

# Recorded Future Alerts v1.3.0 - Anomali ThreatStream Installation Guide

- [Application Description](#)
- [Application Functionality](#)
  - [Recorded Future Classic Alerts](#)
  - [Recorded Future Playbook Alerts](#)
    - [Cyber Vulnerability](#)
      - [Affected Products](#)
    - [Data Leakage on Code Repository](#)
    - [Domain Abuse](#)
    - [Third Party Risk](#)
    - [Identity Novel Exposures](#)
    - [New Playbook Alerts](#)
    - [Updates](#)
  - [Observables](#)
    - [Confidence](#)
- [Installation](#)
  - [Configuration](#)
- [Tags](#)
- [Troubleshooting](#)
  - [Missing Observables](#)
  - [Not fetching alerts](#)
  - [IOC with 0 risk score and no Intelligence Card](#)
- [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 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:

## Threat Model

The screenshot displays the Threat Model interface. On the left, there is a 'Filter Options' sidebar with a search bar and a list of filters. The main area shows a search bar for 'Search Threat Model' and a table of 4204 results. The table has columns for 'TYPE', 'NAME', 'DATE PUBLISHED', 'TAGS', and 'SOURCE'. The first row is an incident titled 'Third Party Risk - Yandex' published on 26 Oct 2023 14:00. Below the table, there are several tags and risk rules associated with the incidents.

TYPE	NAME	DATE PUBLISHED	TAGS	SOURCE
Incident	Third Party Risk - Yandex: task:426fb575-c8e3-4226-a744-0a67c3a5c546	26 Oct 2023 14:00	alert-id:task-426fb575-c8e3-4226-a744-0a67c3a5c546	Recorded Future Alerts
Incident	Data Leakage on Code Repository - Splunk: task:7bdb1275-ea83-4b5a-ae0e-b3fd6656a755	26 Oct 2023 13:55	alert-id:task-7bdb1275-ea83-4b5a-ae0e-b3fd6656a755	Recorded Future Alerts
Incident	Domain Abuse - yuehin.com: task:e282acc2-7f5c-4efc-8a8a-1a3110017220	26 Oct 2023 13:48	alert-id:task-e282acc2-7f5c-4efc-8a8a-1a3110017220	Recorded Future Alerts
Incident	Data Leakage on Code Repository - Palo Alto Networks Inc.: task:6b9f06f2-169f-4840-8801-1708b585682e	26 Oct 2023 13:09	alert-id:task-6b9f06f2-169f-4840-8801-1708b585682e	Recorded Future Alerts
Incident	Company Email on Code Repository: 1P50N	26 Oct 2023 13:06	alert-id:1P50N	Recorded Future Alerts
Incident	Increased IP Address Risk Score - 47.304.179.218, 47... are now Very Malicious: 1P500	26 Oct 2023 13:06	alert-id:1P500	Recorded Future Alerts
Incident	My domains on Dark Web and closed sources: 1P50L	26 Oct 2023 13:06	alert-id:1P50L	Recorded Future Alerts
Incident	IP Address Mentions: 1P50P	26 Oct 2023 13:06	alert-id:1P50P	Recorded Future Alerts
Incident	My brands on Dark Web and closed sources: 1P50a	26 Oct 2023 13:05	alert-id:1P50a	Recorded Future Alerts
Incident	Leaked Credential Monitoring: 1P5kz7	26 Oct 2023 13:05	alert-id:1P5kz7	Recorded Future Alerts

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

ANOMALI | THREATSTREAM

DASHBOARD MANAGE ANALYZE RESEARCH APP STORE

Threat Models List / Incident Detail /

**Brand Name In Suspicious Websites Content (OCR): WRbUwy** Export Actions

**Recorded Future**

PUBLICATION STATUS  
Published

PUBLISHED DATE  
04 Jun 2024 16:57

TLP  
Red

Watch 0 Star 0 Views 0

Share

TAGS  
Visibility  
My Organization

E.g., First Tag, Second Tag

alert-id:WRbUwy

organisation:Professional-Services-Development

owner-name:Professional-Services-Development

recorded-future-alert

rule-name:Brand-name-in-suspicious-websites-con...

source:Image-OCR

VISIBILITY  
My Organization

INTELLIGENCE INITIATIVE  
Add Intelligence Initiative

FEED  
Recorded Future Alerts - Test

Description Associations (0) Investigations (0) Attachments (0) Notes History

View in Recorded Future

## Brand name in suspicious websites content (OCR) - wRbUwy

Alert Created: 2024-06-04 10:10:51  
Status in Portal: New

### AI Insights

A demand for quotes for septic tank work in various locations in France was observed on January 12, 2024, with requests for services related to septic tank installations from multiple individuals. Additionally, a mention of trading platforms and services was made, including futures trading and margin trading. Furthermore, information about a company specializing in engineering services for the insurance sector in Chile was presented. Finally, there were references to tools designed to assist web professionals in managing web services effectively.

