A SANS Product Review

Threat Intelligence Solutions: A SANS Review of Anomali ThreatStream

Written by **TJ Banasik**

October 2020

Sponsored by:

Anomali

Cybersecurity is a daily, ongoing battle between sophisticated and motivated adversaries and defenders seeking not only to mitigate breaches and attacks, but also to prevent them from occurring. As enterprises attempt to evolve from a reactive to a proactive state of cyber defense, they consistently encounter the same issues: data overload and data duplication combined with manpower limitations that impede efforts to do the right things at the right time. Security operations centers (SOCs) today often find themselves either a) relying on the limited data they have time to process, thereby accepting that their decisions will be made based on incomplete knowledge or b) investing in the massive amounts of data, information and intelligence needed to make informed decisions, but then not having sufficient time and expert resources to capitalize on all of that access.

A key strategy for security organizations that want to become intelligence driven is to be proactive in their cyber defense by utilizing external threat data. By understanding external threats, security teams can more effectively anticipate, block and detect active attacks targeting their organization. But striking the right balance between threat intelligence volumes and analytical capacity requires building mature threat intelligence programs that have the right people, processes and technologies. Threat intelligence platforms (TIPs) contribute significantly to building such a program by providing a unifying mechanism to consolidate actionable data at scale, automate analyst research and integrate the outcomes with security controls.

Making threat intelligence useful—by including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace—is time-consuming and labor-intensive. Unfortunately, as much as 80% of analysts' time in most organizations is spent on collection and normalization of data, leaving as little as 20% of their time to focus on understanding and solving security problems. Organizations are constantly seeking to reverse that ratio, in part because they do not have enough talented people or available time to accomplish the critical missions they have. A recent ESG study found that more than 53% of organizations report a critical shortage of cybersecurity skills.[1] But even if the security expert shortage was magically solved, best practice threat intelligence has become a "big data" game that requires a level of intelligent automation not addressable by increased staffing.

Speed is another challenge in making threat intelligence useful. Time-to-detection is a critical component of defending enterprises, as capable attackers sometimes only need a short window to gain access to and exfiltrate valuable assets. Worse still, Verizon reports that 56% of breaches take months or longer to discover,[2] implying enormous "dwell time" for threats. This also speaks to the need to spend *less* time on consumption of data and *more* time making sense of it.

To better understand technologies specifically designed to empower cybersecurity teams to work smarter and faster while capitalizing on massive troves of cyber intelligence, the SANS team took the opportunity to review the Anomali ThreatStream® product. ThreatStream, a TIP providing a unified solution for collecting, curating and disseminating threat intelligence, rationalizes multiple threat data sources into a single high-fidelity repository by automatically normalizing, deduplicating and enriching the threat data; removing false positives; and then associating all related threat indicators. ThreatStream then applies a machine learning algorithm for scoring indicators of compromise (IoCs), which provides much needed context to security professionals looking to understand, evaluate and react at speed. To fulfill the goal of moving from reactive to proactive cybersecurity, technologies like ThreatStream are required to overcome the skills gap and data overload affecting most enterprises.

Anomali ThreatStream Review

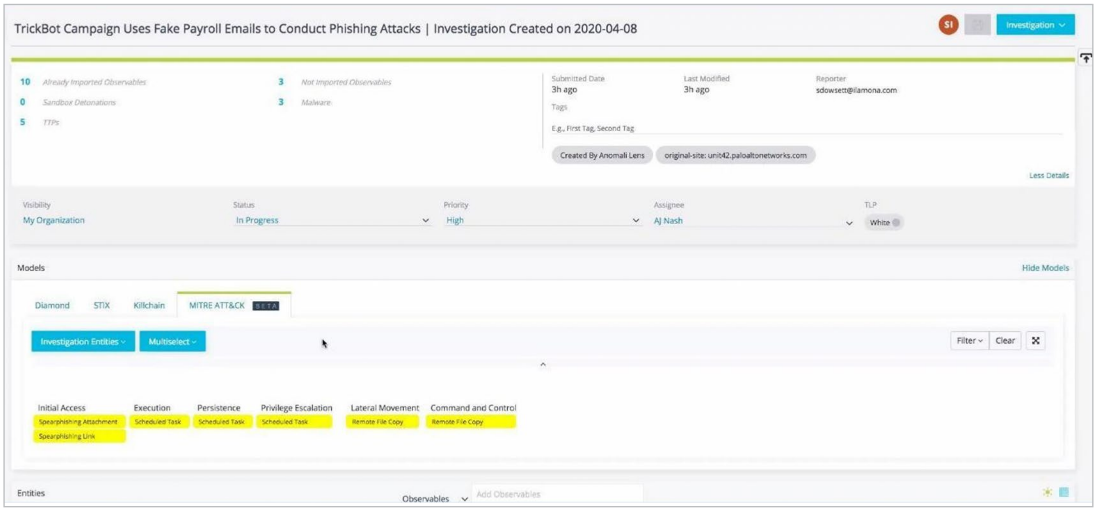
Our review covers three elements:

- Review of ThreatStream's features
- Discussion of complementary Anomali products
- Several use-case performance reviews

[1] Oltsik, J. (2019, January 10). ESG. The Cybersecurity Skills Shortage Is Getting Worse. Retrieved March 30, 2020, from www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse

[2] Verizon. (2019, January 21). 2019 Data Breach Investigations Report. Retrieved March 30, 2020, from https://enterprise.verizon.com/resources/reports/dbir

A model-based approach to threat intelligence analysis allows you to move from simple tracking of atomic threat indicators to understanding real and potential adversaries based on the context and relationships between their known indicators, tactics, techniques, procedures, vulnerabilities and campaigns. Anomali supports the structured analysis of threats across multiple model-based industry standards and frameworks, including STIX™, Diamond, Cyber Kill Chain® and MITRE ATT&CK™. This allows users to quickly identify, profile and defend against actual and potential adversaries targeting their organization. Figure 1 is a sample of a ThreatStream investigation demonstrating indicators, associations, threat group and tactics associated with a TrickBot campaign leveraging phishing as the attack vector.



