KASPERSKY lab

ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ, МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ НИХ

ТЕНДЕНЦИИ КОРПОРАТИВНОЙ ИБ В 2016 ГОДУ

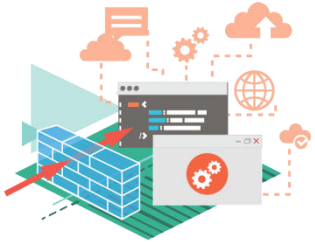
Большинство передовых угроз строятся на базовых техниках и методах социальной инженерии

Недостаток оперативной информации в виду динамического усложнения ИТ инфраструктуры

Существенное снижение затрат и массовый рост предложений (Кибератака-Как-Сервис)

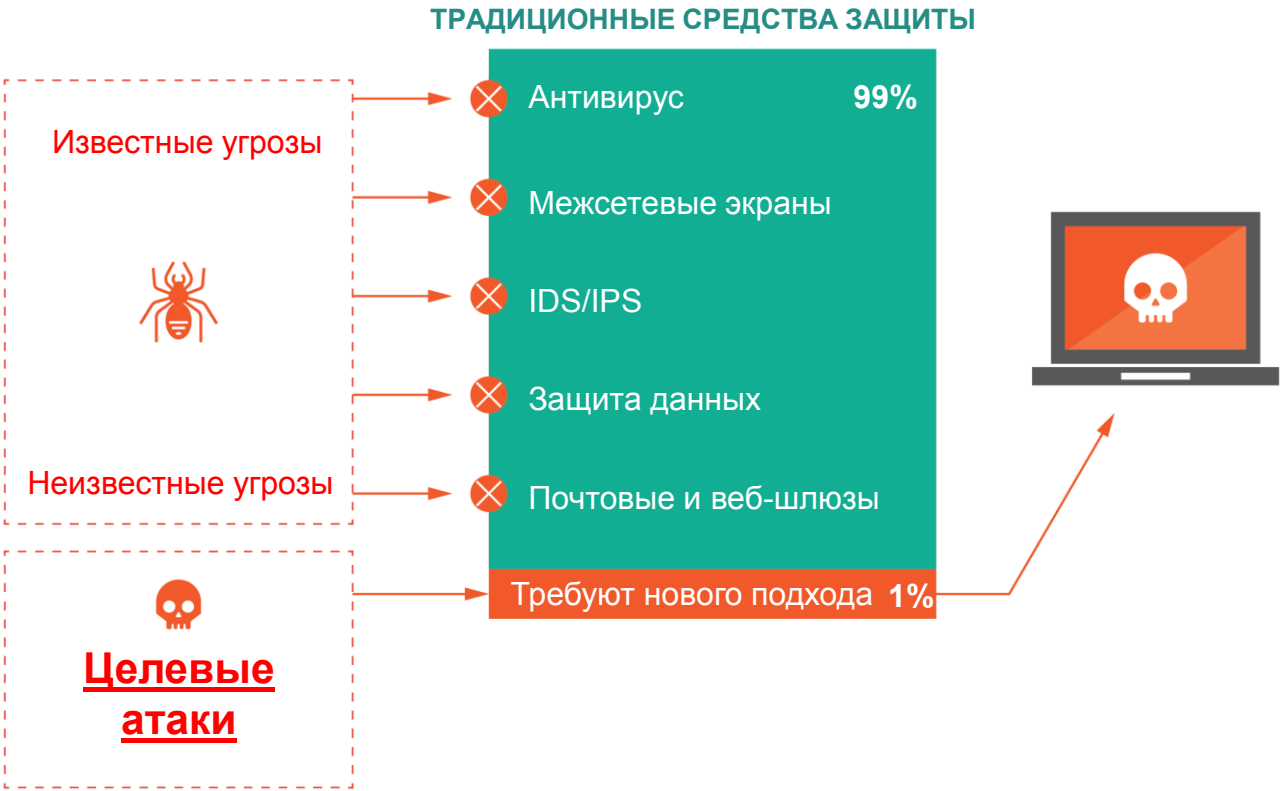
В среднем целевая атака с момента её появления остается необнаруженной более 214 дней

Рост количества атак на поставщиков, 3-их лиц и небольшие компании (SMB)



