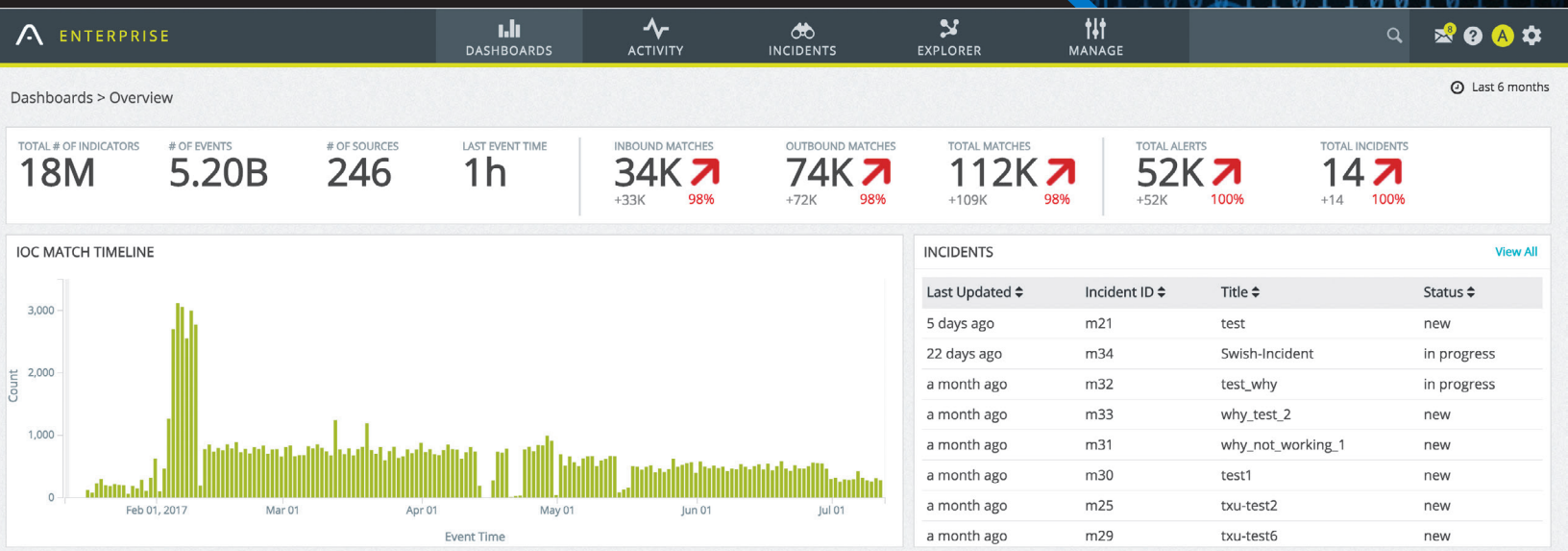
Detecting Existing Threats

Security teams are simultaneously charged with live monitoring their organization's health by comparing new traffic against known threats. Threat intelligence indicators can easily run into millions of indicators, each needing to be evaluated against internal log events. Anomali Enterprise is purpose-built to perform this massive scale intelligence matching, capable of processing millions of IOCs and billions of internal log entries. Positively identified "indicators of interest" are automatically fed to the SIEM for ongoing monitoring or blocking.

Indicators can also be enriched or added to investigations in ThreatStream, Anomali's Threat Intelligence Platform (TIP). Security teams can easily collaborate leveraging Anomali Enterprise's powerful search and scaling along with ThreatStream's integrations, sharing, and data enrichment.

Immediately identify threats with Real-Time Forensics

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



Intuitive interface and dashboards reveal threat matches, streamlines analysis

Core Capabilities

Anomali Enterprise integrates with your existing SIEM and other log sources, maintaining a year or more of historical visibility without duplicating logs. This historical data is continuously correlated against new and existing threat intelligence to uncover evidence of breaches. Real-Time Forensics immediately discovers matches between these data sets, reducing time to detection to a matter of seconds. Anomali Enterprise also provides analysts with tools to categorize and elevate indicator matches for triage and response.

- Quickly identifies newly discovered threats against 365+ days historical data
- Matches billions of daily network events against millions of IOCs in seconds
- Detects malicious activity with DGA algorithms
- Delivers high priority IOCs to SIEMs for ongoing monitoring

DGA

Domain Generation Algorithms are widely used in malware to set up command and control domains. The malware is instructed to phone home to DGA-produced domain names. These domains often live for a day or two and tend to have nonsensical names - e.g., jcxeionotdssqkdun.pw. Given their short lifespans, DGA domains do not make it onto threat intelligence lists. Nevertheless, Anomali Enterprise is able to detect and alert on traffic to DGA domains. The solution discovers DGA activity using sophisticated algorithms and does not rely on documented threat indicators.

Get the Ponemon study:
State of Threat Intelligence:
anomali.com/ponemon

Event Time	Event Source	Destination	URL	DGA Probability	Malware Family	Count
Aug 30th 2017, 19:50:00 -05:00	172.18.15.16	wgtbnpt64a74r7wdnyoygsqpz8s.com	-	0.96	Gameover_DGA, MadMax	11
Aug 30th 2017, 19:50:00 -05:00	172.18.19.14	tjotvtrdd1jdb9hd6xb4o85icf.com	-	1	Gameover_DGA, MadMax	16
Aug 30th 2017, 19:50:00 -05:00	172.18.13.15	1pdhc2u20gf32oqunv8uqpzbgc6.com	-	0.99	Gameover_DGA, MadMax	6
Aug 30th 2017, 19:50:00 -05:00	172.18.20.13	gh8eoyfrvr0ayxxt.com	-	0.903	Bedep, Chinad, Corebot, MadMax	8

Anomali Enterprise has powerful DGA detection capabilities

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