Recorded Future Alerts v1.3.0 - 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:

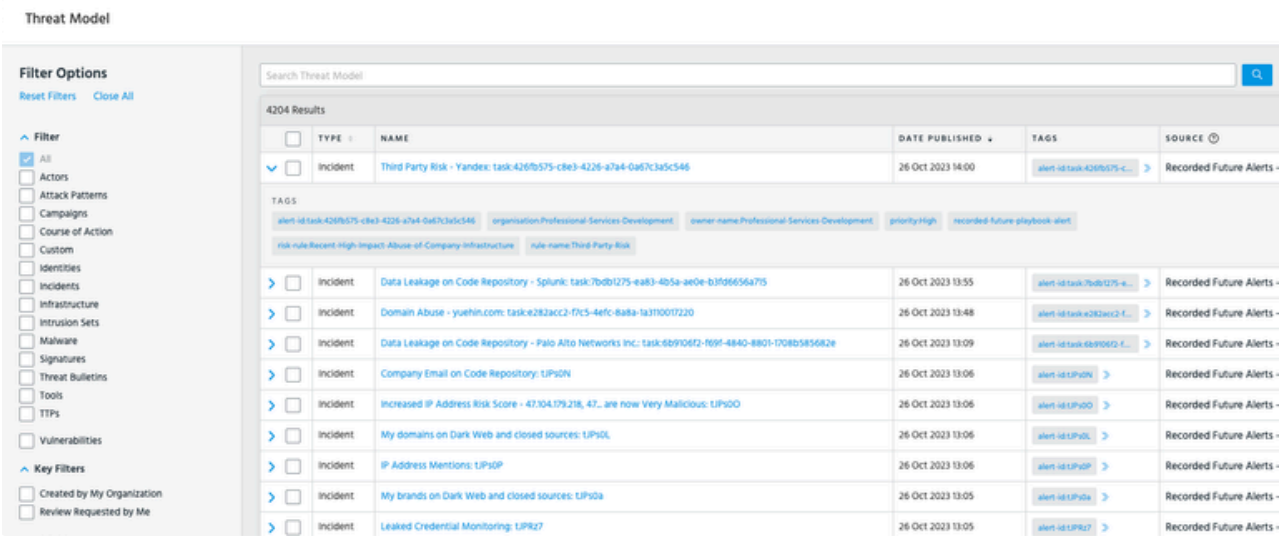
- Delivery of Recorded Future Alert details consumed in Anomali ThreatStream (TS) as Incidents via an Anomali TS Feed.
- Triaging Recorded Future Classic Alerts and Playbook Alerts with the full alert details context directly in the Anomali TS.
- Review trending Intelligence Goals Library (IGL) data.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

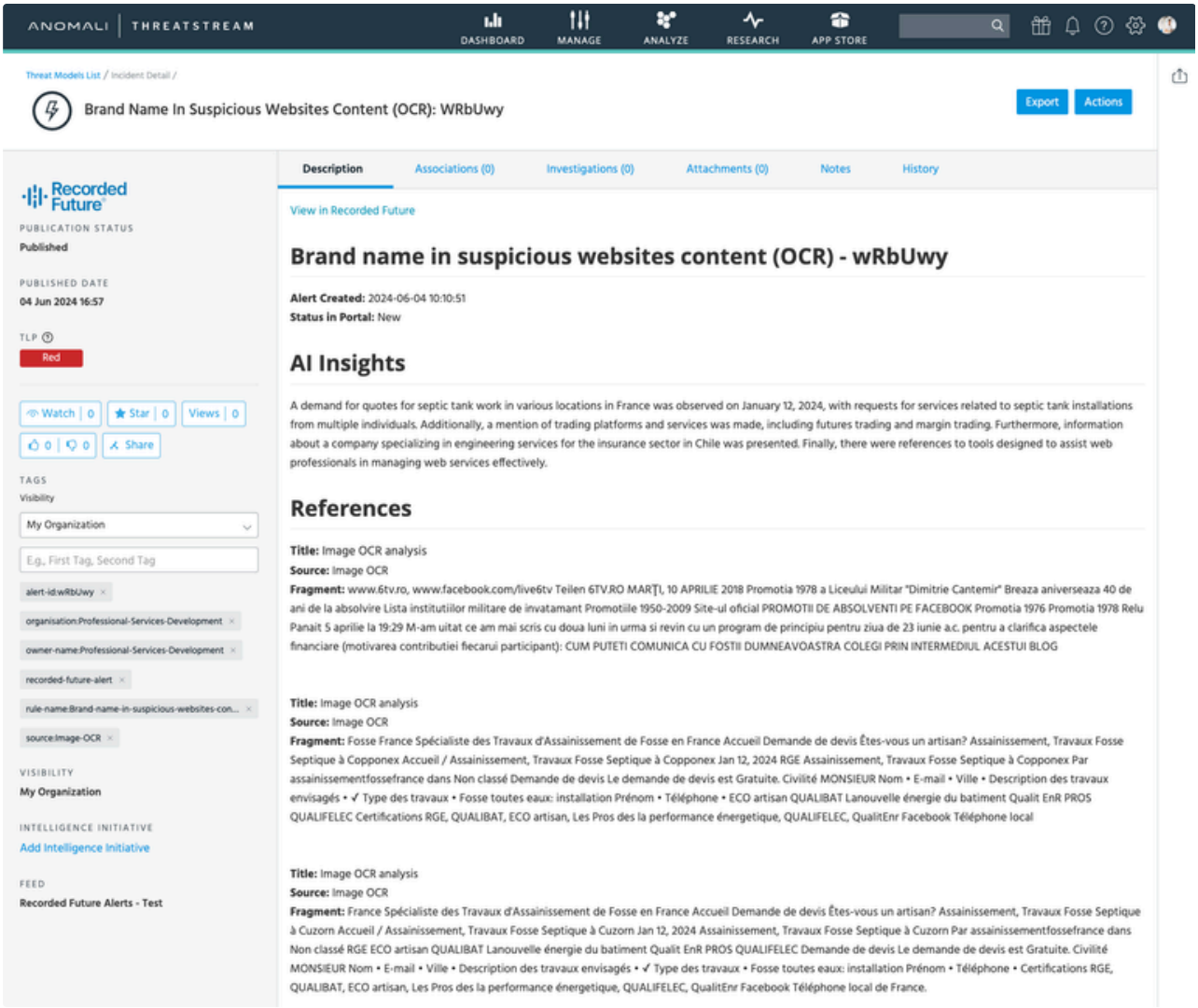
Recorded Future Classic Alerts

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
- Recorded Future AI Insights



