



Real time, machine curated, AI enhanced, threat intelligence delivered right to your Anomali ThreatStream console for early warnings and triage of critical threats



Use case

Customer

An organization trying to proactively detect and triage threats, with access to multiple threat and vulnerability intelligence feeds connected to Anomali ThreatStream

Problem

Team overwhelmed by noisy threat intelligence feeds delivering no context for reported vulnerabilities and IoCs. No easy way to filter threats and vulnerabilities simply based on vendors, products and services used by the organization.

Need

Access to a real time threat feed with ability to filter and contextualize threats and vulnerabilities based on simple list of vendors, products and services.



Solution

Real-time, machine curated, AI enhanced and filtered threats delivered via a premium Anomali ThreatStream App available on the Anomali Marketplace

● Cutting edge threat intel

Patented, machine curated, AI enhanced real-time, threat intelligence surfaces and predicts cvss scores, exploitability, weaponization by crawling www/dark web
Avoid all human induced errors, misses in threat & vulnerability intel.

● Marketplace App

A premium Anomali threat feed integrated with ThreatWorx Attenu8 platform

● Reduced noise and faster triage

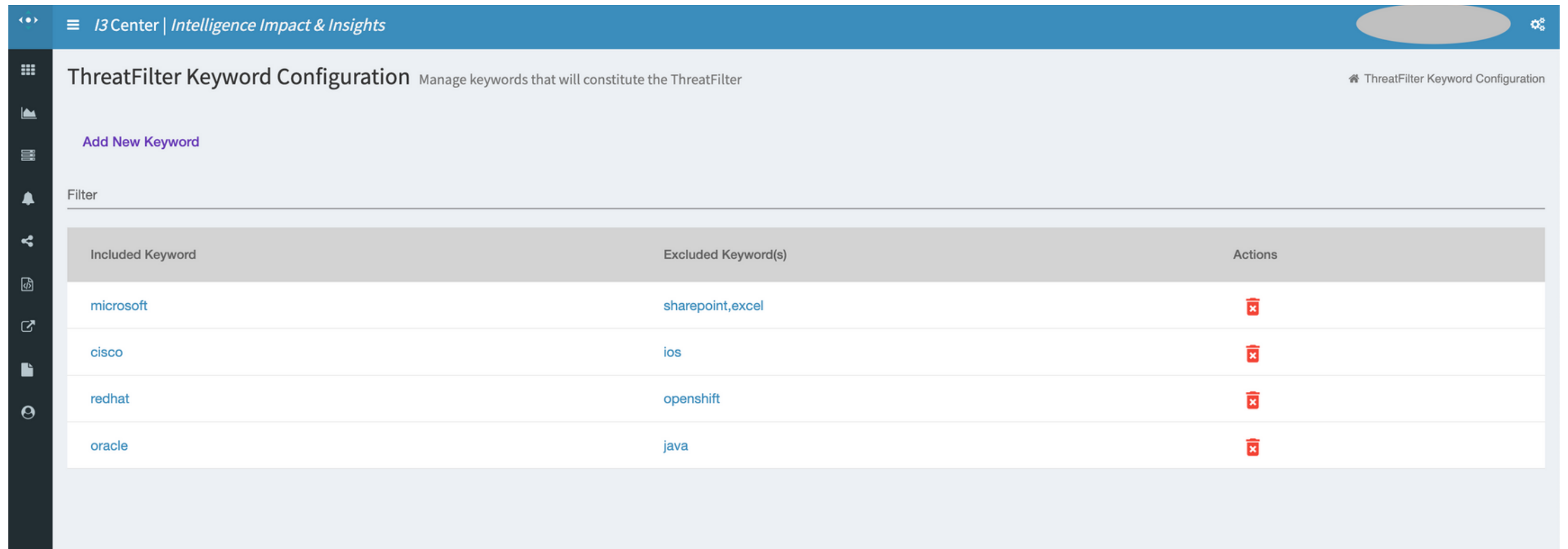
Anomali users see only relevant threats and vulnerabilities which reduces time to detect and triage critical vulnerabilities

How does it work - 1

● Setup your ThreatFilter in ThreatWorx Attenu8 Platform







A ThreatFilter is simply a list of keywords which can include vendors, products, services that the platform uses to filter new threats and vulnerabilities as they surface. ThreatWorx Attenu8 uses these keywords to determine their relevance to the surfaced threats rather than just a find / grep.



