RSA® NETWITNESS®
Intel Feeds Implementation Guide

Kaspersky Threat Intelligence Portal – Threat Lookup

Jeffrey Carlson, RSA Partner Engineering
Last Modified: August 15th, 2017

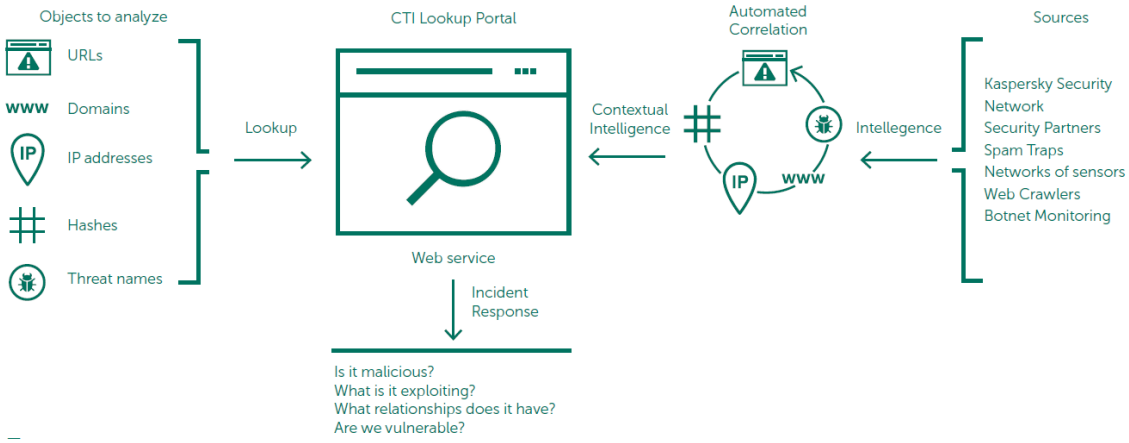
RSA READY

Solution Summary

Cybercrime today knows no borders, and technical capabilities of attackers are improving fast. We are seeing attacks becoming increasingly sophisticated as cybercriminals use dark web resources to threaten their targets. Cyber-threats are constantly growing in frequency, complexity and obfuscation, as new attempts are made to compromise your defenses. Attackers are using complicated kill chains and customized Tactics, Techniques and Procedures (TTPs) in their campaigns to disrupt your business, steal your assets, or cause damage to your clients.

Access to Kaspersky Threat Lookup provides reliable, immediate intelligence about cyber-threats, legitimate objects, and their inter-connections. You also gain access to indicators, enriched with actionable context to inform your business or clients about the associated risks and implications. Now you can mitigate threats and respond to them more effectively, defending against attacks even before they are launched.

Kaspersky Threat Lookup delivers all knowledge acquired by Kaspersky Lab about cyber-threats and their relationships, brought together into a single powerful web service. The goal is to give your security teams as much data as possible, preventing cyber-attacks before they impact your organization. Kaspersky Threat Lookup provides the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical and behavior data, and WHOIS/DNS data. The result is global visibility of new and emerging threats helping you secure your organization and boosting incident response.



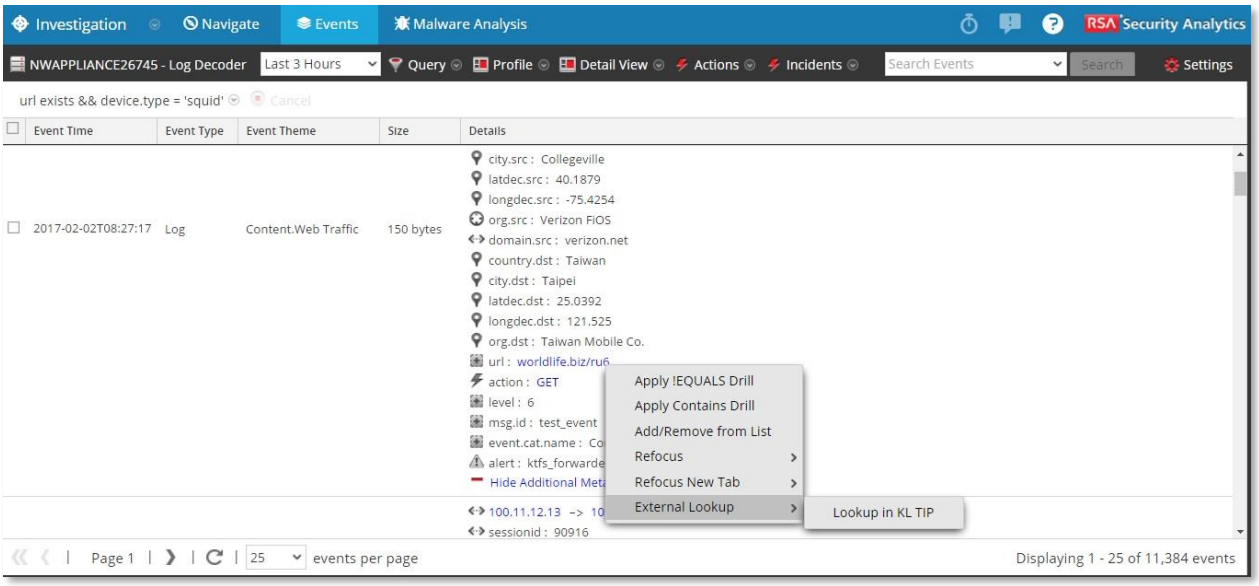
To help you quickly determine whether an object under investigation is dangerous or clean, Kaspersky Lab provides functionality to perform lookup for URLs, IP addresses, and hashes using Kaspersky Threat Intelligence Portal directly from RSA NetWitness interface. For each investigated object, Kaspersky Threat Intelligence Portal also provides a rich set of contextual data to answer the who, what, where, and when questions in order to assist you in making timely decisions and actions.

