

Recorded Future Alerts - QRadar Installation Guide v1.1.0

- [Application Description](#)
- [System Requirements](#)
- [Installation](#)
- [Configuration](#)
 - [Creating an authorized service token](#)
 - [Importing Pulse dashboards](#)
 - [Custom Rules](#)
 - [Increase Max TCP Syslog Payload Length](#)
 - [Recorded Future Alerts configuration](#)
- [Application Functionality](#)
 - [Triage alerts](#)
 - [Triage using AQL](#)
 - [Fetch alerts](#)
 - [Limitations](#)
- [Pulse dashboards](#)
 - [Organisation Filter](#)
 - [Out of the Box Dashboards](#)
 - [Recorded Future Alerts Statistics](#)
 - [Recorded Future Alerts and Recorded Future Playbook Alerts](#)
 - [Recorded Future - Code Repo Leakage](#)
 - [Recorded Future - Cyber Vulnerability](#)
 - [Recorded Future - Domain Abuse](#)
 - [Recorded Future - Domain Code Repository and Recorded Future - Email Code Repository](#)
 - [Recorded Future - Identify Similar Domains](#)
 - [Recorded Future - Leaked Credential Monitoring and Recorded Future - Leaked Email Monitoring](#)
 - [Recorded Future - My domains on Dark Web and closed sources](#)
 - [Recorded Future - Novel Identity Exposure](#)
 - [Recorded Future - Potential Logo Abuse Detection](#)
 - [Recorded Future - Third Party Risk](#)
 - [Recorded Future - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities](#)
- [Supported Alerts](#)
 - [Mapping custom alerts using the DSM Editor](#)
- [Logging & Troubleshooting](#)
 - [Syslog connection issues](#)
 - [Logs indicate alerts were sent to QRadar, but search returns no alerts](#)
 - [Truncation of events](#)
 - [Not fetching alerts](#)
- [Appendix](#)
 - [Supported Classic Alert Rules](#)
 - [Supported Playbook Alert Rules](#)
 - [Out-of-the-box Custom Event Properties \(CEP\)](#)

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 application for IBM QRadar enables:

- Delivery of Recorded Future Alert details consumed in IBM QRadar as events via custom Recorded Future log sources.
- Triaging Recorded Future Alerts and Playbook Alerts with the full alert details context directly in the IBM QRadar product.
- Review trending Intelligence Goals Library (IGL) data.
- Ability to document historical credential leaks.

The Recorded Future Alerts application for IBM QRadar enables better alerts triaging by adding relevant and comprehensive context.

System Requirements

- IBM QRadar version 7.4.1 Fix Pack 2 or higher
- IBM QRadar Authorized Services Token (Admin)
- Recorded Future Alerts for IBM Security QRadar SIEM API Token
- TCP Port 514 open from QRadar server where the application is running to the syslog destination
- Recorded Future account for accessing content when pivoting outside IBM QRadar to the Recorded Future platform

Installation

The preferred installation method for Recorded Future Alerts application is by uploading the application zip file via [Extension Management](#).

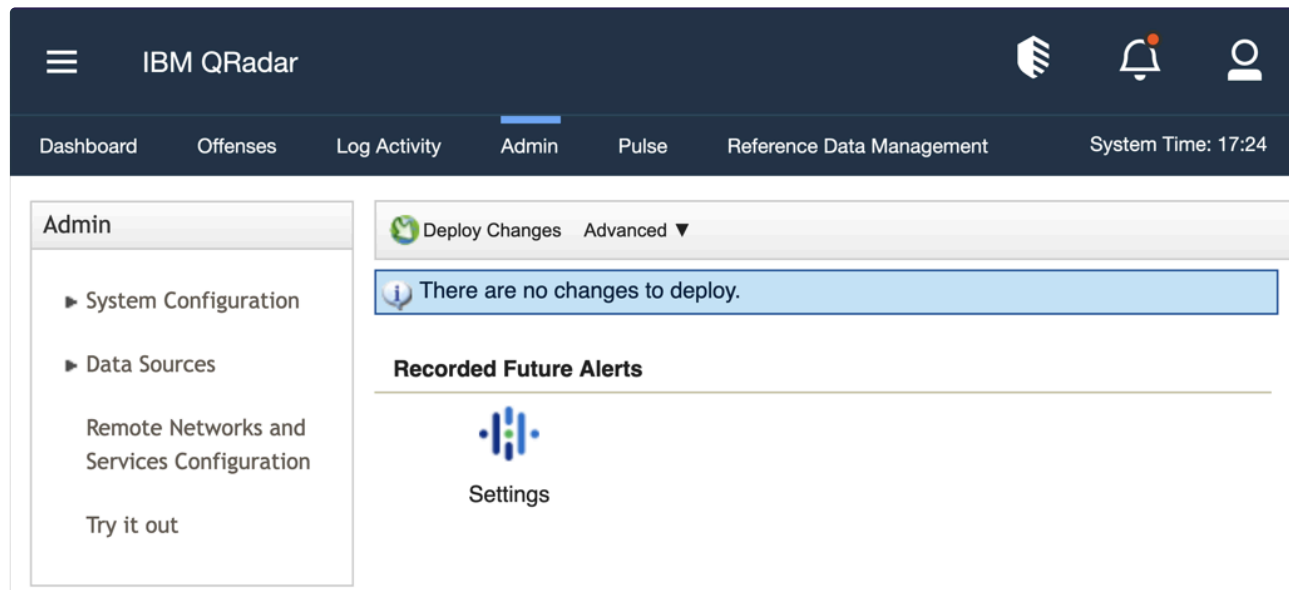
Configuration

Once the Recorded Future Alerts application is installed, the “Settings” icon should be already visible under the “Admin” tab from IBM QRadar in the “Plug-ins” sections.



Before configuring the application itself, please complete these steps in the following order:

1. [Creating an authorized service token](#)
2. [Importing Pulse dashboards](#)
3. [Custom Rules](#)
4. [Increase Max TCP Payload Length](#)
5. [Recorded Future Alerts configuration](#)



Creating an authorized service token

The Recorded Future Alerts application requires an IBM QRadar Authorized Service Token (AST) to operate.

Note: QRoC customers get their AST from the "self Serve App" See: [Authorized service token](#)

S

Please use the following steps to create such a Token that you can later use in the application configuration window:

1. Click on the **Admin** tab
2. Click **Authorized Services**
3. Click **+Add**
4. In the **Authorized Service Label**, type a name for the authorized service
5. From the **Security Profile** list, select **Admin**
6. From the **User Role** list, select **Admin**

7. Set the desired token expiry period

Authorized Service Management

Filter Search Results

User Role (1)

☐ Admin 1

Security Profile (1)

☐ Admin 1

Search Authorized Service

Authorized Service Label	User Role	Security Profile	Authorized By	Last Used
recfut_alerts	Admin	Admin	admin	Fri, 18/11/2022

New Authorized Service

Authorized Service Label
recfut_alerts

Permissions

Security Profile [Manage Security Profiles](#)
Admin

User Role [Manage User Roles](#)
Admin

Expiry Settings

This Authorized Service expires ☐

Cancel Save

8. Click **Save**

Once the service is created, the newly created **Authentication Token** is displayed and can be copied. Please note that, the authorized service token cannot be made visible after you close the **Authorized Service Created Successfully** dialog. Copy the token to a secure location before you close the dialog. Link for reference: [Adding an authorized service](#)

Importing Pulse dashboards

The application comes with a set of dashboards which allow to quickly visualise and effectively triage Recorded Future alerts & playbook alerts in the IBM QRadar Pulse application. To install the dashboards, please follow the steps detailed below:

1. Click on the **Admin** tab
2. Click **Pulse - Dashboard**
3. Click **Synchronize**

Pulse Dashboard Templates

Synchronize

Name

Status

Recorded Future - Email Code Repository

Alerts from Recorded Future. Email Code Repository alert rule.

New

Recorded Future - Identify Similar Domains

New

Recorded Future - Potential Logo Abuse Detection

New

4. Click on the **Pulse** tab
5. Click on the **Dashboard** dropdown
6. Click **Create Dashboard**

Dashboard Offenses Log Activity Admin **Pulse** Reference Data Management

Dashboard
Recorded Future - Alert Details ^

Para
★ Ti

1

Event and flow metrics
Use these default dashboards as a starting point to create your own customized dashboards.

Aler
Miscellaneous metrics
Use these default dashboards as a starting point to create your own customized dashboards.

Offense overview
Use these default dashboards as a starting point to create your own customized dashboards.

Recorded Future - Admin Dashboard

Recorded Future - Alert Details ✓

Recorded Future - Domain Code Repository

Create dashboard

7. Click **Manage templates**
8. Click **Install** for each **Recorded Future** named dashboard

Custom Rules

The application comes with a set IBM QRadar Offense Rules to enable offense generation. These rules can be found in the **Recorded Future Alerts** group.

i By default these rules are enabled and will generate an offense per Recorded Future alert.

⚠ Non parsing alerts will not generate offenses.