TrickBot Campaign Uses Fake Payroll Emails to Conduct Phishing Attacks | Investigation Created on 2020-04-08

10 Already Imported Observables
0 Sandbox Detonations
5 TTPs
3 Not Imported Observables
3 Malware

Submitted Date: 3h ago
Last Modified: 3h ago
Reporter: sdowsett@ilamona.com
Tags: E.g., First Tag, Second Tag
Created By Anomali Lens
original-site: unit42.paloaltonetworks.com

Visibility: My Organization
Status: In Progress
Priority: High
Assignee: AJ Nash
TLP: White

Models

Initial Access	Execution	Persistence	Privilege Escalation	Lateral Movement	Command and Control
Spearphishing Attachment	Scheduled Task	Scheduled Task	Scheduled Task	Remote File Copy	Remote File Copy
Spearphishing Link					

Entities

Figure 1. Investigation

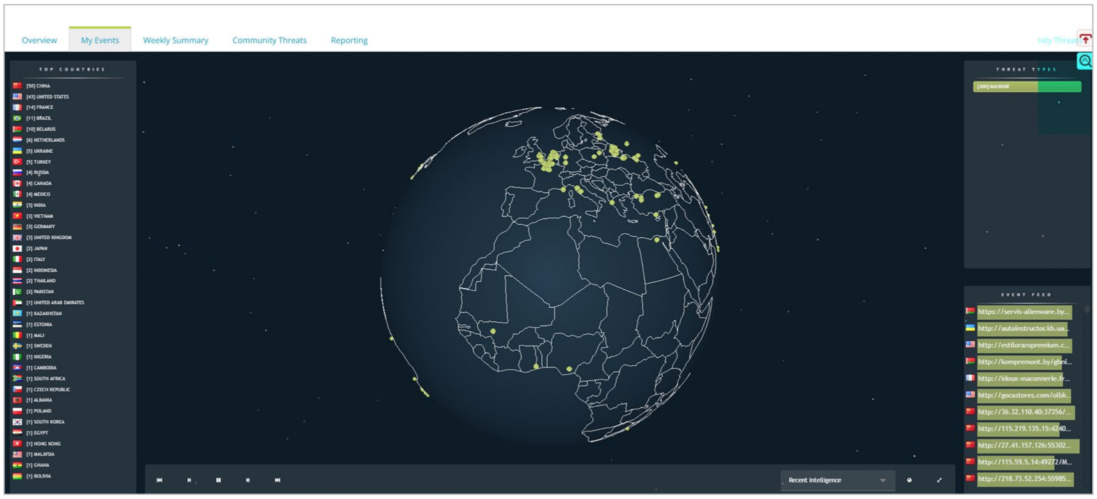
Entering the ThreatStream cloud-based administrative console with the supplied credentials was fast and easy. The SANS team was immediately impressed with the broad array of threat intelligence available when accessing the application for the first time and found the organization of the user interface (UI) simple and intuitive. The default Overview Dashboard, upon entry, highlights several high-level product features, which are appropriately organized in the tabs Manage, Analyze, Research, APP Store and Settings. At a high level, these tabs provide the capability to start with a 10,000-foot view of a security incident and then progress through deepening levels of perspective for supporting threat information.

The ThreatStream dashboard itself provides a summary of Observables, False Positives, Contributions and Last Indicators Received. This page contains an excellent overview for understanding the breadth of ingested indicators as well as the analyst's unique contributions to the mission. The Last Indicator Received also offers a quick health-check, letting the analyst know the platform is operating as expected.

The panels below Observables show a quick graphic summary of Internal, Private Feeds and Open Source Feeds. The Latest Activity panel provides updates on analyst activity, vulnerability updates and threat bulletins, and provides a good heads-up display for required actions each time the analyst accesses the tool. The Overview Dashboard also allows for adding custom widgets for additional functionality such as Attack Metrics, Impacts and Threat Models.

The Dashboard Overview has several additional features across a secondary ribbon: My Events, Weekly Summary, Community Threats and Reporting. The My Events feature provides a geographic representation of threat data across the globe, including filtering for threat data related to your organization. The ThreatStream Dashboard: My Events in Figure 2 begs for space on your SOC's walls!

The Weekly Summary tab provides an assessment of Data Quality, Threats by Severity, Threat Volume and Top Threat Streams. Quantifying the return on security investment (ROSI) for threat intelligence is challenging, and this panel provides useful metrics reporting in an easy-to-decipher dashboard.



