Recorded Future Alerts v1.5.1 - Anomali ThreatStream Installation Guide

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 Alert Feed for Anomali ThreatStream enables:

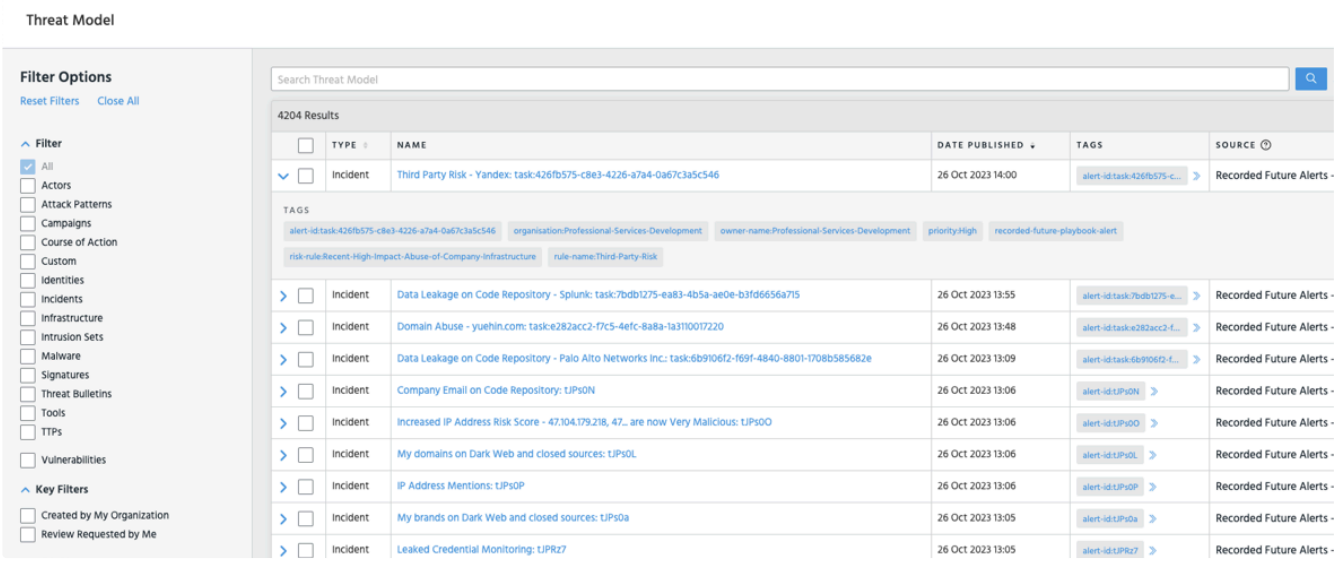
- Delivery of Recorded Future Alert details consumed in Anomali ThreatStream (TS) as Incidents via an Anomali TS Feed.
- Triaging Recorded Future Classic Alerts and Playbook Alerts with the full alert details context directly in the Anomali TS.
- Review trending Intelligence Goals Library (IGL) data.
- Ability to document historical credential leaks.

The Recorded Future Alert Feed for Anomali TS enables better alert triaging by adding relevant and comprehensive context.

Application Functionality

Recorded Future Alerts application's functionality is underpinned by the Recorded Future API, which is the repository from which Anomali TS retrieves the Recorded Future Classic Alerts and Playbook Alerts. The Feed fetches alert details and feeds them to Anomali TS as Incidents. This makes the alert context ready for triaging within Anomali TS.

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



Recorded Future Alerts in Threat Model View

Recorded Future Classic Alerts

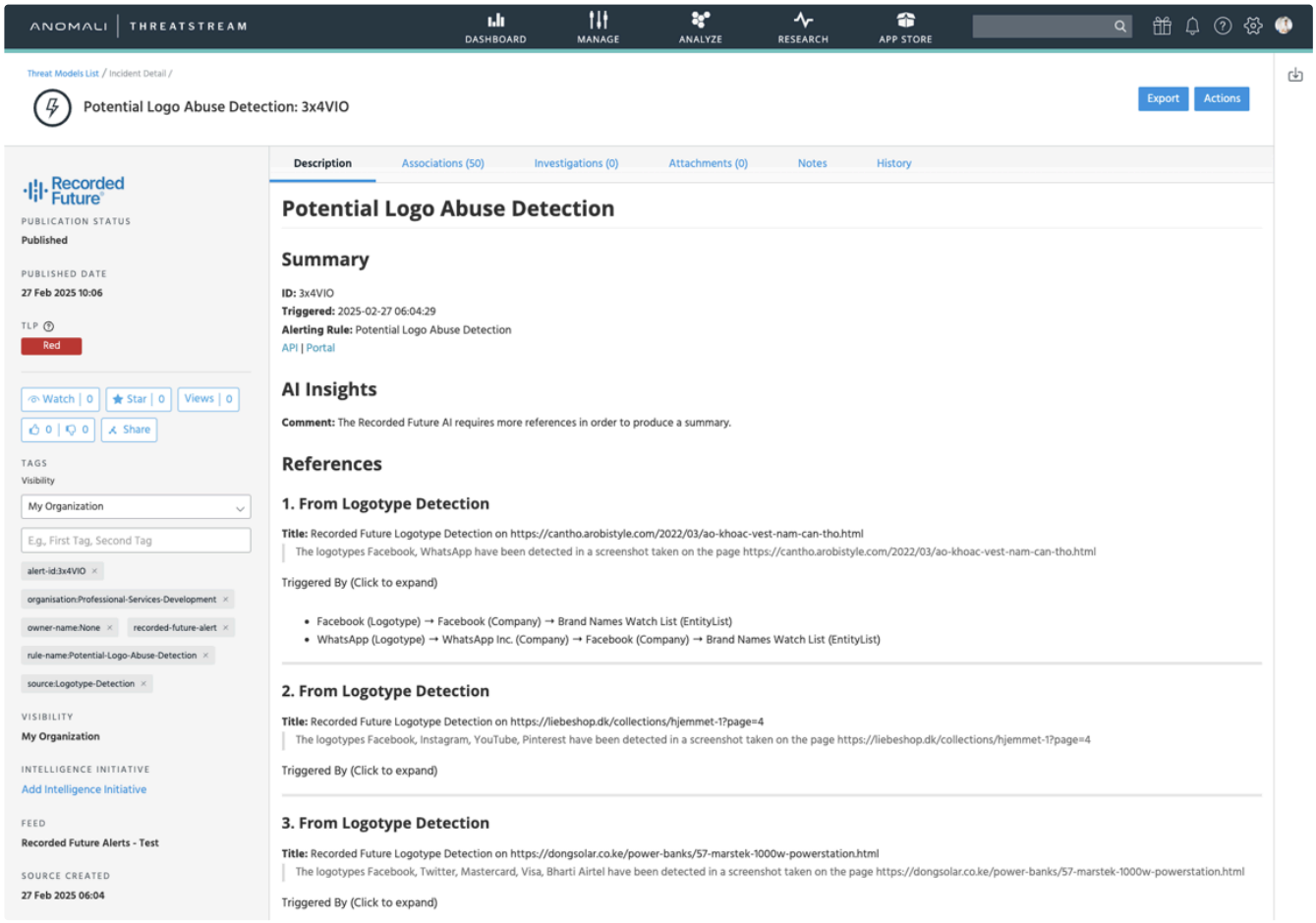
The following classic alerts are supported:

- Intelligence Goal Library (IGL) Alerts
- Custom Alerts

Every Incident created from a Recorded Future Classic Alert contains:

- Tags
- Link to the Recorded Future Platform for further analysis
- Alert Trigger time
- Alert references tables

- Reason for reference inclusion in alert (Triggered by)
- Recorded Future AI Insights



Classic Alert: Potential Logo Abuse Detection

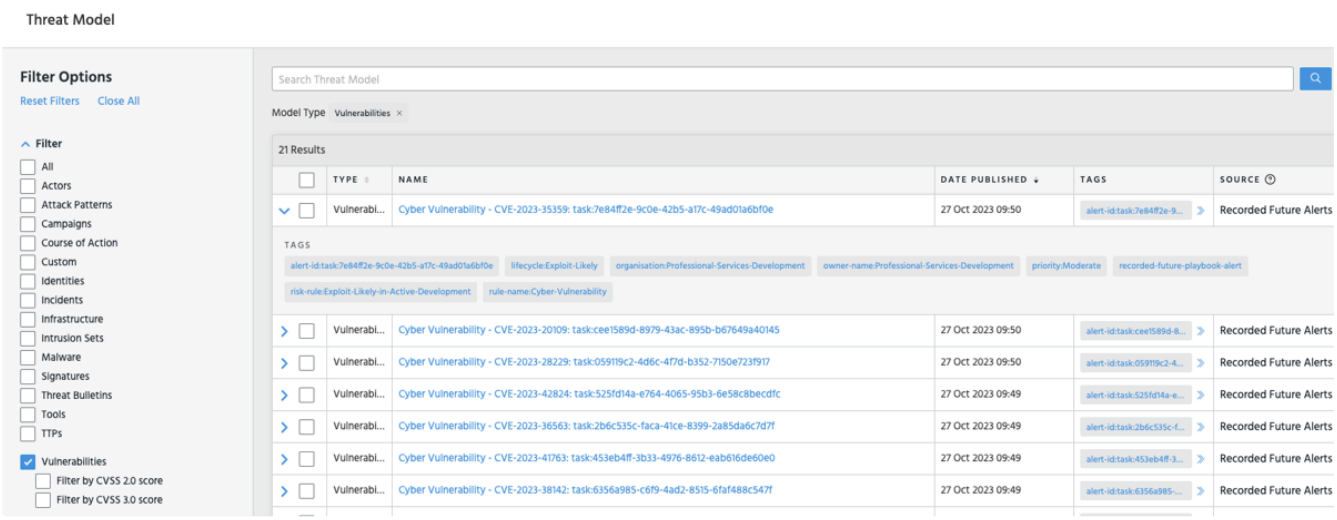
Recorded Future Playbook Alerts

The following playbook alerts are supported:

- Cyber Vulnerability
- Data Leakage on Code Repository
- Domain Abuse
- Identity Novel Exposures
- Third Party Risk
- Malware Report

Cyber Vulnerability

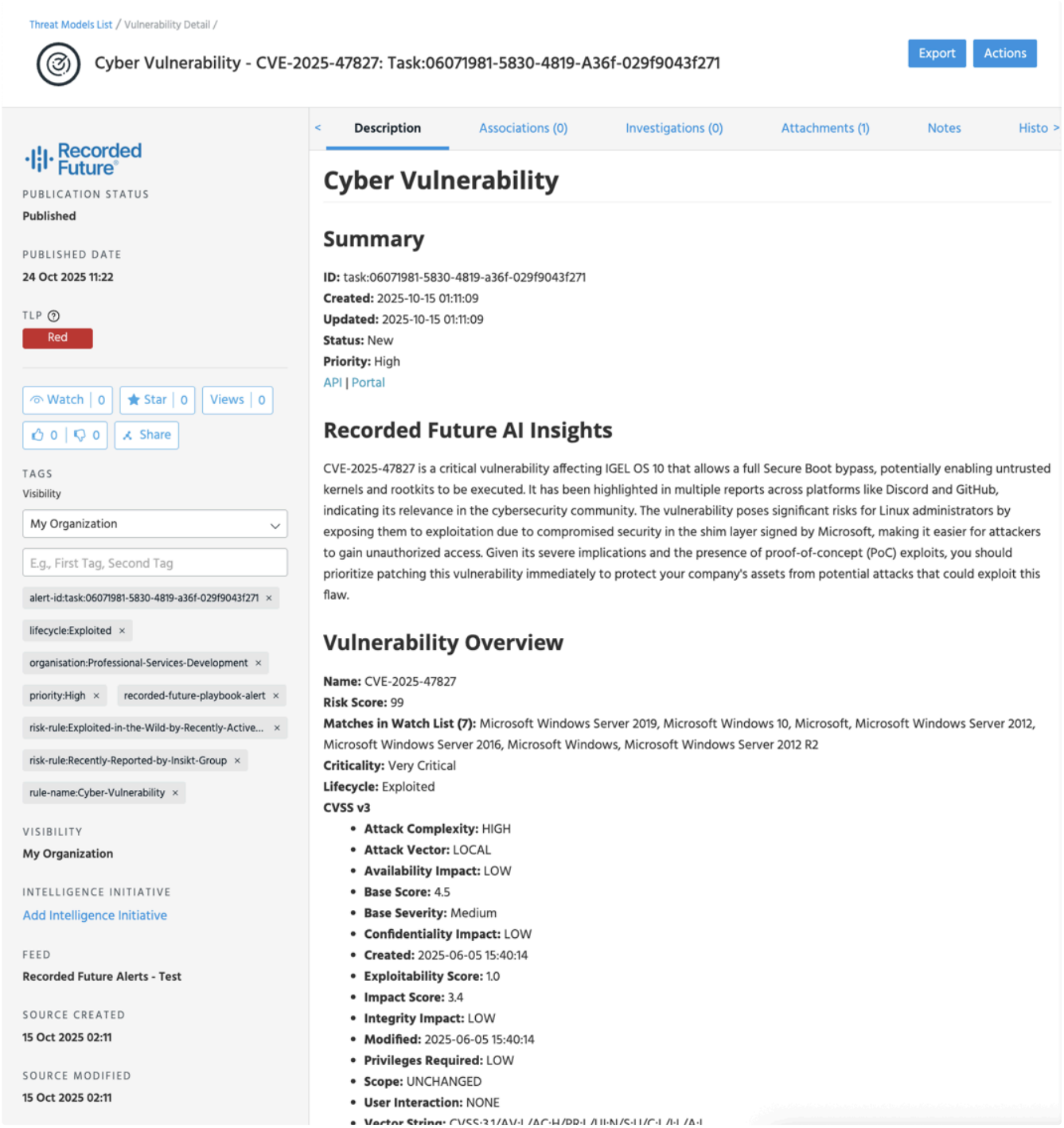
The Cyber Vulnerability Playbook Alerts utilise the `Vulnerability` Threat Model and can be found by selecting `Vulnerabilities` from the **Filter Options** in the `Threat Model` page.