### References

**Title:** Image OCR analysis  
**Source:** Image OCR  
**Fragment:** www.6tv.ro, www.facebook.com/live6tv Teilen 6TV.RO MARȚI, 10 APRILIE 2018 Promotia 1978 a Liceului Militar "Dimitrie Cantemir" Breaza aniverseaza 40 de ani de la absolvire Lista institutiilor militare de invatamant Promotiile 1950-2009 Site-ul oficial PROMOTII DE ABSOLVENTI PE FACEBOOK Promotia 1976 Promotia 1978 Relu Panait 5 aprilie la 19:29 M-am uitat ce am mai scris cu doua luni in urma si revin cu un program de principiu pentru ziua de 23 iunie a.c. pentru a clarifica aspectele financiare (motivarea contributiei fiecarui participant): CUM PUTETI COMUNICA CU FOSTII DUMNEAVOASTRA COLEGI PRIN INTERMEDIUL ACESTUI BLOG

**Title:** Image OCR analysis  
**Source:** Image OCR  
**Fragment:** Fosse France Spécialiste des Travaux d'Assainissement de Fosse en France Accueil Demande de devis Êtes-vous un artisan? Assainissement, Travaux Fosse Septique à Copponex Accueil / Assainissement, Travaux Fosse Septique à Copponex Jan 12, 2024 RGE Assainissement, Travaux Fosse Septique à Copponex Par assainissementfossefrance dans Non classé Demande de devis Le demande de devis est Gratuite. Civilité MONSIEUR Nom • E-mail • Ville • Description des travaux envisagés • ✓ Type des travaux • Fosse toutes eaux: installation Prénom • Téléphone • ECO artisan QUALIBAT Lanouvelle énergie du bâtiment Qualit EnR PROS QUALIFELEC Certifications RGE, QUALIBAT, ECO artisan, Les Pros des la performance énergétique, QUALIFELEC, QualitEnr Facebook Téléphone local

**Title:** Image OCR analysis  
**Source:** Image OCR  
**Fragment:** France Spécialiste des Travaux d'Assainissement de Fosse en France Accueil Demande de devis Êtes-vous un artisan? Assainissement, Travaux Fosse Septique à Cuzorn Accueil / Assainissement, Travaux Fosse Septique à Cuzorn Jan 12, 2024 Assainissement, Travaux Fosse Septique à Cuzorn Par assainissementfossefrance dans Non classé RGE ECO artisan QUALIBAT Lanouvelle énergie du bâtiment Qualit EnR PROS QUALIFELEC Demande de devis Le demande de devis est Gratuite. Civilité MONSIEUR Nom • E-mail • Ville • Description des travaux envisagés • ✓ Type des travaux • Fosse toutes eaux: installation Prénom • Téléphone • Certifications RGE, QUALIBAT, ECO artisan, Les Pros des la performance énergétique, QUALIFELEC, QualitEnr Facebook Téléphone local de France.

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.

## Threat Model

The screenshot shows the Threat Model interface with the following components:

- Filter Options:** A sidebar on the left with a search bar and a list of filters. The 'Vulnerabilities' filter is checked, and sub-filters for 'Filter by CVSS 2.0 score' and 'Filter by CVSS 3.0 score' are also present.
- Search:** A search bar at the top with the text 'Search Threat Model' and a magnifying glass icon.
- Model Type:** A dropdown menu set to 'Vulnerabilities'.
- Results:** A table displaying 21 results. The first row is expanded, showing details for a 'Cyber Vulnerability - CVE-2023-35359'. The table columns are: TYPE, NAME, DATE PUBLISHED, TAGS, and SOURCE.
- Tags:** A section below the first result showing tags such as 'lifecycle:Exploit-Likely', 'organisation:Professional-Services-Development', 'owner-name:Professional-Services-Development', 'priority:Moderate', and 'recorded-future-playbook-alert'.