TOP COUNTRIES

[50] CHINA
[43] UNITED STATES
[14] FRANCE
[11] BRAZIL
[10] BELARUS
[6] NETHERLANDS
[5] UKRAINE
[5] TURKEY
[4] RUSSIA
[4] CANADA
[4] MEXICO
[3] INDIA
[3] VIETNAM
[3] GERMANY
[3] UNITED KINGDOM
[2] JAPAN
[2] ITALY
[2] INDONESIA
[2] THAILAND
[2] PAKISTAN
[1] UNITED ARAB EMIRATES
[1] KAZAKHSTAN
[1] ESTONIA
[1] MALI
[1] SWEDEN
[1] NIGERIA
[1] CAMBODIA
[1] SOUTH AFRICA
[1] CZECH REPUBLIC
[1] ALBANIA
[1] POLAND
[1] SOUTH KOREA
[1] EGYPT
[1] HONG KONG
[1] MALAYSIA
[1] GHANA
[1] BOLIVIA

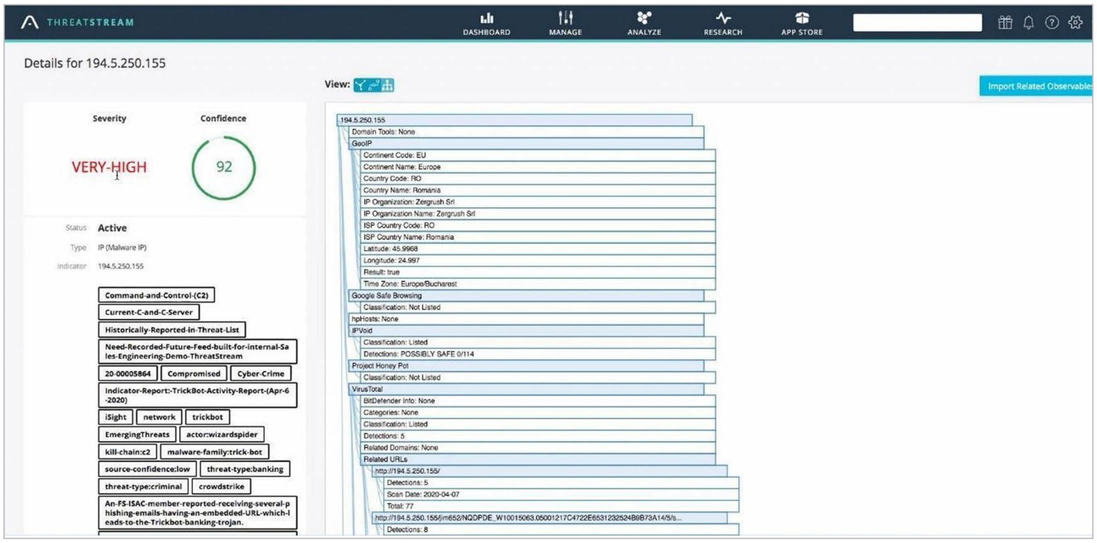
[200] MALWARE

https://servis-alienware.by...
http://autoinstructor.kh.ua...
http://estiloraropremium.c...
http://kompremont.by/gbni...
http://idoux-maconnerie.fr...
http://gocastores.com/olbk...
http://36.32.110.40:37356/...
http://115.219.135.15:4240...
http://27.41.157.126:55302...
http://115.59.5.14:49272/M...
http://218.73.52.254:55985...

Figure 2. Anomali ThreatStream Dashboard: My Events

The Community Threats tab provides the ability to follow Threat Actors, Tactics and Threat Bulletins. This panel struck the SANS team as rather innovative because you can tune into watching a daily threat group report like it's the evening news. If an organization identifies an advanced persistent threat (APT) targeting its network, it can follow the group's activity for proactive ingestion into the intelligence cycle.

ThreatStream's Manage feature provides several options to facilitate ease of managing threat intelligence sources and integrating security controls. These features include drill-downs for Imports, Trusted Circles, Streams, Rules and Source Optimizers. The SANS team was impressed by the flexibility and depth of this feature. Integrating feeds is often a challenging endeavor for security teams, and this feature reduces manual effort. Threat feed integration is a valuable feature for both data consolidation and retaining the value of existing threat intelligence feed investments. The Filter option allows filtering by Status, Import Date and Owner. At first, this page seemed simplistic without the depth of a query language, but it became rapidly evident that this GUI is useful for sorting intel rapidly.



Details for 194.5.250.155

Severity: VERY-HIGH
Confidence: 92

Status: Active
Type: IP (Malware IP)
Indicator: 194.5.250.155

Command-and-Control-(C2)
Current-C-and-C-Server
Historically-Reported-in-Threat-List
Need-Recorded-Future-Feed-built-for-internal-Sales-Engineering-Demo-ThreatStream
20-00005864 | Compromised | Cyber-Crime
Indicator-Report:-TrickBot-Activity-Report-(Apr-6-2020)
iSight | network | trickbot
EmergingThreats | actor:wizardspider
kill-chain:c2 | malware-family:trick-bot
source-confidence:low | threat-type:banking
threat-type:criminal | crowdstrike
An-FS-ISAC-member-reported-receiving-several-phishing-emails-having-an-embedded-URL-which-leads-to-the-Trickbot-banking-trojan.

