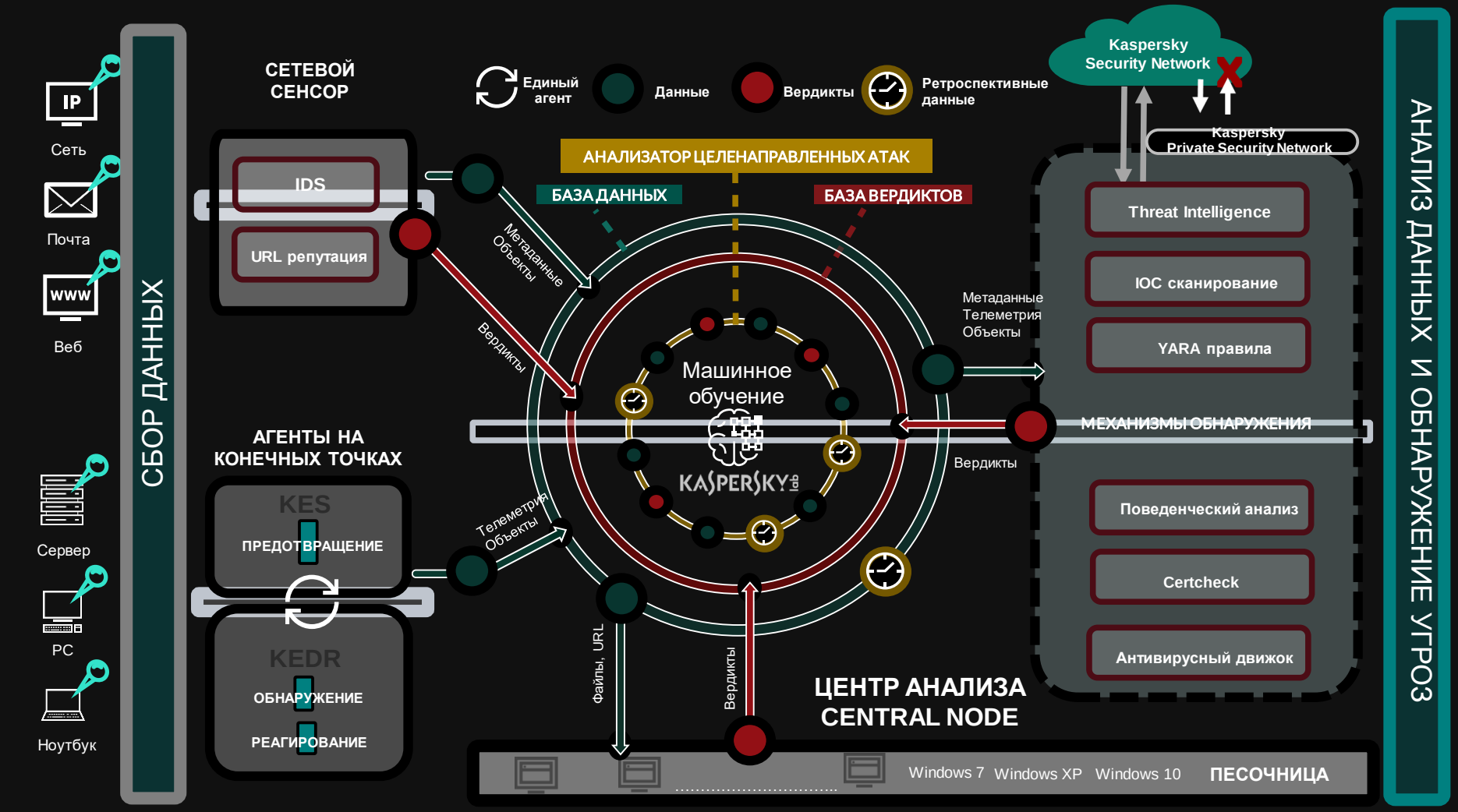
kaspersky

# Путь Казановы, или как живется киберследователю.


© picture-alliance/Unit


СБОР ДАННЫХ
IP
Сеть
Почта
WWW
Веб
Сервер
PC
Ноутбук
СЕТЕВОЙ СЕНСОР
IDS
URL репутация
АГЕНТЫ НА КОНЕЧНЫХ ТОЧКАХ
KES
ПРЕДОТВРАЩЕНИЕ
KEDR
ОБНАРУЖЕНИЕ
РЕАГИРОВАНИЕ
Единый агент
Данные
Вердикты
Ретроспективные данные
АНАЛИЗАТОР ЦЕЛЕНАПРАВЛЕННЫХ АТАК
БАЗА ДАННЫХ
БАЗА ВЕРДИКТОВ
Метаданные
Объекты
Вердикты
Машинное обучение
KASPERSKY
Телеметрия
Объекты
Файлы, URL
Вердикты
Kaspersky Security Network
Kaspersky Private Security Network
Метаданные
Телеметрия
Объекты
Вердикты
МЕХАНИЗМЫ ОБНАРУЖЕНИЯ
Threat Intelligence
IOC сканирование
YARA правила
Поведенческий анализ
Certcheck
Антивирусный движок
ЦЕНТР АНАЛИЗА
CENTRAL NODE
Windows 7
Windows XP
Windows 10
ПЕСОЧНИЦА
АНАЛИЗ ДАННЫХ И ОБНАРУЖЕНИЕ УГРОЗ


