

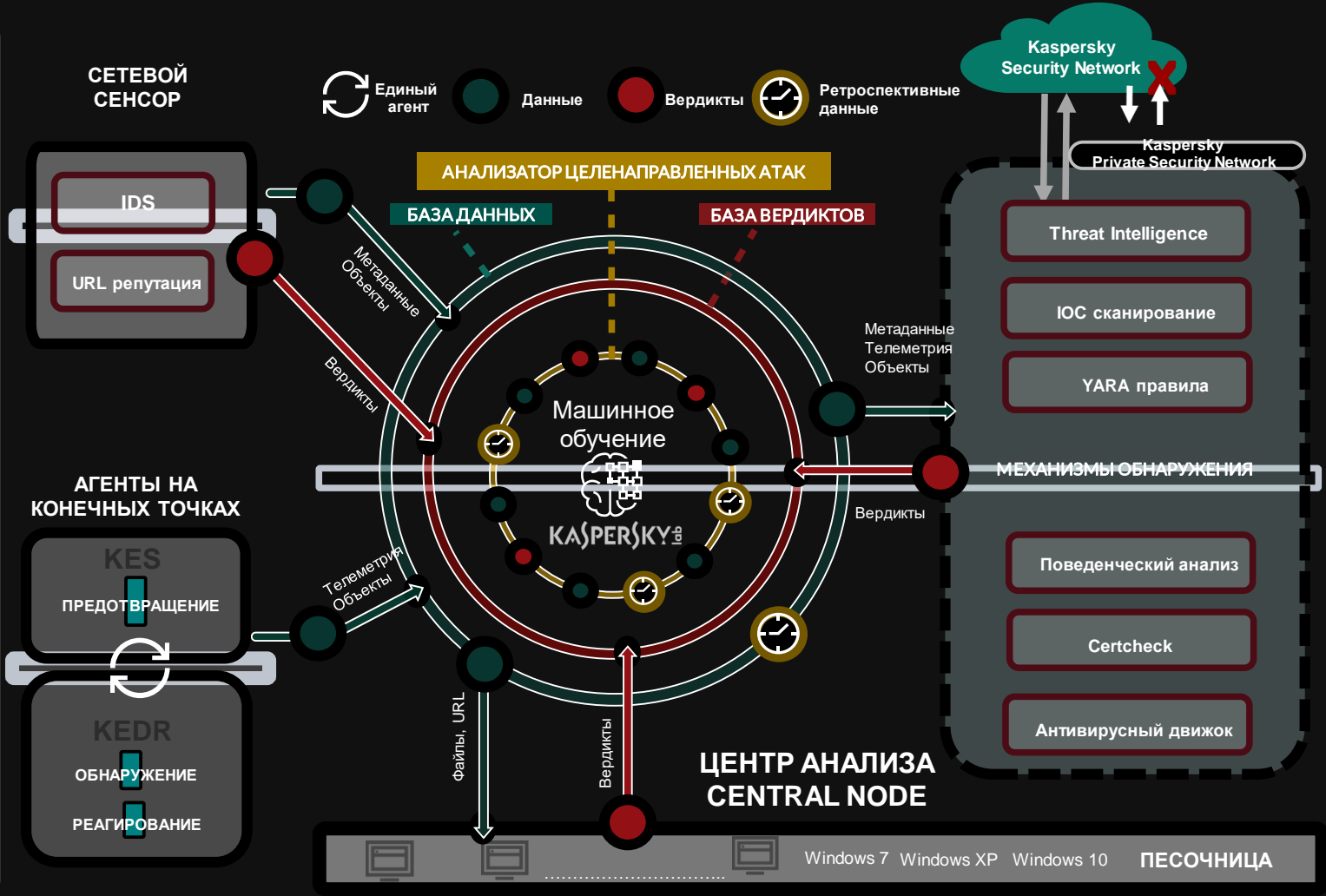
kaspersky

Путь Казановы, или как
живется киберследователю.



