kaspersky

Importing Kaspersky Threat Data Feeds to RSA NetWitness

Product version: 1.0

kaspersky

Dear User,

Thank you for choosing Kaspersky Lab as your security software provider. We hope that this document helps you to use our product.

Document revision date: 09.09.2019

https://www.kaspersky.com
https://help.kaspersky.com
https://support.kaspersky.com

kaspersky

Contents

kaspersky

Introduction

Kaspersky Threat Data Feeds can be imported to RSA NetWitness. RSA NetWitness will match indicators contained in Kaspersky Threat Data Feeds to event fields that are in events received by RSA NetWitness. If a match is detected, RSA NetWitness will add context from the corresponding Kaspersky Threat Data Feeds record to an event.

You can import the following sets of Kaspersky Threat Data Feeds to RSA NetWitness:

- IP Reputation Data Feed—IP addresses with context covering spam hosts, malicious hosts, phishing hosts, Tor exit nodes, proxies, and botnet C&C servers.
- Botnet CnC URL Data Feed—URLs and hashes with context that refer to desktop botnet C&C servers and related malicious objects.
- Malicious URL Data Feed—URLs with context that refer to malicious websites and web pages.
- Phishing URL Data Feed—URLs with context that refer to phishing websites and web pages.
- Malicious Hash Data Feed—File hashes with corresponding context covering the most dangerous, prevalent, or emerging malware.
- P-SMS Trojan Data Feed—Trojan hashes with corresponding context for detecting SMS Trojans that send premium-rate SMS messages to mobile users as well as enable attackers to steal, delete, and respond to SMS messages.
- Mobile Botnet URL Data Feed—URLs with context that cover mobile botnet C&C servers.
- APT IP Data Feed—IP addresses that belong to the infrastructure used in APT campaigns.
- APT Hash Data Feed—Hashes that cover malicious artifacts used by APT actors to conduct APT campaigns
- APT URL Data Feed—Domains that belong to the infrastructure used in APT campaigns.
- Mobile Hash Data Feed—Hashes with context for detecting malicious objects that infect mobile Google Android and Apple iPhone devices.
- Ransomware URL Data Feed—URLs, domains, and hosts with context that cover ransomware links and websites.
- IoT URL Data Feed—URLs with context covering malicious links used to download malware that infects devices that are enabled for Internet of Things (IoT).
- Vulnerability Data Feed—File hashes with context that cover vulnerabilities in applications and cover exploits that use those vulnerabilities.

The process of importing Kaspersky Threat Data Feeds is done using Kaspersky Feed Utility and the `kl_feed_for_rsa` script. The feeds are downloaded and converted to a format that can be imported to RSA NetWitness.

You can also use Kaspersky CyberTrace to integrate Kaspersky Threat Data Feeds with RSA NetWitness. Kaspersky CyberTrace offers the following features:

- Kaspersky CyberTrace is flexible and can be easily integrated into an existing infrastructure, which allows you to avoid the challenges of integrating threat intelligence feeds with RSA NetWitness.
- Kaspersky CyberTrace does not hinder the performance of existing security controls and does not miss detections. The process of parsing and matching incoming data happens inside Kaspersky CyberTrace. This reduces the load on the existing SIEM solution.

- Kaspersky CyberTrace helps to reduce the frequency of false positives.

  For additional information about integrating Kaspersky Threat Data Feeds with RSA NetWitness, see https://support.kaspersky.com/13855.

kaspersky

Hardware and software requirements

This section describes the system requirements of Kaspersky Feed Utility and the `kl_feed_for_rsa` script.

Supported operating systems

Kaspersky Feed Utility runs on 64-bit Linux operating system.

Hardware requirements

Kaspersky Feed Utility requires 800 megabytes (MB) of hard disk space.

Software requirements

To run the `kl_feed_for_rsa` script, Python version 3.0 or later is required.

Software requirements for integration

When integrating with RSA NetWitness, Kaspersky Feed Utility requires RSA NetWitness version 11.2.

Network requirements

The computer on which Feed Utility runs must have access to the website https://wlinfo.kaspersky.com/. Use TCP port 443 as the destination port.

The computer where Kaspersky Feed Utility and the kl_feed_for_rsa script run must have an HTTP service installed. You can use any HTTP service that gives access to files using HTTP protocol.

RSA NetWitness sends requests to this HTTP service to download Kaspersky Threat Data Feeds.

