# Recorded Future Analyst Notes v2.1.1 - Anomali ThreatStream Installation Guide

- · Application Description
- Application Functionality
  - Analyst Notes Topics
    - How Multiple Topics are Handled
  - Notes Details
    - Hunting Package
  - Observables
    - Confidence
    - Tags
  - Associations
- Installation
  - Configuration
- Tags
- Troubleshooting
  - Missing Observables
  - IOC with 0 risk score and no Intelligence Card
- Limitations
  - CVE Enrichment
- CHANGELOG

# **Application Description** *®*

Recorded Future is continuously harvesting data from Open, Deep, and Dark Web sources in real-time including Social media, Forums, Blogs, IRC channels, Paste sites, email groups, onion sites via TOR, and more through a range of collection mechanisms. Thousands of sources are added to our index for customers each week and are currently mining and cross-correlating data from over 750,000+ sources in seven languages with a patented Temporal Analytics™ Engine.

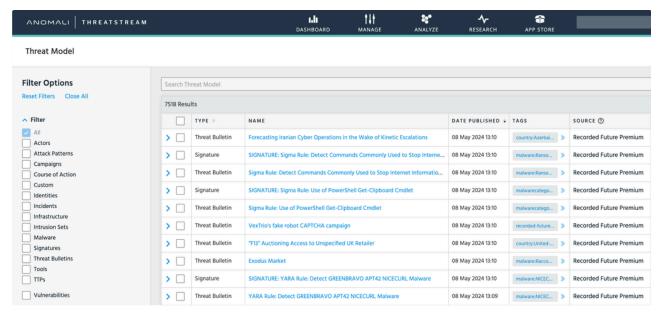
The Recorded Future Analyst Notes for Anomali ThreatStream(TS) enables:

- Delivery of Recorded Future Analyst Notes details into Anomali TS as threat models via an Anomali TS Feed
- Delivery of critical detection rules (Yara/Sigma/Snort) with the Analyst Notes
- Ease of triage of the report with full context and observables extraction

# Application Functionality @

Recorded Future Analyst Notes application's functionality is underpinned by the Recorded Future API, which is the repository from which Anomali TS retrieves the Recorded Future data. The integration fetches analyst notes details and feeds them to Anomali TS. This makes the Analyst Note context ready for triaging within Anomali TS.

Alerts ingested by the Recorded Future Premium Feed can be found in the Threat Model view as shown below:



Recorded Future Analyst Notes in Threat Model View

#### **Analyst Notes Topics** *⊘*

The table below documents analyst note topics supported by the integration and their respective Threat Model types once ingested into Anomali TS.

Analyst Note Topic	Anomali TS Threat Model
Actor Profile	Actor
Cyber Threat Analysis	Threat Bulletin
Executive Insights	Threat Bulletin
Flash Report	Threat Bulletin
Hunting Package	Signature and Threat Bulletin Report
Indicator	Threat Bulletin
Informational	Vulnerability
Malware Tool Profile	Malware
Source Profile	Threat Bulletin
Ransomware Actor Profile	Actor
Ransomware Tool Profile	Malware
Threat Lead	Threat Bulletin
TTP Instance	Threat Bulletin
Validated Intelligence Event	Incident

#### How Multiple Topics are Handled ${\mathscr O}$

The notes ingested are classified based on their higher priority topic, as described below:

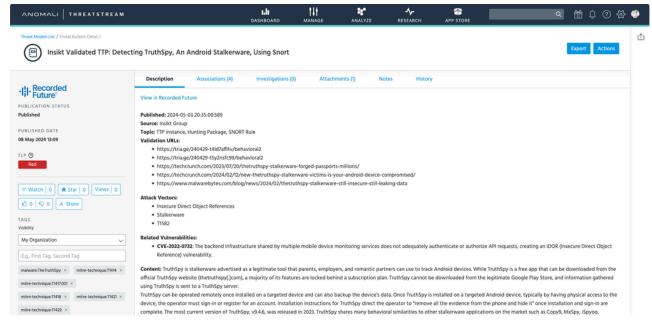
• If a note has only one topic, then that topic will be chosen and the Anomali TS Threat Model will be picked based on the table above.

- If a note has more than one topic the topics are then ordered based on the following priority (lower priority the most important it is):
  - o Priority 1: Hunting Package
  - o Priority 2: Ransomware Tool Profile
  - Priority 3: Ransomware Actor Profile
  - o Priority 4: Malware Tool Profile
  - o Priority 5: Actor Profile
  - o Priority 6: Validated Intelligence Event
  - o Priority 7: Informational
  - o Priority 999: every other topic which always default to a Threat Bulletin Report.
- for example a note with topics Validated Intelligence Event, Hunting Package and Threat Lead will be considered as a Hunting Package note, this will result in the creation of a Signature and Threat Bulletin Reports respectively.