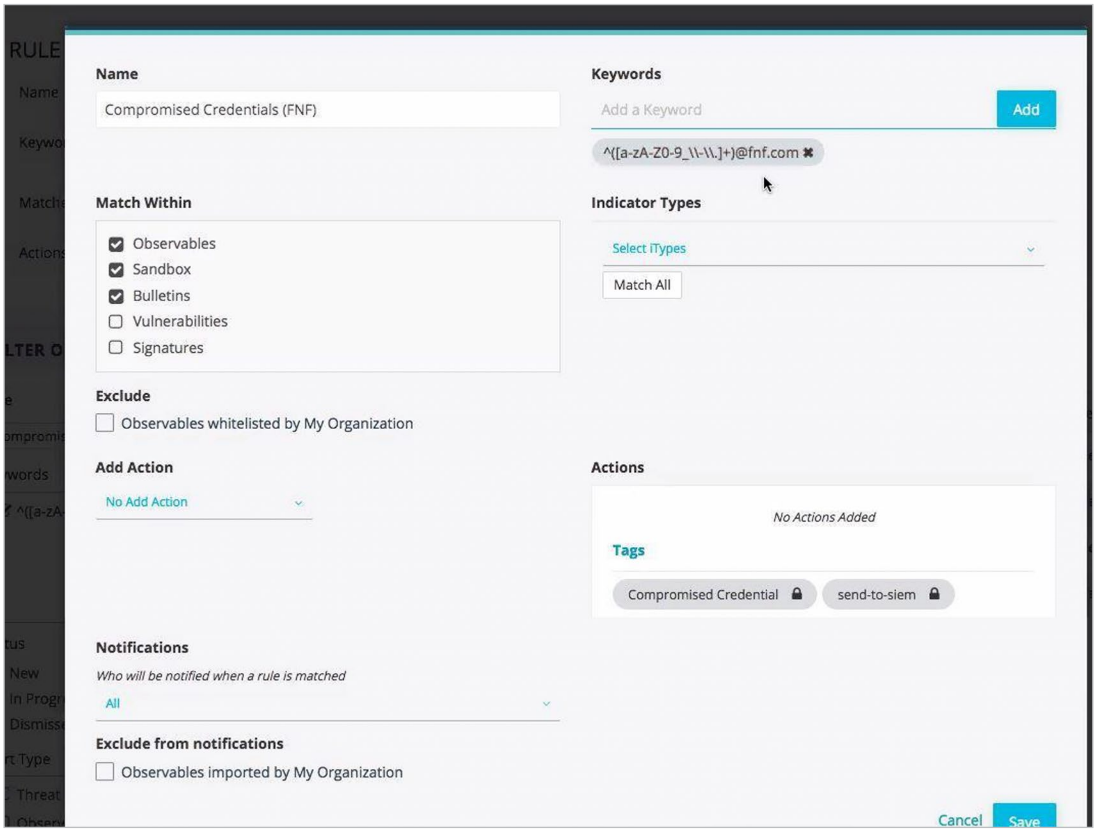
```
194.5.250.155
    Domain Tools: None
    GeoIP
        Continent Code: EU
        Continent Name: Europe
        Country Code: RO
        Country Name: Romania
        IP Organization: Zergrush Srl
        IP Organization Name: Zergrush Srl
        ISP Country Code: RO
        ISP Country Name: Romania
        Latitude: 45.9968
        Longitude: 24.997
        Result: true
        Time Zone: Europe/Bucharest
    Google Safe Browsing
        Classification: Not Listed
    hpHosts: None
    IPVoid
        Classification: Listed
        Detections: POSSIBLY SAFE 0/114
    Project Honey Pot
        Classification: Not Listed
    VirusTotal
        BitDefender Info: None
        Categories: None
        Classification: Listed
        Detections: 5
        Related Domains: None
        Related URLs
            http://194.5.250.155/
                Detections: 5
                Scan Date: 2020-04-07
                Total: 77
            http://194.5.250.155/jim652/NQDPDE_W10015063.05001217C4722E6531232524B9B73A14/5/s...
                Detections: 8
```

Figure 3. Indicators

The Associate Threat Models feature facilitates indicator association with known malware families and threat groups. Threat association is incredibly powerful because it allows the community to collaborate while creating detailed repositories of threat behavior, signatures and tactics. Figure 3 demonstrates the depth of association models with numerous metadata tags, threat evaluation and indicators associated with a single IP address.

ThreatStream's Manage Streams feature provided options for us to easily manage data sources right inside the platform. The platform comes with more than 100 preconfigured streams. Some of these are open source; others are Anomali Community shares, and users can enable or disable them at will. Management of third-party specialized intelligence is done in the APP Store tab, discussed separately in a later section. During our exercise, sorting by Last Seen yielded AlienVault OTX Malicious IPs as the most recent indicators. The SANS team was impressed to see that the feed had been updated within the past three minutes, and it's reassuring to see how fast providers can update data. Drilling down into the AlienVault feed provided organizational classifications, and the provider contributed 128,612 IoCs within the past 90 days. Digging more in depth into the Observed Indicator Type (iType) provided more than 150,000 scanning indicators organized by Date First Seen, Indicator Type, IP Address, Confidence Rating, Country, Source and Tags. The most recent indicators were less than four hours old. It seemed there was too much data on this page, so the SANS team used Filter Options to show the Last 24 Hours, Active, which provided a reduction to about 2,000 indicators. This feature is valuable for analysts seeking to sort through many feeds across thousands of indicators while pivoting into the most critical observables.

ThreatStream's Manage Rules feature provided options for generating custom threat intelligence feeds. Figure 4 is an example of using custom search rules to enable faster decision making.



Name: Compromised Credentials (FNF)

Keywords: Add a Keyword

^([a-zA-Z0-9_\\-\\.]+)@fnf.com ✖

Match Within

☑ Observables

☑ Sandbox

☑ Bulletins

☐ Vulnerabilities

☐ Signatures

Indicator Types: Select iTypes

Match All

Exclude

☐ Observables whitelisted by My Organization

Add Action: No Add Action

Actions

No Actions Added

Tags: Compromised Credential, send-to-siem

Notifications

Who will be notified when a rule is matched

All

Exclude from notifications

☐ Observables imported by My Organization

Figure 4. Custom Search Rules

This feature is like subscribing to a tailored RSS feed with custom filtering. The New Rule Creation provides the capability to match within Observables, Sandbox Reports, Threat Bulletins, Vulnerabilities and Signatures. While this capability is standard across the industry, differentiating factors include whitelist exclusion. This is a great feature to ensure security teams close the loop without viewing behavior they've already triaged. The Add Action configuration stands out as a unique capability for combining a threat intelligence platform with intelligent analyst orchestration and automation options, including Tag with Terms, Associate to Threat Model or Add to Investigation. Add Action adds an incredible level of depth via automation as new threat indicators from the Trusted Circles: Associate Threat Models can be automatically updated in models, tagged to queries and added to investigations. The SANS team observed that this type of capability can update security operations teams within minutes.