# Путь Казановы


ЛЮДИ
ТЕХНОЛОГИИ


Jerzy Kossak
Kutno 1939

# СТРОИМ САМИ?

3 БЕЗОПАСНИКА В ГОД + СОФТ - $200К

SIEM - $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

проверять 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 |

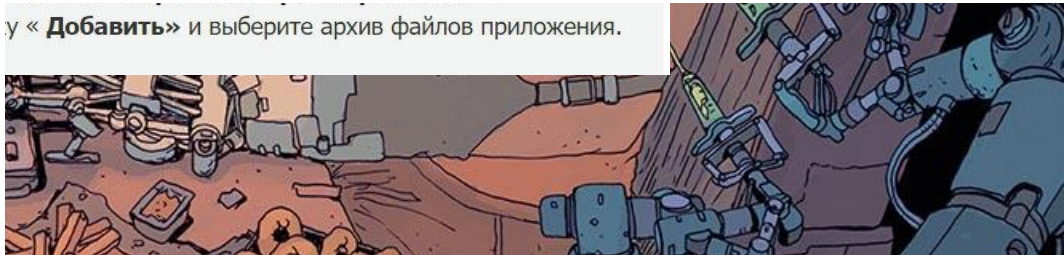
**+$250K**

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

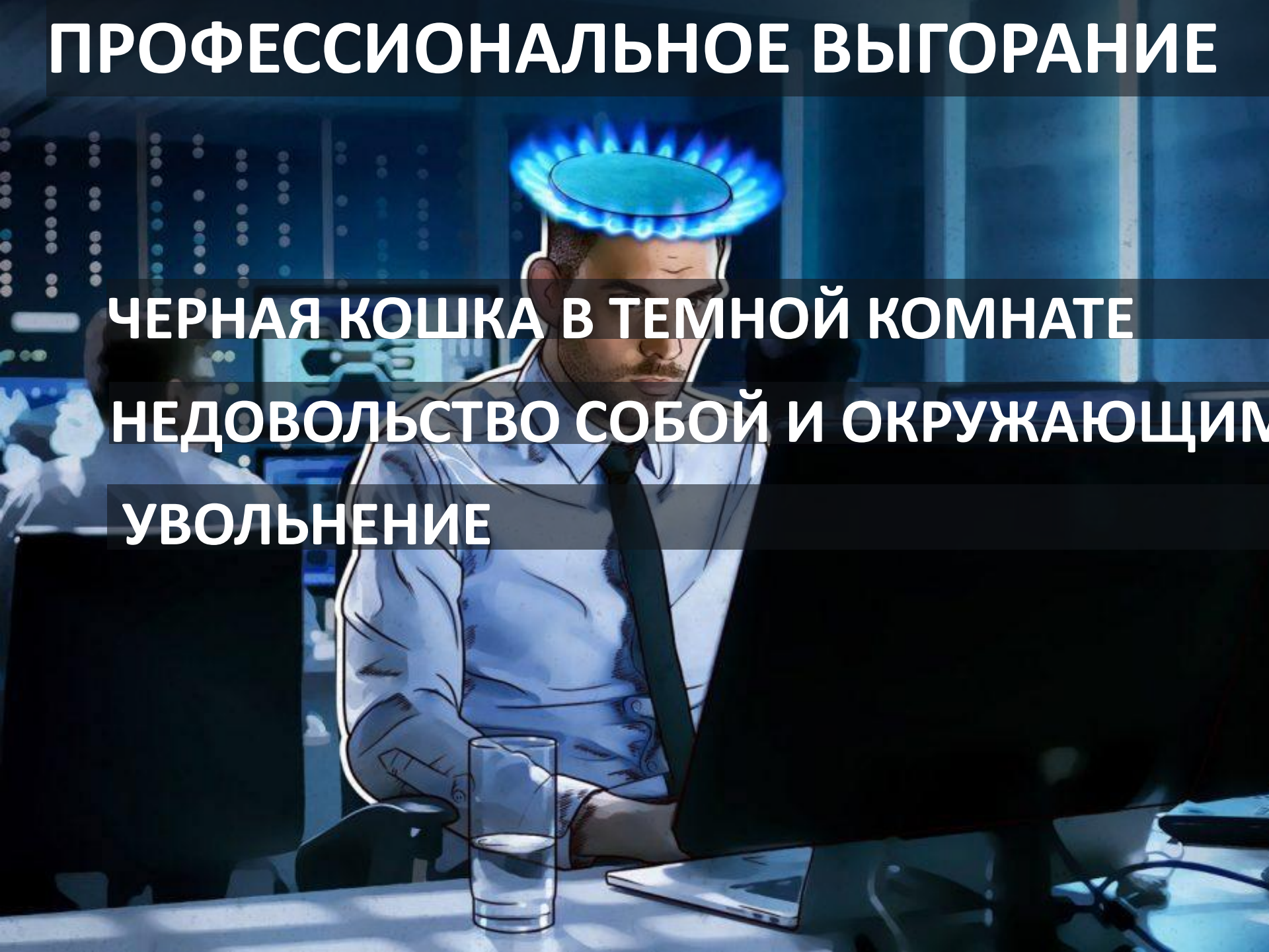
Get more info about Kaspersky Threat Intelligence Portal

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)