Cyber Vulnerability Playbook Alerts as Vulnerabilities in Threat Model View

The Cyber Vulnerability Playbook Alerts contains:

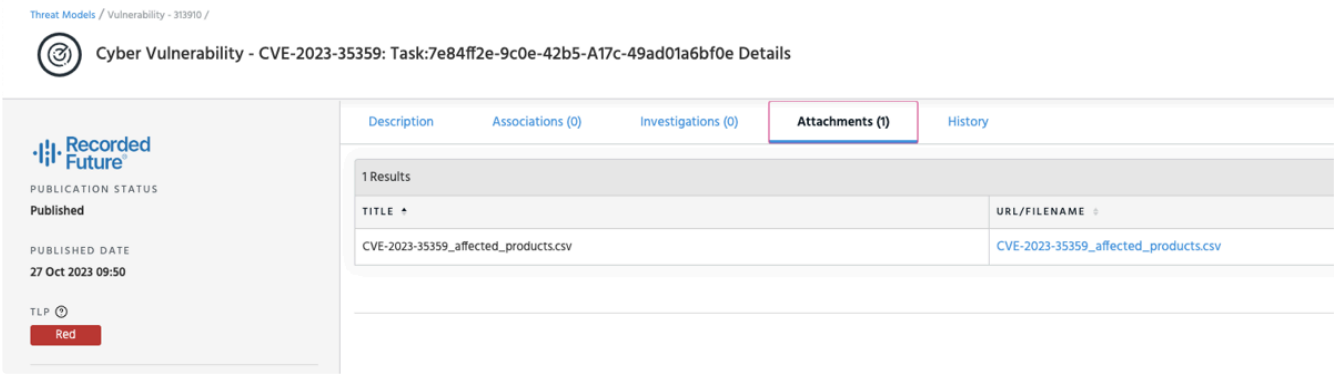
- Recorded Future AI Insights for the reported vulnerability
- Summary of the vulnerability
- CVSS v2 and CVSS v3 score and additional context (if applicable)
- Insikt Notes (if applicable)
- Affected products list
- Tags:
  - `lifecycle` to indicate the exploitability of the vulnerability
  - `risk-rule` indicating which Recorded Future Risk Rules the vulnerability has matched



Playbook Alert: Cyber Vulnerability

Affected Products

A copy of `Affected Products` list can also be found in the `Attachments` tab and is available for download.



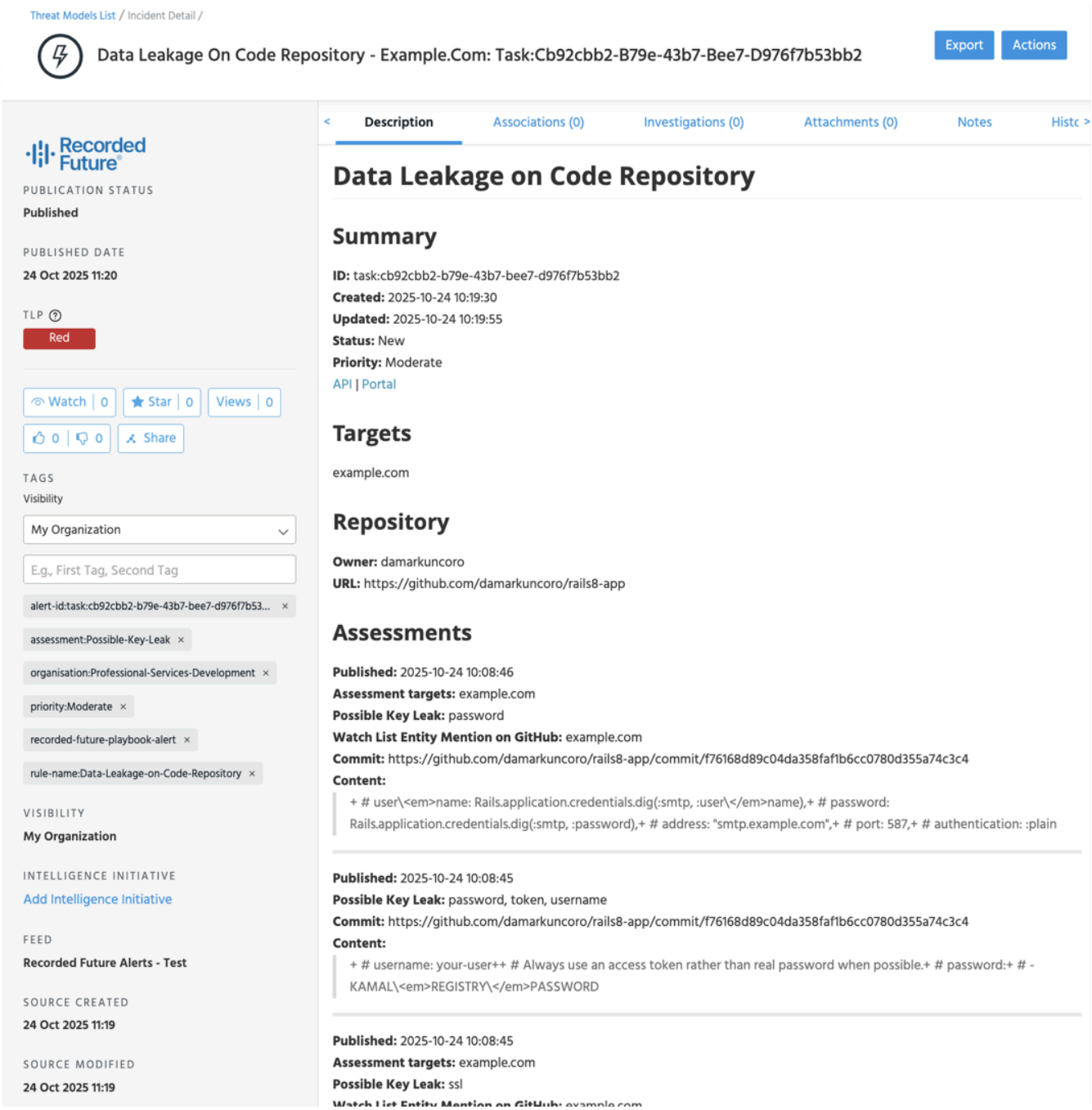
Affected Products attachment

Data Leakage on Code Repository

The Data Leakage on Code Repository Playbook Alerts utilise the `Incident` Threat Model and can be found by selecting the `Incidents` from the **Filter Options** in the `Threat Model` page.