TYPE	NAME	DATE PUBLISHED	TAGS	SOURCE
Vulnerability	Cyber Vulnerability - CVE-2023-35359: task:7e84f2e-9c0e-42b5-a17c-49a001a60f0e	27 Oct 2023 09:50	alert-id:task:7e84f2e-9c0e-42b5-a17c-49a001a60f0e	Recorded Future Alerts
Vulnerability	Cyber Vulnerability - CVE-2023-20109: task:cee1589d-8979-43ac-895b-b67649a40145	27 Oct 2023 09:50	alert-id:task:cee1589d-8979-43ac-895b-b67649a40145	Recorded Future Alerts
Vulnerability	Cyber Vulnerability - CVE-2023-28229: task:059119c2-4d6c-4f78-8352-7150e7237917	27 Oct 2023 09:50	alert-id:task:059119c2-4d6c-4f78-8352-7150e7237917	Recorded Future Alerts
Vulnerability	Cyber Vulnerability - CVE-2023-42824: task:525f014a-e764-4065-930b-6e58c8becdfc	27 Oct 2023 09:49	alert-id:task:525f014a-e764-4065-930b-6e58c8becdfc	Recorded Future Alerts
Vulnerability	Cyber Vulnerability - CVE-2023-36563: task:2b6c335c-faca-41ce-8399-2a85da6c7d7f	27 Oct 2023 09:49	alert-id:task:2b6c335c-faca-41ce-8399-2a85da6c7d7f	Recorded Future Alerts
Vulnerability	Cyber Vulnerability - CVE-2023-41763: task:453eb4ff-3b33-4976-8e12-eab616de0e00	27 Oct 2023 09:49	alert-id:task:453eb4ff-3b33-4976-8e12-eab616de0e00	Recorded Future Alerts
Vulnerability	Cyber Vulnerability - CVE-2023-38142: task:6356a985-c6f9-4ad2-8515-6fa488c547f	27 Oct 2023 09:49	alert-id:task:6356a985-c6f9-4ad2-8515-6fa488c547f	Recorded Future Alerts

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



PUBLICATION STATUS  
**Published**

PUBLISHED DATE  
27 Oct 2023 09:50

TLP

Red

Watch Star Views

Share

TAGS

Visibility

My Organization

E.g., First Tag, Second Tag

alert-id:task:7e84f2e-9c0e-42b5-a17c-49ad01a6bf0e

lifecycle:Exploit Likely

organization: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

Description Associations (0) Investigations (0) Attachments (1) History

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: 18

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/CHA: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