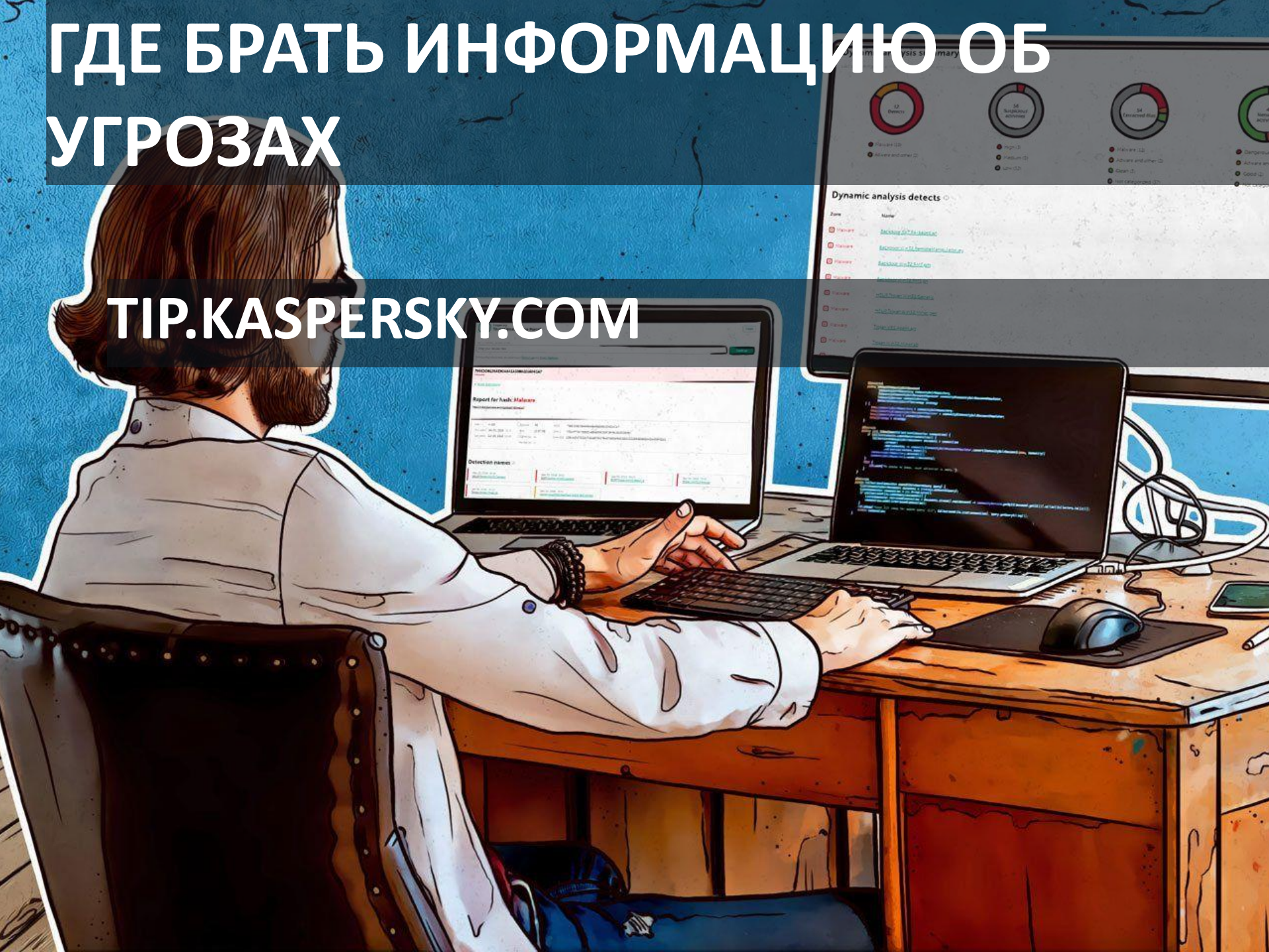
ДОРОГО

НИЗКИЙ ЭФФЕКТ

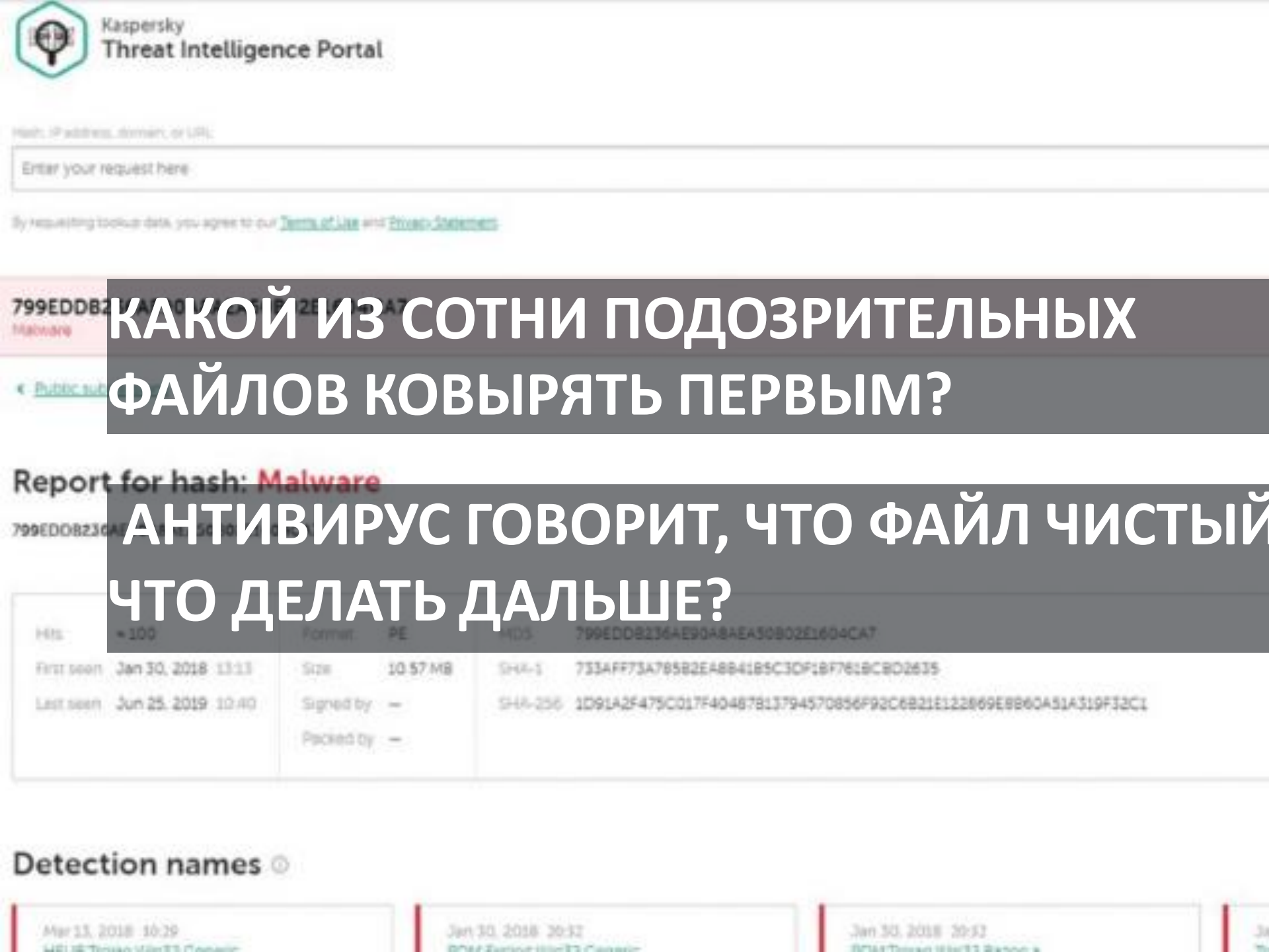
ПРЯМАЯ УГРОЗА БИЗНЕС-ПРОЦЕССАМ