The Data Leakage on Code Repository Playbook Alerts contains:

- Targets related to the leaked data
- Repository where the leaked data is located
- A Recorded Future Assessment on the leaked data
- Affected products list
- Tags:
  - `assessment` indicating the type of leaked data



Playbook Alert: Data Leakage on Code Repository

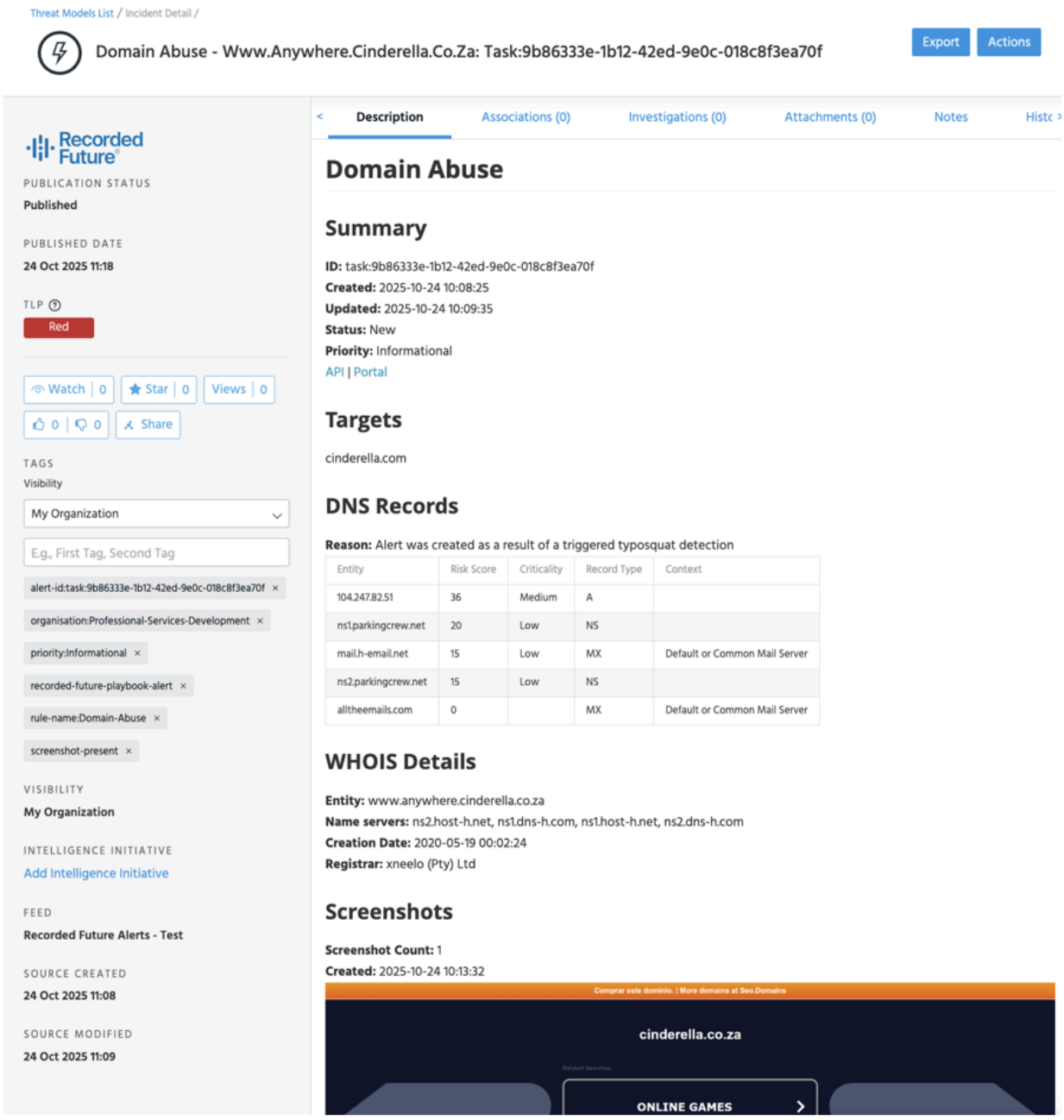
Domain Abuse

The Domain Abuse Playbook Alerts utilise the `Incident` Threat Model and can be found by selecting the `Incidents` from the **Filter Options** in the `Threat Model` page.

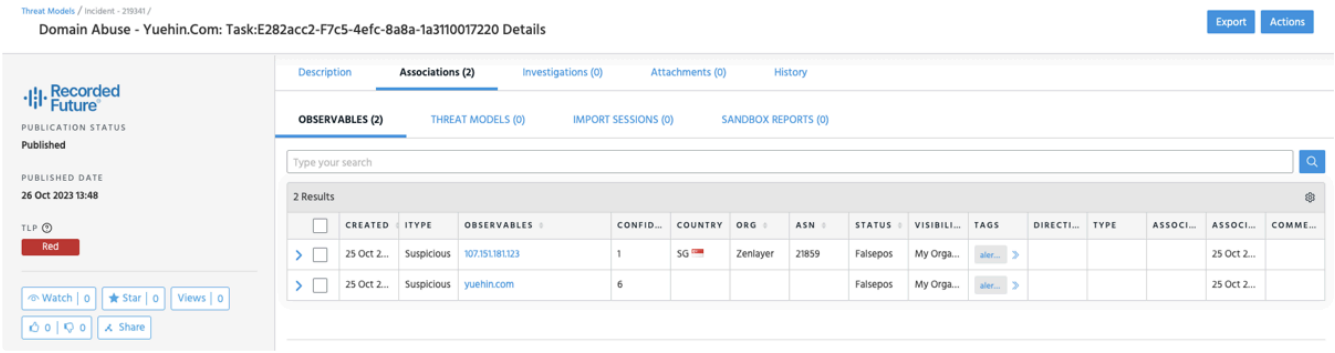
The Domain Abuse Playbook Alerts contains:

- Domains targeted by the typosquat
- Screenshots of the webpage (if available)
- **NS**, **A** and **MX** recorded for the involved domain

- Observables (Anomali provides additional information in regard to the Country, Organisation, ASN and Status of the IOC, if available)