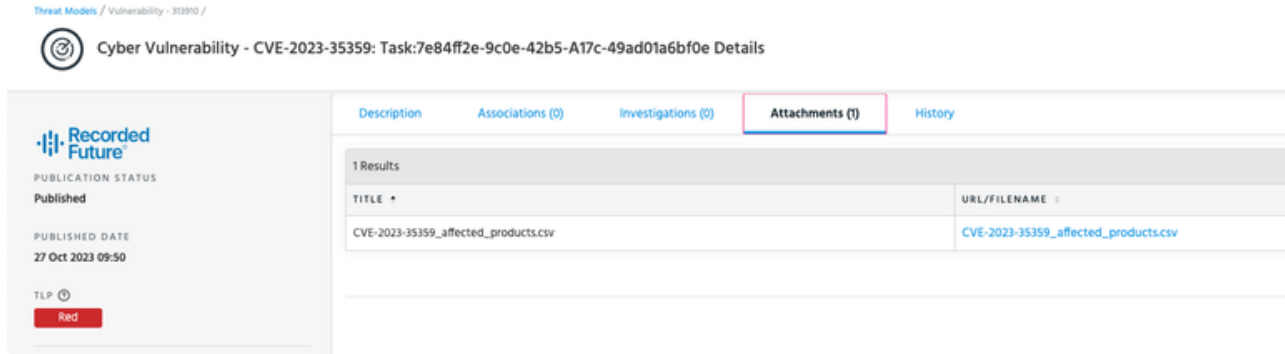
Microsoft Windows 10 1507 10.0.10240.16405 on Arm64	Microsoft Windows 10 1507 10.0.10240.16405 on X86	Microsoft Windows 10 1507 10.0.10240.16405 on X86	Microsoft Windows 10 1507 10.0.10240.16403 on Arm64	Microsoft Windows 10 1507 10.0.10240.16403 on X86	Microsoft Windows 10 1507 10.0.10240.16403 on X86	Microsoft Windows 10 1507 10.0.10240.16403 on X86	Microsoft Windows 10 1507 10.0.10240.16403 on X86	Microsoft Windows 10 1507 10.0.10240.16403 on X86
Microsoft Windows 10 1507 10.0.10240.16430 on X86	Microsoft Windows 10 1507 10.0.10240.16431 on X86	Microsoft Windows 10 1507 10.0.10240.16431 on X86	Microsoft Windows 10 1507 10.0.10240.16431 on X86	Microsoft Windows 10 1507 10.0.10240.16445 on Arm64	Microsoft Windows 10 1507 10.0.10240.16445 on X86	Microsoft Windows 10 1507 10.0.10240.16445 on X86	Microsoft Windows 10 1507 10.0.10240.16445 on X86	Microsoft Windows 10 1507 10.0.10240.16443 on Arm64
Microsoft Windows 10 1507 10.0.10240.16483 on X86	Microsoft Windows 10 1507 10.0.10240.16483 on X86	Microsoft Windows 10 1507 10.0.10240.16487 on Arm64	Microsoft Windows 10 1507 10.0.10240.16487 on X86	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 X86	Microsoft Windows 10 1507 10.0.10240.16520 on X86	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 X86	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 X86	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 X86	Microsoft Windows 10 1507 10.0.10240.16590 on X86
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 X86	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 X86	Microsoft Windows 10 1507 10.0.10240.16644 on X86	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 X86	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 X86	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 X86	Microsoft Windows 10 1507 10.0.10240.16771 on X86	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 X86	Microsoft Windows 10 1507 10.0.10240.16854 on X86	Microsoft Windows 10 1507 10.0.10240.16842 on Arm64	Microsoft Windows 10 1507 10.0.10240.16842 on X86	Microsoft Windows 10 1507 10.0.10240.16842 on X86	Microsoft Windows 10 1507 10.0.10240.16842 on X86	Microsoft Windows 10 1507 10.0.10240.16842 on X86	Microsoft Windows 10 1507 10.0.10240.16842 on X86
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 X86	Microsoft Windows 10 1507 10.0.10240.17071 on X86	Microsoft Windows 10 1507 10.0.10240.17103 on Arm64	Microsoft Windows 10 1507 10.0.10240.17103 on X86	Microsoft Windows 10 1507 10.0.10240.17103 on X86	Microsoft Windows 10 1507 10.0.10240.17103 on X86	Microsoft Windows 10 1507 10.0.10240.17146 on Arm64
Microsoft Windows 10 1507 10.0.10240.17146 on X86	Microsoft Windows 10 1507 10.0.10240.17190 on X86	Microsoft Windows 10 1507 10.0.10240.17190 on Arm64	Microsoft Windows 10 1507 10.0.10240.17190 on X86	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 X86	Microsoft Windows 10 1507 10.0.10240.17202 on X86	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 X86	Microsoft Windows 10 1507 10.0.10240.17236 on X86	Microsoft Windows 10 1507 10.0.10240.17236 on Arm64	Microsoft Windows 10 1507 10.0.10240.17236 on X86	Microsoft Windows 10 1507 10.0.10240.17236 on X86	Microsoft Windows 10 1507 10.0.10240.17236 on X86	Microsoft Windows 10 1507 10.0.10240.17236 on X86	Microsoft Windows 10 1507 10.0.10240.17236 on X86