Резкий спад эффективности периметровой защиты

1% атак

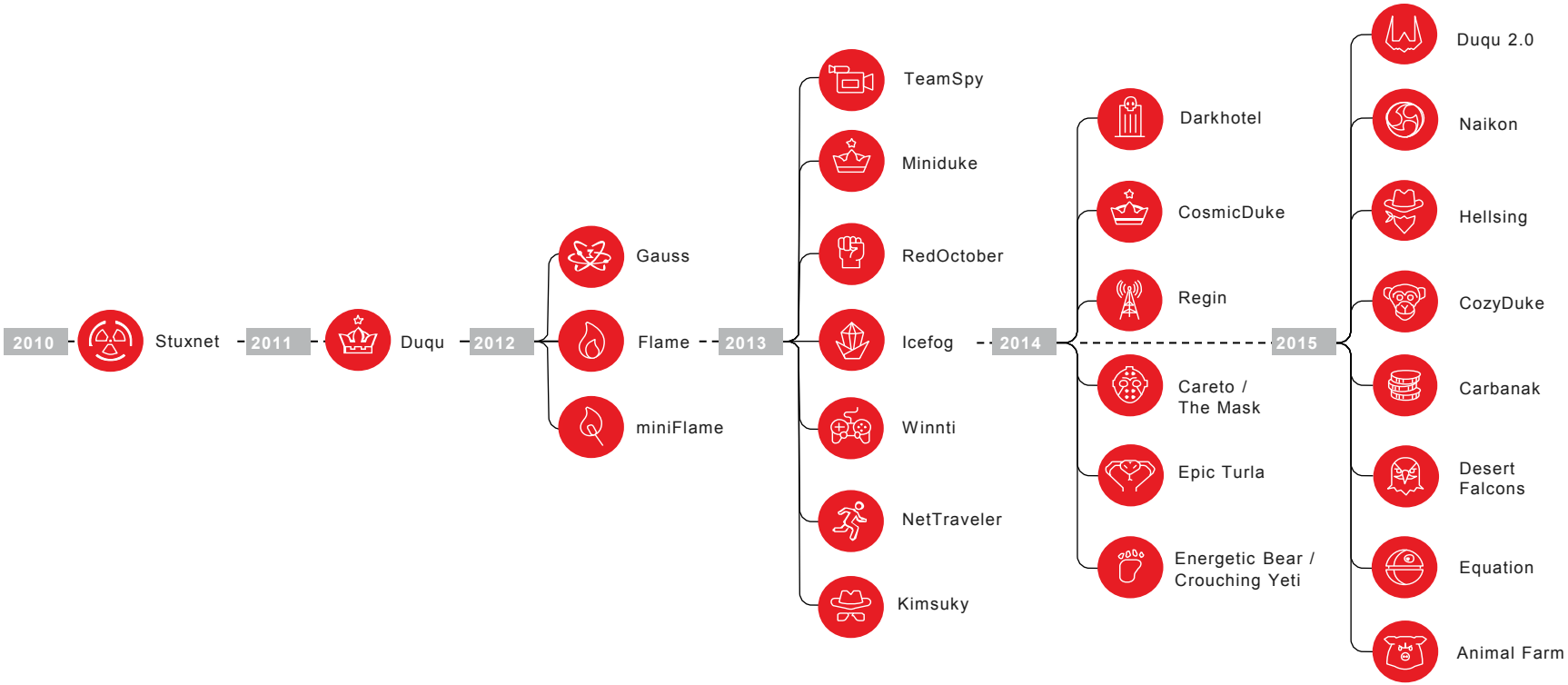

ТРАДИЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ
Известные угрозы
Неизвестные угрозы
Целевые атаки
Антивирус 99%
Межсетевые экраны
IDS/IPS
Защита данных
Почтовые и веб-шлюзы
Требуют нового подхода 1%

ОТ ЧЕГО ЖЕ ЗАЩИЩАТЬСЯ…

Целевая атака –
это непрерывный **процесс** несанкционированной активности в инфраструктуре «цели», удаленно управляемый в режиме реального времени вручную