Increase Max TCP Syslog Payload Length

Because alerts and playbook alerts are sent via syslog and some of the alert payloads can be rather large, this can easily top the QRadar default settings for the Max TCP Syslog Payload Length. This will result in some Recorded Future alert payloads being truncated and not parsing correctly. To avoid this issue from happening, follow the steps outlined below:

1. Click on the **Admin** tab
2. Click **System Settings**
3. Click **Advanced**
4. In the **Max TCP Syslog Payload Length** field, type **12288**

The screenshot shows the 'System Settings' page with a sidebar on the left containing links to various settings categories. The main area displays a list of settings. The 'Max TCP Syslog Payload Length' setting is highlighted with a red box, showing a value of '12,288'. Other settings include 'Global Iptables Access', 'Syslog Event Timeout', 'Partition Testers Timeout', 'Max UDP Syslog Payload Length', 'Max Number of TCP Syslog Connections', 'Max TCP Syslog Connections Per Host', 'Timeout for Idle TCP Syslog Connections', and 'Log and Network Activity Data Export Temporary Directory'.

System Settings	Value
Global Iptables Access (comma separated)	
Syslog Event Timeout (minutes)	720
Partition Testers Timeout (seconds)	30
Max UDP Syslog Payload Length	2,048
Max TCP Syslog Payload Length	12,288
Max Number of TCP Syslog Connections	2,500
Max TCP Syslog Connections Per Host	10
Timeout for Idle TCP Syslog Connections (seconds)	900
Log and Network Activity Data Export Temporary Directory	/store/exports

5. Click **Save**
6. The changes made will require a **Full Deploy**, click on the **Admin** tab
7. From the **Advanced** list, click **Deploy Full Configuration**
8. After services restart, the QRadar deployment is updated to allow TCP packets that are up to **12288** bytes without truncation

i More information about the topic [QRadar: TCP and UDP Syslog Maximum Payload Message Length for QRadar Appliances](#)

Recorded Future Alerts configuration

The configuration page for the Recorded Future Alerts application can be found in the **Admin** tab within the **Plug-ins** section. Once opened the configuration page will enable configuration of

the following parameters:

Recorded Future Settings

[Logs](#)

Configuration retrieved successfully

Save

Recorded Future API

API Key
.....

Provide a Recorded Future API key to authenticate this application. Reach out to [Recorded Future Support](#) to retrieve your key.

☒ SSL Verification

IBM QRadar

Syslog Destination

Send Recorded Future Alerts as events to QRadar (Port 514).

Authorization Token
.....

Create an authorized service token to authenticate this application. To create an authorization token, go to *Authorized Services*.

Unable to fetch log source 'Recorded Future Alerts' status. Reason: Invalid or missing QRadar Authorization Token

Unable to fetch log source 'Recorded Future Playbook Alerts' status. Reason: Invalid or missing QRadar Authorization Token

Recorded Future Alerts

☐ Fetch Alerts

☐ Fetch Playbook Alerts

Select Recorded Future Alerts (Intelligence Goals Library with Custom Alerts) and/or Playbook Alerts to be sent to QRadar.

Alert Poll Frequency (minutes)
60

Time interval for Recorded Future Alerts & Playbook Alerts to be fetched at. Default is 60minutes.

Alerting Rules

Playbook Alerts

Powered by PSEngine

Logs

- *Logs* - links to application logs

Recorded Future API

- *API Key* - Recorded Future API Token

- *SSL verification switch* - Allows to disable SSL certificates verification when reaching out to the Recorded Future API

IBM QRadar

- *Syslog Destination* - IP/Hostname of a QRadar syslog destination which the Recorded Future Alerts application uses to send alerts as events via syslog on port 514.
- *Authorization Token* - IBM QRadar Authorized Service Security Token created in the [previous steps](#)

Recorded Future Alerts

- *Fetch Alerts switch* - when disabled Recorded Future Alerts will not be downloaded
- *Fetch Playbook Alerts switch* - when disabled Recorded Future Playbook Alerts will not be downloaded
- *Alert Poll Frequency* - controls how often the alerts & alert updates (applicable to Playbook Alerts) be ingested. Defaults to 60 minutes, lowest supported interval is 15 minutes.
- *Alerting Rules list* - selected alerting rules will be ingested
- *Playbook Alerts list* - selected playbook alerts will be ingested

 List of alert rules to select will only be available once the configuration has a valid Recorded Future API Key saved.

Application Functionality

Recorded Future Alerts application's functionality is underpinned by the Recorded Future API, which is the repository from which QRadar retrieves the Recorded Future Alerts and Playbook Alerts. The app fetches alert details and provides them to QRadar via two log sources **Recorded Future Alerts** and **Recorded Future Playbook Alerts**. This makes the alerts context ready for triaging and advanced correlation in IBM QRadar.

Triage alerts

Ingested alerts become searchable with the help of AQL queries and a set of [Pulse dashboards](#) detailed later in this document.

Triage using AQL

The query below returns all ingested Recorded Future Alerts from the past 3 days.

```
1 SELECT
2     "Alert ID",
3     "Alert Title" AS "Alert Title",
4     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS 'Triggered Time',
```

```

5     "Alert URL" AS 'Alert URL',
6     logsourcename(logsourceid) AS log_source_name
7 FROM events
8 WHERE (
9     log_source_name = 'Recorded Future Alerts'
10 )
11 GROUP BY "Alert ID"
12 ORDER BY "Triggered Time" DESC last 3 Days

```

The query below returns all ingested Recorded Future Playbook Alerts from the past 3 days.

```

1 SELECT
2     "Entity Name" AS "Entity Name",
3     "Alert ID",
4     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS 'Triggered Time',
5     "Alert URL" AS 'Alert URL',
6     logsourcename(logsourceid) AS log_source_name
7 FROM events
8 WHERE (
9     log_source_name = 'Recorded Future Playbook Alerts'
10 )
11 GROUP BY "Alert ID"
12 ORDER BY "Triggered Time" DESC last 3 Days

```

The query below returns all email addresses and passwords that have been leaked with the market name where they are sold.

```

1 SELECT
2     "Email Leaked" AS "Leaked Email",
3     "Leaked Password",
4     "Alert Source Name" AS "Source Name",
5     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS 'Triggered Time',
6     logsourcename(logsourceid) AS log_source_name
7 FROM events
8 WHERE (
9     "Alert Rule Name"='Leaked Credential Monitoring' AND
10     log_source_name = 'Recorded Future Alerts'
11 )
12 ORDER BY "Triggered Time" DESC last 3 DAYS

```

The query below returns all the similar domains (example typosquats) that have been seen in the last 3 days.

```

1 SELECT
2     "Alert Source Name" AS "Repo Name",
3     "Similar Domain" AS "Domain",
4     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS "Triggered Time",
5     logsourcename(logsourceid) AS log_source_name
6 FROM events
7 WHERE (
8     "Alert Rule Name"='Identify Similar Domains' AND
9     log_source_name = 'Recorded Future Alerts'
10 )
11 ORDER BY "Triggered Time" DESC last 3 DAYS

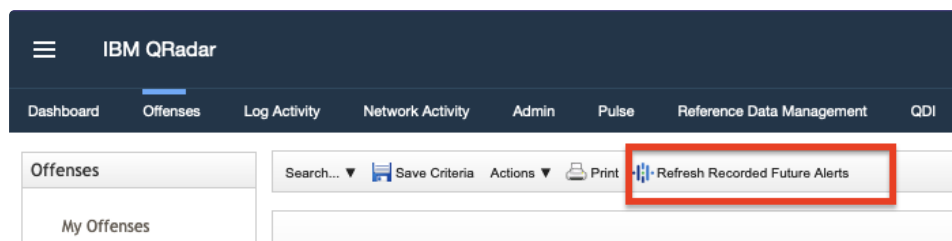
```

The query below returns a list of target domains that have been triggered by the domain abuse playbook alert in the last 3 days.

```
1 SELECT
2     "Entity Name" AS "Domain",
3     "Targets List" AS "Target",
4     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS 'Triggered Time',
5     logsourcename(logsourceid) AS log_source_name
6 FROM events
7 WHERE (
8     "Alert Rule Name" = 'Domain Abuse' AND
9     log_source_name = 'Recorded Future Playbook Alerts'
10 )
11 ORDER BY "Triggered Time" DESC last 3 DAYS
```

Fetch alerts

The users can trigger an alert poll ahead of schedule from the **Offenses** tab.



i Please note it may take some time before new alerts become searchable in QRadar as the system can take time to process the events. The exact amount of time depends on the size and load of the QRadar deployment.

Limitations

Payload size restrictions are in place to minimize payload truncation due to QRadar payload size limitations.

Playbook Alerts

- panel_log limited to 5 LASTEST objects
- Cyber Vulnerability PBA affected_products limited to 10 products
-

Pulse dashboards



Some tables in the dashboards will not present data straight away. It is required that you select the row (alert) that you are interested in to get the details in the subsequent tables.

