Partner Data Sheet

QRadar

Do more with QRadar using the Anomali App

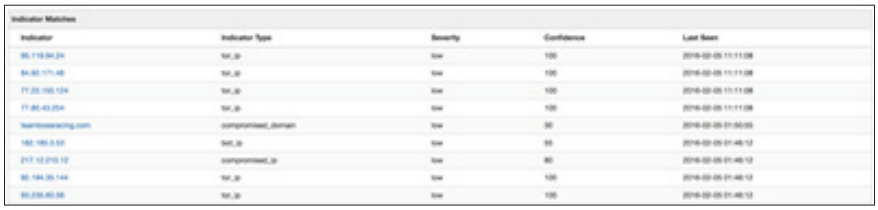
With the app, you can:

- View and monitor current and historic indicators matches on your local event data
- Interact with dashboards to get a multi-dimensional view of indicator matches
- Drill down on a specific indicator match for deeper analysis
- Configure alerts based on conditions of interest to you such as an email notification if a high priority match occurs in the last hour
- Search for specific indicator matches using the familiar QRadar App for search

Product Overview

Why Anomali? Anomali is a security company that offers a SaaS-based threat intelligence platform. Anomali's ThreatStream platform is the first ever community-vetted cyber security intelligence platform that integrates directly with an organization's existing security infrastructure. In real-time, ThreatStream aggregates and analyzes threat intelligence data from hundreds of sources, including open source intelligence, global honey net sensor farms, social media and it's own threat intelligence team, Anomali Labs. That's in addition to the hundreds of organizations that contribute to the ThreatStream community. Each individual indicator of compromise curated is categorized and risk ranked for severity and relevance using data analytics to identify relationships with known threats. A risk score is then assigned to each indicator before it is delivered to your security infrastructure.

The ThreatStream platform enables seamless integration with QRadar by utilizing ThreatStream Link, a lightweight connector. ThreatStream Link allows organizations to dynamically sync threat intelligence from the cloud into security devices where it becomes immediately available for correlation. Beyond just syncing, ThreatStream also delivers purpose built content or correlation instructions so that correlation becomes instantaneous. With ThreatStream, there's no need for lengthy professional services engagements or costly aftermarket configurations. Finally, ThreatStream allows organizations to add and manage custom intelligence feeds, enabling automated risk ranking and distribution for correlation.



ANOMALI

Populating data

The following conditions for event data must be met in order for our app to populate with data as expected:

- QRadar version 7.2.6
- TCP port 8787 open from the QRadar console to ThreatStream Link
- Reference set entries must point the app back to the ThreatStream Link installation

What you can do

Anomali's API enables you to interact with the Anomali ThreatStream platform and use threat intelligence available on it with other tools in your enterprise.

- Import and export intelligence and indicators from and to any source
- Actionable intelligence to existing security controls
- Customized threat data

Making QRadar Even Better with Anomali

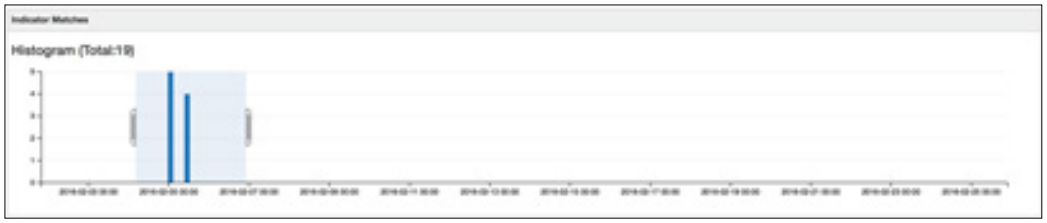
Anomali's QRadar App adds real-time threat intelligence to event data in your QRadar deployment. Threat intelligence is continuously gathered, categorized, risk ranked (for severity and confidence) in Anomali's ThreatStream platform and then delivered in real-time to your Anomali QRadar App for monitoring and detection of security threats in your enterprise infrastructure for the security and threat intelligence teams to quickly see high priority threats to your business. The intelligence is based on common industry-accepted Indicators of Compromise (IOC) such as source and destination IP addresses, email addresses, domains, URLs, and so on, but is enriched with factors such as risk score to add context and relevance to the delivered information.

How it works

QRadar's App is able to display multi-dimensional context for integrated threat intelligence from the ThreatStream platform. This enables users to now see the breakdown of indicators by confidence score, iType, severity, and geographic location. This information is provided by the ThreatStream platform into QRadar through the QRadar API from ThreatStream Link. Once populated, an analyst is able to do further drilldowns into the indicator via any of these datapoints, including the interactive histogram.

Seamless and automated

The Anomali QRadar App provides seamless, automated integration of indicator data to deliver real-time threat intelligence to your QRadar instance so you can start using the threat feeds in meaningful ways more efficiently and more effectively than ever before.



About Anomali

Anomali™ is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, the ThreatStream platform enables organizations to proactively identify and combat cyber threats targeting their operations.

For more information contact Anomali sales at info@anomali.com

ANOMALI

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