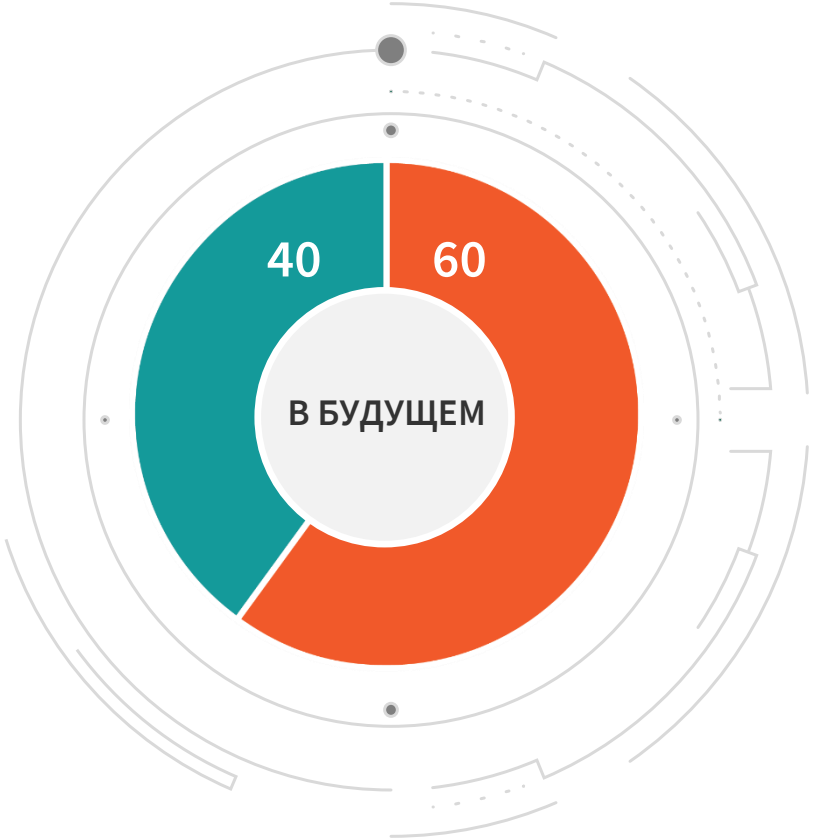
APT – это комбинация утилит, легитимного ПО, передового вредоносного ПО, уязвимостей нулевого дня и т.д..