#### Windows

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

### Affected Products

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



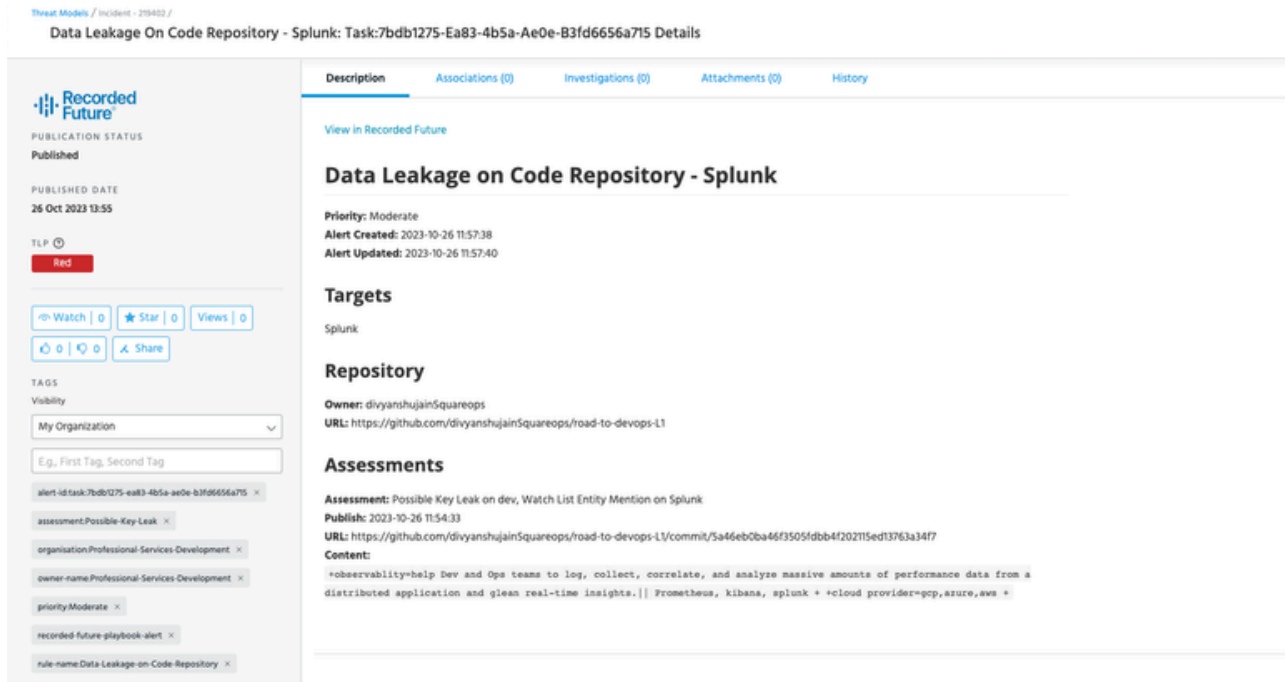
Affected Products attachment

### 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)

Threat Models / Incident - 219341 /

### Domain Abuse - Yuehin.Com: Task:E282acc2-F7c5-4efc-8a8a-1a3110017220 Details

**Recorded Future**  
PUBLICATION STATUS  
Published  
PUBLISHED DATE  
26 Oct 2023 13:48  
TLP  
Red

Watch | 0 Star | 0 Views | 0  
Share

TAGS  
Visibility  
My Organization  
E.g., First Tag, Second Tag  
alert-id:task:e282acc2-f7c5-4efc-8a8a-1a3110017220  
organisation:Professional-Services-Development  
owner-name:Professional-Services-Development  
priority:Moderate  
recorded-future-playbook-alert  
rule-name:Domain-Abuse  
screenshot-present

VISIBILITY  
My Organization  
INTELLIGENCE INITIATIVE  
Add Intelligence Initiative  
FEED  
Recorded Future Alerts - Test

Description Associations (2) Investigations (0) Attachments (0) History

View in Recorded Future

## Domain Abuse - yuehin.com

Priority: Moderate  
Alert Created: 2023-10-23 13:18:19  
Alert Updated: 2023-10-25 17:01:16

### Targets

yuehn.com

### Entity Context

Entity	Risk Score	Criticality	Context
yuehn.com	5	Low	Active Mail Server

### Resolved Records

Entity	Risk Score	Criticality	Record Type	Context
ip:107.151.181.123	0		A	N/A

Screenshot Count: 1

Scanned: 2023-10-23 13:20:59

Welcome to NINGBO YUEHIN INDUSTRIAL CO.,LTD. website!

NINGBO YUEHIN INDUSTRIAL CO.,LTD.  
Expert in the field of conveying system products  
Hotline: 008615258180018

HOME ABOUT US PRODUCTS APPLICATION NEWS SERVICE JOB CONTACT US

### CONVEYOR TRANSMISSION YUEHIN - PRODUCT AREA

DRIVE BELT, GEAR, DRUM, TRAFFIC FACILITIES

SOURCE FACTORY WITH RELIABLE QUALITY

Hot keywords :

Product

- CONVEYOR BELTS
- RUBBER BELTS
- RUBBER SHEET/MAT
- SPROCKET & PULLEY
- RUBBER/PVC HOSE
- ROLLER & IDLER
- TRAFFIC FACILITIES

Recommended products

- RUBBER SHEET
- Flame Retardant Conveyor Roll
- Anti-Static and M-MSI Conveyor Roll

MORE>>>

Playbook Alert: Domain Abuse

Threat Models / Incident - 2024-1 / Domain Abuse - Yuehin.Com: Task:E282acc2-F7c5-4efc-8a8a-1a3110017220 Details Export Actions

**Recorded Future**  
PUBLICATION STATUS  
Published  
PUBLISHED DATE  
26 Oct 2023 13:48  
TLP Red  
Watch Star Views  
Share

Description Associations (2) Investigations (2) Attachments (0) History

OBSERVABLES (2) THREAT MODELS (0) IMPORT SESSIONS (0) SANDBOX REPORTS (0)

Type your search

2 Results

	CREATED	ITYPE	OBSERVABLES	CONFID...	COUNTRY	ORG	ASN	STATUS	VISIBILI...	TAGS	DIRECTI...	TYPE	ASSOCI...	ASSOCI...	COMME...
>	25 Oct 2...	Suspicious	107151181123	1	SG	Zenlayer	21859	Falsepos	My Orga...	<a>View</a>					25 Oct 2...
>	25 Oct 2...	Suspicious	yuehin.com	6				Falsepos	My Orga...	<a>View</a>					25 Oct 2...