Classic Alert: Brand name in suspicious websites content (OCR)

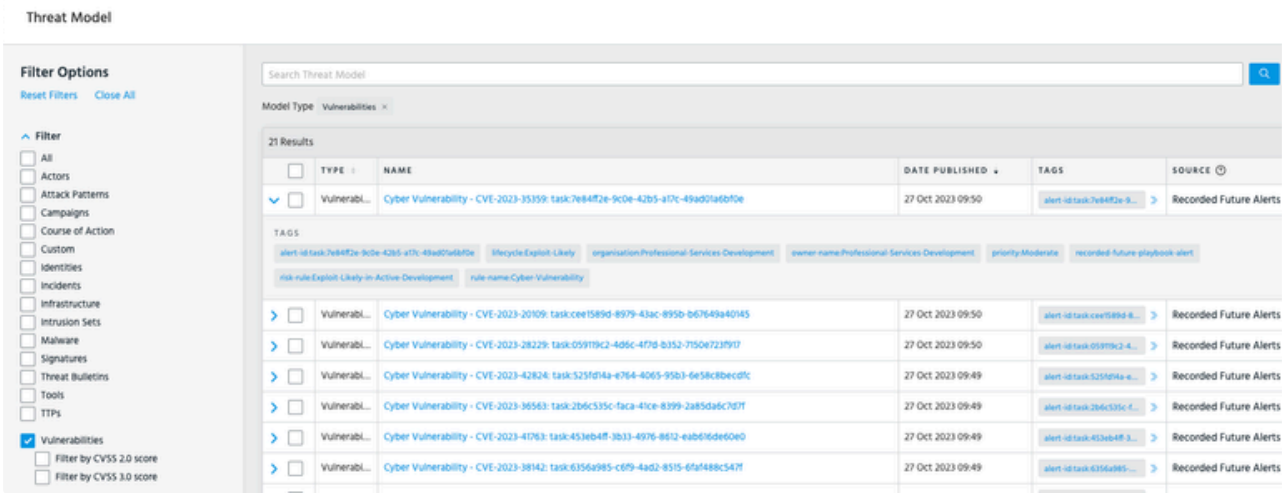
Recorded Future Playbook Alerts

The following playbook alerts are supported:

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

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

Recorded Future

PUBLICATION STATUS
Published

PUBLISHED DATE
27 Oct 2023 09:50

TLP
Red

Watch | 0 Star | 0 Views | 0
0 | 0 Share

TAGS
Visibility
My Organization

E.g., First Tag, Second Tag

alert-id:task:7e84ff2e-9c0e-42b5-a17c-49ad01a6bf0e ×
lifecycle:Exploit-Likely ×
organisation:Professional-Services-Development ×
owner-name:Professional-Services-Development ×
priority:Moderate ×
recorded-future-playbook-alert ×
risk-rule:Exploit-Likely-in-Active-Development ×
rule-name:Cyber-Vulnerability ×

VISIBILITY
My Organization

INTELLIGENCE INITIATIVE
Add Intelligence Initiative

FEED
Recorded Future Alerts - Test

CVSS 2.0 SCORE
N/A

CVSS 3.0 SCORE
7.8

View in Recorded Future

Cyber Vulnerability - CVE-2023-35359

Priority: Moderate
Alert Created: 2023-10-04 07:10:53
Alert Updated: 2023-10-04 07:10:53

> **Recorded Future AI Insights**
>
> Based on the provided information, there is a vulnerability identified as CVE-2023-35359 that should be prioritized for patching. The vulnerability has been flagged as likely to be exploited soon based on intelligence received on October 4, 2023. The Recorded Future Vulnerability Analysis via the National Vulnerability Database has calculated a CVSS v3.1 Score of 6.6 for this vulnerability, indicating a medium severity level. The exploitability metrics suggest that it can be exploited with a low attack complexity and requires local access. The impacts of this vulnerability are rated as high, potentially leading to confidentiality, integrity, and availability compromises. Although specific details about the nature of the vulnerability are not provided in the summary, given its potential exploitation and impact, it is advisable to prioritize patching to mitigate any potential risks associated with this CVE.

Summary

Risk Score: 41
Criticality: Medium
Targets: Microsoft Windows Server 2019, Microsoft, Microsoft Windows Server 2012, Microsoft Windows Server 2016, Microsoft Windows Server 2008, Microsoft Windows, Microsoft Windows Server 2012 R2
Target 7 item(s) from Tech Stack Watch List
Lifecycle: Exploit Likely
Exploit Likely in Active Development: 1 sighting on 1 source: CTCI Intelligence and Research. This vulnerability is flagged as likely to be exploited soon based on intelligence received on October 04, 2023.