We know there are threat data overlaps as attackers hit multiple targets, which are reported by various groups. Source Optimizer allows a rapid comparison to identify Source Reliability, Volume of Signatures and False-Positive Ratings between multiple threat streams. Furthermore, this feature would be invaluable in the decision-making process for acquiring or subscribing to new feeds.

ThreatStream's Analyze Observables capability provides several analytical features, including a Link Analysis Tool. Initially, it appeared simplistic, but when the SANS team right-clicked, it provided a convenient parent/child-type GUI search feature to query associations. It also confirmed the indicator's 10 reporting providers while leveraging Macula machine learning to recommend custom enrichments at the metadata layer.

The ThreatStream Analyze Threat Model feature provided about 20,000 threat model reports. This page offers the same convenient filtering options to reduce data overload. Selecting the Anomali Lens magnifying glass in the top right of the page applied Anomali's Lens product to assess the most essential points of the Threat Model dataset. This feature immediately highlighted Snake and WannaCry as trending via fire icons. This feature was very refreshing, and Anomali Lens enriches the ThreatStream product while reducing analyst fatigue in combing through massive threat datasets.

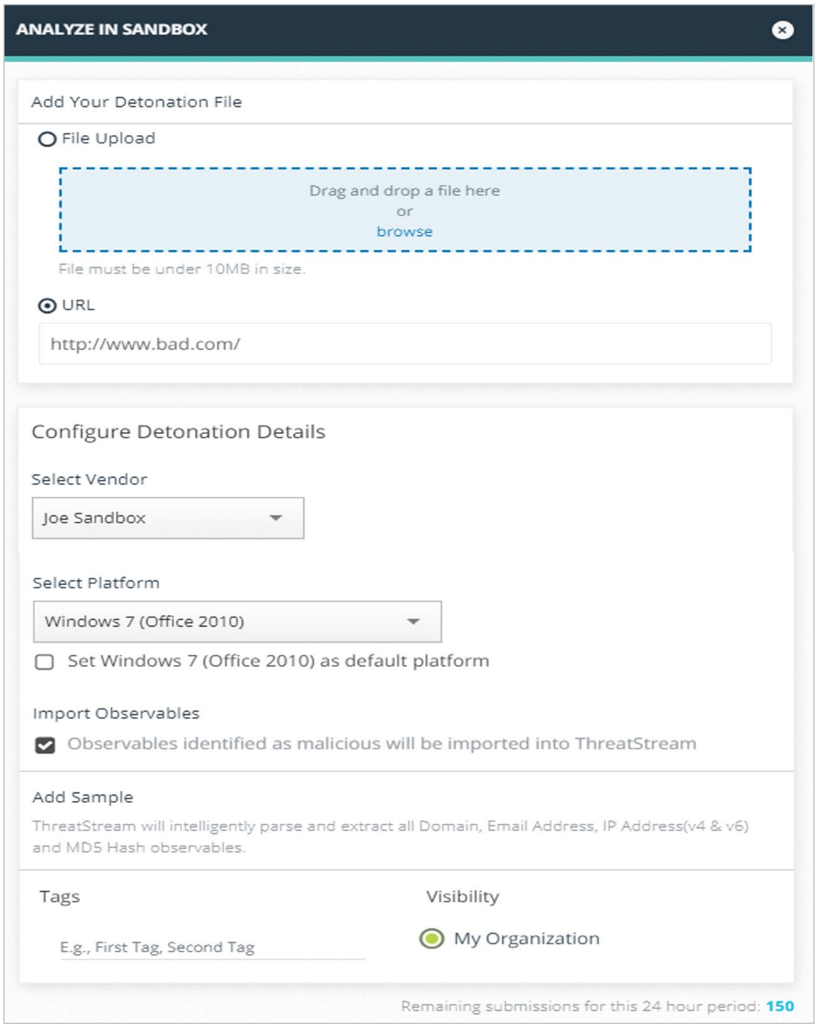
Lastly, the SANS team reviewed ThreatStream's Anomali Preferred Partner (APP) Store, which provides a centralized portal in a tab inside the ThreatStream administrative console to subscribe to some 70 specialized commercial threat intelligence feeds and enrichment offerings from third-party providers. Several free versions of feeds from well-known threat intelligence vendors are also bundled with the ThreatStream subscription, and click-to-activate 30-day trials for most premium feeds in the marketplace provide an excellent avenue for evaluating the best feeds for organizational requirements. This consolidation is incredibly helpful because individually subscribing to and integrating multiple feeds is a time-consuming process, leaving aside the optimization features that ThreatStream provides. Anomali also includes in the platform several Anomali Threat Research feeds and, as discussed earlier, out-of-the-box integration with more than 130 open source feeds.

Complementary Anomali Products

It's important to understand where ThreatStream fits into the Anomali products portfolio. The Anomali suite is composed of three major product offerings: Anomali ThreatStream, Anomali Match™ and Anomali Lens™. Anomali ThreatStream is the flagship product and provides threat intelligence aggregation and integration. Anomali Lens scans webpages for cyber threat data while providing information on severity, confidence rating, type and threat association, as well as an observation assessment. Anomali Match is a real-time threat and breach analytics platform that applies correlation rules and advanced security analysis to cross-correlate data from security information and event management (SIEM) systems and other event sources deployed in an organization's network to threat intelligence available from ThreatStream.