RSA NetWitness Configuration

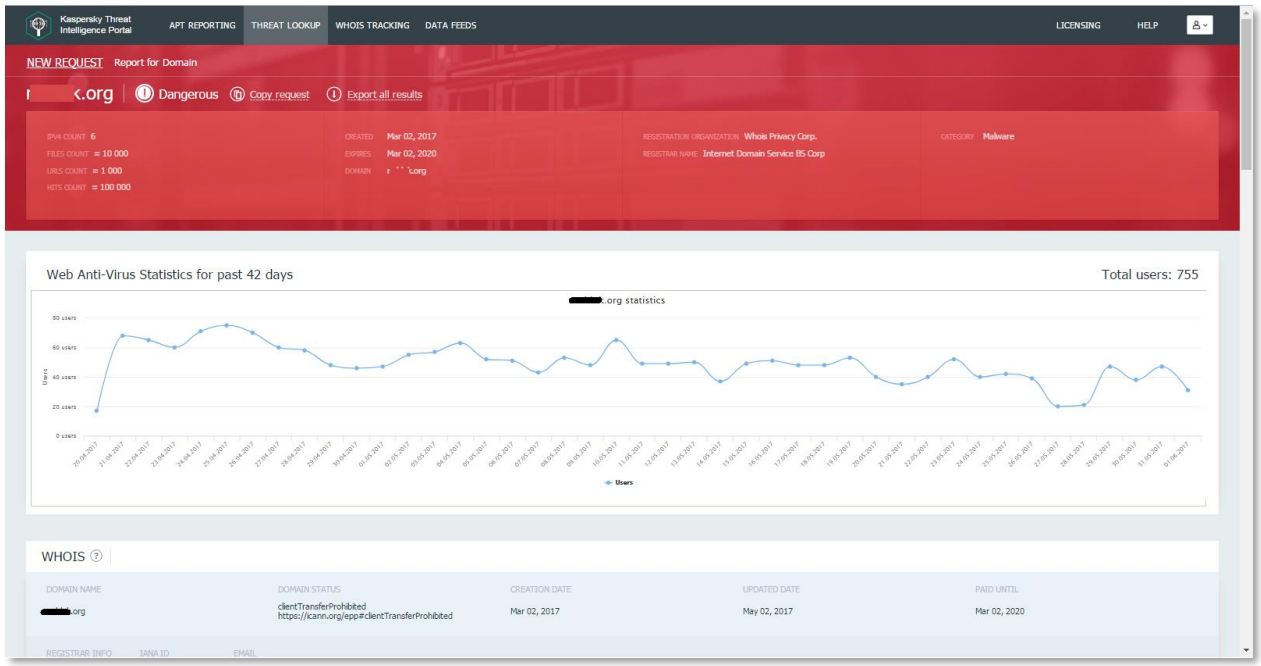
Adding a Context Menu Action for Kaspersky Threat Feed Service

In the Context Menu Actions panel of RSA NetWitness, administrators can view, add, and edit context menu actions for the current instance of NetWitness. Each context menu action applies to a specific context in the NetWitness user interface and appears as an option when you right-click a specific location in the user interface.