CVSS v3

Attack Complexity: LOW
Attack Vector: LOCAL
Availability Impact: HIGH
Base Score: 7.8
Base Severity: HIGH
Confidentiality Impact: HIGH
Created: 2023-08-08 18:15:12
Exploitability Score: 1.8
Impact Score: 5.9
Integrity Impact: HIGH
Modified: 2023-09-06 21:15:12
Privileges Required: LOW
Scope: UNCHANGED
User Interaction: NONE
Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Version: 3.1

Insikt Notes

Title: Summary note for CVE-2023-35359
Published: 2023-10-20 21:05:53
Content: Core impact has added this exploit to their toolset. Several criminal groups use pirated copies of the software. The intelligence was collected from publicly available sources. Naa. A public PoC was validated for this vulnerability. The Admiralty score was A1.
Source: Cyber Threat Cognitive Intelligence (CTCI)

Affected Products

(Truncated - See Attachments)

Microsoft

Microsoft Windows 10 1507 10.0.10240.16405 on Arm64	Microsoft Windows 10 1507 10.0.10240.16405 on X64	Microsoft Windows 10 1507 10.0.10240.16405 on X86	Microsoft Windows 10 1507 10.0.10240.16413 on Arm64	Microsoft Windows 10 1507 10.0.10240.16413 on X64	Microsoft Windows 10 1507 10.0.10240.16413 on X86	Microsoft Windows 10 1507 10.0.10240.16430 on Arm64	Microsoft Windows 10 1507 10.0.10240.16430 on X64
Microsoft Windows 10 1507 10.0.10240.16430 on X86	Microsoft Windows 10 1507 10.0.10240.16433 on Arm64	Microsoft Windows 10 1507 10.0.10240.16433 on X64	Microsoft Windows 10 1507 10.0.10240.16433 on X86	Microsoft Windows 10 1507 10.0.10240.16445 on Arm64	Microsoft Windows 10 1507 10.0.10240.16445 on X64	Microsoft Windows 10 1507 10.0.10240.16445 on X86	Microsoft Windows 10 1507 10.0.10240.16463 on Arm64
Microsoft Windows 10 1507 10.0.10240.16463 on X64	Microsoft Windows 10 1507 10.0.10240.16463 on X86	Microsoft Windows 10 1507 10.0.10240.16487 on Arm64	Microsoft Windows 10 1507 10.0.10240.16487 on X64	Microsoft Windows 10 1507 10.0.10240.16487 on X86	Microsoft Windows 10 1507 10.0.10240.16520 on Arm64	Microsoft Windows 10 1507 10.0.10240.16520 on X64	Microsoft Windows 10 1507 10.0.10240.16520 on X86
Microsoft Windows 10 1507 10.0.10240.16549 on Arm64	Microsoft Windows 10 1507 10.0.10240.16549 on X64	Microsoft Windows 10 1507 10.0.10240.16549 on X86	Microsoft Windows 10 1507 10.0.10240.16566 on Arm64	Microsoft Windows 10 1507 10.0.10240.16566 on X64	Microsoft Windows 10 1507 10.0.10240.16566 on X86	Microsoft Windows 10 1507 10.0.10240.16590 on Arm64	Microsoft Windows 10 1507 10.0.10240.16590 on X64
Microsoft Windows 10 1507 10.0.10240.16590 on X86	Microsoft Windows 10 1507 10.0.10240.16601 on Arm64	Microsoft Windows 10 1507 10.0.10240.16601 on X64	Microsoft Windows 10 1507 10.0.10240.16601 on X86	Microsoft Windows 10 1507 10.0.10240.16644 on Arm64	Microsoft Windows 10 1507 10.0.10240.16644 on X64	Microsoft Windows 10 1507 10.0.10240.16644 on X86	Microsoft Windows 10 1507 10.0.10240.16683 on Arm64
Microsoft Windows 10 1507 10.0.10240.16683 on X64	Microsoft Windows 10 1507 10.0.10240.16683 on X86	Microsoft Windows 10 1507 10.0.10240.16725 on Arm64	Microsoft Windows 10 1507 10.0.10240.16725 on X64	Microsoft Windows 10 1507 10.0.10240.16725 on X86	Microsoft Windows 10 1507 10.0.10240.16771 on Arm64	Microsoft Windows 10 1507 10.0.10240.16771 on X64	Microsoft Windows 10 1507 10.0.10240.16771 on X86
Microsoft Windows 10 1507 10.0.10240.16854 on Arm64	Microsoft Windows 10 1507 10.0.10240.16854 on X64	Microsoft Windows 10 1507 10.0.10240.16854 on X86	Microsoft Windows 10 1507 10.0.10240.16942 on Arm64	Microsoft Windows 10 1507 10.0.10240.16942 on X64	Microsoft Windows 10 1507 10.0.10240.16942 on X86	Microsoft Windows 10 1507 10.0.10240.17024 on Arm64	Microsoft Windows 10 1507 10.0.10240.17024 on X64
Microsoft Windows 10 1507 10.0.10240.17024 on X86	Microsoft Windows 10 1507 10.0.10240.17071 on Arm64	Microsoft Windows 10 1507 10.0.10240.17071 on X64	Microsoft Windows 10 1507 10.0.10240.17071 on X86	Microsoft Windows 10 1507 10.0.10240.17113 on Arm64	Microsoft Windows 10 1507 10.0.10240.17113 on X64	Microsoft Windows 10 1507 10.0.10240.17113 on X86	Microsoft Windows 10 1507 10.0.10240.17146 on Arm64
Microsoft Windows 10 1507 10.0.10240.17146 on X64	Microsoft Windows 10 1507 10.0.10240.17146 on X86	Microsoft Windows 10 1507 10.0.10240.17190 on Arm64	Microsoft Windows 10 1507 10.0.10240.17190 on X64	Microsoft Windows 10 1507 10.0.10240.17190 on X86	Microsoft Windows 10 1507 10.0.10240.17202 on Arm64	Microsoft Windows 10 1507 10.0.10240.17202 on X64	Microsoft Windows 10 1507 10.0.10240.17202 on X86
Microsoft Windows 10 1507 10.0.10240.17236 on Arm64	Microsoft Windows 10 1507 10.0.10240.17236 on X64	Microsoft Windows 10 1507 10.0.10240.17236 on X86	Microsoft Windows 10 1507 10.0.10240.17319 on Arm64	Microsoft Windows 10 1507 10.0.10240.17319 on X64	Microsoft Windows 10 1507 10.0.10240.17319 on X86	Microsoft Windows 10 1507 10.0.10240.17354 on Arm64	Microsoft Windows 10 1507 10.0.10240.17354 on X64