Use Case 1: Phishing Link Analysis

A phishing attack is the most common scenario encountered by incident response teams. Analyzing a phishing email often requires movement between several tools for analysis, detonation, investigation and sharing. Accessing the Anomali ThreatStream platform consolidates Investigation, Sandbox and Explore functions. Navigating to the Investigations page to Create New Investigation is a good starting point. Creating a new investigation provides a tracking mechanism to align all related indicators into a single investigation. ThreatStream Investigation provides a great base to consolidate relevant artifacts for centralized tracking.



ANALYZE IN SANDBOX

Add Your Detonation File

○ File Upload

Drag and drop a file here
or
browse

File must be under 10MB in size.

● URL

http://www.bad.com/

Configure Detonation Details

Select Vendor

Joe Sandbox

Select Platform

Windows 7 (Office 2010)

□ Set Windows 7 (Office 2010) as default platform

Import Observables

☑ Observables identified as malicious will be imported into ThreatStream

Add Sample

ThreatStream will intelligently parse and extract all Domain, Email Address, IP Address(v4 & v6) and MD5 Hash observables.

Tags

E.g., First Tag, Second Tag

Visibility

● My Organization

Remaining submissions for this 24 hour period: 150

Figure 5. Anomali ThreatStream Integrated Sandboxing

Next, the ThreatStream Research feature provides a tight integration with multiple sandbox vendors. This allows the analyst to remain in a single research space covering multiple functions while reducing fatigue in tooling. Detonation options are provided for key sandboxing use cases: Email, attachment or URL detonations are available across multiple target operating environments (Microsoft Windows 10, Microsoft Windows 7 and macOS). The detonation of our example “www.bad.com” in Windows 7, which is shown in Figure 5, yielded findings within three minutes of processing. This feature does a great job of processing suspect artifacts while starting and continuing an investigation.

Next, the analyst leverages the indicators extracted with the ThreatStream Explore feature. Adding our sample www.bad.com and a few auto-generated hashes produce association mappings. Figure 6 demonstrates entity enrichment, which provides an awesome mind-map and searching feature for the analyst to compare indicators to determine if there is an association. ThreatStream rapidly centralized artifacts, detonated the phishing URL and correlated related indicators across Threat Models.

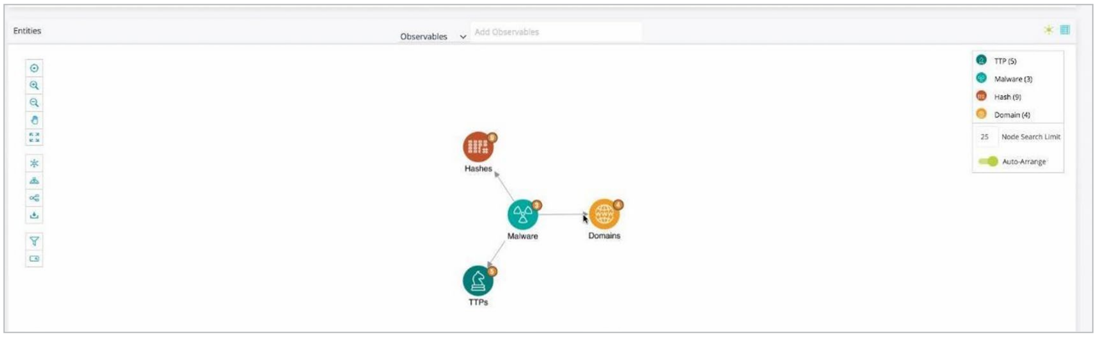
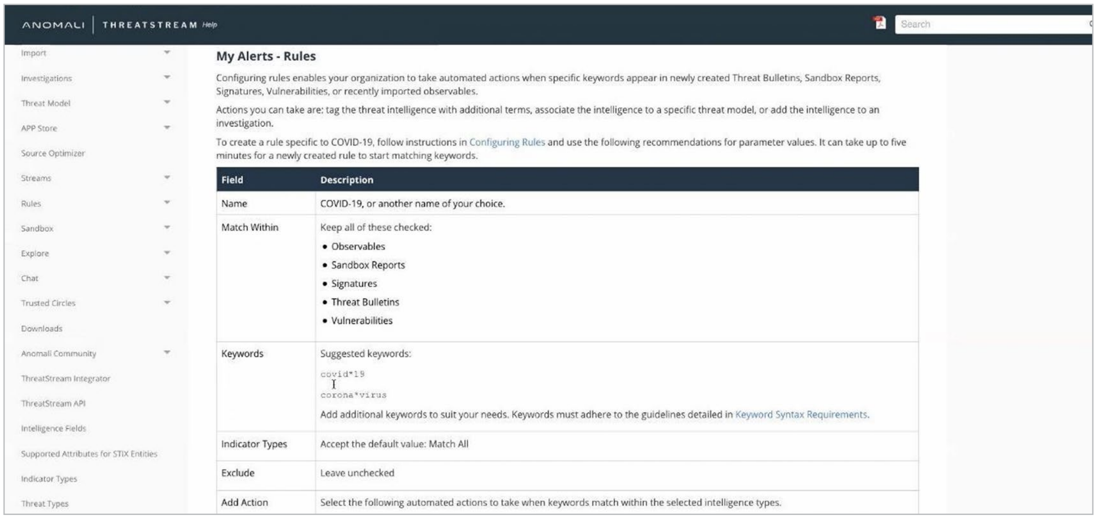


Figure 6. Entity Enrichment

Use Case 2: Distribute Threat Intelligence

The second use case aligns with reporting threat data internally within an organization. Accessing the ThreatStream Analyze overview page provides a dashboard for tracking threat actors. Analyze is unique because, generally, these types of dashboards are used for incidents and events rather than actors. The page is so full featured that it requires a pan downward to view the multiple windows, including Actors, Patterns, Campaigns, Incidents, Malware, Signatures, Bulletins, and Tools. Figure 7 shows a sample page for indicators associated with COVID-19.