ЦЕЛЕВЫЕ АТАКИ: УЖЕ ПОВСЕДНЕВНОСТЬ

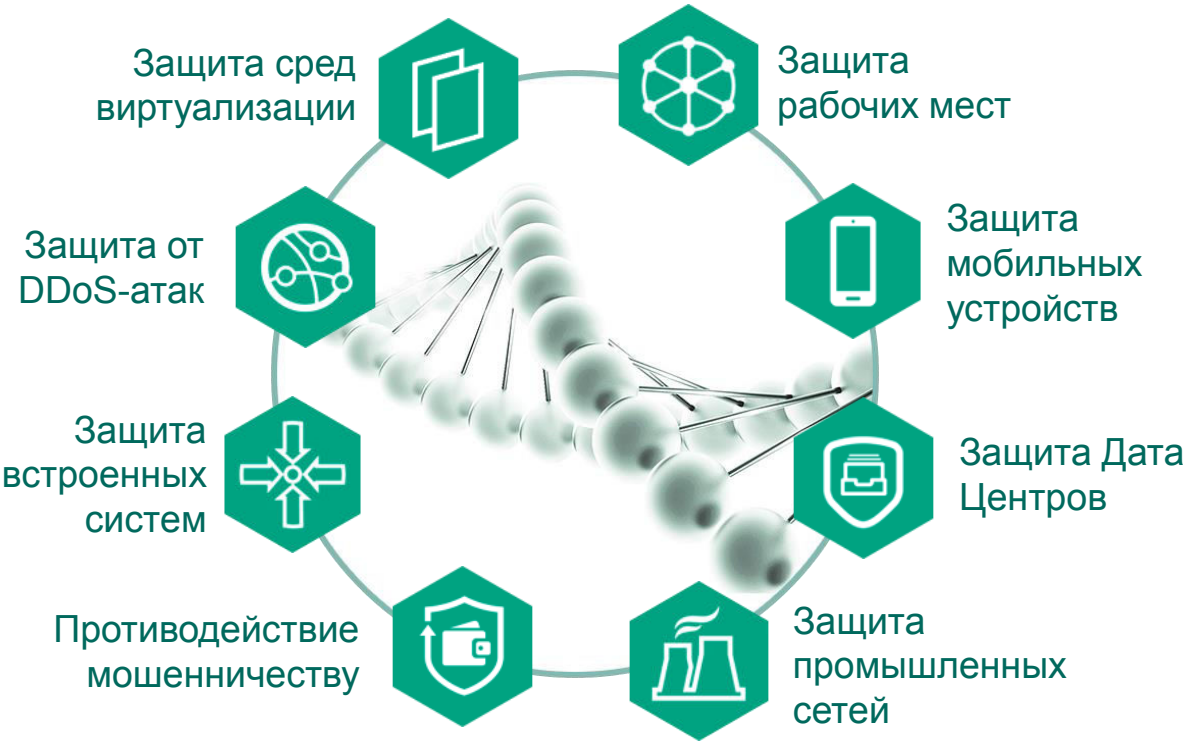


ОЖИДАНИЯ БИЗНЕСА: РАСШИРЕНИЕ ИНВЕСТИЦИЙ ВНЕ ПРОТИВОДЕЙСТВИЯ

- **Текущий размер инвестиций: 80% на превентивные технологии / 20% на обнаружение, реагирование и прогнозирование (Крупные компании: 90%/10%)**
- **Планы опрошенных заказчиков на ближайшие 3 года: 40% / 60%**
- **Основано на опросе проведенном Лабораторией Касперского в ноябре 2015 года. Более 6700 компаний опрошенных по миру.**



ЦЕЛЕВЫЕ РЕШЕНИЯ ЛК



ПОДХОД ЛАБОРАТОРИИ КАСПЕРСКОГО

ПРОГНОЗИРОВАТЬ

- Разведка киберугроз
- Отчеты о киберугрозах
- Анализ защищенности
- Анализ кибербезопасности индустриальных систем

ПРЕДОТВРАЩАТЬ

- Устранение уязвимостей
- Средства защиты узла и сети
- Обучение сотрудников

ЛИКВИДИРОВАТЬ ПОСЛЕДСТВИЯ

- Расследование инцидентов
- Цифровая криминалистика
- Анализ вредоносного ПО

ОБНАРУЖИВАТЬ

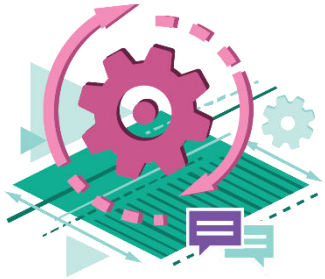
- Выявление целенаправленных атак
- Потоки данных об угрозах
- Экспертный мониторинг

KASPERSKY ANTI TARGETED ATTACK PLATFORM

АРХИТЕКТУРА РЕШЕНИЯ KATA

Сбор данных

- Сенсоры
  - Сетевой
  - Web
  - Email
  - рабочих станций



Анализ

- Processing engines
- AV engine
- Risk Engine
- Targeted Attack Analyzer
- Advanced Sandbox