kaspersky

Distribution kit contents

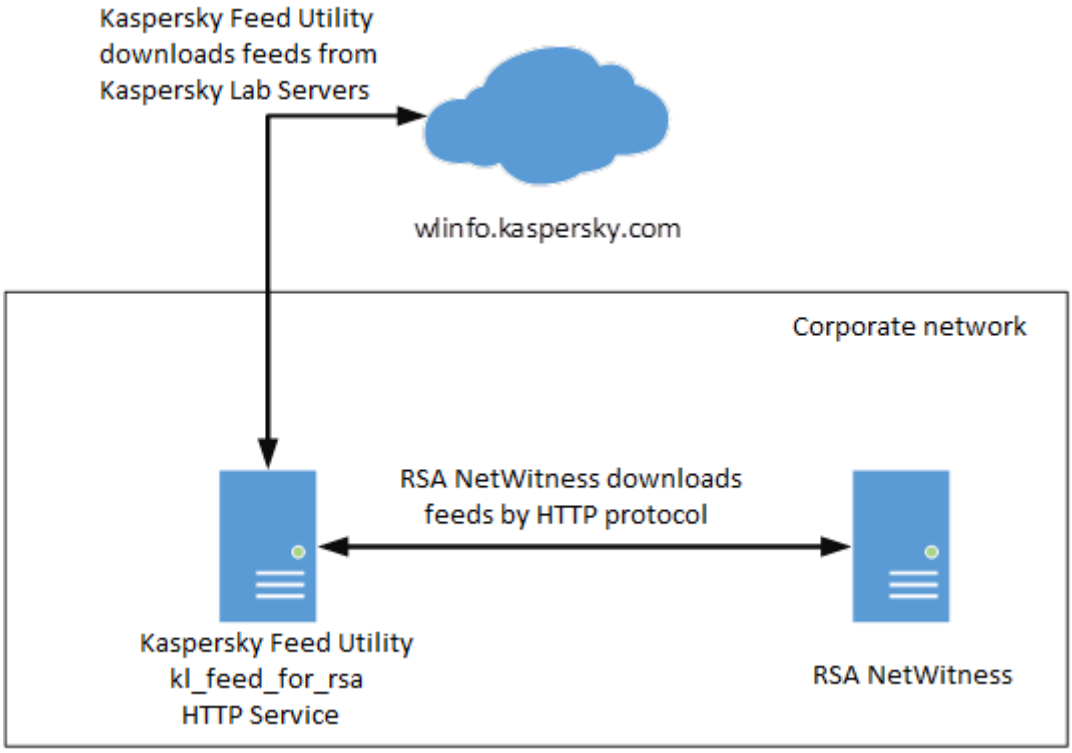
The table below describes the package contents.

File name	Comments
`bin/kl_feed_util`	Feed Utility binary file.
`bin/kl_feed_for_rsa.py`	Script for converting Kaspersky Threat Data Feeds to the format required by RSA NetWitness.
`bin/kl_feed_util.conf`	Kaspersky Feed Utility configuration file.
`bin/kl_feed_util.sh`	Script for the serial calling the `kl_feed_util` utility and the `kl_feed_for_rsa.py` script.
`doc/Kaspersky_Feed_Utility.html`	Kaspersky Feed Utility documentation.
`doc/license.txt`	End User License Agreement (EULA).
`doc/legal_notices.txt`	Information about third-party code.
`doc/Importing_Threat_Data_Feeds_to_RSA_Netwitness.pdf`	Instruction on how to integrate Kaspersky Threat Data Feeds with RSA NetWitness

Scenario: Feeds integration with RSA NetWitness

The scenario for integration of Kaspersky Threat Data Feeds with RSA NetWitness proceeds in stages:

1. Every 15 minutes, the `cron` utility runs Kaspersky Feed Utility.
2. Kaspersky Feed Utility downloads Kaspersky Threat Data Feeds from the wlinfo.kaspersky.com server.
3. The `kl_feed_for_rsa` script converts files (containing Kaspersky Threat Data Feeds indicators) that are to be imported to RSA NetWitness.
4. Every 30 minutes, RSA NetWitness sends an HTTP request to the computer on which Kaspersky Feed Utility runs, and downloads files containing indicators from Kaspersky Threat Data Feeds.



kaspersky

Configuring Kaspersky Feed Utility

This section explains how to configure Feed Utility for importing Kaspersky Threat Data Feeds.

► *To configure Kaspersky Feed Utility:*

1. On the computer that has the HTTP service, create the `/opt/kaspersky/feed_util` directory.
2. Unpack the archive containing Kaspersky Feed Utility and `kl_feed_for_rsa` to this directory.
3. Copy the certificate for downloading Kaspersky Threat Data Feeds to the `/opt/kaspersky/feed_util/`bin directory.

   Make sure that the certificate name is *feeds.pem*.
4. Open the `/opt/kaspersky/feed_util/bin/kl_feed_util.conf` configuration file.
5. Locate the `FeedsDir` element. In this element, specify the full path to a directory where the processed feeds will be stored.

   This directory must be located on the computer that has the HTTP service. RSA NetWitness will download feeds from this directory by using the HTTP protocol. Make sure that RSA NetWitness can access the contents of this directory by using HTTP.
6. Read and accept the End User License Agreements (EULA) by specifying the `accepted` value in the `EULA` element.

   Kaspersky Feed Utility runs only if the EULA is accepted.
7. In the `enabled` attribute of necessary feeds, specify `true`.

   > Do not enable demo feeds and commercial feeds at the same time.
8. In the `AddURLProtocol` element, specify 0 if the events received by RSA NetWitness are not contained the protocol in the URL field.
9. Save and close the `/opt/kaspersky/feed_util/bin/kl_feed_util.conf` configuration file.
10. If necessary, specify proxy settings for Kaspersky Feed Utility so that it has access to wlinfo.kaspersky.com.

    To specify the proxy settings, run the `kl_feed_util` file with the `–set-proxy username:password@host:port` parameter. Here, `username:password` is the user name and password for authentication on the proxy server (if necessary), and `host:port` constitutes the address and port of the proxy server.