ThreatFilter Keyword Configuration Manage keywords that will constitute the ThreatFilter

[Add New Keyword](#)

Filter

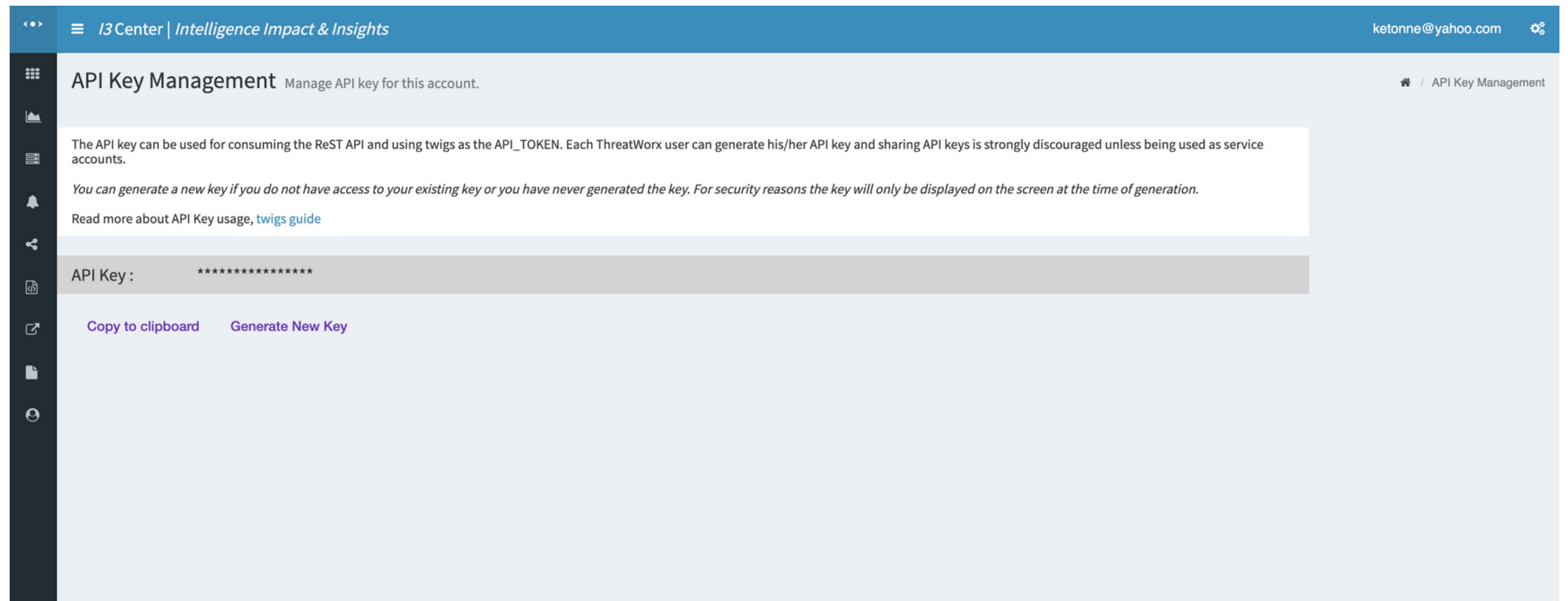
Included Keyword	Excluded Keyword(s)	Actions
microsoft	sharepoint,excel	
cisco	ios	
redhat	openshift	
oracle	java	

