Enterprise / MSSP / Law-enforcement

▶ INTELLIGENCE SERVICE: THREAT DATA FEEDS

Get more from your SIEM system with an additional layer of protection against malware and dangerous URLs by leveraging KL's comprehensive intelligence data.

Malware families and variations have grown exponentially in the last few years; Kaspersky Lab is currently detecting about 325,000 unique new malware samples every day. To defend their endpoints against these threats, most organizations deploy classical protection measures like anti-malware solutions, intrusion prevention or threat detection systems. In a fast-changing environment where cybersecurity is always trying to stay one step ahead of cybercrime, these classical solutions need to be reinforced with access to up-to-the-minute threat intelligence.

Kaspersky Lab's Threat Data Feeds are designed to integrate into existing Security Information and Event Management (SIEM) systems, providing an additional layer of protection. Integration makes it possible to correlate the logs coming to the SIEM from different network devices with the URL feeds from Kaspersky Lab. **A connection with HP ArcSight SIEM is included.**

USE CASES / SERVICE BENEFITS

- **Improves the SIEM solution by leveraging data about harmful URLs from Kaspersky Lab feeds.** The SIEM is notified about malware URLs, phishing URLs, Botnet C&C URLs from logs coming to the SIEM from different network devices (user PCs, network proxies, firewalls, other servers)
- **Research purposes.** Leveraging the information about harmful URLs and MD5 hashes of malicious files in research purposes

FEED DESCRIPTION

Kaspersky Lab offers two types of Threat Data Feeds:

1. Malicious URLs and masks
2. MD5 hashes of malicious objects database

FEED DESCRIPTION
Malicious URLs – a set of URLs covering the most harmful links and websites. Masked and non-masked records are available.
Phishing URLs – a set of URLs identified by Kaspersky Lab as phishing sites. Masked and non-masked records are available.
Botnet C&C URLs – a set of URLs of botnet command and control (C&C) servers and related malicious objects. Mobile C&Cs are included.
Malware Hashes (ITW) – a set of file hashes covering the most dangerous in-the-wild (ITW) malware encountered by Kaspersky Security Network users. The base contains hashes with Kaspersky verdicts for each object.
Malware Hashes (UDS) – a set of file hashes detected by Kaspersky cloud technologies (UDS - Urgent Detection System) based on a file's metadata and statistics (without having the object itself). This allows the system to identify malware that is not detected by other methods. This can also be described as "recently identified malware hashes"
Android Malware Hashes – a set of file hashes for detecting malicious objects that infect mobile Android platforms

WHY KASPERSKY LAB?

- Founded and led by the world's foremost security expert, Eugene Kaspersky
- Partnerships with global law enforcement agencies such as Interpol and CERTS
- Cloud-based tools monitoring millions of cyberthreats across the globe in real time
- Global teams analyzing and understanding Internet threats of all kinds
- World's largest independent security software company — focused on threat intelligence and technology leadership
- Undisputed leader in more independent malware detection tests than any other vendor
- Identified as a Leader by Gartner, Forrester and IDC

For more information on Kaspersky Intelligence Services, please contact us via intelligence@kaspersky.com.
TO LEARN MORE VISIT www.kaspersky.com.

KASPERSKY lab