    Example: `./kl_feed_util --set-proxy 'user:pass@proxy.example.com:3128'`
11. On the computer with the HTTP service, run the following commands to set up regular updating of Kaspersky Threat Data Feeds:

    ```
    crontab -l > /tmp/crontab_list
    ```

    ```
    echo "*/15 * * * * /opt/kaspersky/feed_util/bin/kl_feed_util.sh" >> /tmp/crontab_list
    ```

    ```
    crontab /tmp/crontab_list
    ```

    Kaspersky Threat Data Feeds will be updated every 15 minutes.

12. Run the `/opt/kaspersky/feed_util/bin/kl_feed_util.sh` script.

    If no errors occur, the following message will be printed to the console:

    ```
    [  OK  ]
    ```

Make sure that no errors occur during the feeds update and Kaspersky Threat Data feeds download. The feeds are downloaded to the directory specified in the `FeedsDir` element of the `kl_feed_util.conf` configuration file. If errors occur, they will be printed to the console.

Scenario: Importing Kaspersky Threat Data Feeds to RSA NetWitness

The scenario to import Kaspersky Threat Data Feeds to RSA NetWitness proceeds in stages:

1. Configuring RSA NetWitness (on page 11).
2. Adding Kaspersky Threat Data Feeds to RSA NetWitness (on page 15).
3. Specifying parsing rules for Kaspersky Threat Data Feeds (on page 17).

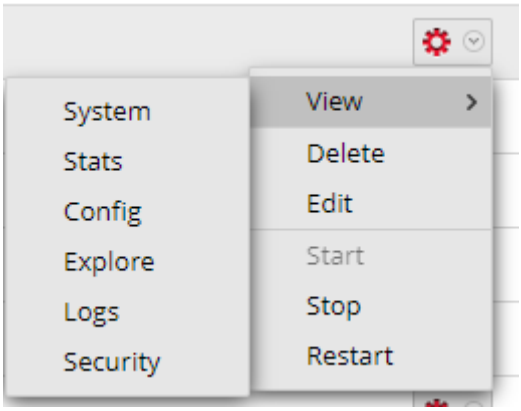
In this chapter

Configuring RSA NetWitness for downloading feeds

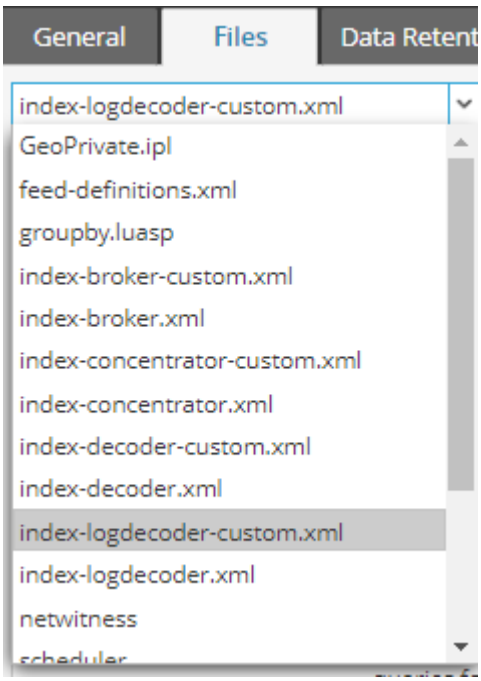
This section explains how to configure RSA NetWitness for downloading feeds.

► *To configure RSA NetWitness for downloading feeds:*

1. Open the **Admin/Services** page of the RSA NetWitness web interface.
2. In the Log Decoder actions, select **View > Config**.



3. On the **Files** tab, in the left drop-down list, select **index-logdecoder-custom.xml**.



4. In the input window, add the following after the line `<!-- *** Please insert your custom keys or modifications below this line *** -->`:

```
<!--Kaspersky Threat Data Feeds metafields-->

            <key description="Threat score of IP" format="Text"
level="IndexNone" name="kl.threat_score" defaultAction="Open"/>

            <key description="Top 100 ports through which attackers
downloaded malware from this resource" format="Text" level="IndexNone"
name="kl.ports" defaultAction="Open"/>

            <key description="Threat category" format="Text"
level="IndexNone" name="kl.category" defaultAction="Open"/>

            <key description="Threat level" format="Text"
level="IndexNone" name="kl.severity" defaultAction="Open"/>

            <key description="Date of first detect" format="Text"
level="IndexNone" name="kl.first_seen" defaultAction="Open"/>

            <key description="Date of last detect" format="Text"
level="IndexNone" name="kl.last_seen" defaultAction="Open"/>

            <key description="Index of popularity" format="Text"
level="IndexNone" name="kl.popularity" defaultAction="Open"/>

            <key description="Threat name" format="Text"
level="IndexNone" name="kl.threat" defaultAction="Open"/>

            <key description="Behaviour of threat" format="Text"
level="IndexNone" name="kl.behaviour" defaultAction="Open"/>

            <key description="Associated url" format="Text"
level="IndexNone" name="kl.mask" defaultAction="Open"/>
```