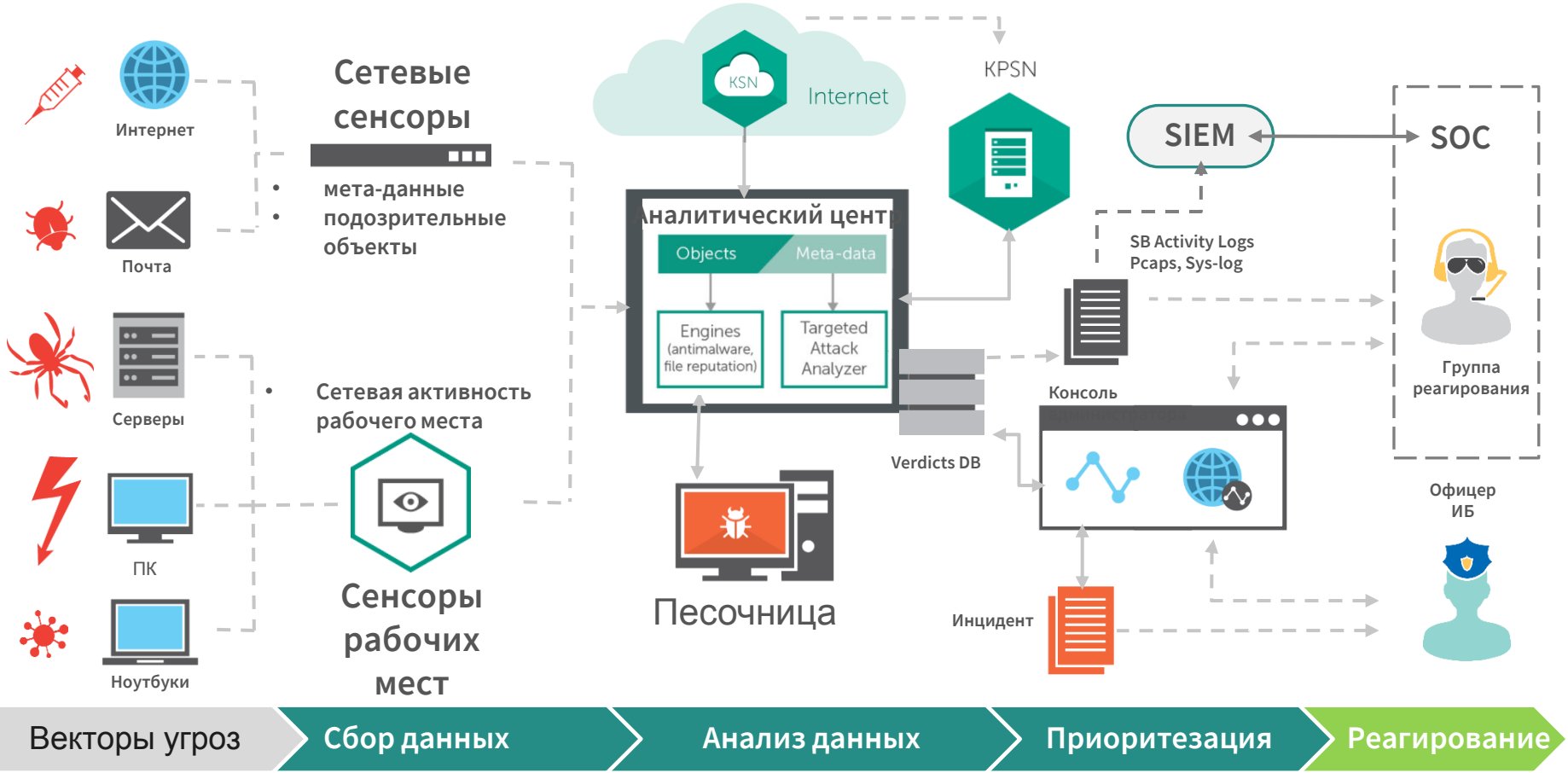
Вердикт

- Визуализация
- Логи активностей
- Записи трафика (Pcaps)
- Syslog

Реагирование

- Сервисы оперативного реагирования экспертами ЛК
- Обучение

KASPERSKY ANTI TARGETED ATTACK PLATFORM



Векторы угроз | Сбор данных | Анализ данных | Приоритезация | Реагирование

СБОР ДАННЫХ: РАБОЧИЕ МЕСТА, СЕТЕВАЯ АКТИВНОСТЬ, ПОЧТА И WEB

- Задача: мониторинг активности корпоративной среды и сбор объектов для анализа

- Решение: специализированные сенсоры сбора данных:
  - Сетевой трафик
  - Сессии пользователей (прокси)
  - Почтовые сообщения
  - Сетевая активность рабочих станций и серверов

АНАЛИЗ ДАННЫХ: АНАЛИЗАТОР ЦЕЛЕВЫХ АТАК

- **Задача: корреляция событий и вердиктов ИБ связанных с целевыми атаками**

- **Подход:**
  - **Обнаружение аномалий путем анализа мета-данных**
  - **Корреляция данных сетевого уровня, рабочих станций и серверов**
  - **Связка разноплановых событий в единый инцидент или в привязке к пользователю**