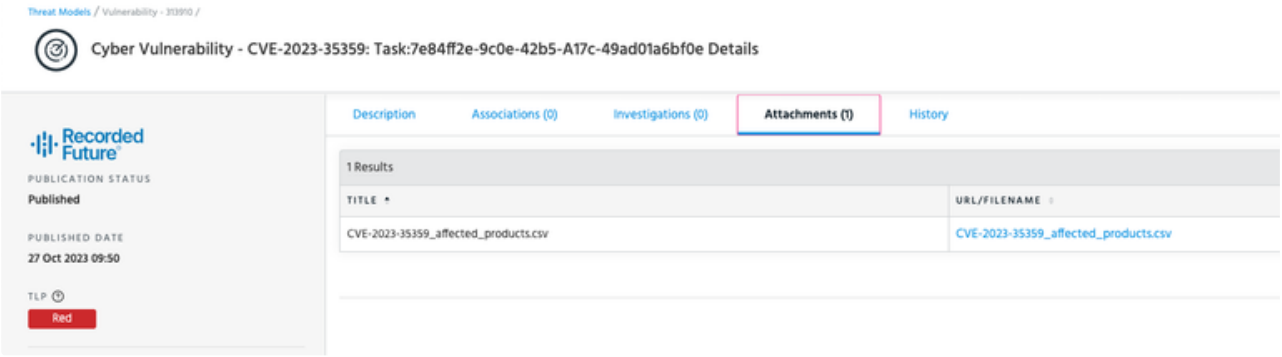
Windows

Windows Server 2008 Service Pack 2 for 32-bit systems	Windows Server 2008 Service Pack 2 x86

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.