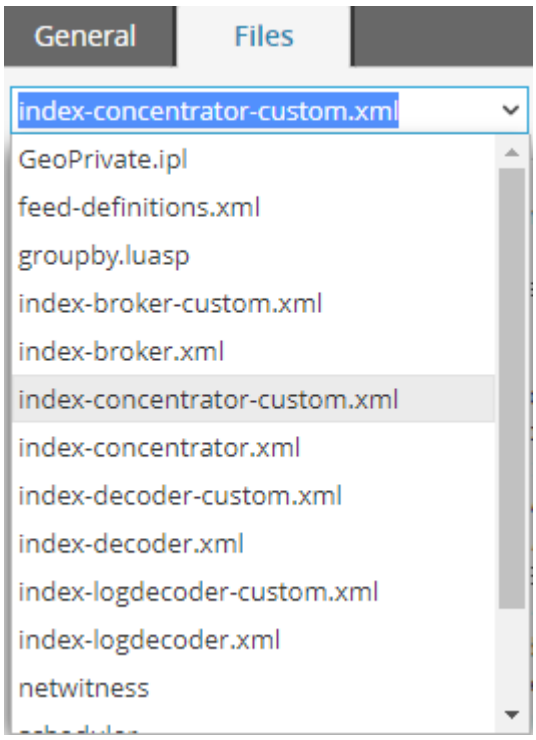
```
            <key description="The category of organization the attack
is aimed at" format="Text" level="IndexNone" name="kl.industry"
defaultAction="Open"/>

            <key description="The name of the attack to which the file
belongs." format="Text" level="IndexNone" name="kl.pub_name"
defaultAction="Open"/>

            <key description="Name of Kaspersky Threat Data Feed"
format="Text" level="IndexNone" name="kl.feed_name"
defaultAction="Open"/>

<!-- END -->
```

5. Click **Apply**.
6. Open the **Admin/Services** page.
7. In the Concentrator actions, select **View > Config**.
8. In the **Files** drop-down list, select **index-concentrator-custom.xml**.



9. In the input window, add the following after the line `<!-- *** Please insert your custom keys or modifications below this line *** -->`:

```
<!--Kaspersky Threat Data Feeds metafields-->

            <key description="Threat score of IP" format="Text"
level="IndexValues" name="kl.threat_score" valueMax="0"
defaultAction="Open"/>

            <key description="Top 100 ports through which attackers
downloaded malware from this resource" format="Text" level="IndexNone"
name="kl.ports" valueMax="0" defaultAction="Open"/>
```

```
            <key description="Threat category" format="Text"
level="IndexValues" name="kl.category" valueMax="0"
defaultAction="Open"/>

            <key description="Threat level" format="Text"
level="IndexValues" name="kl.severity" valueMax="0"
defaultAction="Open"/>

            <key description="Date of first detect" format="Text"
level="IndexNone" name="kl.first_seen" valueMax="0"
defaultAction="Open"/>

            <key description="Date of last detect" format="Text"
level="IndexNone" name="kl.last_seen" valueMax="0"
defaultAction="Open"/>

            <key description="Index of popularity" format="Text"
level="IndexValues" name="kl.popularity" valueMax="0"
defaultAction="Open"/>

            <key description="Threat name" format="Text"
level="IndexValues" name="kl.threat" valueMax="0"
defaultAction="Open"/>

            <key description="Behaviour of threat" format="Text"
level="IndexNone" name="kl.behaviour" valueMax="0"
defaultAction="Open"/>

            <key description="Associated url" format="Text"
level="IndexValues" name="kl.mask" valueMax="0" defaultAction="Open"/>

            <key description="The category of organization the attack
is aimed at" format="Text" level="IndexNone" name="kl.industry"
valueMax="0" defaultAction="Open"/>

            <key description="The name of the attack to which the file
belongs." format="Text" level="IndexNone" name="kl.pub_name"
valueMax="0" defaultAction="Open"/>

            <key description="Name of Kaspersky Threat Data Feed"
format="Text" level="IndexValues" name="kl.feed_name" valueMax="0"
defaultAction="Open"/>

<!-- END -->
```

10. Click **Apply**.
11. Open the **Admin/Services** page.
12. In the Concentrator and Log Decoder actions, click **Restart** and accept the service restart.

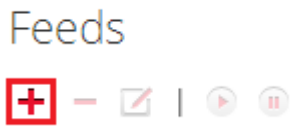
During a restart of Log Decoder, RSA NetWitness does not receive event sources data.

Adding Kaspersky Threat Data Feeds to RSA NetWitness

This section explains how to add Kaspersky Threat Data Feeds to RSA NetWitness.