How does it work - 2

● Get your ThreatWorx API key



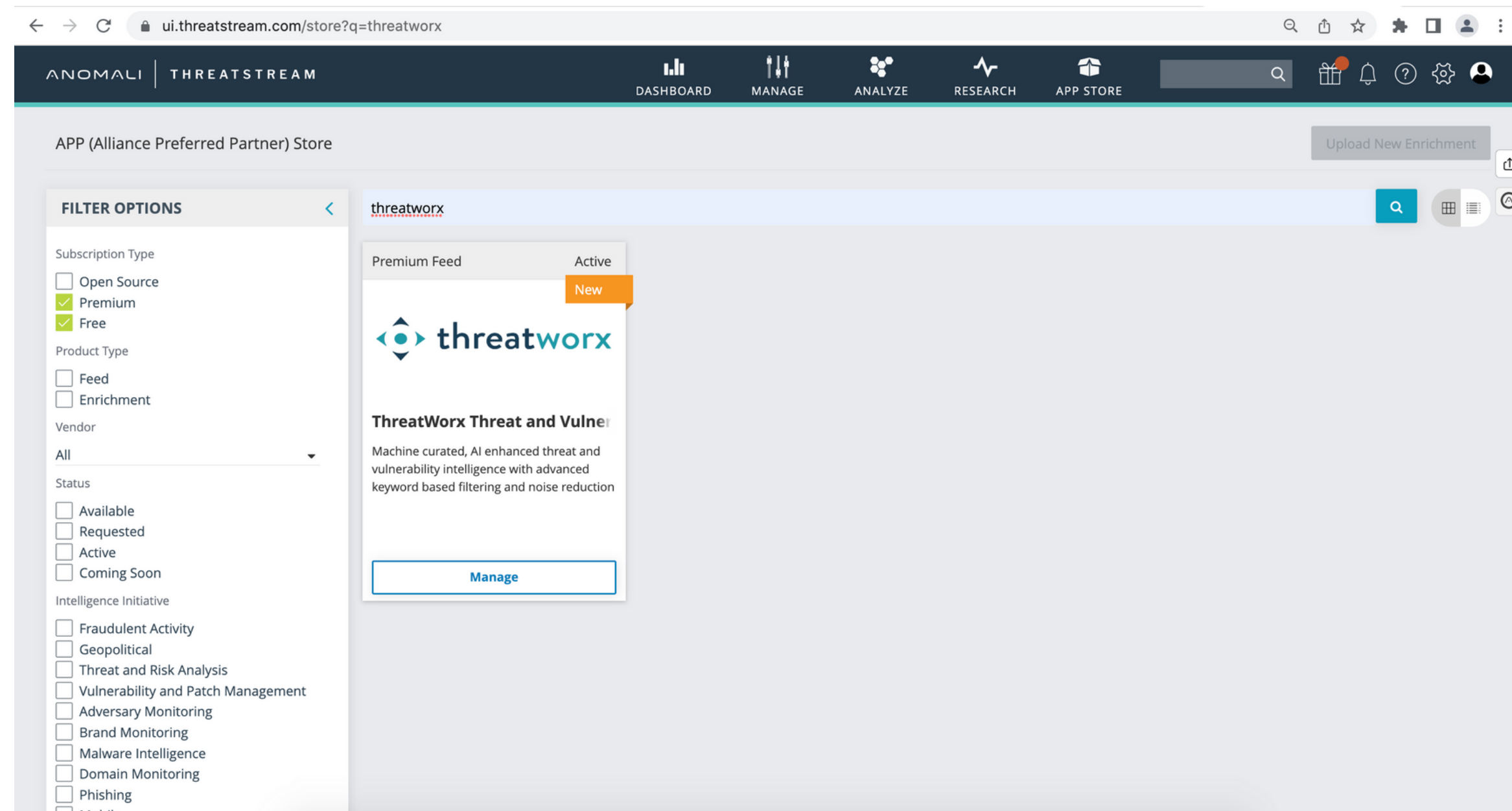
ThreatWorx ReST API allows downstream applications to integrate and build custom workflows for triage and remediation