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

Threat Models List / Incident Detail / **Third Party Risk - Alibaba (99): Task:85743a62-Fa26-43a4-Aadf-Cf3563dfa3a3** Export Actions

**Recorded Future**  
PUBLICATION STATUS  
Published  
PUBLISHED DATE  
30 Jan 2024 09:17  
TLP Red  
Watch Star Views  
Share

Tags  
Visibility  
My Organization  
E.g., First Tag, Second Tag  
alert-id:task:85743a62-fa26-43a4-aadf-cf3563dfa3a3  
organisation:Professional-Services-Development  
owner-name:Professional-Services-Development  
priority:high recorded-future-playbook-alert  
risk-rule:Hosts-Recently-Communicating-With-C&C...  
risk-rule:Recent-High-Impact-Abuse-of-Company-L...  
rule-name:Third-Party-Risk

Visibility  
My Organization  
Intelligence Initiative  
Add Intelligence Initiative  
Feed

Description Associations (6) Investigations (0) Attachments (0) History

View in Recorded Future

### Third Party Risk - Alibaba (99)

Priority: High  
Alert Created: 2023-08-30 16:33:38  
Alert Updated: 2024-01-29 16:48:16

### Malicious Network

#### Hosts Recently Communicating With C&C Server

Added on: 2024-01-29 16:46:00  
Summary: 605 sightings: Active command and control communication on uncommon ports related to malware from 8 hosts including 47.57.181.106, 47.74.17.23, 47.57.242.27. 4 related malware families including PlugX, Cobalt Strike: C2Concealer, Cobalt Strike. Last observed on Jan 28, 2024.

#### Evidence

**Observed Network Traffic - Client IP 47.57.242.27**

- Recent Timestamp: 2024-01-04 18:43:40
- Malware IP Address: 122.254.94.69 (49)
- Malware IP Risk Description: 18 sightings on 1 source: Recorded Future Command & Control Validation. Recorded Future analysis validated 122.254.94.69:8000 as a command and control server for PlugX on Jan 30, 2024 Mitigated by being in Multi-Domain IP Addresses (Allow List).
- Malware Family: PlugX

**Observed Network Traffic - Client IP 47.57.242.27**

- Recent Timestamp: 2024-01-07 16:53:00
- Malware IP Address: 143.198.214.96 (99)
- Malware IP Risk Description: 1 sighting on 1 source: Recorded Future Command & Control Validation. Recorded Future analysis validated 143.198.214.96:33434 as a command and control server for Cobalt Strike: C2Concealer on Jan 29, 2024
- Malware Family: Cobalt Strike: C2Concealer

**Observed Network Traffic - Client IP 47.74.17.23**

- Recent Timestamp: 2024-01-08 13:14:43
- Malware IP Address: 103.145.191.118 (99)

Playbook Alert: Third Party Risk



Third Party Risk - Alibaba (99): Task:85743a62-Fa26-43a4-Aadf-Cf3563dfa3a3

Export Actions

Recorded Future

PUBLICATION STATUS: Published

PUBLISHED DATE: 30 Jan 2024 09:17

TLP: Red

Watch Star Views

Share

TAGS: Visibility My Organization

E.g., First Tag, Second Tag

Third Party Risk - Alibaba (99): Task:85743a62-Fa26-43a4-Aadf-Cf3563dfa3a3

organization: Professional Services Development

center name: Professional Services Development

priority: high

recorded future playbook alert

Description Associations (0) Investigations (0) Attachments (0) History

OBSERVABLES (6) THREAT MODELS (0) IMPORT SESSIONS (0) SANDBOX REPORTS (0)

Type your search

6 Results

CREATED	TYPE	OBSERVABLES	CONFIDENCE	COUNTRY	ORG	ASN	STATUS	VISIBILI...	TAGS	DIRECT...	TYPE	ASSOCI...	ASSOCI...	COMME...
26 Jan 2...	Suspicious IP	10.24.58.15	39	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
26 Jan 2...	Suspicious IP	8.192.132.92	95	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...

TAGS

Third Party Risk - Alibaba (99): Task:85743a62-Fa26-43a4-Aadf-Cf3563dfa3a3

organization: Professional Services Development

center name: Professional Services Development

26 Jan 2...	Suspicious IP	10.76.154.38	100	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
26 Jan 2...	Suspicious IP	47.59.57.38	98	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
26 Jan 2...	Suspicious IP	121.418.223	72	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...
06 Oct 2...	Suspicious IP	26.104.81.101	80	CN	Hangzhou Alibaba Advertising ...	37963	Active	My Orga...	...					30 Jan 2...