► *To add Kaspersky Threat Data Feeds to RSA NetWitness:*

1. Open the **Configure/Custom Feeds** page.
2. Click the **+** button to add a new feed.



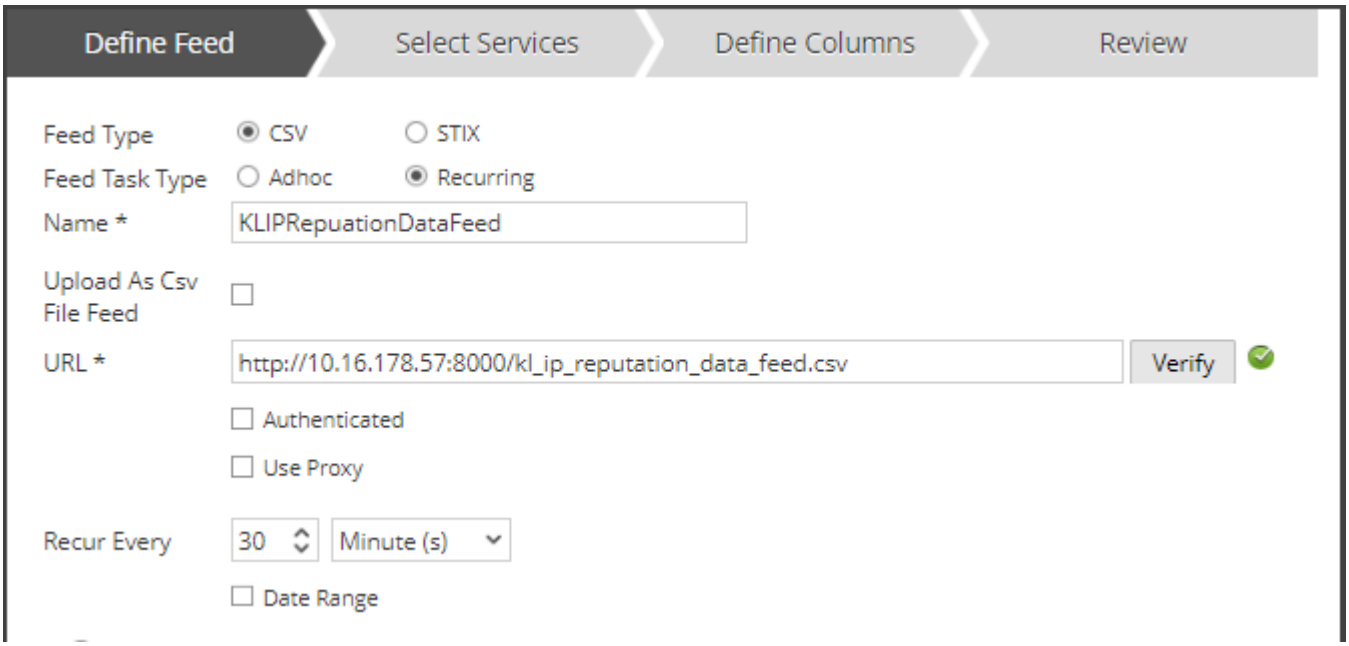
3. Select **Custom Feed**.
4. Click **Next**.
5. On the **Define Feed** page, perform the following:
   a) In the **Feed Type** field, specify the `CSV` value.
   b) In the **Feed Task Type** field, specify the `Recurring` value.
   c) In the **Name** field, specify the name of the feed that you want to add.

      In the **Name** field, you can specify only Latin letters. Punctuation marks are not allowed.

   d) In the **URL** field, specify the URL address of the feed that you add. For example, http://10.16.178.57:8000/kl_ip_reputation_data_feed.csv.
   e) If you add a feed with a URL, select **Define Upload As Csv File**.

      It is recommended to click the **Verify** button to make sure that RSA NetWitness has access to the feed.

f) In the **Recur Every** field, specify `30 Minutes`.