#### Notes Details @

Ingested Analyst Note Threat Model contains:

- · Title of the note
- · Link to the Recorded Future portal to the specific note
- Source
- Topic
- Validation URLs (If Available)
- · Any attack vector related to the tool or actor described (If Available)
- · Any vulnerability used or mentioned in the note along with a description (If Available)
- The full content of the note
- Attachment in the Attachments tab (If available)
- Malware Tools Profile & Ransomeware Tool Profile (Malware Threat Model)
  - The Malware Types and Execution Platforms fields are included if available. The Malware Family field is always set to "Malware Instance".
- Observables, see the **Observables** section for more information (If Available)
- 1 Every note topic might produce some tags specific to the note type, check the Tags section for the full list.

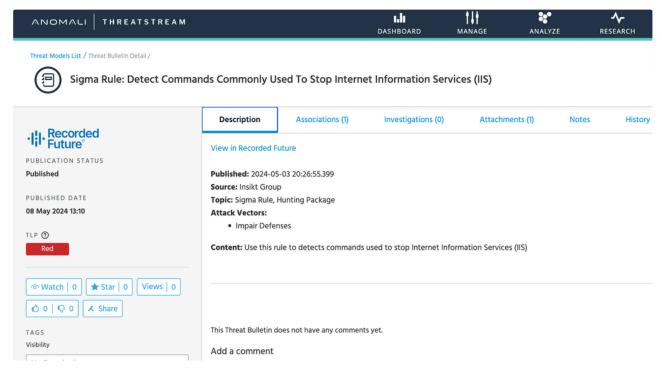


Recorded Future Analyst Note in Anomali TS

#### **Hunting Package** *𝒜*

Hunting Package notes contain detections rules (Yara, Sigma or Snort) that help detecting malicious activities. These notes will create two reports that are associated together:

- · First report: of Threat Bulletin Detail type, will contain all the standard details plus the attachment of the detection rule
- Second report: of type Signature, will contain the plain text payload of the detection rule. The report title is prefixed with "Signature:"



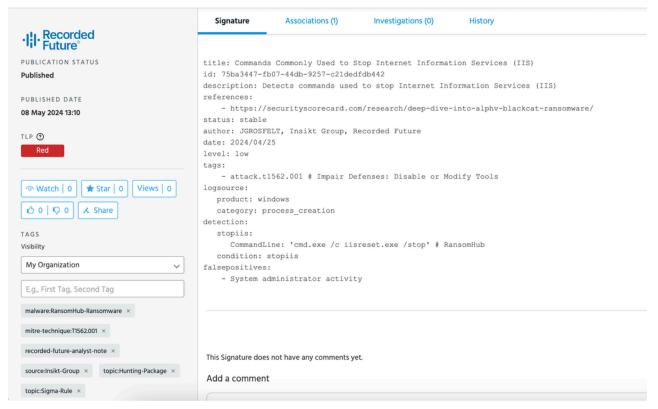
First report of Threat Bulletin Detail



Threat Models List / Signature Detail /



SIGNATURE: Sigma Rule: Detect Commands Commonly Used To Stop Internet Information Services (IIS)



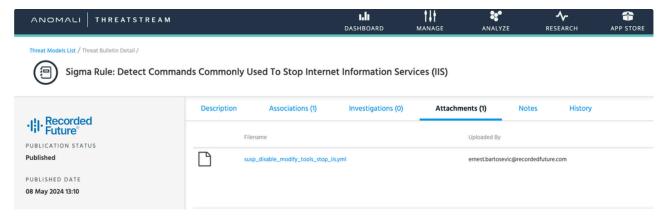
Second Report of type Signature

Navigating in Associations > Threat Models, the linked note will be found.



Signature: Sigma rule linked with Threat Bulletin Report

The Threat Bullet Detail report will have the attachment available to download:



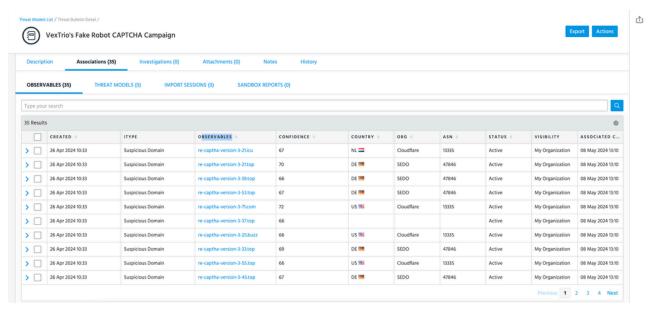
Yara rule as an attachment in Threat Bulletin Report

#### Observables @

Some notes might might contain a domain, hash, IP address or a URL. This will result in the creation of observables along with a Recorded Future Risk Score (if available). Only Very Malicious and Malicious IOCs will be added as Observables. The IType varies based on the most critical Recorded Future Risk Rule associated with the IOC.

#### **Confidence** *⊘*

The confidence of each observable will be equal to the Recorded Future risk score of the observable plus 1. The addition of 1 is to match the Anomali scale which goes up to 100 instead of 99.



Observables associated from an Analyst Note in Anomali TS

#### Tags @

The created Observables will contain **Tags** in relation to the ingested Analyst Note Threat Model. Please see the **Tags** section of the install guide for more information.