How does it work - 3


- **Get the ThreatWorx Premium Feed App from the Anomali Marketplace**

💡 Activate the app using your ThreatWorx API key



THREATWORX THREAT AND VULNERABILITY INTELLIGENCE
✕

Machine curated, AI enhanced threat and vulnerability intelligence with advanced keyword based filtering and noise reduction



Product Type Premium Feed	Vendor ThreatWorx	Status Active
------------------------------	----------------------	---

Health
Credentials

Channel Name ▾	History	Health ▾	Last Run ▾	Interval ▾
ThreatWorx Threat And Vulnerability Intelligence - Threa...	<div style="display: flex; justify-content: space-around;"> <div style="width: 15px; height: 15px; background-color: gray;"></div> <div style="width: 15px; height: 15px; background-color: gray;"></div> <div style="width: 15px; height: 15px; background-color: gray;"></div> <div style="width: 15px; height: 15px; background-color: gray;"></div> <div style="width: 15px; height: 15px; background-color: gray;"></div> <div style="width: 15px; height: 15px; background-color: gray;"></div> <div style="width: 15px; height: 15px; background-color: red;"></div> <div style="width: 15px; height: 15px; background-color: orange;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: red;"></div> <div style="width: 15px; height: 15px; background-color: orange;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: green;"></div> <div style="width: 15px; height: 15px; background-color: red;"></div> </div>	✓	29 May 2023 12:10	1h