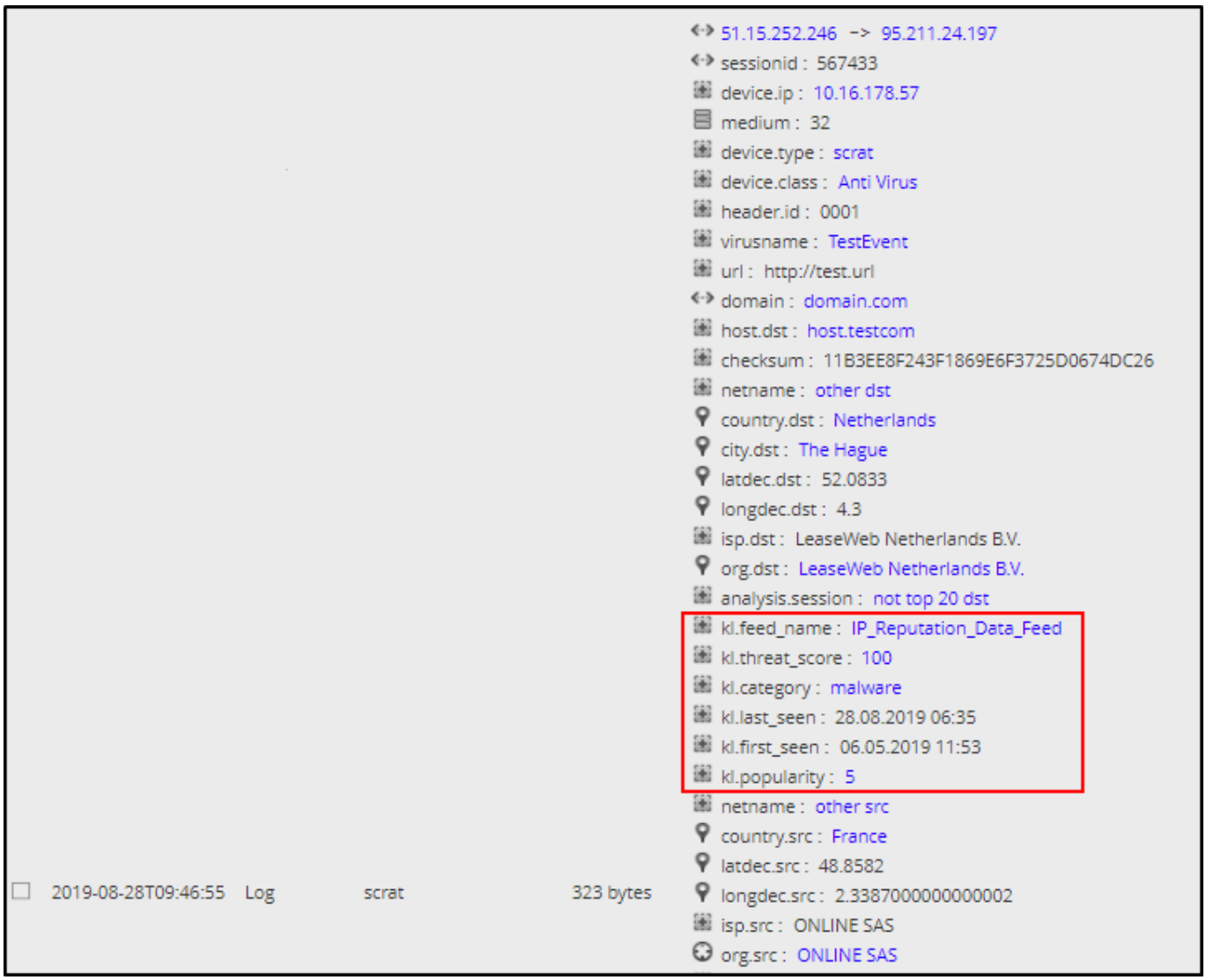


g) Click **Next**.

6. On the **Select Services** page, specify a Log Decoder that must use the downloaded feed to match with events received by this decoder.
7. Click **Next**.
8. On the **Define Columns** page, specify parsing settings for Kaspersky Threat Data Feeds in RSA NetWitness (for more information, see page 17).
9. Click **Next**.
10. On the **Review** page, check that all specified settings are correct.
11. Click **Finish** if all specified settings are correct.

    If the feed is added successfully, this feed is given the **Completed** status on the **Configure/Custom Feeds** page.

After the actions above are performed, Log Decoder will match the fields from the received events with indicators from the downloaded feed. If a match is detected, the context from the Kaspersky Threat Data Feed record with matching indicator will be added to the event:



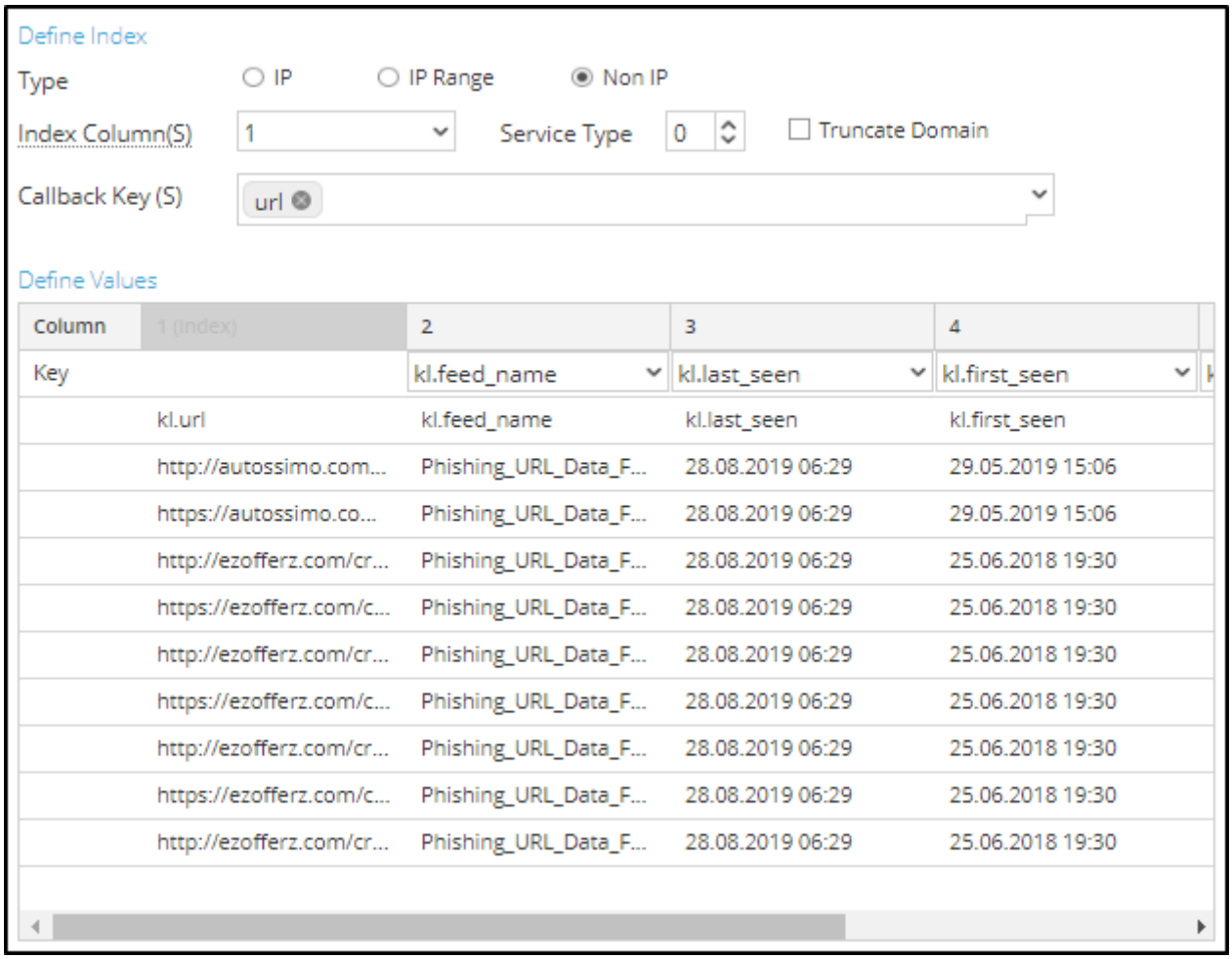
Specifying parsing rules for Kaspersky Threat Data Feeds

Each feed must be imported to RSA NetWitness using the settings below.