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)



Export

Actions



PUBLICATION STATUS

Published

PUBLISHED DATE

09 Feb 2024 14:58

TLP

Red

Watch 0

Star 0

Views 0

Like 0

Share

TAGS

Visibility

My Organization

E.g., First Tag, Second Tag

alert-id:task:e217266a-a84b-4d3c-a971-da6d8f66a21b

assessment:Malware

assessment:Technology

malware-family:Vidar

organisation:Professional-Services-Development

owner-name:Professional-Services-Development

plain-text-password priority:High

recorded-future:playbook-alert

rule-name:Novel-Identity-Exposure

VISIBILITY

My Organization

INTELLIGENCE INITIATIVE

Add Intelligence Initiative

FEED

Recorded Future Alerts - Test

Description

Associations (1)

Investigations (0)

Attachments (0)

History

View in Recorded Future

# Novel Identity Exposure - y.babakr.ncbs@norsegods.online

Priority: High

Alert Created: 2023-12-06 17:42:01

Alert Updated: 2023-12-06 17:42:01

## Summary

Identity: y.babakr.ncbs@norsegods.online

Password: Yy123412341234

Authorization URL: https://norsegods.online/vpn/tmindex.html

IP Address: 196.132.51.48

## Dump Details

Name: Stealer Malware Logs 2023-10-29

Description: This credential data was derived from stealer malware logs. These logs are legally obtained through proprietary methods from multiple underground sources. Most data is available within 48 hours after the infection. Refer to exfiltration date for each specific exposure.

## Exposed Secret

Properties: Letter, Number, UpperCase, LowerCase, AtLeast12Characters

SHA1: 8a986b8ef0c0431d648077978c81bd9dadcdffb8

SHA256: 5bbf9fac4f73e4f1fdcd9c5234e8bcf2334e926f70fb98af2859a56983d437d0

NtLm: a76e3ce44bd8c5e7fc99abf6c338da48

Md5: 5a3e36afd452e412d5aa9708f6148c49

## Compromised Host

Operating System: Windows 10 Pro [x64]

OS User Name: Yaooo

File Path Location: C:\Users\Yaooo\AppData\Local\282c9ace-690b-4630-90f1-5663f8a36fe1\build2.exe

Exfiltration Date: 2023-10-29 07:15:33

Time Zone: UTC+02:00

Name of the Machine: DESKTOP-DNJKH40

User Account Control Setting: N/A

Antivirus: N/A

## Malware

Malware Family: Vidar

## Technology

Category: VPN

Tag: Citrix NetScaler Access Gateway

Playbook Alert: Novel Identity Exposures



Description **Associations (1)** Investigations (0) Attachments (0) History

**OBSERVABLES (1)** THREAT MODELS (0) IMPORT SESSIONS (0) SANDBOX REPORTS (0)

Type your search

1 Results

<input type="checkbox"/>	CREATED	ITYPE	OBSERVABLES	CONFIDENCE	STATUS	TAGS	ASSOCI...
<input checked="" type="checkbox"/>	29 Jan 2024 12:02	Compromised Account Email	y.babakr.ncbs@norsegods.online	20	Active	alert-id:task:e21726...	09 Feb 2...

TAGS

alert-id:task:e217266a-a84b-4d3c-a971-da6d8f66a21b assessment:Malware assessment:Technology malware-family:Vidar plain-text-password

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.



Recorded Future

PUBLICATION STATUS  
**Published**

PUBLISHED DATE  
**12 Feb 2024 10:46**

TLP  
Red

Watch | 0
Star | 0
Views | 0

Like | 0
Dislike | 0
Share

TAGS

Visibility

My Organization

E.g., First Tag, Second Tag

alert-id:task-4c331f47-8cde-466a-b896-702973af1271

alert-not-fully-supported

organisation:Professional-Services-Development

owner-name:Professional-Services-Development

priority:Informational

recorded-future-playbook-alert

rule-name:A-Future-Playbook-Alert

VISIBILITY

**My Organization**

Description

Associations (1)

Investigations (0)

Attachments (0)

History

! This alert is not fully supported yet. For full details check the portal !

View in Recorded Future

## A Future Playbook Alert - Subject X

**Priority:** Informational  
**Alert Created:** 2024-02-11 11:46:41  
**Alert Updated:** 2024-02-12 06:52:33

### Targets

target 1, target 2

---

This incident does not have any comments yet.

Add a comment Private ●

↶ ↷
**B** *i* U 🔗 x<sub>2</sub> x<sup>2</sup> Open Sans 15 🔍 🗨️ 🗑️

☰ ☰ ☰ ☰ ☰ ☰ ☰ ☰ ☰ ☰
🗨️ 🗨️ 🗨️ 🗨️ 🗨️ 🗨️
🔗 🗑️ 🗑️

Type something

Characters : 0

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](mailto:support@recordedfuture.com).