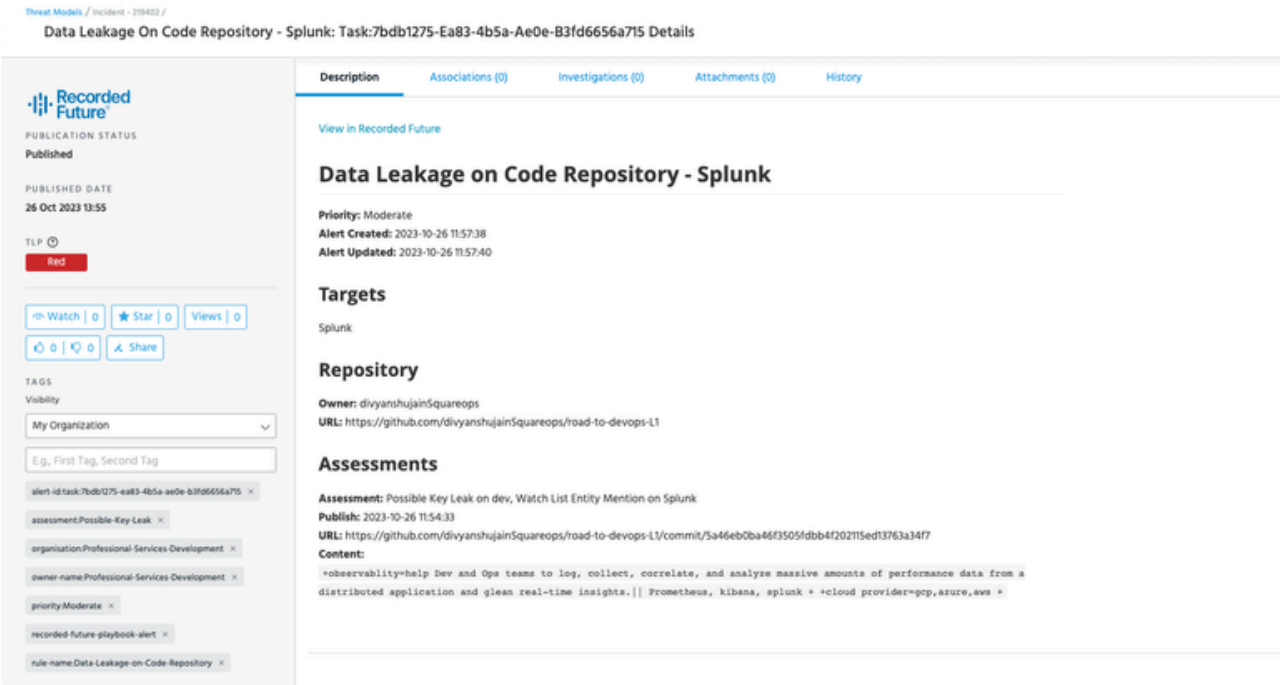
Affected Products attachment

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



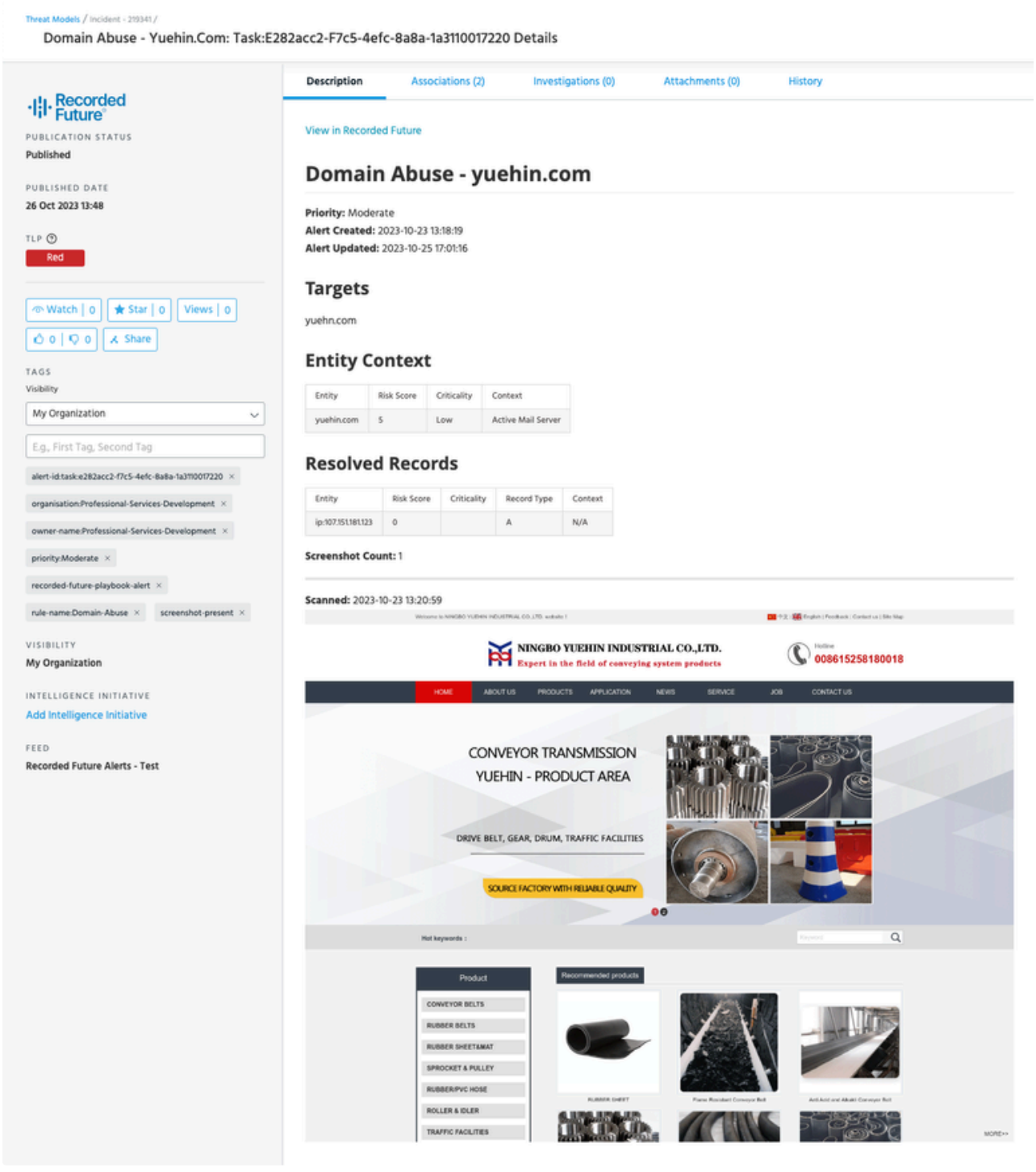
Playbook Alert: Data Leakage on Code Repository

Domain Abuse

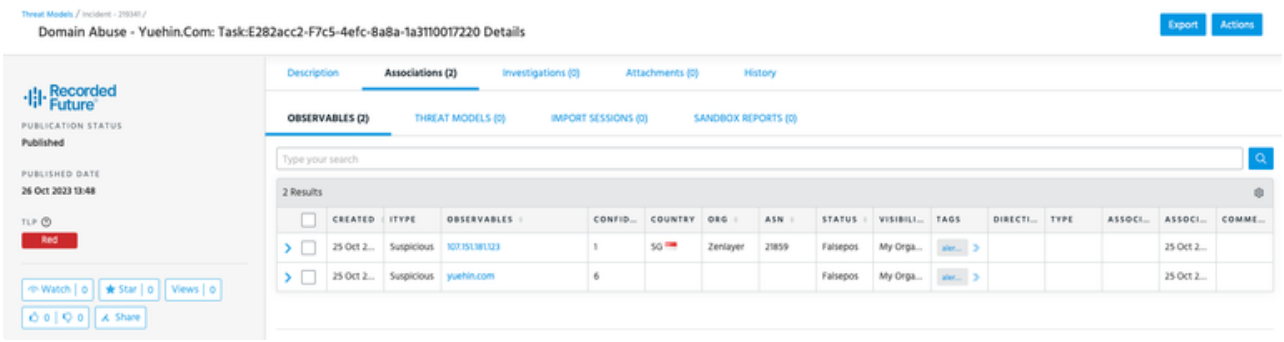
The Domain Abuse Playbook Alerts utilise the `Incident` Threat Model and can be found by selecting the `Incidents` from the **Filter Options** in the `Threat Model` page.