For feeds that contain the URL of malicious feeds (**kl_malicious_url_data_feed.csv, kl_botnetcnc_url_data_feed.csv, kl_phishing_url_data_feed.csv, kl_mobile_botnet_url_data_feed.csv, kl_ransomware_url_data_feed.csv, kl_iot_url_data_feed.csv**), the following are required:

- The **Type** field must contain the `Non IP` value.
- The **Index Column** field must contain the `1` value.
- The **Service Type** field must contain the `0` value.
- The **Truncate Domain** field must contain the `not checked` value.

- The **Callback Key(s)** field must contain all of the RSA NetWitness fields, which can include URLs (for example, the **url** field).
- The **Define Values** table must contain metafields that have names similar to the names of the feed fields:



> If the drop-down list of the **Define Values** table does not contain a value similar to the date field in the feed, select the `kl.first_seen` value.

For feeds that contain malicious domains (**kl_malicious_url_data_feed_domain.csv, kl_botnetcnc_url_data_feed_domain.csv, kl_phishing_url_data_feed_domain.csv, kl_mobile_botnet_url_data_feed_domain.csv, kl_apt_url_data_feed_domain.csv, kl_ransomware_url_data_feed_domain.csv**), the following is required:

- The **Type** field must contain the `Non IP` value.
- The **Index Column** field must contain the `1` value.
- The **Service Type** field must contain the `0` value.
- The **Truncate Domain** field must contain the `checked` value.

- The **Callback Key(s)** field must contain all of the RSA NetWitness fields, which can include domains (for example, the **domain** and **domain.dst** field).
- The **Define Values** table must contain metafields that have names similar to the names of the feed fields.

For feeds that contain malicious hosts (**kl_malicious_url_data_feed_host.csv, kl_botnetcnc_url_data_feed_host.csv, kl_phishing_url_data_feed_host.csv, kl_mobile_botnet_url_data_feed_host.csv, kl_ransomware_url_data_feed_host.csv, kl_apt_url_data_feed_host.csv**), the following is required:

- The **Type** field must contain the `Non IP` value.
- The **Index Column** field must contain the `1` value.
- The **Service Type** field must contain the `0` value.
- The **Truncate Domain** field must contain the `not checked` value.
- The **Callback Key(s)** field must contain all of the RSA NetWitness fields, which can include hosts (for example, the **host.dst** and **host.src** fields).
- The **Define Values** table must contain metafields that have names similar to the names of the feed fields.

For feeds that contain malicious hashes (**kl_botnetcnc_url_data_feed_checksum.csv, kl_ip_reputation_data_feed_checksum.csv, kl_malicious_hash_data_feed.csv, kl_psms_trojan_data_feed.csv, kl_mobile_botnet_url_data_feed_checksum.csv, kl_apt_hash_data_feed.csv, kl_mobile_botnet_data_feed.csv, kl_ransomware_url_data_feed_checksum.csv, kl_iot_url_data_feed_checksum.csv, kl_vulnerability_data_feed_vuln.csv, kl_vulnerability_data_feed_exploits.csv, kl_malicious_url_data_feed_checksum.csv**), the following are required:

- The **Type** field must contain the `Non IP` value.
- The **Index Column** field must contain the `1` value.
- The **Service Type** field must contain the `0` value.
- The **Truncate Domain** field must contain the `not checked` value.
- The **Callback Key(s)** field must contain all of the RSA NetWitness fields, which can include hashes (for example, the **checksum** field).
- The **Define Values** table must contain metafields that have names similar to the names of the feed fields.

For feeds that contain IPs (**kl_ip_reputation_data_feed.csv, kl_apt_ip_data_feed.csv**), the following is required:

- The **Type** field must contain the `IP` value.
- The **Index Column** field must contain the `1` value.
- The **CIDR** field must contain the `not checked` value.
- The **Define Values** table must contain metafields that have names similar to the names of the feed fields.

kaspersky

Configuring the updating of Kaspersky Threat Data Feeds in RSA NetWitness

This section describes the pre-defined settings for the Kaspersky Threat Data Feeds updating in RSA NetWitness.

The following settings are available:

- A set of fields that is specified in the `RequiredFields` element and is downloaded to RSA NetWitness from the feeds.
- Filters that apply to the feeds.

By default, the first 100 000 records with the most popular indicators are downloaded, keeping the RSA NetWitness performance rate and detection rate in balance:

Feeds	Set of fields	Filters

Malicious URL Exact Data Feed	`urls/url`
	`domains/domain`
	`hosts/host`
	`popularity`
	`last_seen`
	`first_seen`
	`category`
	`files/MD5`
	`files/SHA1`
	`files/SHA256`
	`files/threat`
		First 100 000 records.

BotnetCnC URL Exact Data Feed	`urls/url`
	`domains/domain`
	`hosts/host`
	`popularity`
	`last_seen`
	`first_seen`
	`threat`
	`files/MD5`
	`files/SHA1`
	`files/SHA256`
		First 100 000 records.