## Confidence

The confidence of each observable is set as follows:

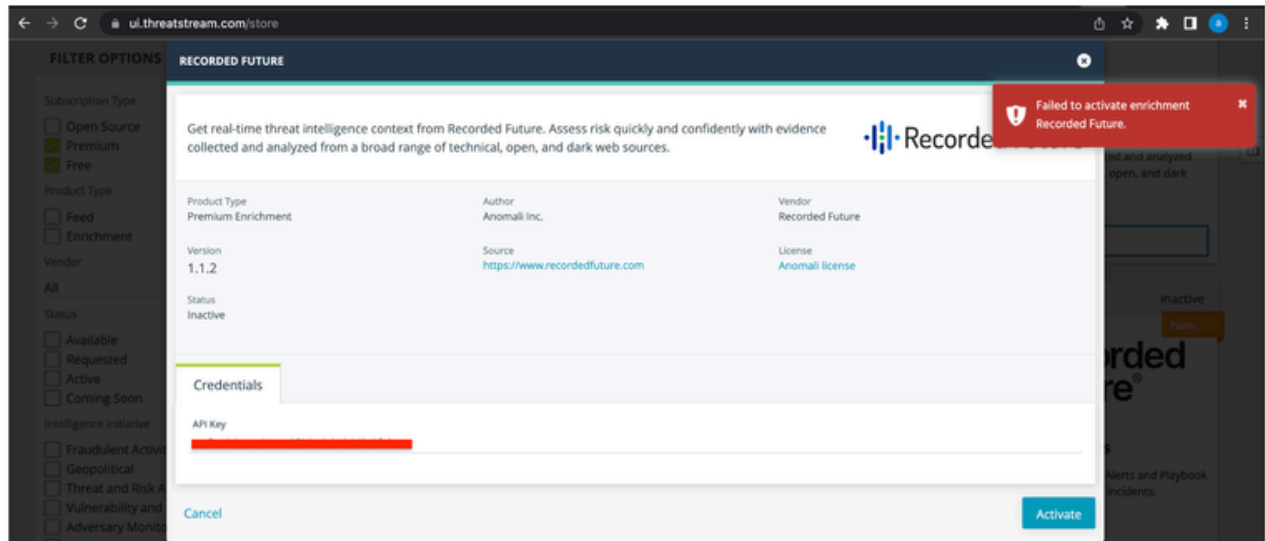
- For Playbook Alerts: this will be equal to the Recorded Future risk score of the observable plus 1, as shown in the screenshot above. The addition of 1 is to match the Anomali scale which goes up to 100 instead of 99.
- For classic alerts: the default confidence is 16 for all ITypes except for `Compromised 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	✓	✓	<code>alert-id:wyf7g0</code>	Recorded Future Alert ID
alert-not-fully-supported		✓	<code>alert-not-fully-supported</code>	Indicates that a Recorded Future Playbook Alert is new and not yet fully supported
assessment		✓	<code>assessment:Possible-Key-Leak</code>	Indicates the assessment made by Recorded Future
author	✓	✓	<code>author:Bot</code>	Author of the data

lifecycle		✓	lifecycle:Exploited	Indicates the lifecycle stage of a vulnerability
malware-family	✓	✓	malware-family:Lumma	Indicates stealer malware name
organisation	✓	✓	<i>organisation:PS-Development</i>	The organisation of the alert
owner-name	✓	✓	<i>owner-name:Moise</i>	The owner of the alert
plain-text-password		✓	<i>plain-text-password</i>	Indicates that the Incident contains a plain text password
priority		✓	<i>priority:High</i>	Indicates the priority of a Recorded Future Playbook Alert
recorded-future-alert		✓	<i>recorded-future-alert</i>	Indicates that this is a Recorded Future Alert
recorded-future-playbook-alert		✓	<i>recorded-future-playbook-alert</i>	Indicates that this is a Recorded Future Playbook Alert
risk-rule		✓	<i>risk-rule:Recent-Validated-Cyber-Attack</i>	Name of the matched Recorded Future Risk Rule
rule-name	✓	✓	<i>rule-name:Leaked-Credential-Monitoring</i>	Recorded Future Alert rule name
screenshot-present		✓	<i>screenshot-present</i>	Indicates that the Incident contains a screenshot
source	✓	✓	<i>source:Genesis-Store</i>	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 `[anomaly_ts]` stanza
- 

## [1.0.0 GA] - 2023-03-08

## Added

- Official package release