Also note that for more details all the dashboards link back to the Recorded Future Portal. A valid Recorded Future account is needed to see those details.

Below are reported all the actions that you can perform without having access to the Recorded Future App.

Organisation Filter

Every user will have a filter called “Organisation” in each dashboard. This is used to filter for specific Recorded Future Alerts based on the Organisation in which the alert triggered. To select an organisation, just enter a part of the organisation name and click Update



Organisation	Time Value	★ Time Period	
Org1	10	Days	Update

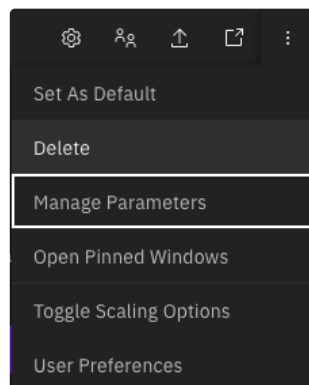
If you want to see all the alerts from all the organisations, enter a dot (.)



★ Organisation	Time Value	★ Time Period	
.	10	Days	Update

If you do not have Multi-Org enabled in the Recorded Future Portal, just configure the Organisation filter, with the dot (.) character:

- In the top right side click on the three dots
- Click on **Manage Parameters**



- Search for “Organisation”
- Set “Default value” as .

- Click **Save**

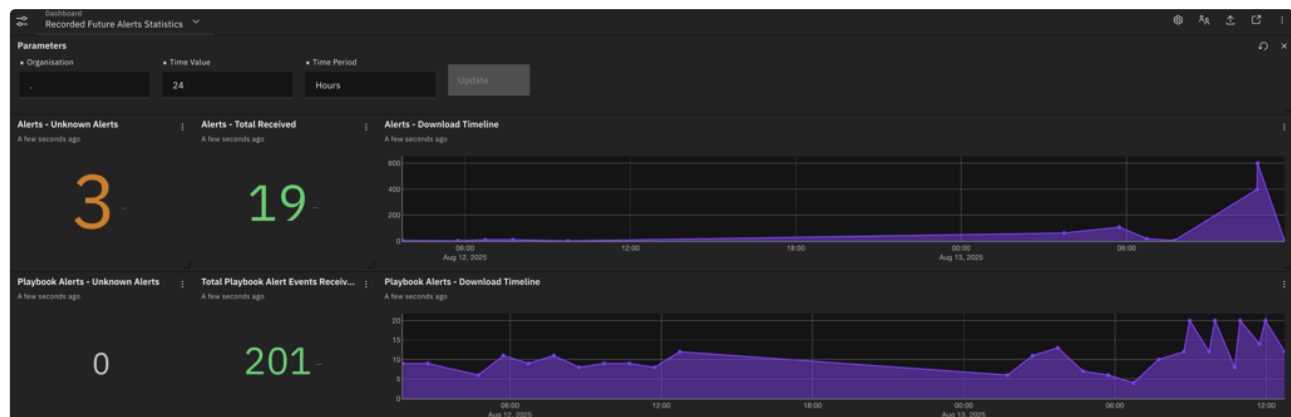
Out of the Box Dashboards

Below is the list of Alert Rules that have out of the box dashboards to use:

- Code Repo Leakage
- Cyber Vulnerability
- Domain Abuse
- Domain Code Repository
- Email on Code Repository
- Identify Similar Domains
- Leaked Credential Monitoring
- Leaked Email Monitoring
- Novel Identity Exposure
- My domains on Dark Web and closed Sources
- New Critical or Pre NVD Watch List Vulnerabilities (Global)
- New Critical or Pre NVD Watch List Vulnerabilities (Tech Stack)
- Potential Logo Abuse Detection

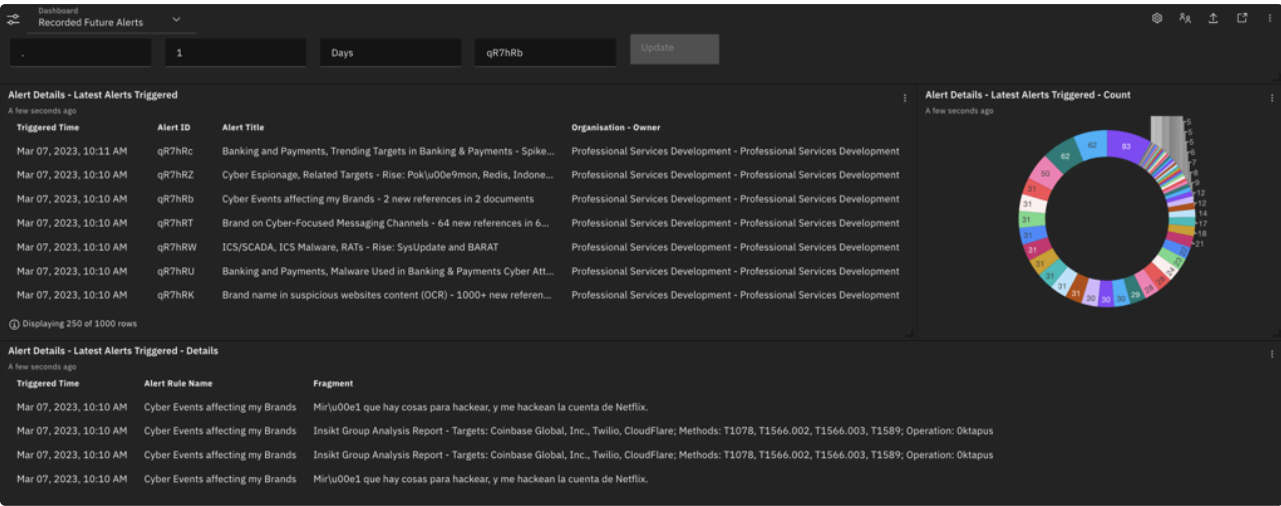
Recorded Future Alerts Statistics

This dashboard shows the number of alerts that failed to be ingested in the **Alerts - Unknown Events** and **Playbook Alerts - Unknown Events**, the number of total alert ingested for both Legacy and Playbook and the Timeline of the ingested alerts.

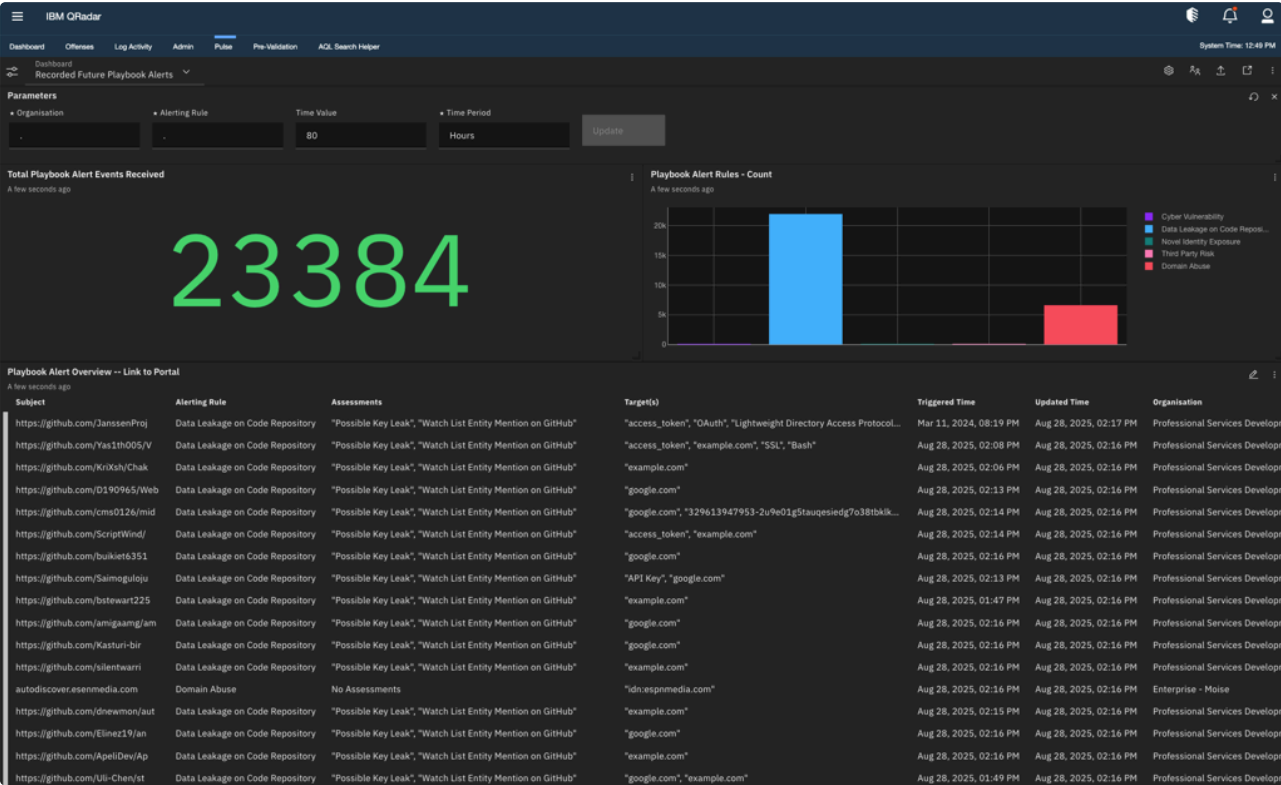


Recorded Future Alerts and Recorded Future Playbook Alerts

These two dashboards show an overview of the alerts that have been ingested.