- IP
- Сеть
- Почта
- Веб
- Сервер
- PC
- Ноутбук

СБОР ДАННЫХ



Единый агент Данные Вердикты Ретроспективные данные

АНАЛИЗ ДАННЫХ И ОБНАРУЖЕНИЕ УГРОЗ

СЕГОДНЯ

АД ЧЕЛОВ
ДЯДЯ ВАНЯ

ЗАВТРА

Ваня СЕМЕНОВИЧ

ЛОВЕЛАС

Путь Казановы

A black and white photograph of Winston Churchill. He is wearing a dark top hat, a dark suit jacket, a white shirt, and a dark bow tie with a light-colored pattern. He is making a V-sign gesture with his right hand. The background is slightly blurred, showing other people in similar attire.

ЛЮДИ

ТЕХНОЛОГИИ



Jules Bonate
Kästner 1939

СТРОИМ САМИ?

3 БЕЗОПАСНИКА В ГОД + СОФТ - \$200К

СИЕМ - \$100К

ИТОГО: \$300К

И ВСЕ?

ХА! КАК БЫ НЕ ТАК!!!

Kaspersky Threat Data Feeds

Как скачать разъем SIEM для IBM QRadar

2019 фев 07 ID: 13854



проверить URL-адреса, хэши файлов и IP-адреса,



Kaspersky Industrial CyberSecurity for Networks Additional Sensor, Limited Updates

Base

1 year

KL49362A*FS

Threat Intelligence

Kaspersky Threat Data Feeds - Whitelisting	Base	1 year	KL79112A*FS	3 363 750,00
Kaspersky Threat Data Feeds - IP reputation & URL & Hash & Mobile Threat & Whitelisting	Base	1 year	KL79122A*FS	1 755 000,00
Kaspersky Threat Data Feeds - Ransomware URL	Base	1 year	KL79132A*FS	1 868 750,00
Kaspersky Threat Data Feeds - APT IOC	Base	1 year	KL79142A*FS	3 363 750,00
Kaspersky Threat Data Feeds - All In One	Base	1 year	KL79152A*FS	17 192 500,00
Kaspersky Threat Data Feeds - Malicious URL	Base	1 year	KL79612A*FS	1 270 750,00
Kaspersky Threat Data Feeds - URL	Base	1 year	KL79622A*FS	3 363 750,00
Kaspersky Threat Data Feeds - URL & Hash	Base	1 year	KL79632A*FS	5 980 000,00
Kaspersky Threat Data Feeds - Mobile Threat	Base	1 year	KL79642A*FS	2 242 500,00
Kaspersky Threat Data Feeds - IP reputation	Base	1 year	KL79672A*FS	3 363 750,00
Kaspersky Threat Data Feeds - Phishing URL	Base	1 year	KL79682A*FS	1 270 750,00
Kaspersky Threat Data Feeds - Botnet C&C URL	Base	1 year	KL79692A*FS	1 270 750,00
Kaspersky Threat Data Feeds - URL & Hash & Mobile Threat & IP Reputation	Base	1 year	KL79702A*FS	9 100 000,00
Kaspersky Threat Data Feeds - Transforms for Maltego XM/Classic	Base	1 year	KL79712A*FS	747 500,00
Kaspersky Threat Data Feeds - URL & Hash & Mobile Threat	Base	1 year	KL79752A*FS	7 475 000,00
Kaspersky Financial Threat Intelligence Reporting - Full Reports and IOCs	Base	1 year	KL73212A*FS	7 800 000,00
Kaspersky Financial Threat Intelligence Reporting - Executive Summary and IOCs	Base	1 year	KL73222A*FS	5 850 000,00
Kaspersky APT Intelligence Reporting - Executive Summary + 3 Full APT reports	Base	1 year	KL72802A*FS	3 120 000,00
Kaspersky APT Intelligence Reporting - Executive Summary	Base	1 year	KL72832A*FS	1 560 000,00
Kaspersky APT Intelligence Reporting - Executive Summary and IOCs	Base	1 year	KL72842A*FS	5 850 000,00
Kaspersky APT Intelligence Reporting	Base	1 year	KL72892A*FS	7 800 000,00

+\$250K

threats and their relationships, brought together into a single, powerful web service.