Demo BotnetCnC URL Data Feed	mask type popularity last_seen first_seen threat files/MD5 files/SHA1 files/SHA256	First 100 000 records.
Phishing URL Exact Data Feed	urls/url domains/domain hosts/host last_seen first_seen popularity industry	First 100 000 records.
IP Reputation Data Feed Demo IP Reputation Data Feed	ip threat_score category last_seen first_seen popularity files/MD5 files/SHA1 files/SHA256 files/threat	Records with a threat_score value greater than 75.
Malicious Hash Data Feed Demo Malicious Hash Data Feed	md5 sha1 sha256 last_seen first_seen popularity threat	First 100 000 records.
P-SMS Trojan Data Feed	MD5 Date AV Verdict	First 100 000 records.

Mobile Botnet URL Data Feed	mask type files/MD5 files/SHA1 files/SHA256 threat popularity last_seen first_seen files/Behaviour	First 100 000 records.
APT IP Data Feed	ip detection_date publication_name	First 100 000 records.
APT Hash Data Feed	MD5 detection_date publication_name	First 100 000 records.
APT URL Data Feed	mask type detection_date publication_name	First 100 000 records.
Mobile Malicious Hash Feed	md5 sha1 sha256 last_seen first_seen popularity threat	First 100 000 records.
Ransomware URL Data Feed	mask type last_seen first_seen popularity files/MD5 files/SHA1 files/SHA256 files/threat	First 100 000 records.

IoT URL Data Feed	mask type last_seen first_seen port popularity files/MD5 files/SHA1 files/SHA256 files/threat	First 100 000 records.
Vulnerability Data Feed	detection_date severity vulnerable_files/md5 vulnerable_files/sha1 vulnerable_files/sha256 exploits/md5 exploits/sha1 exploits/sha256 exploits/threat	First 100 000 records.

kaspersky

Adding and removing context fields

All of the fields, which are imported from Kaspersky Threat Data Feeds to RSA NetWitness, are specified in the `RequiredFields` element of the `kl_feed_util.conf` configuration file. You can add fields to this element and remove fields from this element. The fields below cannot be removed, because all of these contain matching indicators:

- `type`—For the Ransomware URL, Mobile Botnet URL, Demo BotnetCnC URL, APT URL, IoT URL feeds
- `mask`—For the Ransomware, Mobile BotnetC&C , Demo BotnetC&C URL, BotnetC&C URL, APT, IoT URL feeds
- `MD5`
- `ip`

If the fields is removed from / added to the `RequiredFields` element and the feed has been imported to RSA NetWitness, perform the following:

1. Open the **Configure/Custom Feeds** page in RSA NetWitness.
2. Open the feed settings.
3. On the **Define Columns** page, update the settings. If the added field is not needed to search in RSA NetWitness, specify the name of this field in the **Define Values** table.

If the field is added to the `RequiredFields` element, and this field is not included in the list from step 4 of the procedure to configure RSA NetWitness for downloading feeds (see page 11), and you also want to search values from this field in RSA NetWitness, perform the following:

1. Open the **Admin/Services** page of the RSA NetWitness web interface.
2. In the Log Decoder actions, select **View > Config**.
3. In the **Files** drop-down list, select **index-logdecoder-custom.xml**.
4. In the input window, add the following after the line `<!--Kaspersky Threat Data Feeds metafields-->`:

   `<key description="%DESCRIPTION%" format="Text" level="IndexNone" name="kl.%FIELD_NAME%" defaultAction="Open"/>`, where `%DESCRIPTION%` is a brief description of the field, and `%FIELD_NAME%` is a field name (the maximum number of characters is 13).
5. Click **Apply**.
6. Open the **Admin/Services** page.
7. In the Concentrator actions, select **View > Config**.
8. In the **Files** drop-down list, select **index-concentrator-custom.xml**.

   In the input window, add the following after the line `<!--Kaspersky Threat Data Feeds metafields-->`

   `<key description="%DESCRIPTION%" format="Text" level="IndexValues" name="kl.%FIELD_NAME%" defaultAction="Open"/>`

   where `%DESCRIPTION%` is a brief description of the field, and `%FIELD_NAME%` is a field name (the maximum number of characters is 13).
9. Click **Apply**.

10. Open the **Admin/Services** page.
11. In the Concentrator and LogDecoder actions, click **Restart** and accept the service restart. Note that while LogDecoder restarts, RSA NetWitness does not receive event sources data.

kaspersky

The kl_feed_for_rsa script

The `kl_feed_for_rsa` script performs the following:

1. Processes Kaspersky Threat Data Feeds, which are located in the directory that is specified in the `FeedsDir` element of the `kl_feed_util.conf` configuration file. The configuration file has to be located in the same directory with the `kl_feed_for_rsa` script.
2. Makes CSV files with Kaspersky Threat Data Feeds contents.
3. Saves these CSV files to the directory, which is specified in the `FeedsDir` element of the `kl_feed_util.conf` configuration file.

kaspersky

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against digital threats, including viruses and other malware, unsolicited email (spam), and network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky Lab was founded in Russia in 1997. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3,000 skilled professionals.

Products. Kaspersky Lab products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with centralized management tools, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky Lab products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky Lab virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include their signatures in databases used by Kaspersky Lab applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus engine in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website:	https://www.kaspersky.com
Virus encyclopedia:	https://securelist.com
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab Community:	https://community.kaspersky.com