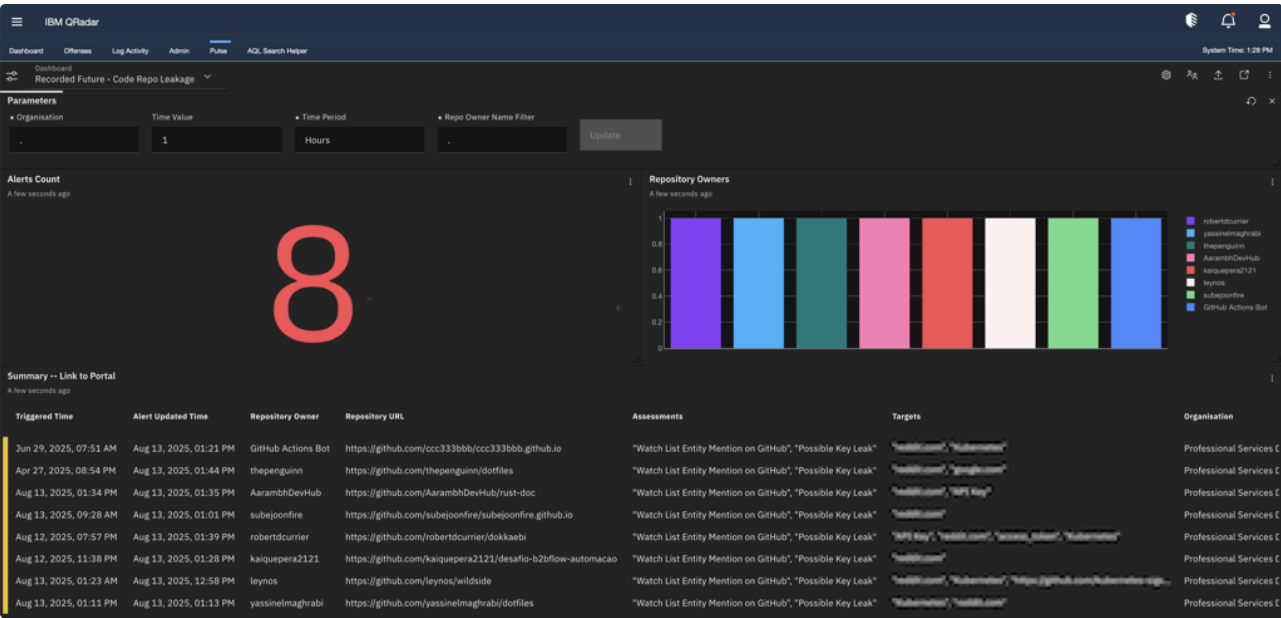
In the dashboard above, clicking on any of the alerts in the **Alert Details - Latest Alerts Triggered** will populate the widget below it (**Alert Details - Latest Alerts Triggered - Details**) with details on the specific alert.



Recorded Future Playbook Alerts

Recorded Future - Code Repo Leakage

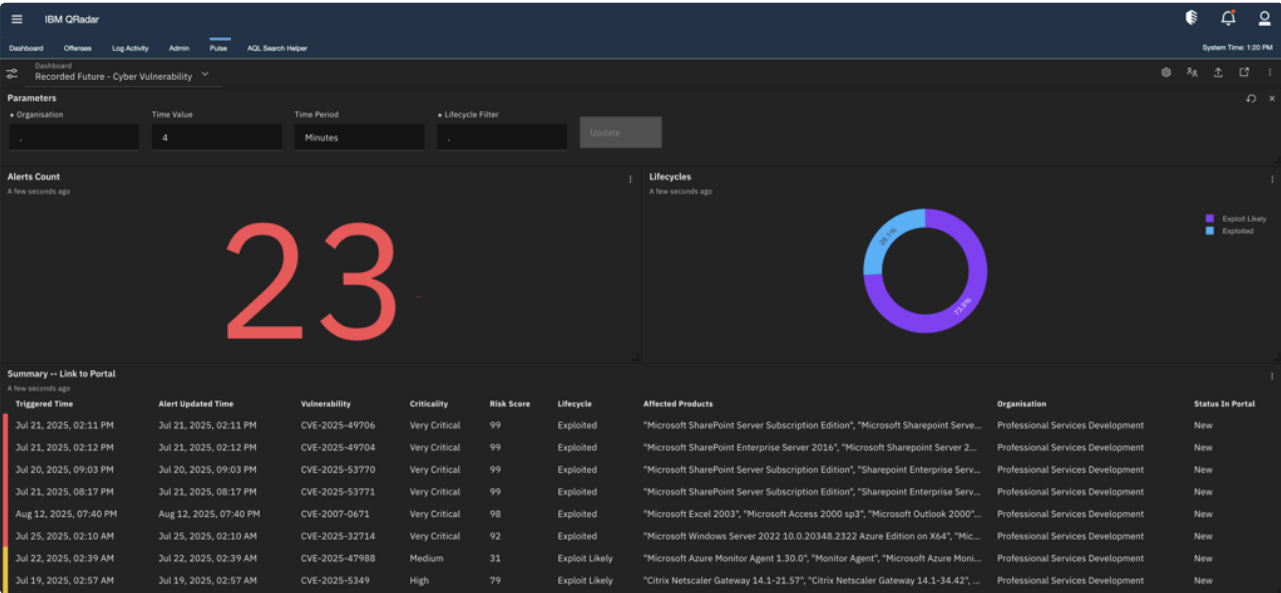
This dashboard shows the details of each code repository leakage alert that has been received. Clicking on a repository owner name in the chart will fill the **Repo Owner Name Filter** and populate the Summary table showing all alerts sharing the repository owner name.



Recorded Future - Code Repo Leakage

Recorded Future - Cyber Vulnerability

This dashboard shows the details of each cyber vulnerability alert that has been received. Clicking on a lifecycle inside the doughnut will fill the Lifecycle Filter and populate the Summary table matching the vulnerability lifecycle stage.



Recorded Future - Cyber Vulnerability

Recorded Future - Domain Abuse

This dashboard shows the details of each domain abuse alert that has been received. Clicking on an alert in the Domain Abuse - Summary will populate the underlying tables with the details of the Whois data, DSN, MX and NS records.

- **Domain Abuse - Domain Whois** will redirect you to the the Recorded Future portal - a valid account is required - to view the full alert and the screenshot. The column **screenshot** will give you an idea if there is a screenshot or not with the values **Retrieved / Not Found**
- **Domain Abuse - Domain DNS Records** will redirect you to the enrichment of the **A Record IP**. The geolocation on the right side is provided by QRadar **GEO::LOOKUP** and it is related to the location of the IP.
- **Domain Abuse - Domain MX and NS Records** shows the details of the MX Domain and IP, along with a list of NS Names.

IBM QRadar

Dashboard

Offenses

Log Activity

Admin

Pulse

Reference Data Management

System Time: 09:26

Dashboard

Recorded Future - Domain Abuse

Parameters

★ Organisation

Time Value

★ Time Period

Domain Filter

Update

Domain Abuse - Count

Domain Abuse - Summary

569

Triggered Time	Updated Time	Domain	Context	Risk Score	Target
Jul 06, 2022, 07:43 PM	Feb 25, 2023, 02:45 PM	fast.cyou	"Phishing Host"	5	"idn:fast.co", "idn:fast.com.tw", "idn:fast.no", "idn:fast.org"
Aug 03, 2022, 12:58 AM	Feb 25, 2023, 03:05 PM	venmopay.mobi	N/A	5	"idn:venmopay.org", "idn:venmopay.net"
Oct 14, 2022, 05:48 AM	Feb 25, 2023, 03:22 PM	linaray.com	"Phishing Host"	5	"idn:linaray.com"
Jul 29, 2022, 08:26 AM	Feb 25, 2023, 05:31 PM	mypatpal.com	"Phishing Host"	5	"idn:mypatpal.com"
Oct 22, 2022, 02:42 PM	Feb 25, 2023, 04:59 PM	zycv.com	"Active Mail Server"	5	"idn:zycv.com", "idn:zycv.org"

Domain Abuse - Domain Whois -- Link to Alert in Portal

Domain Abuse - Domain DNS Records -- Link to IP Enrichment

Domain Abuse - Domain DNS Records on Map

Domain	Context	Country	State	City	Name	Screenshot
zycv.com	"Phishing Host"	China				Retrieved
zycv.com	"Phishing Host"	China				Retrieved
zycv.com	"Phishing Host"	China				Retrieved
zycv.com	"Phishing Host"	China				Retrieved
zycv.com	"Phishing Host"	China				Retrieved