# ГДЕ БРАТЬ ИНФОРМАЦИЮ ОБ УГРОЗАХ

TIP.KASPERSKY.COM

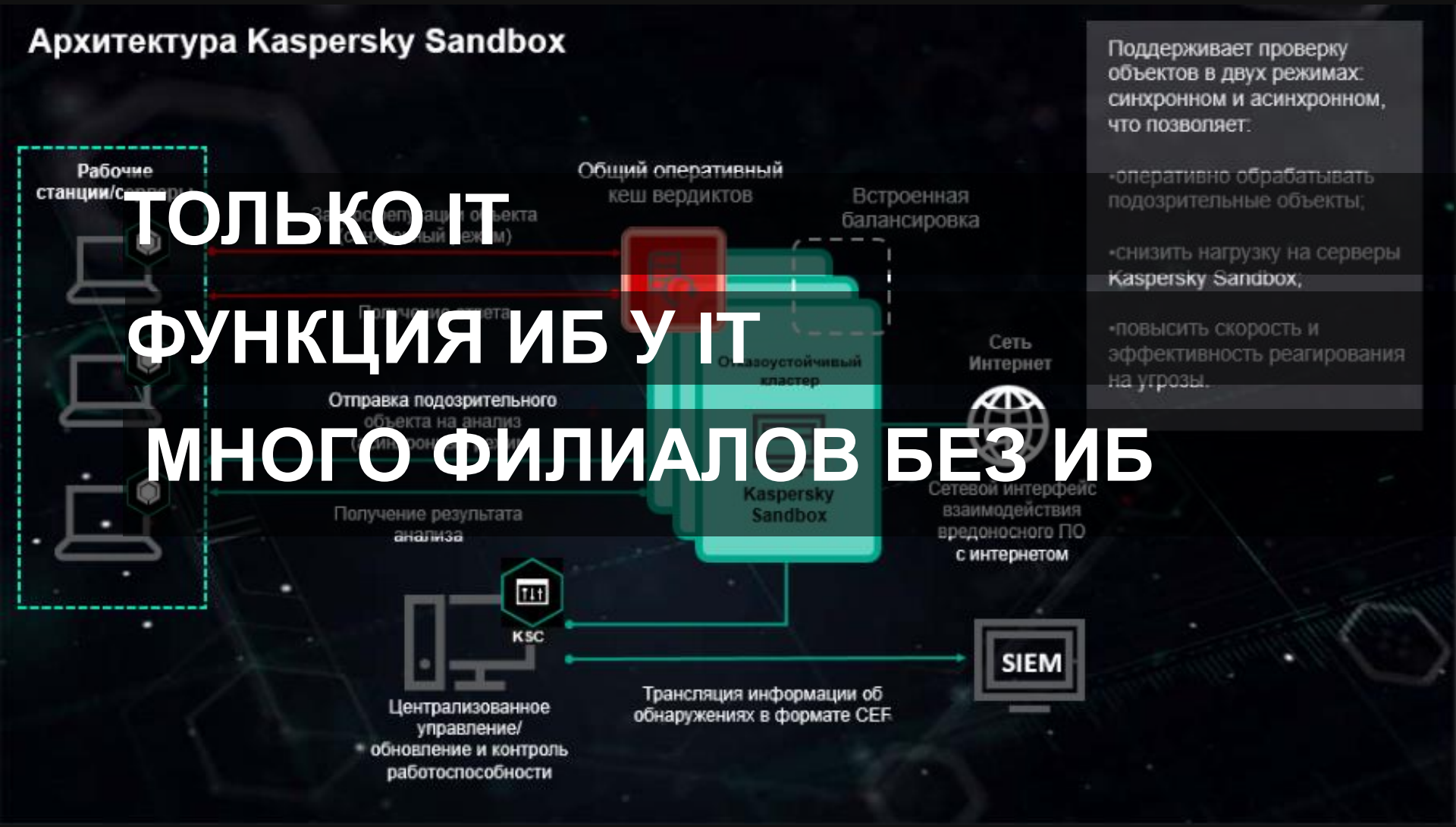



CASANOVA




# КАКОЙ ИЗ СОТНИ ПОДОЗРИТЕЛЬНЫХ ФАЙЛОВ КОВЫРЯТЬ ПЕРВЫМ?

# АНТИВИРУС ГОВОРИТ, ЧТО ФАЙЛ ЧИСТЫЙ ЧТО ДЕЛАТЬ ДАЛЬШЕ?




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

kaspersky

# Спасибо

kaspersky.ru