Selecting a sample threat group, FIN10 yields a treasure trove of actor information. This threat-profile Description page has a Wikipedia-like presentation, which is something that traditionally requires countless hours of open source research. This feature has enough depth to provide a detailed profile of threat actors, but in a bite-size format requiring only two to three minutes of reading. Accessing ThreatStream Associations provides a time-saving pivot point to other applicable ThreatStream features such as Observables, Threat Modules, Sessions and Sandboxing. Drilling down into the actor's Threat Models provided 10 detailed Tactics, Techniques and Procedures, which each yielded incredibly detailed descriptions of attack methods aligned to the MITRE ATT&CK framework.



My Alerts - Rules

Configuring rules enables your organization to take automated actions when specific keywords appear in newly created Threat Bulletins, Sandbox Reports, Signatures, Vulnerabilities, or recently imported observables.

Actions you can take are: tag the threat intelligence with additional terms, associate the intelligence to a specific threat model, or add the intelligence to an investigation.

To create a rule specific to COVID-19, follow instructions in Configuring Rules and use the following recommendations for parameter values. It can take up to five minutes for a newly created rule to start matching keywords.

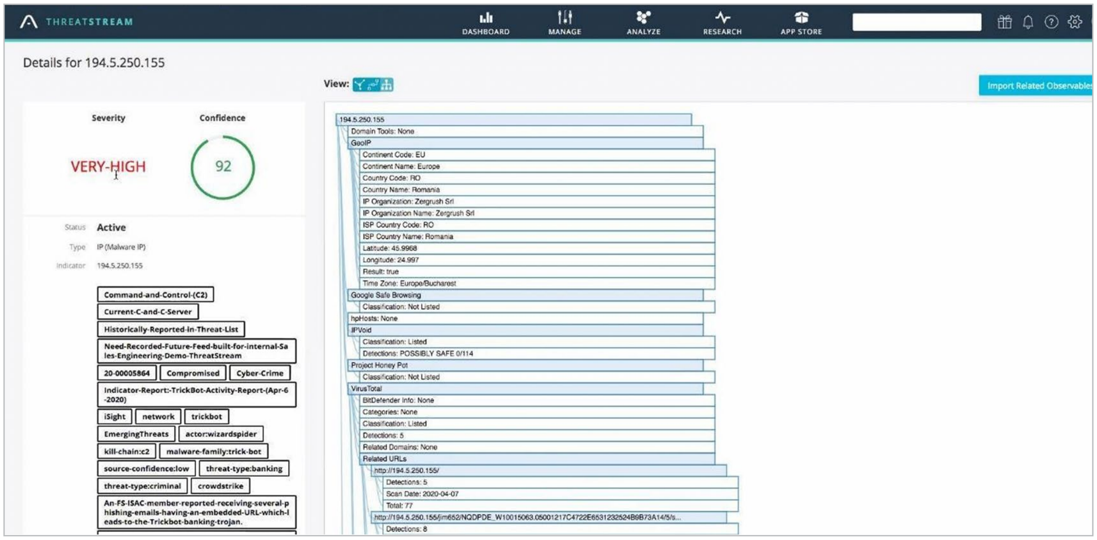
Field	Description
Name	COVID-19, or another name of your choice.
Match Within	Keep all of these checked: • Observables • Sandbox Reports • Signatures • Threat Bulletins • Vulnerabilities

Keywords	Suggested keywords:
	`covid*19`
	`corona*virus`
	Add additional keywords to suit your needs. Keywords must adhere to the guidelines detailed in Keyword Syntax Requirements.

Indicator Types	Accept the default value: Match All
Exclude	Leave unchecked
Add Action	Select the following automated actions to take when keywords match within the selected intelligence types.

Figure 7. COVID-19 Indicators

The ThreatStream Analyze Observables feature provides another rich overview of indicators. The filtered criteria are automatically mirrored across a search bar, which rapidly builds a customized query. A few quick filters promptly delivered a query and narrowed hundreds of thousands of indicators into a small, customized subset. Drilling down into a malware file hash provides a massive amount of threat data. The SANS team was impressed at the sheer breadth of information for a single indicator at the lowest level of threat intelligence. Figure 8 shows the depth of indicators and associations for a single IP address.