Domain	A Record IP	IP Risk Score	IP Info
zycv.com	199.59.243.222	50	"C&C Server"
zycv.com	199.59.243.222	46	"C&C Server"
zycv.com	162.55.217.94	25	"Phishing Host"
zycv.com	162.55.217.94	25	"Phishing Host"
zycv.com			

Domain Abuse - Domain MX and NS Records

Domain	MX Record	MX Risk Score	MX Info	NS Names
zycv.com				["idn:contact.skype.id.18606008806.myym.com", "idn:contact.wechat.or.qq.id.5300066.myym.com", "idn:contact.wh..."]
zycv.com				["idn:contact.skype.id.18606008806.myym.com", "idn:contact.wechat.or.qq.id.5300066.myym.com", "idn:contact.wh..."]
zycv.com				["idn:contact.skype.id.18606008806.myym.com", "idn:contact.wechat.or.qq.id.5300066.myym.com", "idn:contact.wh..."]
zycv.com				["idn:contact.skype.id.18606008806.myym.com", "idn:contact.wechat.or.qq.id.5300066.myym.com", "idn:contact.wh..."]
zycv.com				["idn:contact.skype.id.18606008806.myym.com", "idn:contact.wechat.or.qq.id.5300066.myym.com", "idn:contact.wh..."]

Recorded Future - Domain Code Repository and Recorded Future - Email Code Repository

The **Domain Filtered** and **Email Filtered** tables have been created with the idea of showing all the alerts involving a specific domain or email. Clicking on any entry in that table will redirect you to the alert in the Recorded Future Portal.

Example of Recorded Future - Domain Code Repository below:

Dashboard
Recorded Future - Domain Code Repository

Parameters

Organisation

Time Value

Time Period

Domain Filter

Update

Domains on Code Repo - Details

Triggered Time	Domain	Repo Name	Fragment	Author	Organisation - Owner
Mar 07, 2023, 10:05 AM	2023-02-14.json	GitHub	2023-02-14.json says it stopped largest DDoS attack on record": {"http...	Lilengun	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:05 AM	2023-02-23.json	GitHub	2023-02-23.json ": {"https://therecord.media/russia-radio-hackers-fa...	Lilengun	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:05 AM	2022-10-25.md	GitHub	2022-10-25.md claims attack on Wisconsin school district](https://ther...	Lilengun	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:05 AM	settings.py	GitHub	settings.py ") SOCIAL_AUTH_GOOGLE_OAUTH2_SECRET = str(os.geten...	Annymars23	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:05 AM	bookshop-site-data.json	GitHub	bookshop-site-data.json //akash-writes.medium.com/\"/\"works_butto...	akashTheCommunityGuy	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:05 AM	Virtual_keyboard.md	GitHub	Virtual_keyboard.md : Tutorial Part 1: https://medium.com/@wang33he...	yushan1089	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:05 AM	CyberSecurityRSS-tiny.opml	GitHub	CyberSecurityRSS-tiny.opml ={"rss" htmlUrl="http://regiero.github.io/...	Lilengun	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:05 AM	S-bash-approvalgates-5691-0014.yml	GitHub	S-bash-approvalgates-5691-0014.yml@gmail.com - email@example.c...	jfbetapipeorg	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:05 AM	u6c42.txt	GitHub	PHP[u6784[u9020http[u5934[u53d1[u9001[u8bf7[u6c42.txt (\$_REQ...	tophub100	Professional Services Development - Professional Services Development

Domains on Code Repo - Repo ...

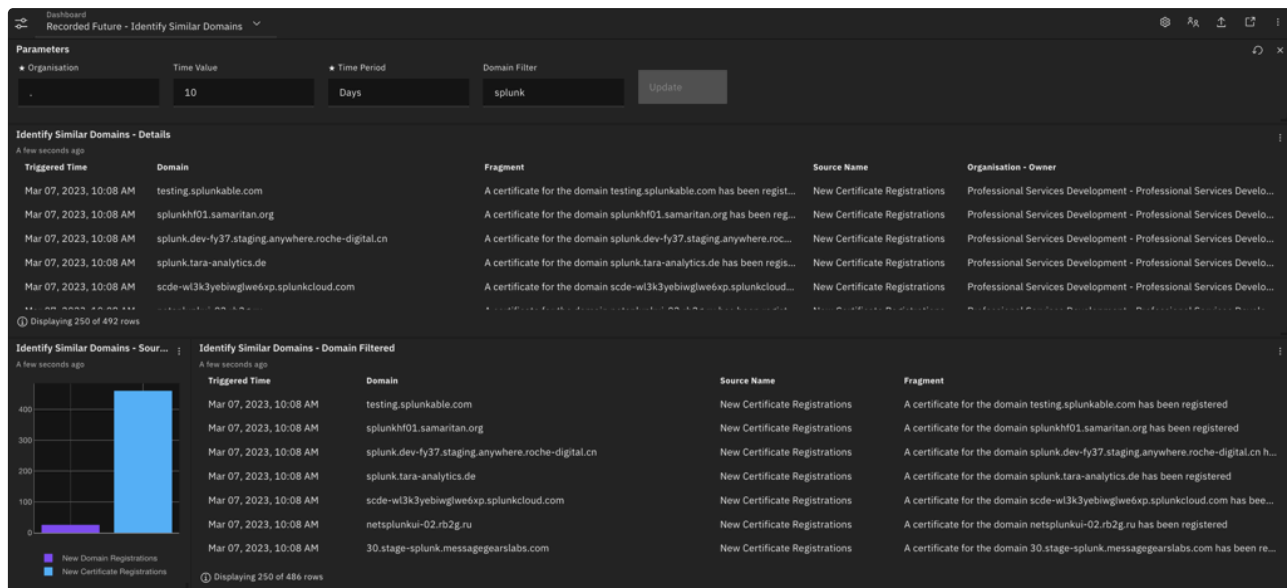
Domains on Code Repo - Domain Filtered

Triggered Time	Domain	Repo Name	Author	Fragment	Repo URL
Mar 05, 2023, 10:03 AM	splunk-enterprise-panel.yaml	GitHub	ictmuzi	splunk-enterprise-panel.yaml id: splunk-enterprise-panel info: na...	https://github.com/ictmuzi/Muscan/blob/master/tools/nuclei-te...
Mar 05, 2023, 10:03 AM	splunk-enterprise-panel.yaml	GitHub		splunk-enterprise-panel.yaml id: splunk-enterprise-panel info: na...	
Feb 24, 2023, 10:04 AM	splunk_go	GitHub	steevex35	splunk_go /open-telemetry/opentelemetry-collector-contrib/test...	https://github.com/steevex35/opensearchexporter/blob/main/te...
Feb 16, 2023, 10:04 AM	webpack.splunkapp	GitHub		webpack.splunkapp.config.js = require("@splunk/webpack-config...	
Feb 16, 2023, 10:04 AM	splunk_create.conf	GitHub	marcusschiesser	splunk_create.conf # this file is generated by @splunk/create aut...	https://github.com/marcusschiesser/xveditor/blob/master/splun...
Feb 16, 2023, 10:04 AM	splunk.env	GitHub	marcusschiesser	splunk.env SPLUNK_PASSWORD=splunkdev SPLUNK_START_AR...	https://github.com/marcusschiesser/xveditor/blob/master/splun...

Recorded Future - Domain Code Repository

Recorded Future - Identify Similar Domains

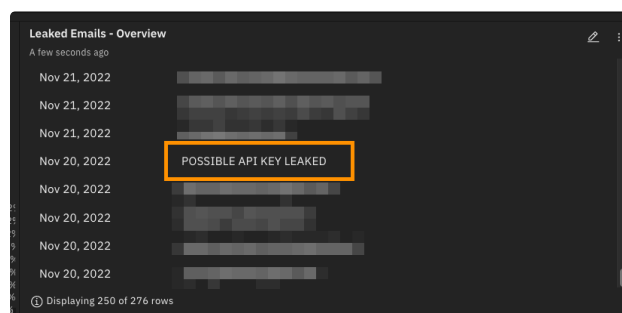
Similar to the above dashboards, the Identify Similar Domains shows alerts triggering from the homonym alert. The **Domain Filter** works the same as the “Recorded Future - Domain Code Repository” dashboard.