[Get more info about Kaspersky Threat Intelligence Portal](#)

Request Access

у «Добавить» и выберите архив файлов приложения.





ПРОФЕССИОНАЛЬНОЕ ВЫГОРАНИЕ



ЧЕРНАЯ КОШКА В ТЕМНОЙ КОМНАТЕ

НЕДОВОЛЬСТВО СОБОЙ И ОКРУЖАЮЩИМ

УВОЛЬНЕНИЕ

THREAT HUNTING СОБСТВЕННЫМИ РУКАМИ (БЕЗ EDR)

A detailed illustration of a prehistoric scene. In the foreground, a large mammoth with thick brown fur and curved tusks stands in a snowy, rocky landscape. Several hunters, dressed in animal skins and carrying spears, are positioned around the mammoth. One hunter in the center-right is holding a spear high, ready to throw it. In the background, more hunters are visible, some carrying spears and others carrying bundles. The scene is set in a mountainous, forested area with a sunset or sunrise sky.

ДОРОГО

НИЗКИЙ ЭФФЕКТ

ПРЯМАЯ УГРОЗА БИЗНЕС-ПРОЦЕССАМ



CASANOVA



Hash, IP address, domain, or URL:

Enter your request here

By requesting look-up data, you agree to our [Terms of Use](#) and [Privacy Statement](#).

799EDDB236A4E90A8AEA50802E1604CA7

Malware

Public

КАКОЙ ИЗ СОТНИ ПОДОЗРИТЕЛЬНЫХ
ФАЙЛОВ КОВЫРЯТЬ ПЕРВЫМ?