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



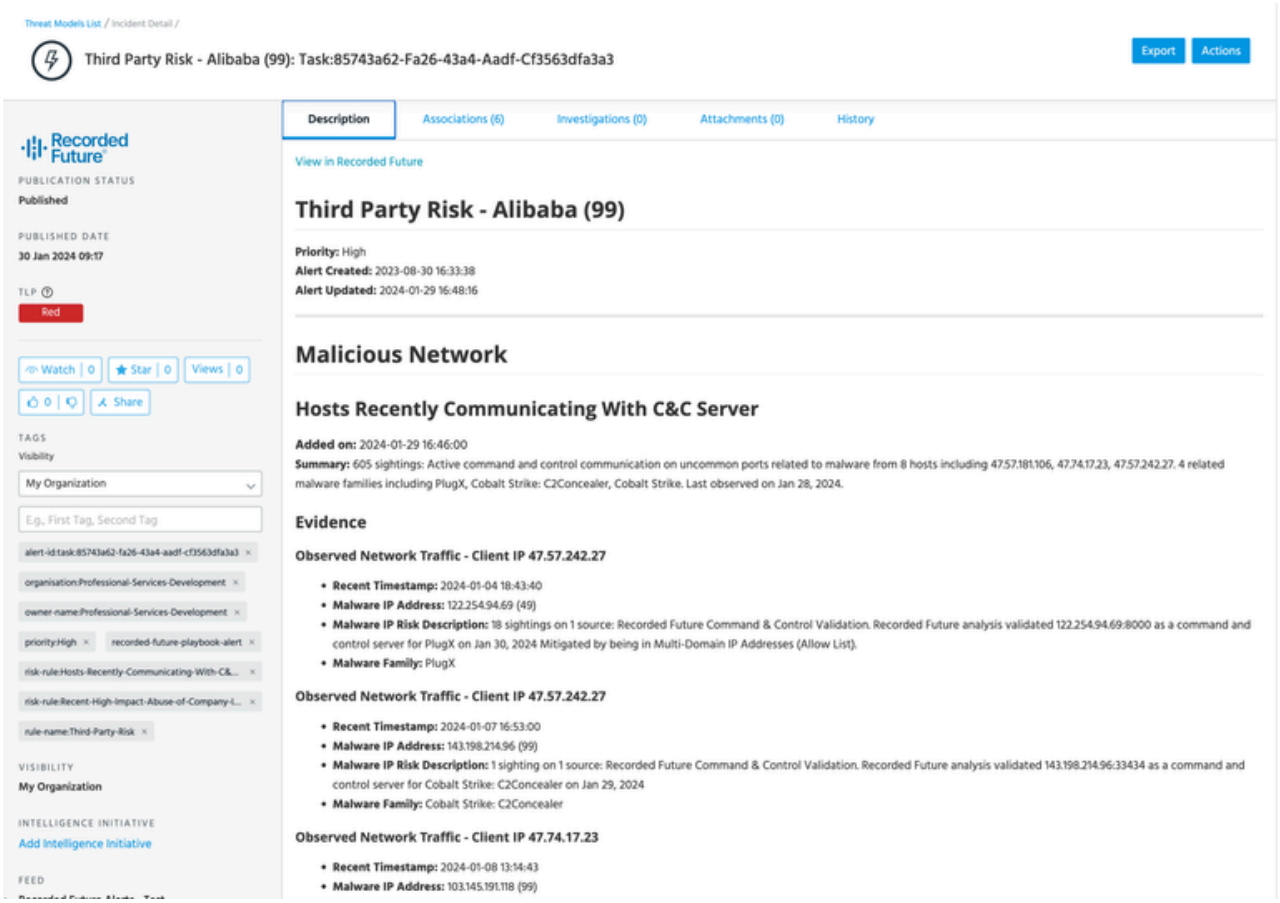
Playbook Alert: Domain Abuse - Observables

Third Party Risk

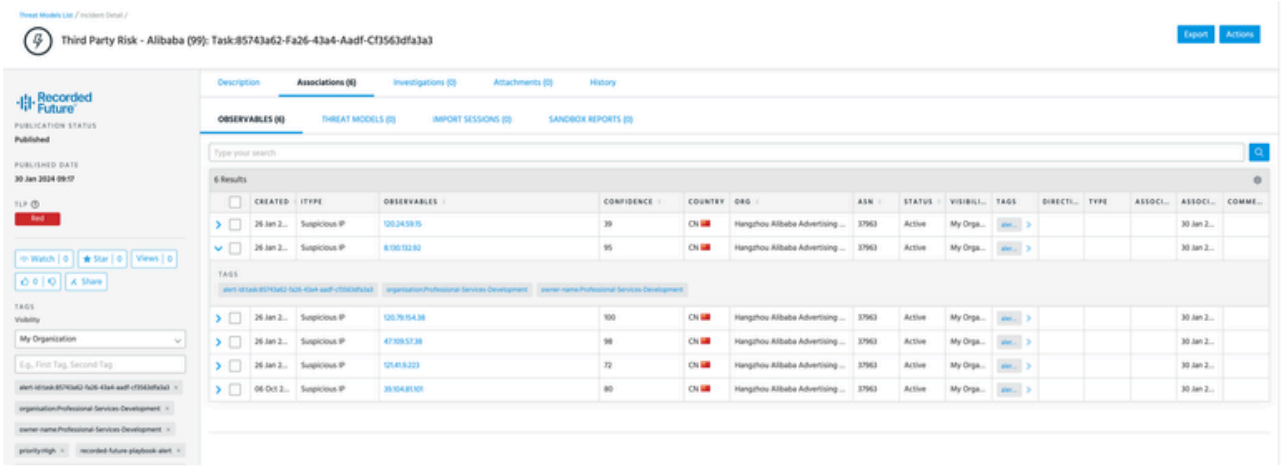
The Third Party Risk Playbook Alerts utilise the `Incident` Threat Model and can be found by selecting the `Incidents` from the **Filter Options** in the `Threat Model` page.