Details for 194.5.250.155

VERY-HIGH

92

Status Active
Type IP (Malware IP)
Indicator 194.5.250.155

Command-and-Control-(C2)
Current-C-and-C-Server
Historically-Reported-in-Threat-List
Need-Recorded-Future-Feed-built-for-internal-Sales-Engineering-Demo-ThreatStream
20-00005864 Compromised Cyber-Crime
Indicator-Report:-TrickBot-Activity-Report-(Apr-6-2020)
iSight network trickbot
EmergingThreats actor:wizardspider
kill-chain:c2 malware-family:trick-bot
source-confidence:low threat-type:banking
threat-type:criminal crowdstrike
An-FS-ISAC-member-reported-receiving-several-phishing-emails-having-an-embedded-URL-which-leads-to-the-Trickbot-banking-trojan.

```
194.5.250.155
  Domain Tools: None
  GeoIP
    Continent Code: EU
    Continent Name: Europe
    Country Code: RO
    Country Name: Romania
    IP Organization: Zergrush Srl
    IP Organization Name: Zergrush Srl
    ISP Country Code: RO
    ISP Country Name: Romania
    Latitude: 45.9968
    Longitude: 24.997
    Result: true
    Time Zone: Europe/Bucharest
  Google Safe Browsing
    Classification: Not Listed
  hpHosts: None
  IPVoid
    Classification: Listed
    Detections: POSSIBLY SAFE 0/114
  Project Honey Pot
    Classification: Not Listed
  VirusTotal
    BitDefender Info: None
    Categories: None
    Classification: Listed
    Detections: 5
    Related Domains: None
    Related URLs
      http://194.5.250.155/
        Detections: 5
        Scan Date: 2020-04-07
        Total: 77
      http://194.5.250.155/jim652/NQDPDE_W10015063.05001217C4722E6531232524B9B73A14/5/s...
        Detections: 8
```

Figure 8. Indicators

Understanding that this level of depth translates across millions of threat indicators is a significant distinguishing factor. It raised the question: “How could we, as analysts, brief our leadership on this type of data?” Fortunately, the Anomali team provided a PDF export that immediately uploaded the threat data into an executive-level presentation format.

Use Case 3: Trusted Circles Sharing

The last use case aligns with sharing threat data with the community. Accessing the ThreatStream Manage Trusted Circles module provides an overview of currently accessible trusted communities. Selecting Show Public Circles immediately populates the screen with 81 available public circles. The options appear like a social media friend page, which guides the user toward understanding the value of sharing threat data across the information security community. Selecting the Members drop-down sorts to the Public Circle with the greatest number of members: CISA’s Cyber Information Sharing and Collaboration Program (CISCP), which has 776 members. Selecting Request Invite returns a notification that the request is submitted to the respective community ThreatStream administrator for approval. Choosing Create New Circle is a very cool feature along the same lines as creating a group on a social media page. The SANS team created a group and marked it as “Anonymous.” The simple Edit option allowed reconfiguration to Public Circle. Private Circles provide valuable opportunities for sharing an organization’s threat data while also controlling distribution. Selecting Share Intelligence opened a highly versatile upload portal, including options for STIX, Email/Phishing and Threat Models. Adding the phishing URL indicators from our first use case allowed us to share the data via our Public Circle.

An interesting distinction is the ability to share this data across multiple Trusted Circles. The SANS team felt this was a critical capability for sharing the highest severity IoCs, for example, the indicators shared across the community during the WannaCry outbreak. Definitions also provided the ability to expire data across fixed and custom time ranges. Attacks often abandon techniques after detection, so this configuration does a great job of reinforcing the time-bound approach to threat data.

Summary

Our experience with Anomali ThreatStream was overwhelmingly positive. It proved to be a very powerful threat intelligence platform that has significant benefits for security and intelligence analysts struggling to aggregate intelligence, enabling them to make sense of it quickly to recommend or take actions critical to the security of their organization. The unified platform empowers users to research, report and disseminate intelligence across complex hybrid and cloud environments. We found the platform remarkably easy to use. Within minutes of first starting, we were able to investigate threats, analyze URLs, detonate suspicious files within a sandbox, create investigations that included compelling visual network diagramming, and access Trusted Circles that allowed us to confidentially share intelligence with selected partners within a secure environment.

In this review, we took special note of ThreatStream's ease of integration of intelligence feeds, powerful analysis features, deep investigation capabilities and mature threat-sharing methods. This breadth of capabilities addresses virtually all the threat intelligence challenges identified, including threat data aggregation, analyst time savings and false-positive reductions. The efficient aggregation of threat data is a capability nearly impossible to replicate by applying traditional techniques across numerous individual feeds and using manual analytical methods. Based on the depth of portal features, we recommend ThreatStream for mid- to senior-level analysts, although Lens appears to help bridge the productivity gap for less experienced analysts.

Anomali's complementary products, Anomali Match and Anomali Lens, have a "built-by-analysts-for-analysts" feel to them and significantly enhance the value of Anomali's suite of products as an operational intelligence platform.

As security professionals continue to struggle to balance the opportunity (and need) for massive threat and security telemetry data collection with the lack of resources and time available to capitalize on the required access to data, information and intelligence, they need tools that are easier to use, with deep and robust capabilities to search intuitively for threat data, IoCs and adversary behavior. Anomali ThreatStream can help analysts immensely and promises to turbocharge any security program. Tools and capabilities like the ones available through Anomali are critical to the success of cyber threat intelligence (CTI) programs seeking to move from a reactive to a proactive security stance.

About the Author

TJ Banasik is a SANS analyst and has consulted with numerous organizations in cybersecurity across the government, military and commercial sectors. A security operations expert, TJ has extensive experience in security engineering, incident response, insider threat and threat vulnerability management. TJ has worked as senior program manager for Microsoft Azure Government and director of security operations for Veritas Technologies. He worked previously as Senior Security Operations Center manager for the U.S. Government Accountability Office (CSRA) and Army Officer with Army Cyber Command (ARCYBER). TJ holds the GCIH, GCWN, GCIA, GCFA, GCCC, GSEC, GPEN and CISSP-ISSEP, -ISSAP, -ISSMP certifications. He holds a graduate degree in intelligence studies concentration cyber from American Military University (AMU).

Sponsor

SANS would like to thank this paper's sponsor:

ANOMALI®