Report for hash: **Malware**

799EDDB236A4E90A8AEA50802E1604CA7

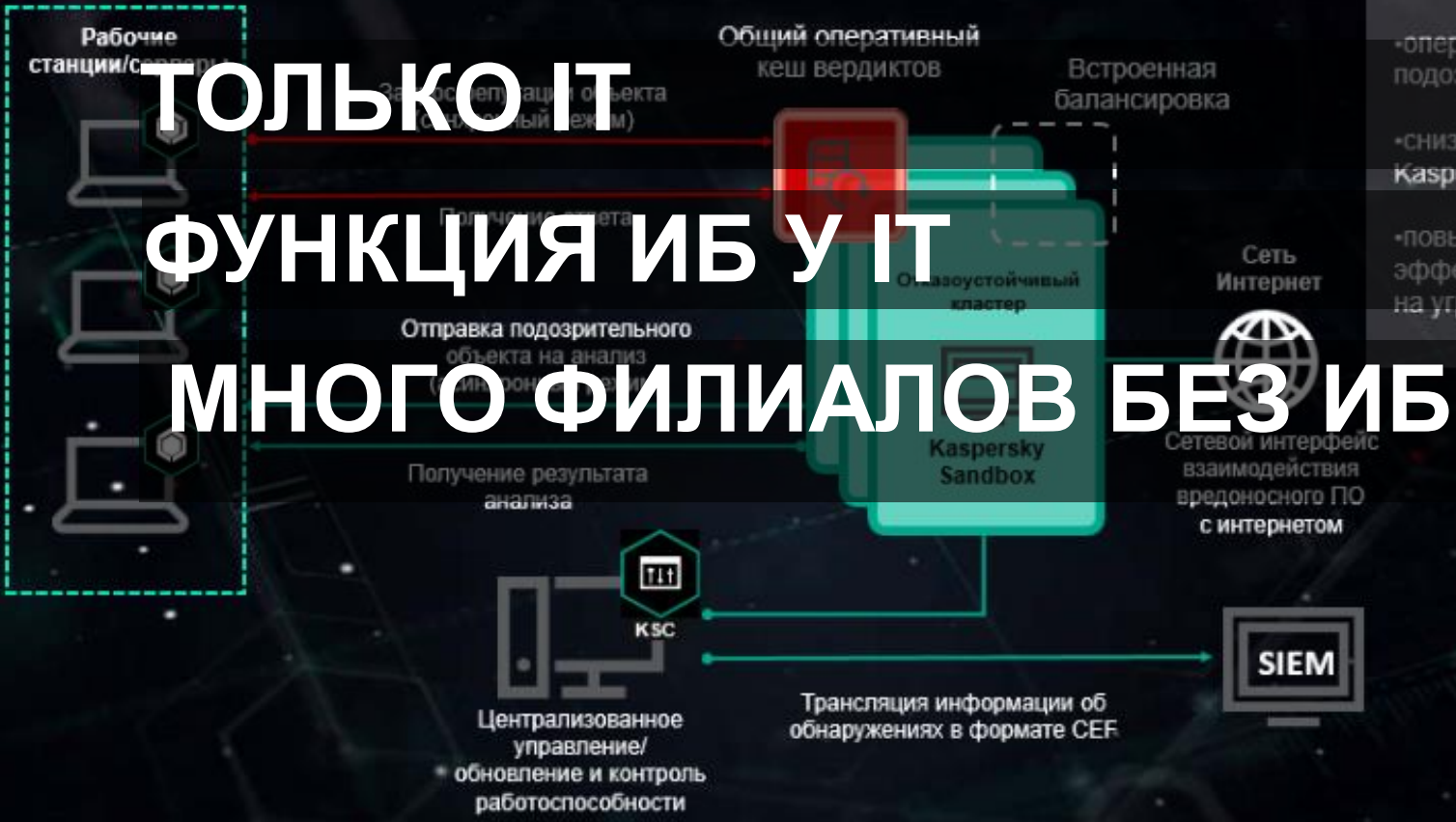
АНТИВИРУС ГОВОРИТ, ЧТО ФАЙЛ ЧИСТЫЙ
ЧТО ДЕЛАТЬ ДАЛЬШЕ?

Hits	> 100	Format	PE	MD5	799EDDB236A4E90A8AEA50802E1604CA7
First seen	Jan 30, 2018 13:13	Size	10.57 MB	SHA-1	733AFF73A785B2EA8B4185C3DF18F7618CB02635
Last seen	Jun 25, 2019 10:40	Signed by	—	SHA-256	1D91A2F475C017F40487813794570856F92C6B21E122869E8B60A51A319F32C1
		Packed by	—		

Detection names

Mar 13, 2018 10:29 HEUR:Trojan-Min33-Coinminer	Jan 30, 2018 20:52 PCML:EvilWin32.Coinminer	Jan 30, 2018 20:52 PCML:Trojan-Min33-Bacon.s	Jan 30, 2018 20:52 PCML:Trojan-Min33-Bacon.s
---	--	---	---

Архитектура Kaspersky Sandbox



Поддерживает проверку объектов в двух режимах: синхронном и асинхронном, что позволяет:

- оперативно обрабатывать подозрительные объекты;
- снизить нагрузку на серверы Kaspersky Sandbox;
- повысить скорость и эффективность реагирования на угрозы.

**ТОЛЬКО IT
ФУНКЦИЯ ИБ У IT
МНОГО ФИЛИАЛОВ БЕЗ ИБ**

kaspersky

Спасибо

kaspersky.ru

ВЕЛИКИЕ СТРОЙКИ КОММУНИЗМА



3UH8UpdZOL3UH8UpdZOL

НАШ ВЫИГРЫШ – ИХ ПРОИГРЫШ