АНАЛИЗ ДАННЫХ: ПЕСОЧНИЦА

- Задача: выявление вредоносной активности объектов на основе поведения
- Решение: Песочница
  - На основе внутреннего решения ЛК
  - 10-лет разработки и развития
- Поддерживаемые среды
  - Windows XP, Windows 7 (x32/x64)
  - Android

АНАЛИЗ ДАННЫХ: ПОЛУЧЕНИЕ РАСШИРЕННОЙ КАРТИНКИ

- **Задача: получение данных об угрозе из разнородных источников анализа**

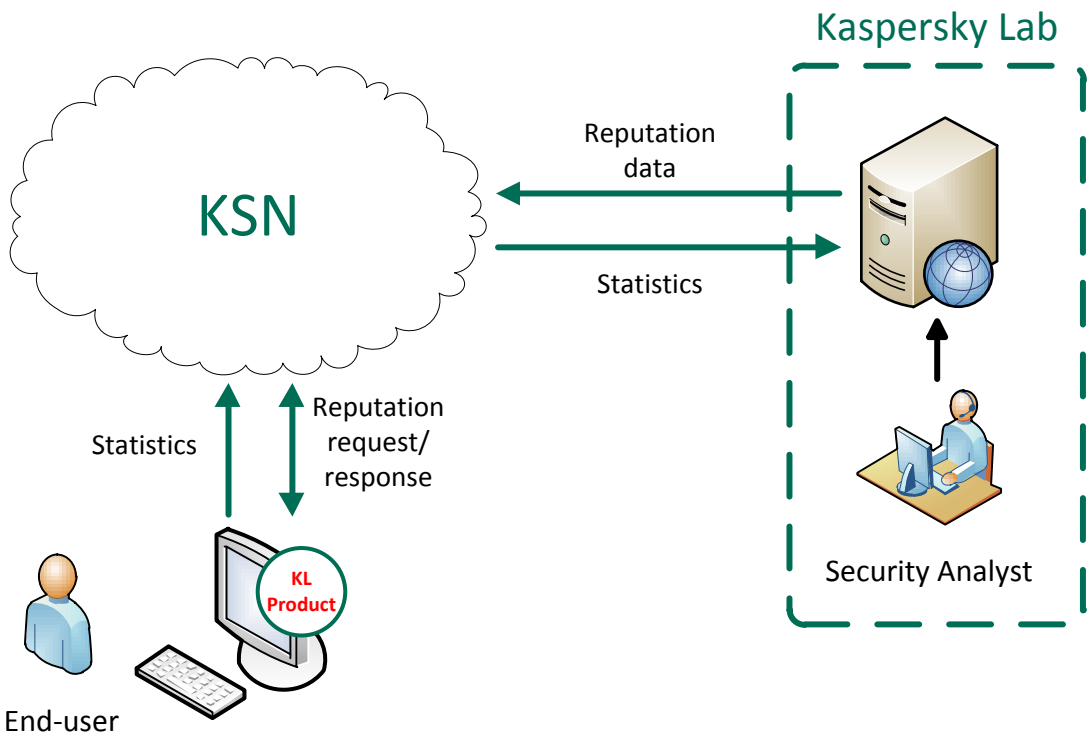
- **Решение:**
  - **Получение вердиктов антивирусного движка**
  - **Шаблоны детектирования на основе настраиваемых правил (YARA)**
  - **Обнаружение попыток соединения с известными вредоносными хостами**
  - **Репутационные данные для обнаружения подозрительного вредоносного ПО и соединений**

ВЫНЕСЕНИЕ ВЕРДИКТОВ: ВИЗУАЛИЗАЦИЯ И РАССЛЕДОВАНИЕ

- **Задача: представление результатов для удобства реагирования**

- **Решение: Консоль визуализации и администрирования**
  - **Мониторинг в реальном времени**
  - **Поиск по событиям**
  - **Интеграция с SIEM-системами (HP Arcsight, IBM Qradar, SPLUNK)**
  - **Event log, Syslog**

KASPERSKY SECURITY NETWORK

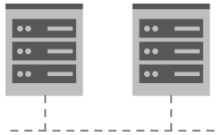


Продукты ЛК используют облачную базу знаний для получения информации об угрозах.
Использования облачных технологий позволяет эффективно решать задачу оперативности обновлений баз знаний и экономии локальных вычислительных ресурсов.
В случае согласия пользователя продукты обмениваются посредством облака информацией об угрозах.
Статистика обрабатывается экспертами ЛК для выявления новых угроз.