Playbook Alert: Domain Abuse



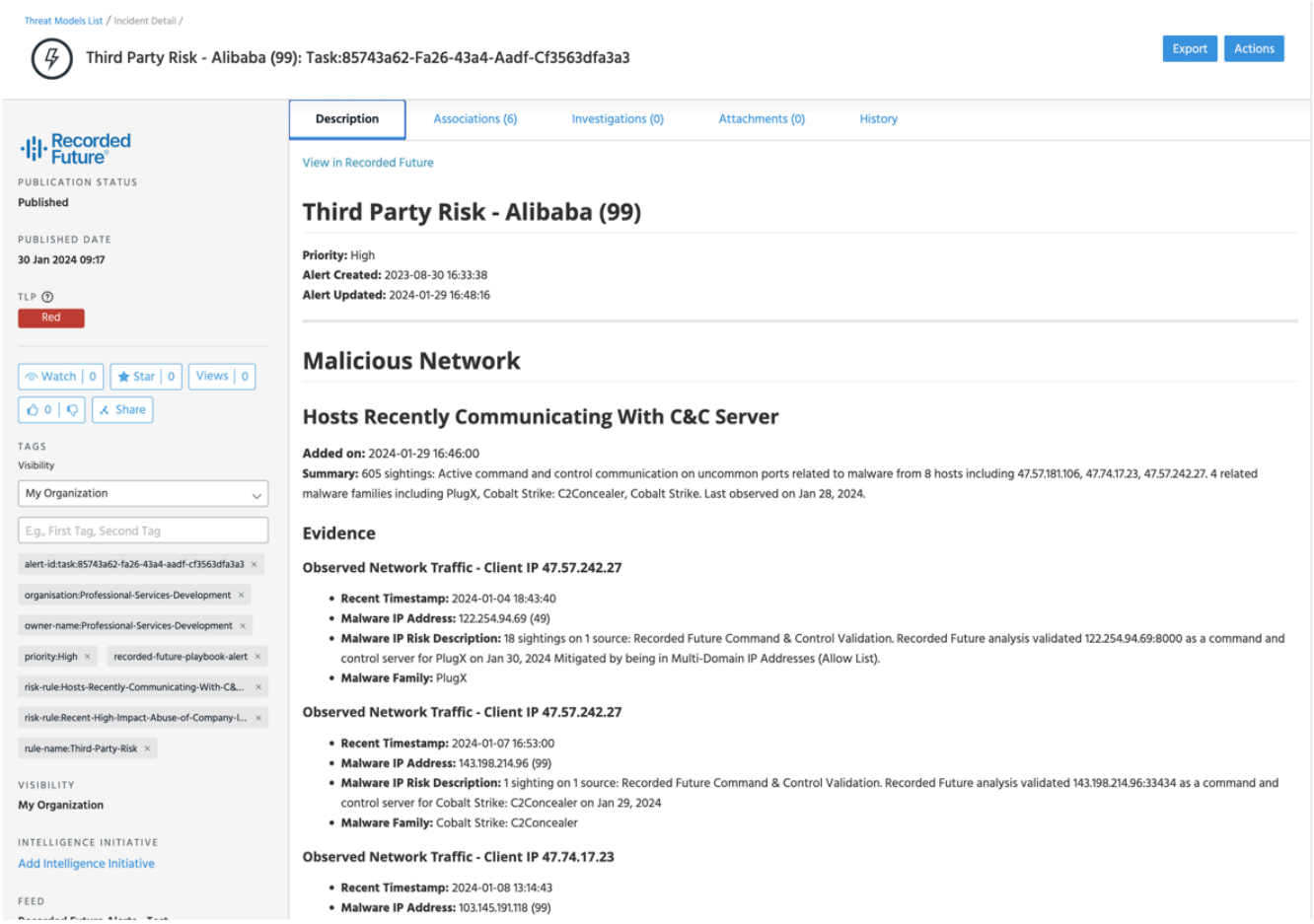
Playbook Alert: Domain Abuse - Observables

Third Party Risk

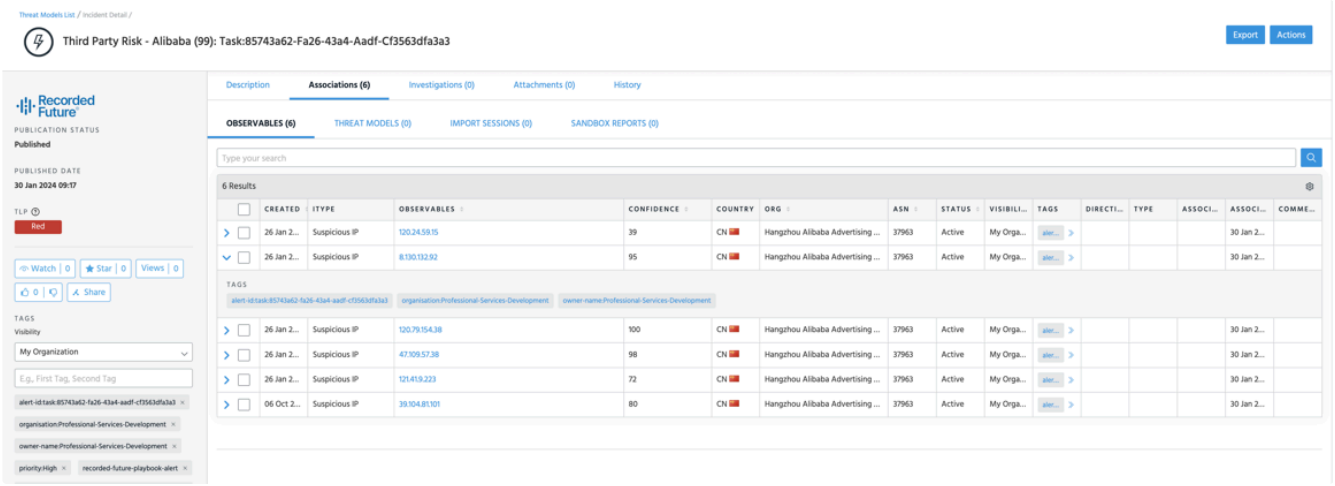
The Third Party Risk Playbook Alerts utilise the `Incident` Threat Model and can be found by selecting the `Incidents` from the **Filter Options** in the `Threat Model` page.

The Third Party Risk Playbook Alerts contains:

- Evidence for increased Third Party Risk
- Insikt Notes (if available)
- Observables (if available)
- Risk score of the company associated with the alert
- Tags:
  - `risk-rule` indicating which Recorded Future Risk Rules matched the third party entity