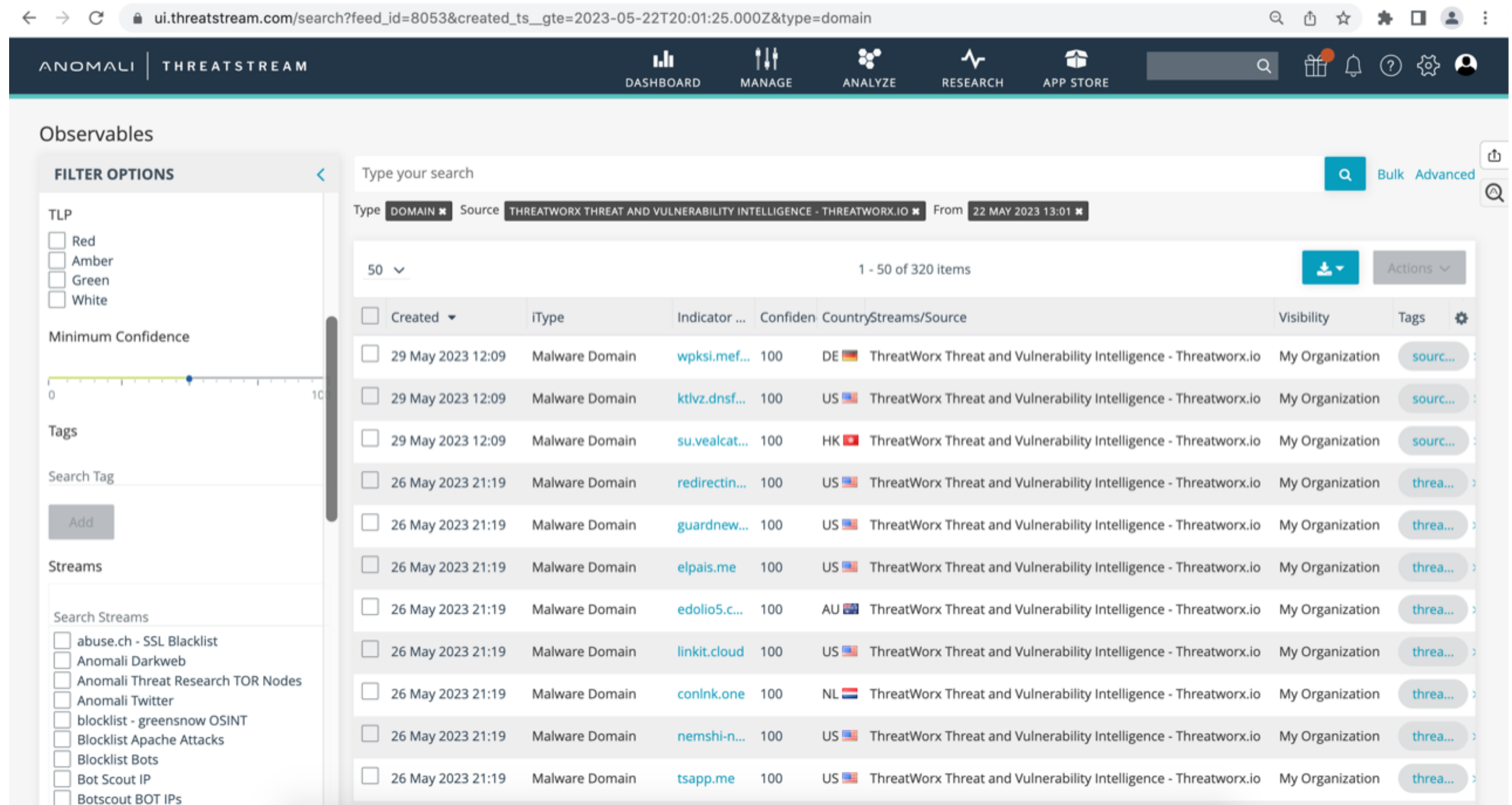
☒ Send Error Notifications

No Data Threshold
Never ▼

Cancel
Deactivate
Save Changes

How does it work - 5

- Threat / Malware Feed is available in Anomali ThreatStream Console



The screenshot displays the Anomali ThreatStream console interface. The top navigation bar includes the Anomali ThreatStream logo and several menu items: DASHBOARD, MANAGE, ANALYZE, RESEARCH, and APP STORE. A search bar is located on the right side of the navigation bar.

The main content area is titled "Observables" and features a "FILTER OPTIONS" sidebar on the left. The sidebar includes sections for TLP (Red, Amber, Green, White), Minimum Confidence (a slider from 0 to 100), Tags (a search bar and an "Add" button), and Streams (a list of streams with checkboxes). The main area shows a search results table with columns: Created, iType, Indicator, Confidence, Country, Streams/Source, Visibility, and Tags. The table displays 50 items, with a total of 320 items available. The search criteria are: Type: DOMAIN, Source: THREATWORX THREAT AND VULNERABILITY INTELLIGENCE - THREATWORX.IO, From: 22 MAY 2023 13:01.

Created	iType	Indicator	Confidence	Country	Streams/Source	Visibility	Tags
29 May 2023 12:09	Malware Domain	wpksi.mef...	100	DE	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	source...
29 May 2023 12:09	Malware Domain	ktlvz.dnsf...	100	US	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	source...
29 May 2023 12:09	Malware Domain	su.vealc...	100	HK	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	source...
26 May 2023 21:19	Malware Domain	redirectin...	100	US	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	threa...
26 May 2023 21:19	Malware Domain	guardnew...	100	US	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	threa...
26 May 2023 21:19	Malware Domain	elpais.me	100	US	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	threa...
26 May 2023 21:19	Malware Domain	edolio5.c...	100	AU	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	threa...
26 May 2023 21:19	Malware Domain	linkit.cloud	100	US	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	threa...
26 May 2023 21:19	Malware Domain	conlnk.one	100	NL	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	threa...
26 May 2023 21:19	Malware Domain	nemshi-n...	100	US	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	threa...
26 May 2023 21:19	Malware Domain	tsapp.me	100	US	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	My Organization	threa...