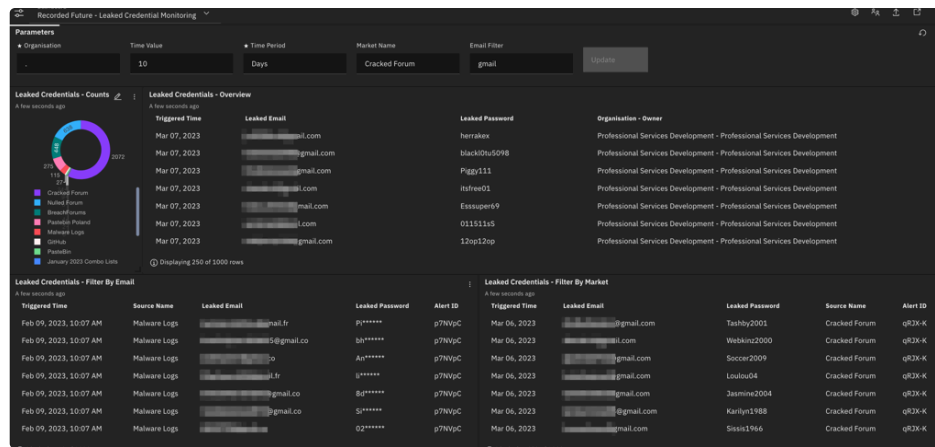


Recorded Future - Identify Similar Domains

Recorded Future - Leaked Credential Monitoring and Recorded Future - Leaked Email Monitoring

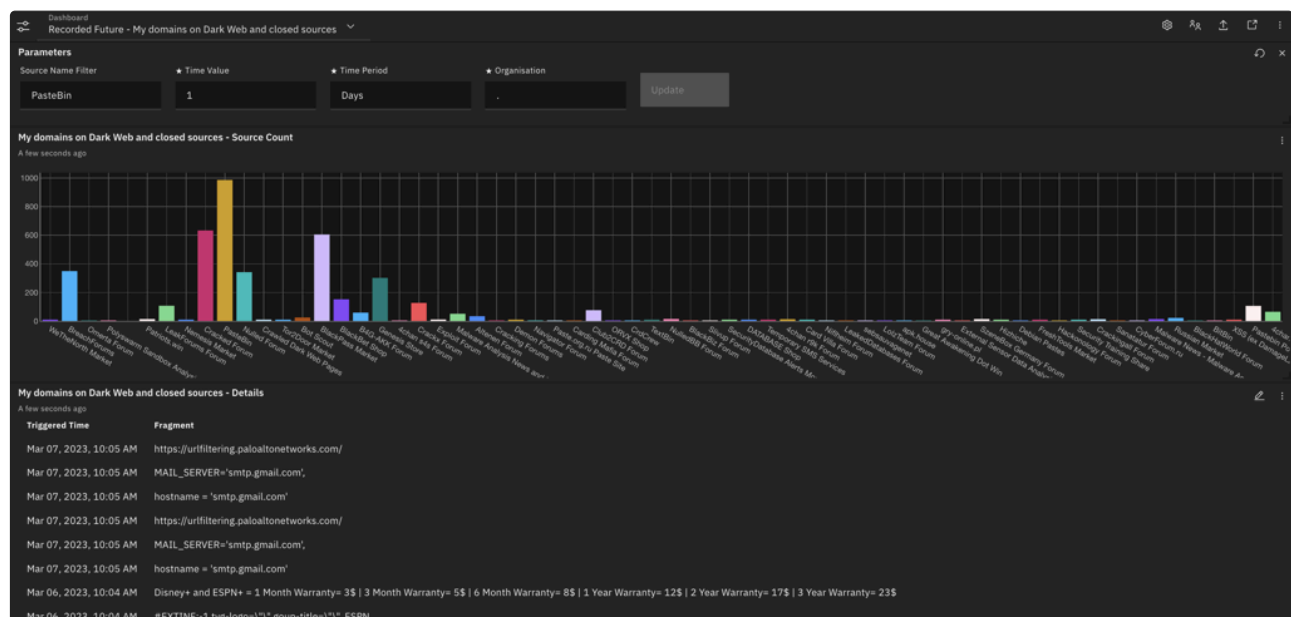
These two dashboards work in the same way as well. Both the dashboards allow to filter for Email which will populate the **Filter by Email** table (bottom) or the **Filter by Market** table on the right. Both filters allow free-text of the whole Email/Market name or part of it. In the example we have used **tesla** as a search filter. The idea is to enable you to search for all the activities in a specific Market or for a specific email address or mail domain. Leaked password in Leaked Email Monitoring might not be present due to the nature of the alert. There is a chance that an API Key will be captured by the alert rule. If that is the case it will be displayed with the text **POSSIBLE API KEY LEAKED** and it is required for you to log into the Recorded Future app to see the details.





Recorded Future - My domains on Dark Web and closed sources

With this dashboard you will see a list of all the sources that triggers the alert with a counter of the number of alert that triggered. Clicking on each column will show the **Fragment** of the alert to give you a brief idea of what the alert is about. Clicking on the alert row itself will redirect you to the portal.



Recorded Future - My domains on Dark Web and closed sources

Recorded Future - Novel Identity Exposure

This dashboard shows the details of each identity exposure alert that has been received. Clicking on an alert in the **Summary** widget will populate the underlying table with the full details of the alert (unavailable fields remain blank and shown in the image below).

Additionally, the user can use the **Identity** and **Password** parameters to filter through alerts in the **Alert Overview** widget. Both parameters are using **IMATCHES** regex which gives the user enough flexibility to retrieve multiple alerts matching the query. Both filters default to `.` which results in matching all alerts.

⚠ The **Password** column will display the plain text password when available, otherwise a password hint concatenated with three asterisks will be displayed.
To enable clear text passwords, please refer to this [support article](#).

IBM QRadar

DashboardOffensesLog ActivityAdminPulsePre-ValidationAQI Search Helper

System Time: 12:47 PM

Dashboard

Recorded Future - Novel Identity Exposure

Parameters

Organisation

Time Value

Time Period

Identity

Password

Update

Alerts Count

4 minutes ago

11

Summary

4 minutes ago

Triggered Time	Updated Time	Subject	Authorization URL	Domain(s)	Organisation	Status In Portal
Aug 25, 2025, 10:05 PM	Aug 25, 2025, 10:05 PM	spkotputlibehror@norsegods.online	https://norsegods.online/owa/	"norsegods.online"	Professional Services Development	New
Aug 25, 2025, 10:05 PM	Aug 25, 2025, 10:05 PM	11617285@norsegods.online	https://quantumsecure.io/LoginPoint/	"norsegods.online", "quantumsecure.io"	Professional Services Development	New
Aug 25, 2025, 10:05 PM	Aug 25, 2025, 10:05 PM	spkotputlibehror@norsegods.online	https://quantumsecure.io/owa/	"norsegods.online", "quantumsecure.io"	Professional Services Development	New
Aug 25, 2025, 10:05 PM	Aug 25, 2025, 10:05 PM	2402220d@norsegods.online	https://quantumsecure.io.anydesk.com	"norsegods.online", "quantumsecure.io.anydesk.com"	Professional Services Development	New
Aug 26, 2025, 10:05 PM	Aug 26, 2025, 10:05 PM	bhanudurganath.angam@norsegods.online	https://norsegods.online/LoginPoint/	"norsegods.online"	Professional Services Development	New
Aug 26, 2025, 10:05 PM	Aug 27, 2025, 02:32 AM	bhanudurganath.angam@norsegods.online	https://norsegods.online/LoginPoint/	"norsegods.online"	Professional Services Development	InProgress

Alert Overview -- Link to Portal

4 minutes ago

Identity	Password	Assessments	Exfiltration Date	Authorization URL	IP Address	Compromised Host OS	Compromised Host Name	Compromised Host OS Username	Malware Family
spkotputlibehror@norsegods.online	SPKTP#9636	"Technology", "Malware"	Aug 25, 2025, 02:00 AM	https://norsegods.online/owa/	47.15.104.138	Windows 11 Pro (10.0.26100) x64	DESKTOP-5G4DT8D	admin	LummaC2
bhanudurganath.angam@norsegods.online	bhanu3003	"Technology", "Malware"	Jul 16, 2025, 10:37 PM	https://norsegods.online/LoginPoint/	49.205.249.170	Windows 10 Pro (10.0.19045) x64	REYNA	Vishwanth Rao	LummaC2
11617285@norsegods.online	par.25.dsp.0715	"Technology", "Malware"	Aug 18, 2025, 07:40 PM	https://quantumsecure.io/LoginPoint/	79.50.217.158	Windows 11	UFFICIO	luigi	Vidar
2402220d@norsegods.online	Ve4%IDvbZt+H25	"Technology", "Malware"	Aug 24, 2025, 02:31 PM	https://quantumsecure.io.anydesk.com	116.87.100.74	Windows 11	RITHVIK	rithv	Vidar
spkotputlibehror@norsegods.online	SPKTP#9636	"Technology", "Malware"	Aug 25, 2025, 02:00 AM	https://quantumsecure.io/owa/	47.15.104.138	Windows 11 Pro (10.0.26100) x64	DESKTOP-5G4DT8D	admin	LummaC2
oliviaeman02@norsegods.online	M21392139m	"Malware"	Aug 26, 2025, 06:00 PM	https://acme.com	154.80.88.176		olivi		Unknown Stealer
cgcacrik@norsegods.online	Mureg165	"Malware"	Aug 20, 2025, 06:07 PM	https://norsegods.online/member.php	108.72.36.199	Windows 10 Home	DESKTOP-07PMHHP	Chris	Vidar
seckos71@norsegods.online	Andre@1945	"Malware"	Aug 01, 2025, 05:20 PM	https://quantumsecure.io/member.php	75.177.38.17	Windows 10 22H2 build 19045 (64 Bit)		steph	RhadamanthysVariant Stealer
jibertelli@norsegods.online	newyork71	"Malware"	Jul 30, 2025, 04:52 AM	https://quantumsecure.io/member.php	72.203.24.138	Windows 10 22H2 build 19045 (64 Bit)		Tristen	RhadamanthysVariant Stealer

Recorded Future - Novel identity Exposure

Recorded Future - Potential Logo Abuse Detection

This dashboard will provide value if you have access to the Recorded Future App since clicking on any row will link you directly to the screenshot taken from page that has your company logo on it.