After a context menu action for Kaspersky Threat Feed Service is added to RSA NetWitness, users can select any indicator (IP address, URL, or hash) of any event and right-click it to perform lookup in Threat Intelligence Portal, as it is shown in the figure below.

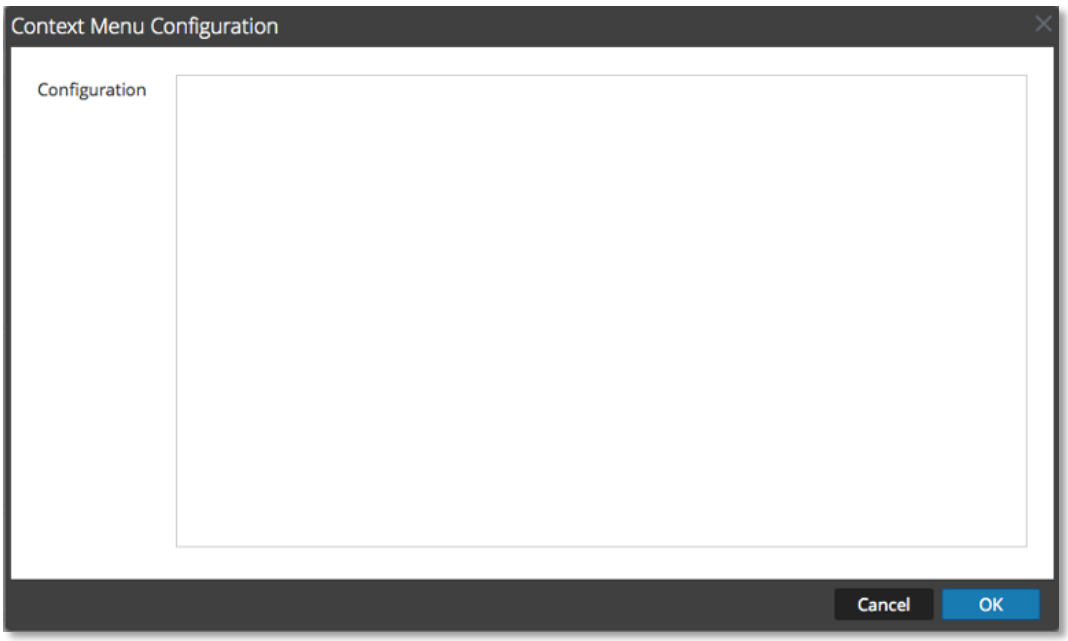


A new window will be opened in the default browser. This window will contain a lookup result for the requested indicator within the Kaspersky Threat Intelligence Portal interface:

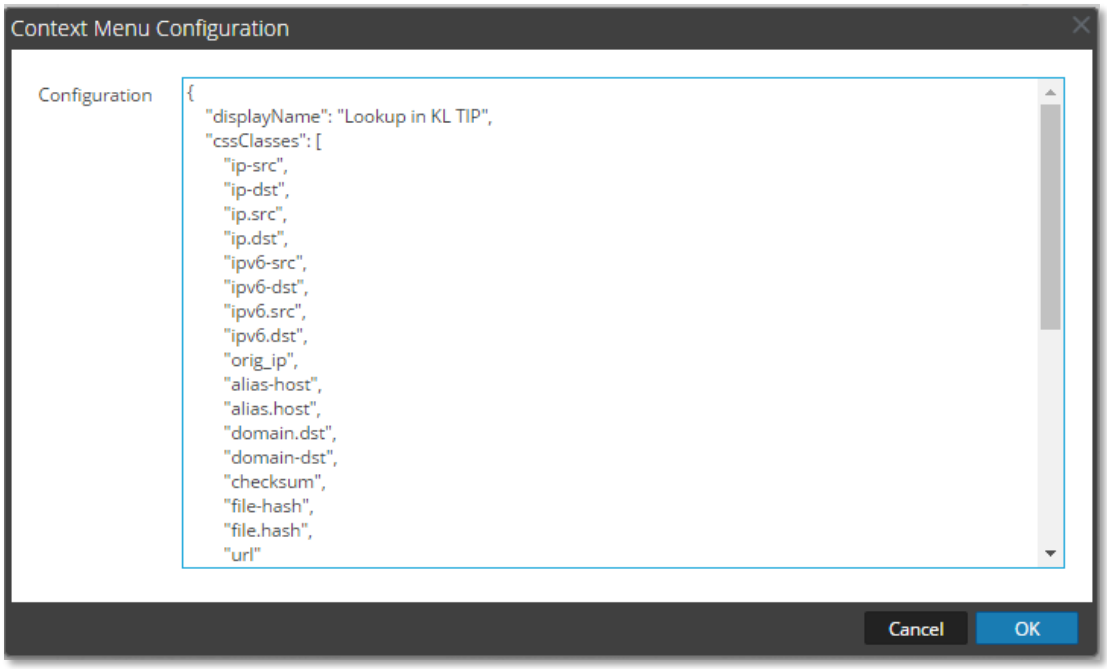


To add this context menu action in RSA NetWitness, perform the following steps:

1. In the NetWitness menu, select **Administration > System**.
2. In the options panel, select **Context Menu Actions**.
3. In the toolbar, click the **Add** button (+).
4. The **Context Menu Configuration** dialog is displayed.



5. Enter the CSS code prepared by Kaspersky Lab. This code defines the context menu action (see Appendix).

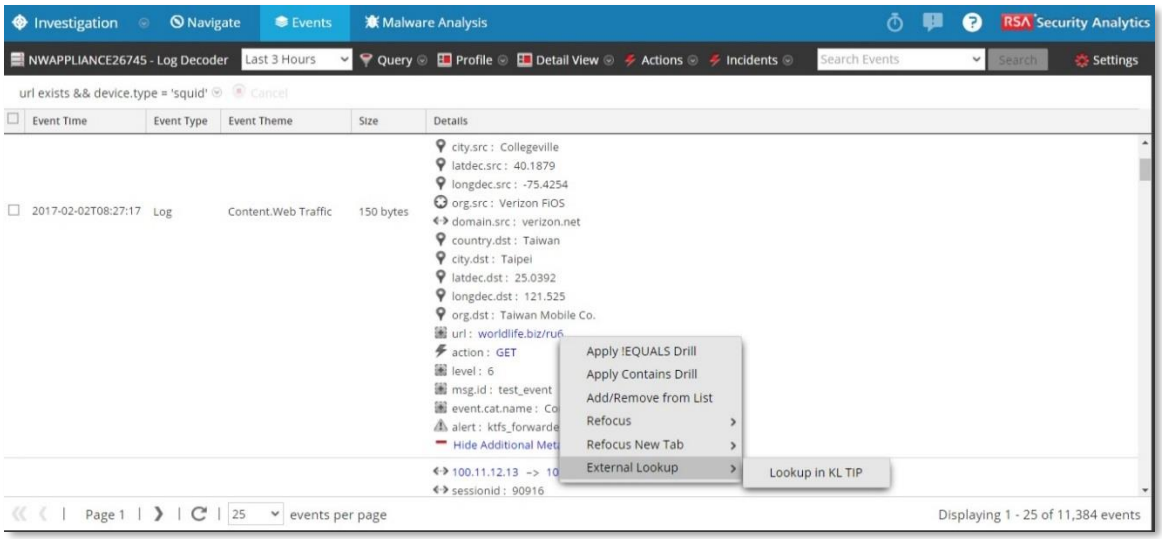


6. Click **OK**.

   The new context menu action is created and added to the end of the list of context menu actions.

7. To activate the new context menu action, reload the RSA page in the browser.

   The context menu action becomes available in the form with events.



Important: Please contact Kaspersky Cybersecurity Service team (intelligence@kaspersky.com) to request a certificate. This certificate must be imported to a browser that is used for working with RSA NetWitness.

Appendix A

```
{
    "displayName": "Lookup in KL TIP",
    "cssClasses": [
        "ip-src",
        "ip-dst",
        "ip.src",
        "ip.dst",
        "ipv6-src",
        "ipv6-dst",
        "ipv6.src",
        "ipv6.dst",
        "orig_ip",
        "alias-host",
        "alias.host",
        "domain.dst",
        "domain-dst",
        "checksum",
        "file-hash",
        "file.hash",
        "url"
    ],
    "description": "Lookup in KL TIP",
    "type": "UAP.common.contextmenu.actions.URLContextAction",
    "version": "1",
    "modules": [
        "investigation"
    ],
    "local": "false",
    "groupName": "externalLookupGroup",
    "urlFormat": "https://tip.kaspersky.com/search?searchString={0}",
    "disabled": "",
    "id": "KL_TIP_Lookup",
    "moduleClasses": [
        "UAP.investigation.navigate.view.NavigationPanel",
        "UAP.investigation.events.view.EventGrid"
    ],
    "openInNewTab": "true",
    "order": "30"
}
```