Playbook Alert: Third Party Risk



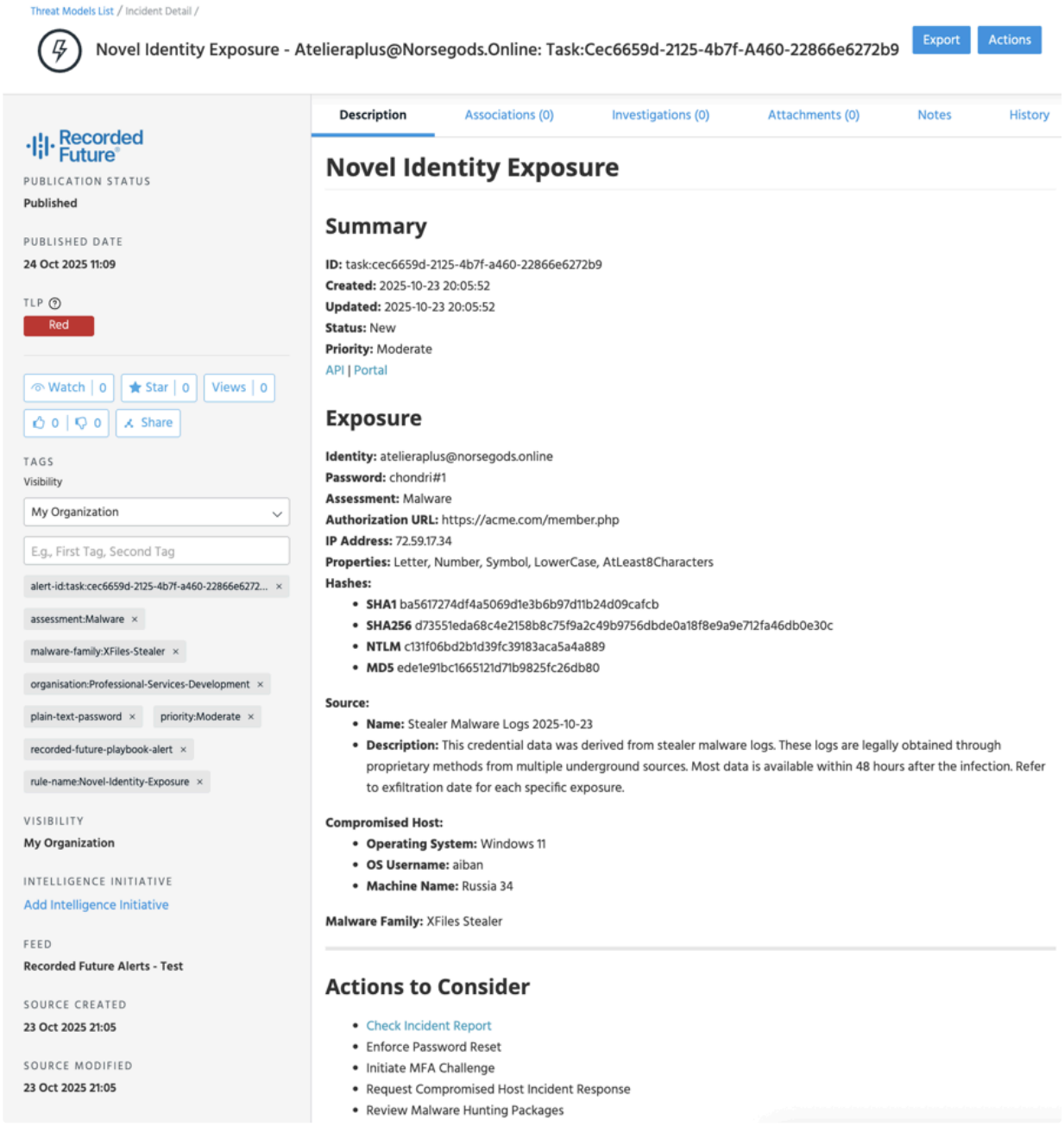
Playbook Alert: Third Party Risk - Observables

Identity Novel Exposures

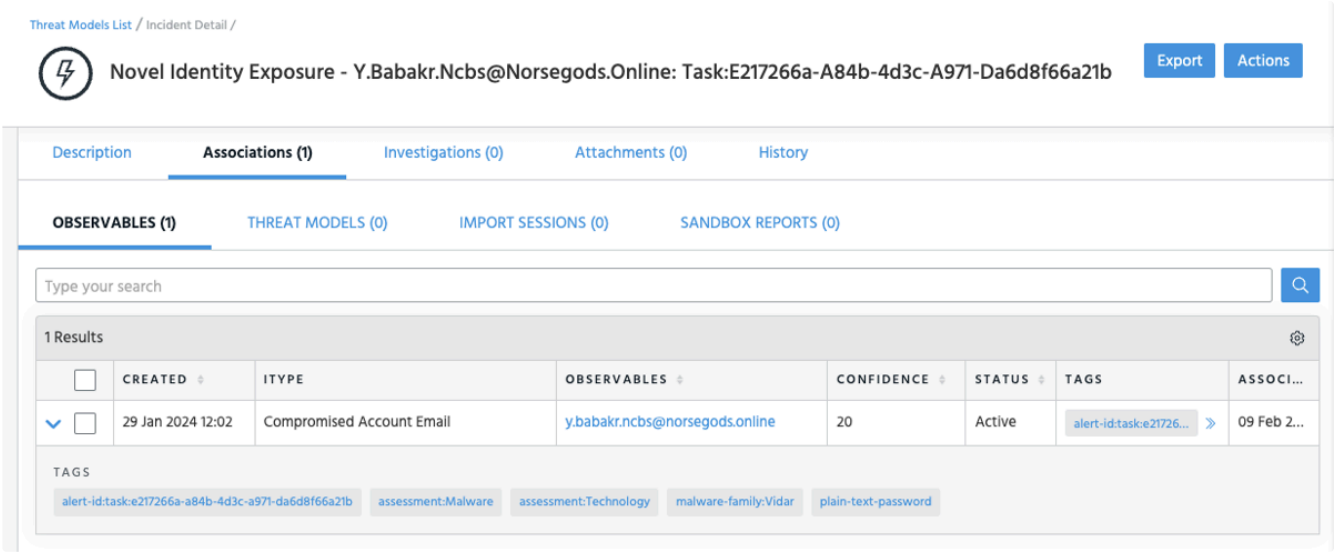
The Identity Novel Exposures Playbook Alerts utilise the `Incident` Threat Model and can be found by selecting the `Incidents` from the **Filter Options** in the `Threat Model` page.

The Identity Novel Exposures Playbook Alerts contains:

- The identity that was exposed
- Password hint or clear text password (Enabling cleartext passwords within Identity Intelligence)
- Authorization URL
- IP Address (if available)
- Dump details
- Exposed secret details
- Compromised host (if available)
- Malware family name (if available)
- Technology (if available)
- Observable of the exposed identity with `Confidence` of 20
- Tags
  - `assessment` indicating the type of exposure
  - `plain-text-password` indicating the Anomali TS incident contains a plain text password
  - `malware-family` the stealer malware family name (if available)