Triggered Time	Malicious URL	Alert URL	Organisation - Owner
Mar 07, 2023, 10:08 AM	http://hardrockhotel.fr/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://2020tokyoolympic.com/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://shopping.center/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://ns12.mgtwzp.site/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	https://redirectings.info/Allgftcardgveaways?ts1=PIRSING	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://www.bankwezen.xyz/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	https://facebook.oia.bio/yb5hz	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://pma.dorue.site/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://myccconfidential.com/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://kidsparadise.org/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://appleorigin.com/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://ahfc.com.cn/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://saudiaramco.fr/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://vorweggeher.de/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://new.veranstaltungsummessebau.de/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development
Mar 07, 2023, 10:08 AM	http://secure2help-paypal.com/	https://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services Development

Recorded Future - Potential Logo Abuse Detection

Recorded Future - Third Party Risk

This dashboard shows the details of each third party risk alert that has been received.

Triggered Time	Updated Time	Company	Assessments	Company Criticality	Company Risk Score	Risk Rules	Owner Name	Status in Portal
Aug 24, 2023, 05:06 PM	Aug 13, 2025, 07:15 AM	IBM	"Security Incidents"	Medium	64	"Recent Reported Cyber Attack", "Recent Validated Cyber Attack", "R..."	Professional Services Development	InProgress
Aug 10, 2025, 08:36 AM	Aug 12, 2025, 06:10 PM	IBM	"Malicious Network Activity"	High	89	"Recent High-Impact Abuse of Company Infrastructure"	Professional Services Development	New
Aug 08, 2025, 05:25 PM	Aug 12, 2025, 05:14 PM	IBM	"Malicious Network Activity"	Medium	64	"Hosts Recently Communicating With C&C Server"	Professional Services Development	New

Recorded Future - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities

This single dashboard combines the Tech Stack - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities and the Global - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities alert rules, one for table. The alerts are sorted by Criticality Level and display the CVE that triggered the alert, the severity and a description. If the Description field is empty we have provided the nvd.com link.

Triggered Time	Vulnerability ID	Vulnerability Level	Vulnerability Description
Nov 29, 2022	CVE-2022-4135	Very Critical	Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page...
Oct 27, 2022	CVE-2022-42827	Very Critical	https://nvd.nist.gov/vuln/detail/CVE-2022-42827
Nov 09, 2022	CVE-2022-41091	Very Critical	https://nvd.nist.gov/vuln/detail/CVE-2022-41091
Nov 09, 2022	CVE-2022-41073	Very Critical	https://nvd.nist.gov/vuln/detail/CVE-2022-41073
Nov 29, 2022	CVE-2022-0698	Very Critical	Microweber version 1.3.1 allows an unauthenticated user to perform an account takeover via an XSS on the 'select-file' parameter.
Nov 09, 2022	CVE-2022-41128	Very Critical	https://nvd.nist.gov/vuln/detail/CVE-2022-41128

Vulnerability Risk, New Critical and Pre NVD Watch List Vulnerabilities

Supported Alerts

Recorded Future Intelligence Goals Library Alerts are supported and DSM mapped by default. For a complete list of supported alerts please refer to the [Appendix](#).

In order to parse custom alerts utilise the DSM Editor to map the custom alerts to a new QID. For more information please refer to [Mapping custom alerts using the DSM Editor](#).

Mapping custom alerts using the DSM Editor

1. Click on the **Log Activity** tab
2. Select one or more events that are shown as **Unknown**
3. From the **Actions** list select **DSM Editor**.

Original Filters:
Log Source Type is Recorded Future Alerts (Clear Filter)

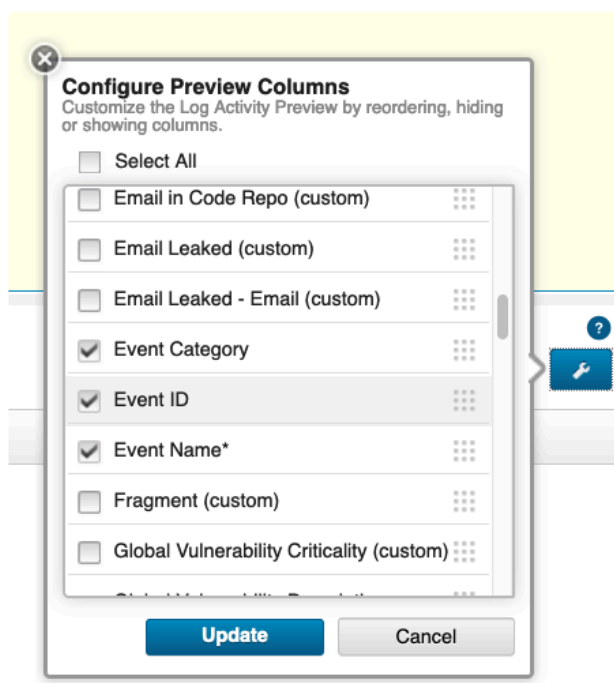
Current Filters:
Low Level Category is Unknown (Clear Filter)

Current Statistics

Total Results	115 (247.1KB Total)	Compressed Data Files Searched	Subsearch (No Compressed Data Files)	Duration	5ms
Data Files Searched	Subsearch (No Data Files)	Index File Count	Subsearch (No Index Files)	More Details	

	Event Name	Log Source	Event Count	Time	Low Level Category
	Unknown	Recorded Future Alerts	1	21 Nov 2022, 06:59:15	Unknown
	Unknown	Recorded Future Alerts	1	21 Nov 2022, 06:59:15	Unknown

4. Click on the **Settings** icon (bottom right hand side) and select the following fields: **Event Category, Event ID, Event Name, Low Level Category**.

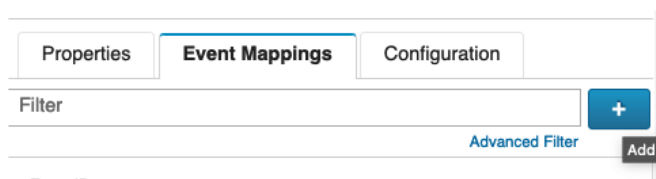


- Review the **Log Activity (Preview)** pane. The DSM will have Event Category and Event ID extracted and ready to go as shown below:

Log Activity Preview (Parsed but not Mapped:2/2)
A preview of the payloads in the Workspace as they would appear in the Log Activity viewer using the current configuration.

Event Category	Event ID	Event Name*	
rf_alert	Custom rule - Brand Mentions	Unknown	
rf_alert	Custom rule - Typosquatting	Unknown	

- Click on the **Event Mappings** tab
- Click on the blue plus icon “+”



- Select the corresponding Event Category and Event ID combination, for example:

Create a new Event Mapping

Enter an Event ID and Event Category combination to map to a QID record. A QID record allows a human-meaningful name and description to be associated with an event, as well as a Low Level Category and Severity value, which can in turn be used to trigger rules and building blocks.

Unknown Event Mappings

This table lists the Event ID/Event Category combinations that are parsed from events within the Workspace that do not currently have a corresponding Event Mapping. This table displays all Event Mappings that should be created for all events within the Workspace to parse successfully. Click on a row in this table to copy the Event ID and Event Category values into the corresponding text fields below.