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



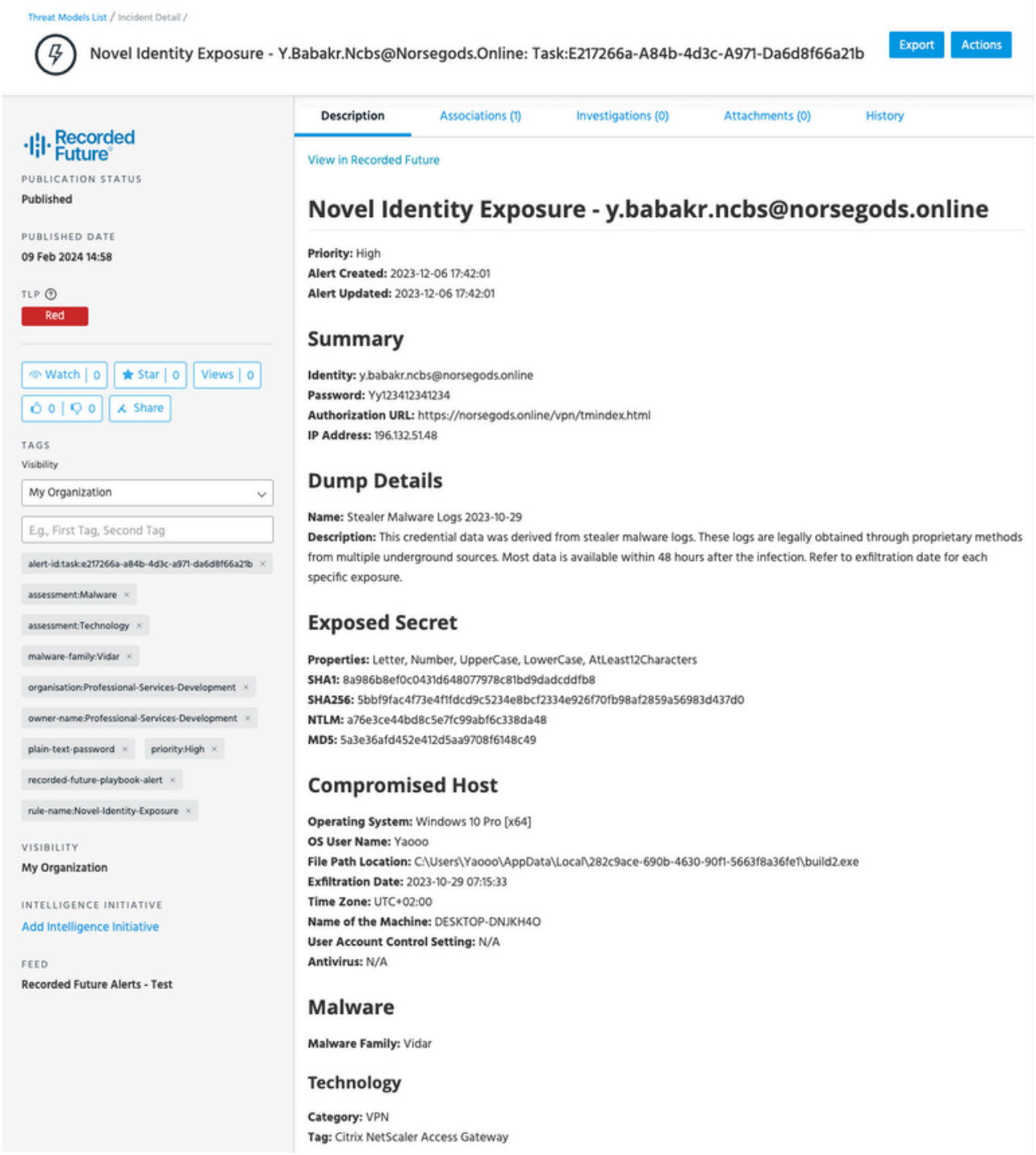
Playbook Alert: Third Party Risk - Observables

Identity Novel Exposures

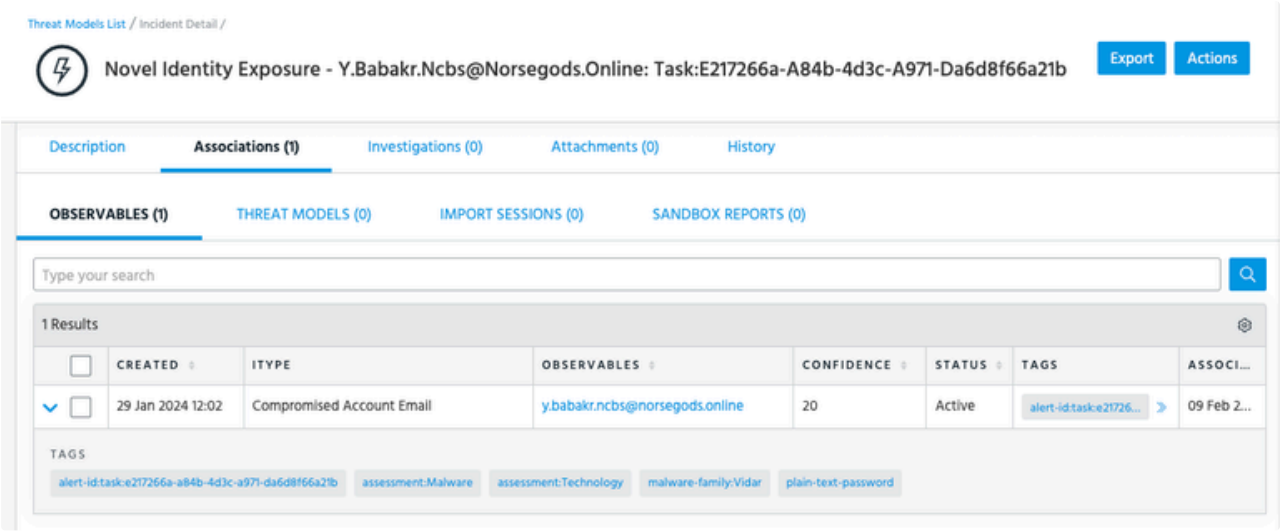
The Identity Novel Exposures Playbook Alerts utilise the `Incident` Threat Model and can be found by selecting the `Incidents` from the **Filter Options** in the `Threat Model` page.