How does it work - 6

● Vulnerability Feed is available in Anomali ThreatStream Console

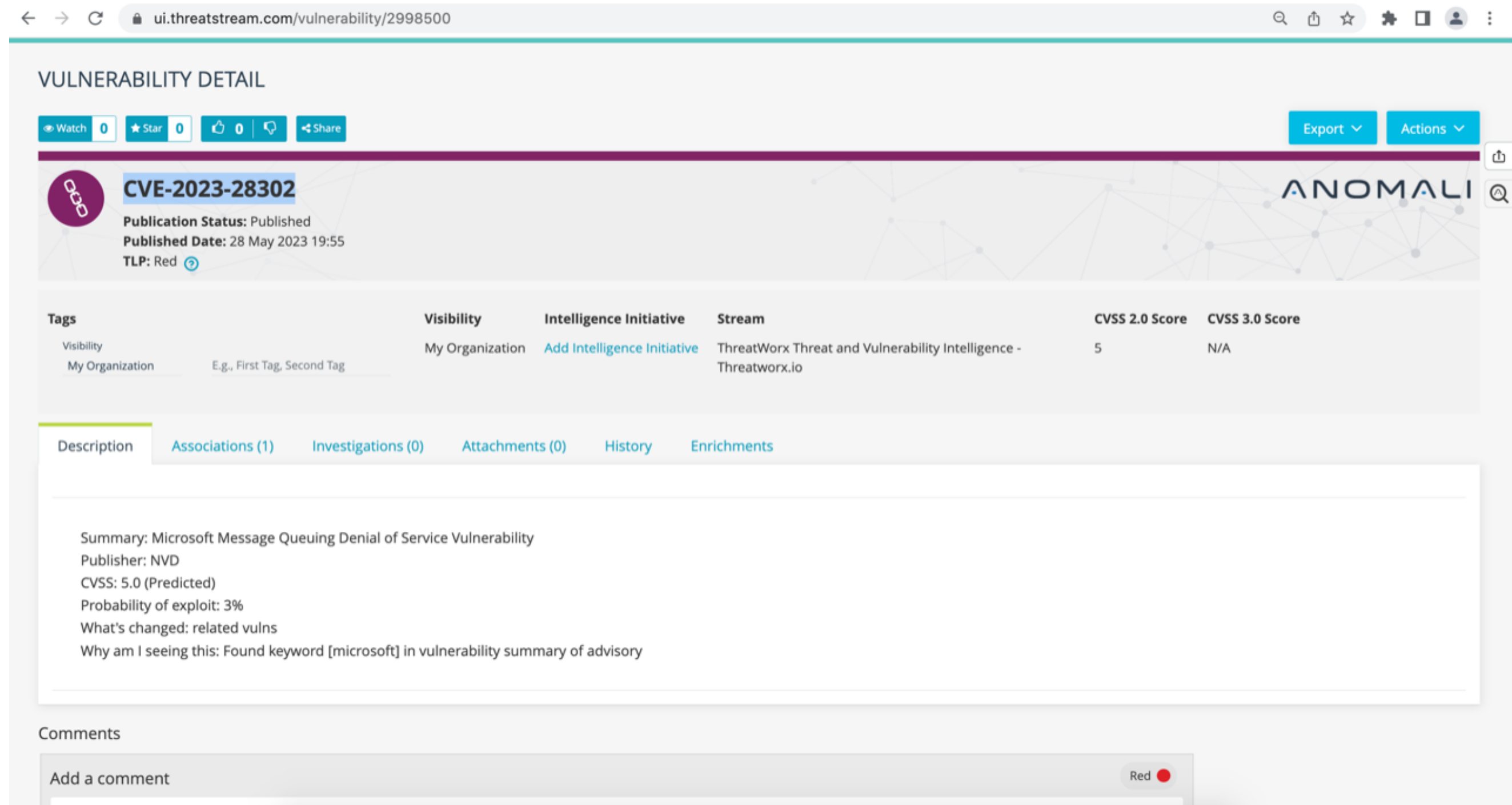
← → ↻ ui.threatstream.com/threatmodels?model_type=vulnerability 🔍 📄 ⭐ ⚙️ 🗑️ 👤 ⋮