Playbook Alert: Novel Identity Exposures



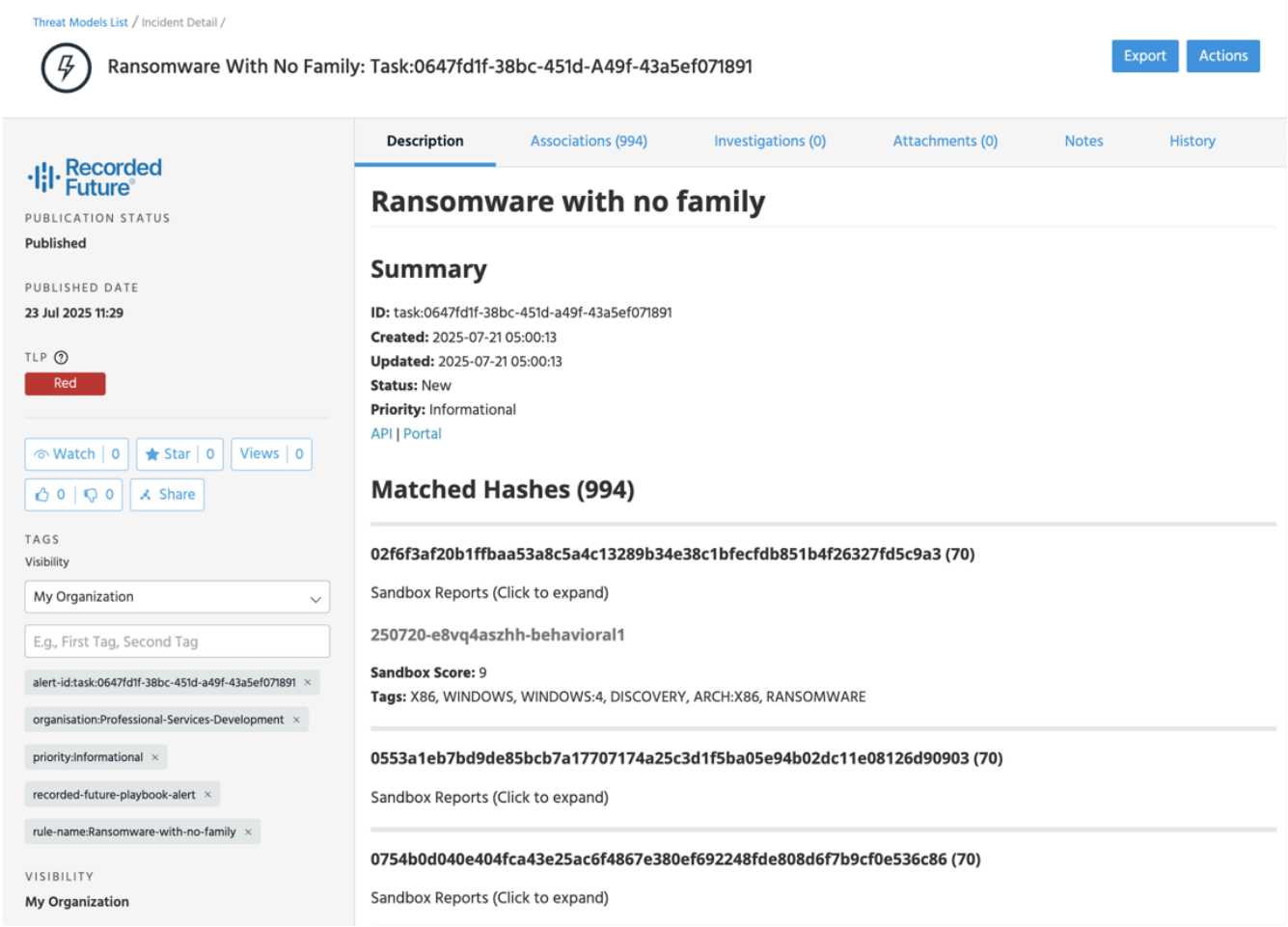
Playbook Alert: Novel Identity Exposures: Observables

Malware Report (Malware Intelligence)

The Malware Report Playbook Alerts utilise the `Incident` Threat Model and can be found by selecting the `Incidents` from the **Filter Options** in the `Threat Model` page.

The Malware Report Playbook Alerts contains:

- Matched hashes
- Observables of the matches hashes with `Confidence` equivalent to Recorded Future Risk Score + 1
- Sandbox Reports
  - Score
  - Tags
- Tags
  - `malware-family` identified malware family name (if available)



Updates

One of the unique aspects of Recorded Future Playbook Alerts is that these alerts will receive updates and these updates will also propagate to Anomali TS by updating the `Description` tab and other relevant data inside the appropriate `Threat Model`.

Observables

Not all Recorded Future Alerts are equal meaning not every `Incident` will have `Observables` available in the `Associations` tab. The list below summarises which alerts will produce `Observables` when available.

Recorded Future Classic Alerts

- Leaked Credential Monitoring
- Leaked Email Monitoring

Recorded Future Playbook Alerts

- Domain Abuse
- Third Party Risk

- Identify Similar Domains
- IP Address Mentions
- Increased IP Address Risk Score
- Increased Domain Risk Score
- Potential Logo Abuse Detection
- Novel Identity Exposures
- Malware Report

New in v1.3.0:

- Select more Classic Alerts (IGL or Custom) to create Observables with the desired iType
- Disable Observable creation for the predefined Classic Alerts (listed above)
- Override the Observable iType for the predefined Classic alerts (listed above)

For more information please contact support at support@recordedfuture.com.

Confidence

The confidence of each observable is set as follows:

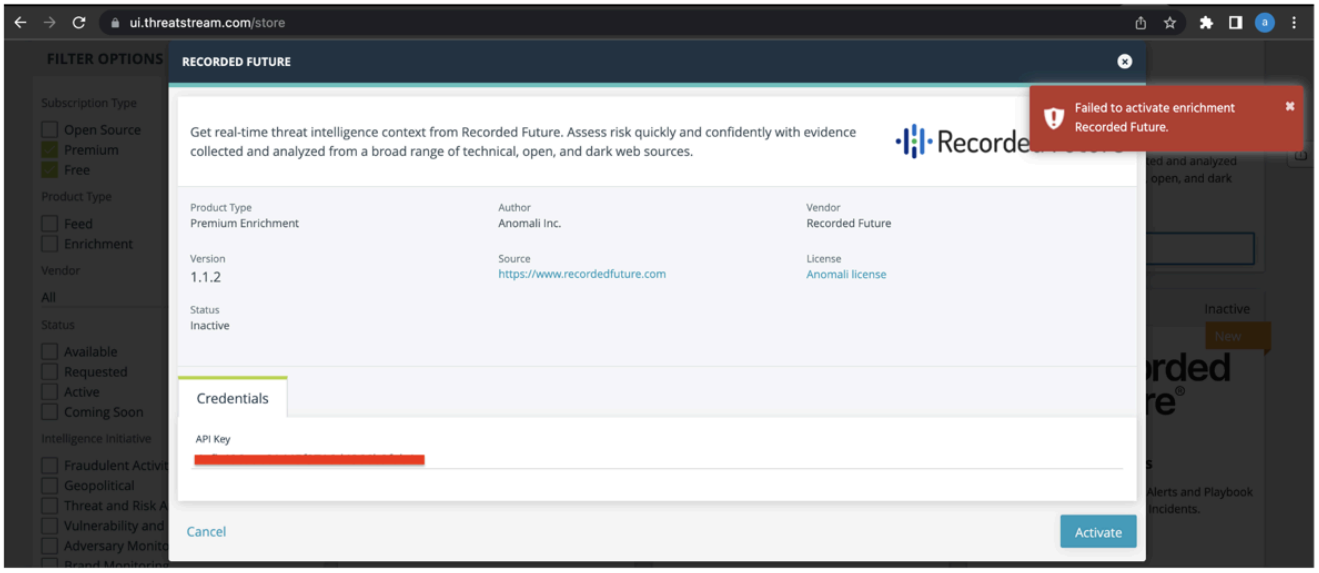
- For Playbook Alerts: this will be equal to the Recorded Future risk score of the observable plus 1, as shown in the screenshot above. The addition of 1 is to match the Anomali scale which goes up to 100 instead of 99.
- For classic alerts: the default confidence is `16` for all ITypes except for `Compromised Emails` ITypes which will be `20`.