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

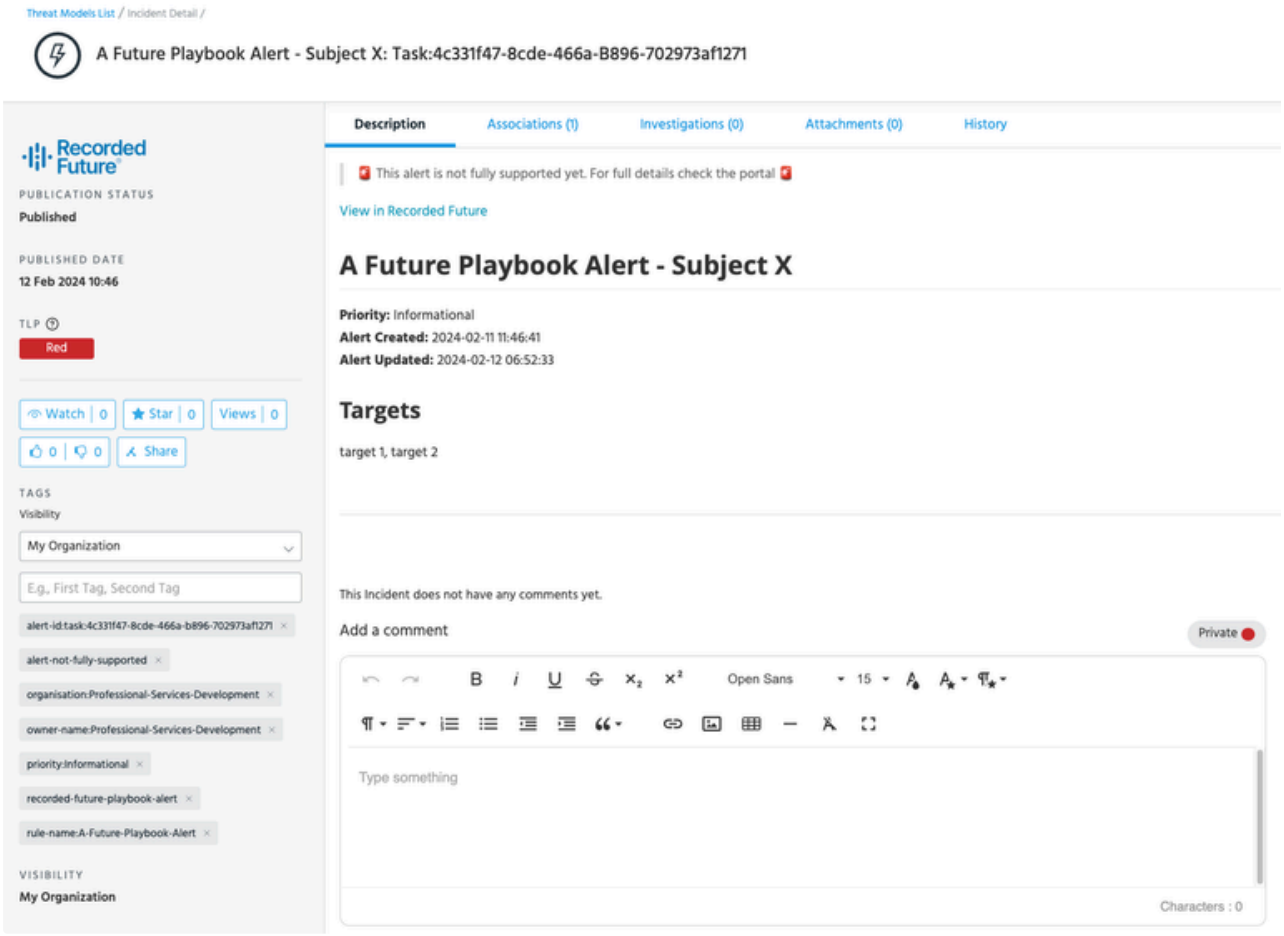
New Playbook Alerts

Brand new Playbook Alerts (not documented above) will be fed into Anomali TS, but will visualise only the core alert context.

The new playbook alerts contain the following:

- Link to the Recorded Future Portal for further analysis
- Alerting rule name
- Alert Priority
- Alert creation and update times
- Targets
- Tags
  - `alert-not-fully-supported` indicating the playbook alert is not yet fully supported

Note that the example below is just a representative mock.



Example of how new, not yet fully support Playbook Alerts will look like

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
- Identify Similar Domains
- IP Address Mentions
- Increased IP Address Risk Score
- Increased Domain Risk Score
- Potential Logo Abuse Detection

Recorded Future Playbook Alerts

- Domain Abuse
- Third Party Risk
- Novel Identity Exposures

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:

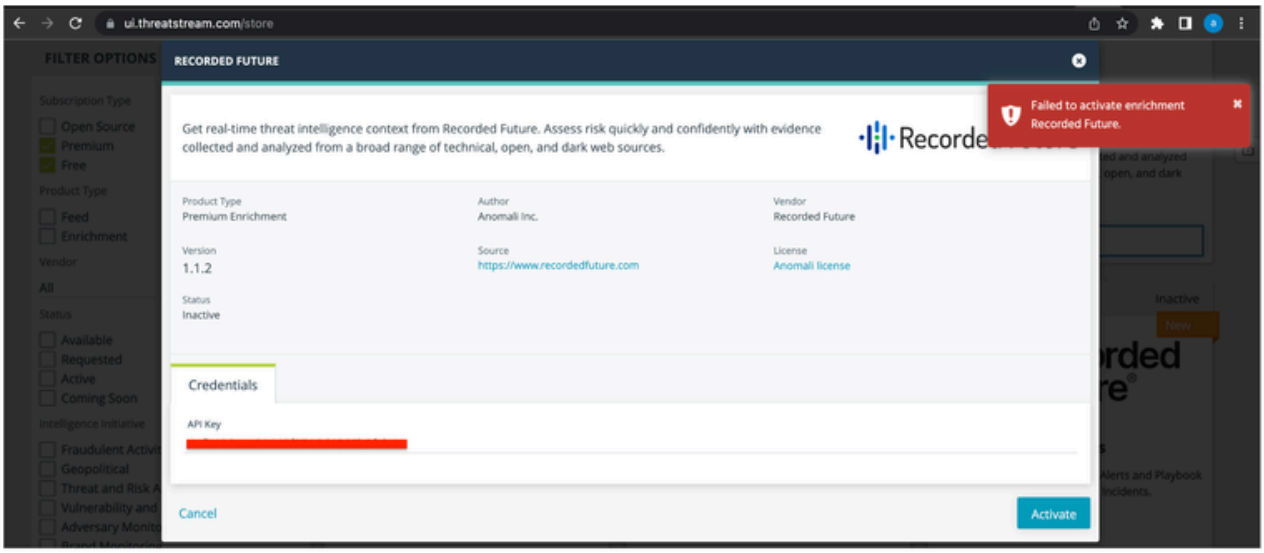
- For Playbook Alerts: this will be equal to the Recorded Future risk score of the observable plus 1, as shown in the screenshot above. The addition of 1 is to match the Anomali scale which goes up to 100 instead of 99.
- For classic alerts: the default confidence is `16` for all ITypes except for `Compromised 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
alert-not-fully-supported		✓	alert-not-fully-supported	Indicates that a Recorded Future Playbook Alert is new and not yet fully supported
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.

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

[1.3.0] - 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

[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