Event ID	Event Category
Custom rule - Brand Mentions	rf_alert
Custom rule - Typosquatting	rf_alert

Event ID ⁱ

Custom rule - Brand Mentions

Event Category ⁱ

rf_alert

QID Record

[Choose QID...](#)

Create

Close

- Click **Choose QID...**
- Click **Create New QID Record**
- Provide the new QID record with the necessary information, such as name, description, high and low level categories, for example:

QID Records

Create New QID Record

Name	Log Source Type
Alert - Brand Mentions (custom)	Recorded Future Alerts
Description	High Level Category
This is a custom alert to track brand mentions on the dark web.	Suspicious Activity
	Low Level Category
	Suspicious Activity
	Severity
	3

Save [Go Back](#)

- Click **Save**
- Select the newly created QID and click **OK**
- Click **Create**

15. Click **Save**

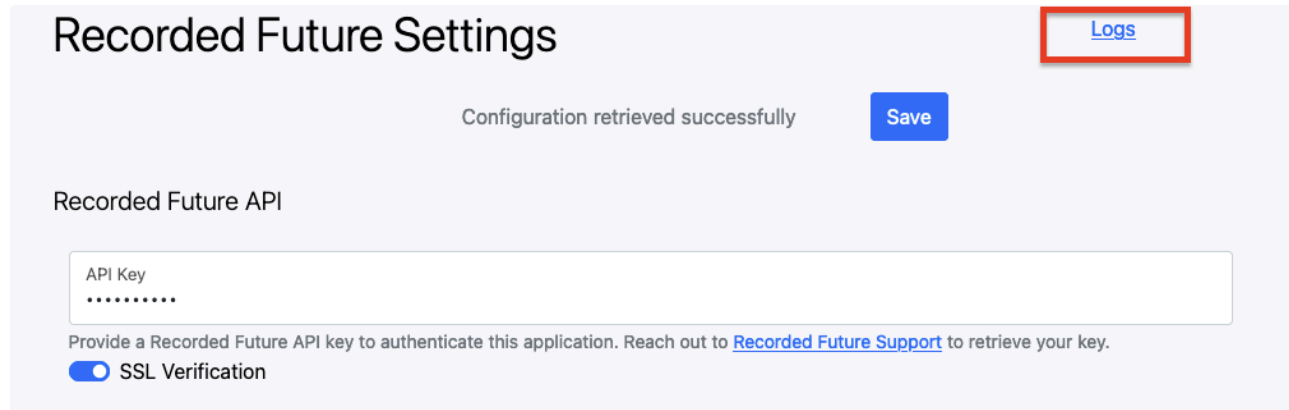
 To find out more about the DSM Editor, please visit [DSM Editor overview](#)

Logging & Troubleshooting

Please refer to the following URL for instructions on how to download QRadar Application logs.

<https://www.securitylearningacademy.com/course/view.php?id=4818>

Additionally, application logs are available in the application configuration page.



Syslog connection issues

Verify application container can reach the syslog destination via TCP 514.

1. Connect to the backend of QRadar console / App Node
2. Open a shell inside the application container

```
1 /opt/qradar/support/recon connect <app id>
```

3. Send a test syslog message

```
1 nc -w 0 <syslog destination ip> 514 <<< "Syslog-test-message"
```

4. On the QRadar Console run a payload search for **Syslog-test-message** and verify the test message is found.
5. If the the above steps fail, then verify network routing and firewall settings.

Logs indicate alerts were sent to QRadar, but search returns no alerts

After alert events have been sent to QRadar via Syslog the Event Pipeline in QRadar needs to process and store those events, this can take several minutes. Meaning that a search might not find the events that have been ingested a minute ago. Wait for a few minutes and try again.

Truncation of events

Not all Recorded Future alerts are equal and some are rather large and might get truncated by the QRadar event pipeline. Try increasing the **Max TCP Syslog Payload Length** from 12K to a larger value, but please do so careful and involve IBM QRadar Support if needed as increasing the size can have a negative impact on the performance of QRadar.

To increase the **Max TCP Syslog Payload Length**, click [here](#).

Reference: [QRadar: TCP and UDP Syslog Maximum Payload Message Length for QRadar Appliances](#)

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.

Appendix

Supported Classic Alert Rules

- Analyst-On-Demand Report
- Banking and Payments, Attackers in Banking & Payments Cyber Attacks
- Banking and Payments, Malware Used in Banking & Payments Cyber Attacks
- Banking and Payments, Banking Trojans, ATM Malware, Exploit Kits Malware
- Banking and Payments, Trending Targets in Banking & Payments
- Banking and Payments, Vulnerabilities Recently Related to Banking & Payments
- Brand name in suspicious websites content (OCR)
- Brand on Cyber-Focused Messaging Channels
- Brand Mentions with Cyber entities
- Company Email on Code Repository
- Credit Card Monitoring
- Cyber Espionage, RATs, Exploits, and Rootkits
- Cyber Espionage, Related Targets
- Cyber Espionage, Related Vulnerabilities
- Cyber Espionage, APT Threat Actors
- Cyber Events affecting my Brands
- Domains on Code Repositories
- Executive Impersonation on Social Media

- Executive Impersonation on professional networking website
- Exploit Kit Modification
- Gift Card Monitoring
- Global Third-Party Risk, Risk
- Global Third-Party Risk, Trend
- Global Trends, Trending Attackers
- Global Trends, Trending Operations
- Global Trends, Trending Vulnerabilities
- Global Trends, Trending Methods
- Global Trends, Trending Targets
- Global Vulnerability Risk, New Critical or Pre NVD Vulnerabilities
- Global Vulnerability Risk, Vendors and Products Mentioned with Vulnerabilities
- Global Vulnerability Risk, Vulnerabilities Recently Linked to Malware
- Global Vulnerability Risk, Vulnerabilities Recently Linked to Pentest Tools
- Global Vulnerability Risk, Vulnerabilities, New Exploit Chatter
- ICS/SCADA, ICS Malware, RATs
- ICS/SCADA, Trending Targets in ICS/SCADA
- ICS/SCADA, Vulnerabilities Related to ICS/SCADA Cyber Attacks
- ICS/SCADA, Attackers in ICS/SCADA Cyber Attacks
- ICS/SCADA, Malware Used in ICS/SCADA Cyber Attacks
- IP Address Mentions
- Identify Similar Domains
- Increased Domain Risk Score
- Increased IP Address Risk Score
- Industry Risk, Trending Attackers in Industry
- Industry Risk, Trending Companies in Industry
- Industry Risk, Trending Industry Peers in Watch List
- Industry Risk, Trending Methods in Industry
- Infrastructure and Brand Risk, Brand Names in Watch Lists
- Infrastructure and Brand Risk, Potential Typosquatting Watch List Domains
- Leaked Credential Monitoring
- Leaked Email Monitoring
- Mentions of Service Disruptions

- My brands on Dark Web and closed sources
- My domains on Dark Web and closed sources
- Phishing or Spam Campaigns (Phishing Related to Operations)
- Possible Fake Apps Detection
- Potential Logo Abuse Detection
- Ransomware, Software Recently Linked to Ransomware
- Ransomware, Vulnerabilities Recently Linked to Ransomware
- Target Trends, Trending Attackers Linked to Targets
- Target Trends, Trending Methods Linked to Targets
- Target Trends, Trending Operations Linked to Targets
- Target Trends, Trending Related Attackers
- Target Trends, Trending Targets in Watch List
- Third-Party Risk, Risk
- Third-Party Risk, Trend
- Trends, Trending Operations in Watch List
- Trends, Trending Watch List Attackers
- Trends, Trending Watch List Methods
- Trends, Trending Watch List Operations
- Trends, Trending Watch List Targets
- Trends, Trending Watch List Vulnerabilities
- Vulnerability Risk, Watch List Vendors & Products Mentioned with Vulnerabilities
- Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities
- Vulnerability Risk, Watch List Vulnerabilities Linked to Pentest Tools
- Vulnerability Risk, Watch List Vulnerabilities New Exploit Chatter
- Vulnerability Risk, Watch List Vulnerabilities Recently Linked to Malware
- Vulnerability Risk, Watch List Vulnerabilities with Proof of Concept code available

Supported Playbook Alert Rules

- Code Repository Leakage
- Cyber Vulnerability
- Domain Abuse
- Novel Identity Exposure
- Third Party Risk

Out-of-the-box Custom Event Properties (CEP)

- Affected Products
- Alert Category
- Alert ID
- Alert Priority
- Alert Rule Name
- Alert Seq
- Alert Seq Total
- Alert Source Name
- Alert Title
- Alert Triggered Time
- Alert URL
- Alert Updated Time
- Assessments
- Authorization URL
- Compromised Host Name
- Compromised Host OS
- Compromised Host OS Username
- DNS - A Record IP
- DNS - A Record IP Info
- DNS - A Record IP Risk Score
- DNS - NS
- Detected Technologies
- Domain Abuse Context
- Domain Code Repo
- Email Leaked
- Email Leaked - Email
- Email in Code Repo
- Entity Criticality
- Entity Subject
- Entity Risk Score
- Exfiltration Date
- Exposed Secret Clear Text Value

- Exposed Secret MD5
- Exposed Secret NTLM
- Exposed Secret Properties
- Exposed Secret SHA1
- Exposed Secret SHA256
- Exposed Secret Type Hint
- Exposed Secret Type
- Fragment
- Global Vulnerability Criticality
- Global Vulnerability Description
- Global Vulnerability ID
- Global Vulnerability Level
- Global Vulnerability Source URL
- Latest Screenshot
- Leaked Password
- Logo ID
- Logo URL
- MX - Domain
- MX - Domain Info
- MX - Domain Risk Score
- Malicious Infrastructure IP
- Malware Family Name
- Owner Name
- Repo Source Author
- Repo URL
- Repository Owner
- RF Organisation
- Similar Domain
- Status In Portal
- Targets List
- Vulnerability Lifecycle Stage
- Whois - City
- Whois - Country

- Whois - Name
- Whois - State