Select Users	<input type="checkbox"/>	Vulnerability	CVE-2023-24598	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
Owner	<input type="checkbox"/>	Vulnerability	CVE-2023-24599	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
Select Users	<input type="checkbox"/>	Vulnerability	CVE-2023-24600	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
	<input type="checkbox"/>	Vulnerability	CVE-2023-24601	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
	<input type="checkbox"/>	Vulnerability	CVE-2023-24602	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
	<input type="checkbox"/>	Vulnerability	CVE-2023-24603	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
	<input type="checkbox"/>	Vulnerability	CVE-2023-24604	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
	<input type="checkbox"/>	Vulnerability	CVE-2023-24605	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
	<input type="checkbox"/>	Vulnerability	CVE-2023-22970	Published	Analyst	<input checked="" type="checkbox"/> NVD CVEs	Analyst	28 May 2023 20:15
	<input type="checkbox"/>	Vulnerability	CVE-2021-1439	Published	ThreatWorx Threat an	My Organization	devops+org_id_5249@...	28 May 2023 19:55
	<input type="checkbox"/>	Vulnerability	CVE-2021-1423	Published	ThreatWorx Threat an	My Organization	devops+org_id_5249@...	28 May 2023 19:55
	<input type="checkbox"/>	Vulnerability	CVE-2021-1449	Published	ThreatWorx Threat an	My Organization	devops+org_id_5249@...	28 May 2023 19:55
	<input type="checkbox"/>	Vulnerability	CVE-2021-1437	Published	ThreatWorx Threat an	My Organization	devops+org_id_5249@...	28 May 2023 19:55
	<input type="checkbox"/>	Vulnerability	CVE-2022-20677	Published	ThreatWorx Threat an	My Organization	devops+org_id_5249@...	28 May 2023 19:55
	<input type="checkbox"/>	Vulnerability	CVE-2023-28302	Published	ThreatWorx Threat an	My Organization	devops+org_id_5249@...	28 May 2023 19:55
	<input type="checkbox"/>	Vulnerability	CVE-2023-2491	Published	ThreatWorx Threat an	My Organization	devops+org_id_5249@...	28 May 2023 19:55
	<input type="checkbox"/>	Vulnerability	CVE-2023-24540	Published	ThreatWorx Threat an	My Organization	devops+org_id_5249@...	28 May 2023 19:55

Previous 1 2 3 4 5 6 Next

How does it work - 7

● Vulnerability Details from ThreatWorx available in ThreatStream Console



The screenshot displays the ThreatStream Console interface for a specific vulnerability. The browser address bar shows the URL `ui.threatstream.com/vulnerability/2998500`. The page title is "VULNERABILITY DETAIL".

At the top, there are interaction buttons: Watch (0), Star (0), Like (0), and Share. On the right, there are "Export" and "Actions" buttons. The "ANOMALI" logo is visible in the top right corner.

The main content area features a purple circular icon with "PCC" and the vulnerability ID **CVE-2023-28302**. Below this, the publication status is "Published", the published date is "28 May 2023 19:55", and the TLP is "Red".

A table provides additional details:

Tags	Visibility	Intelligence Initiative	Stream	CVSS 2.0 Score	CVSS 3.0 Score
Visibility My Organization	My Organization	Add Intelligence Initiative	ThreatWorx Threat and Vulnerability Intelligence - Threatworx.io	5	N/A

Below the table, there are tabs for "Description", "Associations (1)", "Investigations (0)", "Attachments (0)", "History", and "Enrichments". The "Description" tab is active, showing the following summary:

- Summary: Microsoft Message Queuing Denial of Service Vulnerability
- Publisher: NVD
- CVSS: 5.0 (Predicted)
- Probability of exploit: 3%
- What's changed: related vulns
- Why am I seeing this: Found keyword [microsoft] in vulnerability summary of advisory

At the bottom, there is a "Comments" section with an "Add a comment" input field and a "Red" status indicator.

The Result

- **Real time, machine curated, AI enhanced, filtered threat intelligence delivered to your Anomali ThreatStream Console**