Installation

The preferred installation method for the Recorded Future Alert Feed is through the Anomali TS App Store.

Configuration

Once the application is installed please set the Recorded Future token and click `Activate`.



Tags

Recorded Future Alert Feed uses a set of common tags that are added to Observable and Incidents. These tags help to quickly and easily search and build dashboards from the Recorded Future alert data. Note that tags are limited to 50 per alert.

Tag	Observable	Threat Model	Example	Description
alert-id	✅	✅	*alert-id:wyf7g0*	Recorded Future Alert ID
assessment		✅	assessment:Possible-Key-Leak	Indicates the assessment made by Recorded Future
author	✅	✅	*author:Bot*	Author of the data
lifecycle		✅	lifecycle:Exploited	Indicates the lifecycle stage of a vulnerability
malware-family	✅	✅	malware-family:Lumma	Indicates stealer malware name
organisation	✅	✅	*organisation:PS-Development*	The organisation of the alert
owner-name	✅	✅	*owner-name:Moise*	The owner of the alert

plain-text-password		✅	*plain-text-password*	Indicates that the Incident contains a plain text password
priority		✅	*priority:High*	Indicates the priority of a Recorded Future Playbook Alert
recorded-future-alert		✅	*recorded-future-alert*	Indicates that this is a Recorded Future Alert
recorded-future-playbook-alert		✅	*recorded-future-playbook-alert*	Indicates that this is a Recorded Future Playbook Alert
risk-rule		✅	risk-rule:Recent-Validated-Cyber-Attack	Name of the matched Recorded Future Risk Rule
rule-name	✅	✅	*rule-name:Leaked-Credential-Monitoring*	Recorded Future Alert rule name
screenshot-present		✅	*screenshot-present*	Indicates that the Incident contains a screenshot
source	✅	✅	*source:Genesis-Store*	Source of the data

Troubleshooting

Missing Observables

In some cases an `Incident` 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.

Not fetching alerts

The integration only fetches alerts with a status of `no-action` or as shown in the portal `New`. Verify that the alerts you wish to fetch have this status set.

Custom Alerts (created with AQB) not ingesting

By default Recorded Future Custom Alerts created using the Advanced Query Builder (AQB) are private to the user and are not visible to the Anomali integration. To share a custom Alert with your Anomali ThreatStream (TS) instance please follow this support article.

IOC with 0 risk score and no Intelligence Card

There might be playbook alerts (specifically Domain Abuse, Third Party Risk and Cyber Vulnerability) 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 an alert for completeness of information. The occurrences of such IOC is expected to be very low.

CHANGELOG

[1.5.1] - 2026-03-05

Added

- User set Playbook Alert rule names are now used in the Anomali Threat Model title field, as well as the `alert-rule` tag, instead of the default rule name.

[1.5.0] - 2026-02-03

Added

- Support for `Malware Report` Playbook Alert

Changed

- Updated Incident layout for the following Playbook Alerts
  - `Domain Abuse`
  - `Code Repo Leakage`
  - `Cyber Vulnerability`
  - `Third Party Risk`
  - `Identity Novel Exposures`
- Optimised ingestion of `Domain Abuse` Playbook Alerts which results in much faster ingestion times
- `PSEngine` upgraded to v2.4.2
- `Anomali Feeds SDK` upgraded to v2.6.0

[1.4.3] - 2026-01-05

Added

- Classic Alerts entity tags optimisation.

[1.4.2] - 2025-09-15

Changed

- Alert ingestion optimisations

[1.4.1] - 2025-05-07

Fixed

- Classic Alerts
  - Missing reference fragment sometimes prevented alert ingestion.
- Playbook Alerts
  - Domain Abuse MX records sometimes caused alert fetch to fail.

Changed

- `PSEngine` upgraded to v2.0.5

[1.4.0] - 2025-03-24

Added

- Classic Alerts
  - `Source Created` time is now set using the alert created time
  - Triggered by now tells the user why a specific reference has matched and is part of the alert
  - Observables are now created from alert rule `Malicious Infrastructure on Monitored IP Addresses`
- Playbook Alerts
  - `Source Created` time is now set using the alert created time
  - `Source Modified` time is not using the alert updated time

Changed

- Classic Alerts
  - New enhanced layout
- Playbook Alerts
  - `Source Created` time is now set using the alert created time
  - `Source Modified` time is not using the alert updated time

Fixed

- Classic Alerts
  - Hashes from sandbox analysis references are now created as Observables

Removed

- Playbook Alerts

- Alert Created / Updated removed from the description in favour of `Source Created` and `Source Modified`

[1.3.1] - 2024-08-14

Fixed

- Playbook Alerts
  - Novel Identity Exposure
    - An incorrectly formatted password hint no longer stops ingestion of playbook alerts.
  - Cyber Vulnerability
    - Unusual vulnerability names such as '0.0.0.0 day' no longer stop ingestion of playbook alerts.

[1.3.0] - 2024-07-01

Added

- Classic Alerts
  - Support for custom Observables mapping
- `rule-name` tag added to Observables

Changed

- Classic Alerts
  - New layout

Fixed

- Classic Alerts
  - Some Observables from URLs were not being enriched correctly

[1.2.0] - 2024-03-14

Added

- Support for `Identity Novel Exposures` Playbook Alert
- New Tags (see install guide for complete list)

Changed

- `PSEngine` upgraded to v1.12.0
- `Anomali Feeds SDK` upgraded to v2.5.17

- `Anomali Feeds SDK` upgraded to v2.5.17

[1.1.0] - 2023-11-03

Added

- Classic Alerts now support `Recorded Future AI Insights`
- Classic Alerts contain the full Insikt Analyst Note text instead of a fragment
- Playbook Alert `Domain Abuse` now displays the `Targets` of a typosquat
- Support for `Code Repository Leakage`, `Cyber Vulnerability` and `Third-Party Risk` Playbook Alert
- Generic Incident for not yet fully supported Playbook Alerts - New Tags (see install guide for complete list)

Changed

- Classic Alerts IOC enrichment is now enabled by default for all clients
- `Anomali Feeds SDK` upgraded to v2.5.16
- `PSEngine` upgraded to v1.10.2

Fixed

- Removed reference count from the `Incident Name`
- `PSEngine` upgraded which fixed the `limit` parameter issue when paginating through results

Removed

- Removed `enrich_alerts` parameter from `[anomali_ts]` stanza

[1.0.0 GA] - 2023-03-08

Added

- Official package release