#### Associations @

The following associations are made by the integration:

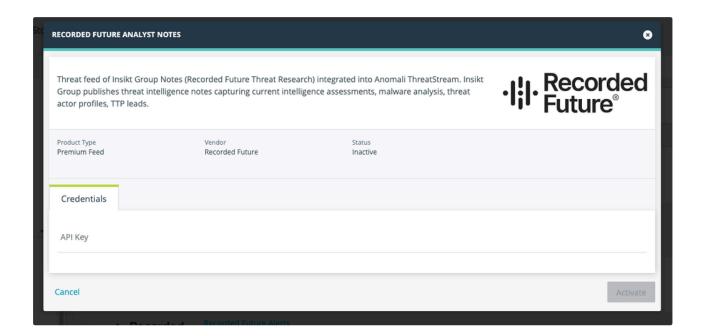
- · Between a Signature and the related Threat Bulletin Report, as seen in section Hunting Packages
- Between any report if they have the same entities as they are likely to be related to each other

#### Installation @

The preferred installation method for the Recorded Future Analyst Notes is through the Anomali TS App Store.

#### **Configuration** *@*

Once the application is installed please set the Recorded Future API Key and click Activate.



# Tags *∂*

Recorded Future Analyst Notes integration uses a set of common tags that are added to the Threat Models and Observables. These tags help to quickly and easily search and build dashboards from the Recorded Future Analyst Note data.

Please note the Observables column in the table below indicates which tags are also applicable to observables.

Tag	Analyst Note Topic	Threat Model Type	Observabl es	Example	Description
alias	Actor Profile	Actor		alias:KillMilk	Indicates the alias given to a threat actor or group.
analyst-note-id	All		✓	analyst-note-id:2VjmPm	Recorded Future Analyst Note ID
country	All			country:Italy	Indicates the country target of the note.

malware	All		malware:UPSTYLE	Indicates the name of the malware mentioned.
malwarecategory	All		malwarecategory:Bac kdoor	Indicates the name of the malware types of malware mentioned.
mitre-tactic	All		mitre-tactic:TA0001	Indicates any MITRE ATT&CK tactics used.
mitre-technique	All		mitre- technique:T1053.003	Indicates any MITRE ATT&CK technique used.
recorded-future- analyst-note	All		recorded-future- analyst-note	Indicates that the Threat Model is a Recorded Future Analyst Note.
source	All	<b>✓</b>	source:Insikt-Group	Indicates the source of the note itself.
topic	All	<b>✓</b>	topic:TTP-Instance	Indicates the topic(s) of the note.

# **Troubleshooting** *⊘*

#### Missing Observables *⊘*

In some cases a threat model report might display a certain amount of observables in the Description tab and yet contain less in the Associations tab, this is due to the fact that Anomali TS has a whitelisting mechanism that prevents certain Observables from being ingested. For more information please contact the Anomali Support team.

#### IOC with 0 risk score and no Intelligence Card *⊘*

There might be an Analyst Note where an IOC might have a risk score of 0 but no information in the intelligence card associated with it in the Recorded Future Portal. That is expected, we decided to still show those IOCs related to the note for completeness of information. The occurrences of such IOC is expected to be very low.

#### **Limitations** @

#### **CVE Enrichment** @

The Informational topic creates an analyst note under the Vulnerability threat model. The Vulnerability threat model does not contain CVSS and CVSSv3 information due to data not being available for the Threat and SecOps modules.

#### **CHANGELOG** @

## [2.1.1] - 2025-05-08 @

#### Added *∂*

• Support for Executive Insights topic

### [2.1.0] - 2025-01-31 @

#### Added *⊘*

- · Analyst Note Threat Model now sets the Source Created time using the Analyst Note published time
- Analyst Note Threat Model now sets applicable Target Industry (when available)
- Support for Ransomware Actor Profile and Ransomware Tool Profile topics
- Observables now contain the following tags in relation to the Analyst Note they were extracted from:
  - o analyst-note-id:<id>
  - o topic:<topic name>
  - o source:<source name>
- 1 Please see the installation guide **Tags** section for more information about the new Observables tags.

#### Changed *∂*

- Analyst Note Threat Model Description no longer shows Published time as it has been replaced by Source Created field in the Anomali User Interface
- · Dependency updates:
  - Anomali Feeds SDK upgraded to v2.5.22
  - PSEngine upgraded to v2.0.1

# [2.0.0] - 2024-05-10 @

#### Added *⊘*

- Support for Hunting Package and TTP Instance topics
- Detection rule support (Threat Model Signature ) for:
  - Sigma
  - Yara
  - Snort
- Analyst note file attachments are attached to the respective threat model
- New tags (see installation guide above)

#### Changed @

- New Analyst Note layout across various Threat Model types
- Indicator confidence is now set like this: Recorded Future risk score + 1
- Priority based selection of Threat Model based on Analyst Note topic
- Various improvements and optimisations of the app
- · Dependency updates:
  - Anomali Feeds SDK upgraded to v2.5.17
  - Introduced integrations library PSEngine v1.12.0

# [1.0.0 GA] - 2021-06-18 @

# Added *⊘*

Official package release