KPSN - ПРИВАТНАЯ ИНСТАЛЛЯЦИЯ РЕШЕНИЯ

Соответствие требованиям регуляторов и стандартам ИБ

Kaspersky **Private** Security Network



Локально размещаемая версия базы KSN

- Соответствие требованиям
- регуляторов
- Стандарты безопасности
- Бизнес необходимость
- ИТ-требования

Основные преимущества KPSN:

- размещение репутационной базы ЛК (полный набор данных) внутри защищаемой инфраструктуры
- исключение передачи информации вне контролируемой сети
- одностороннее получение оперативных обновлений от KSN
- высокая производительность (сотни тысяч запросов)
- осведомленность в режиме реального времени

СЕРТИФИКАЦИЯ ФСТЭК

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

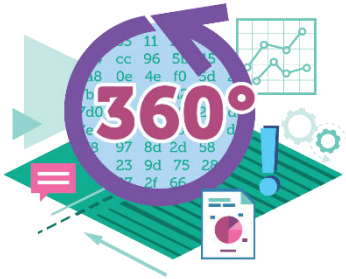
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3556

Выдан 20 апреля 2016 г.
Действителен до 20 апреля 2019 г.

Настоящий сертификат удостоверяет, что **программный комплекс «Kaspersky Security Center совместно с Kaspersky Private Security Network»**, разработанный и производимый АО «Лаборатория Касперского» в соответствии с техническими условиями ТУ 643.46856491.00082-01, функционирующее в средах операционных систем, указанных в формуляре 643.46856491.00082-03 30 01, является программным средством антивирусной

В БЛИЖАЙШЕЙ ПЕРСПЕКТИВЕ



Интеграция

- Интеграция с существующими решениями Лаборатории Касперского
- Автоматизация реагирования на выявленные инциденты

Реагирование

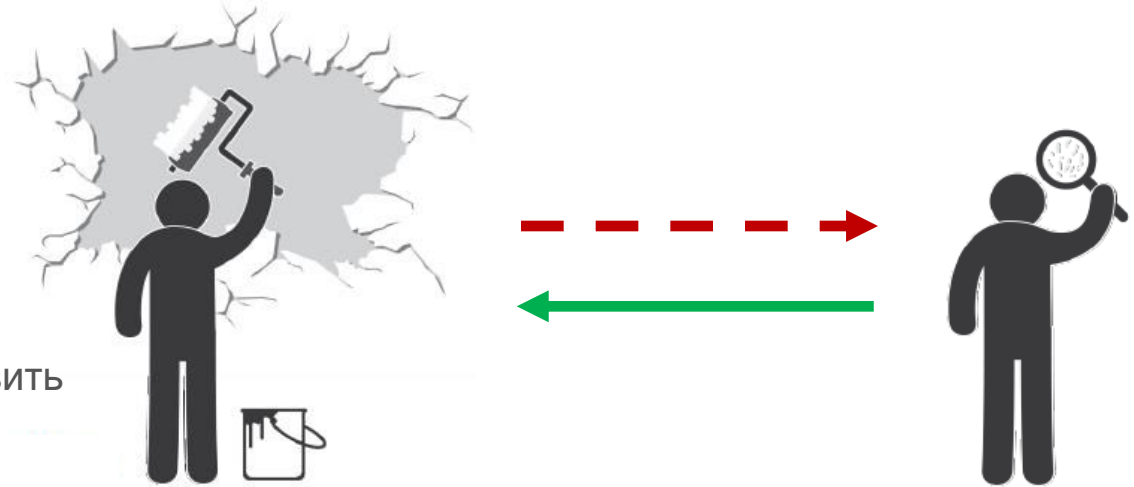
- Новый модуль решения (EDR) разработанный для автоматизации расследований и сбора электронных доказательств

Аналитика

- Аналитическая платформа для выявления угроз и глубокого расследования

ОБУЧЕНИЕ РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

Быстро восстановить системы

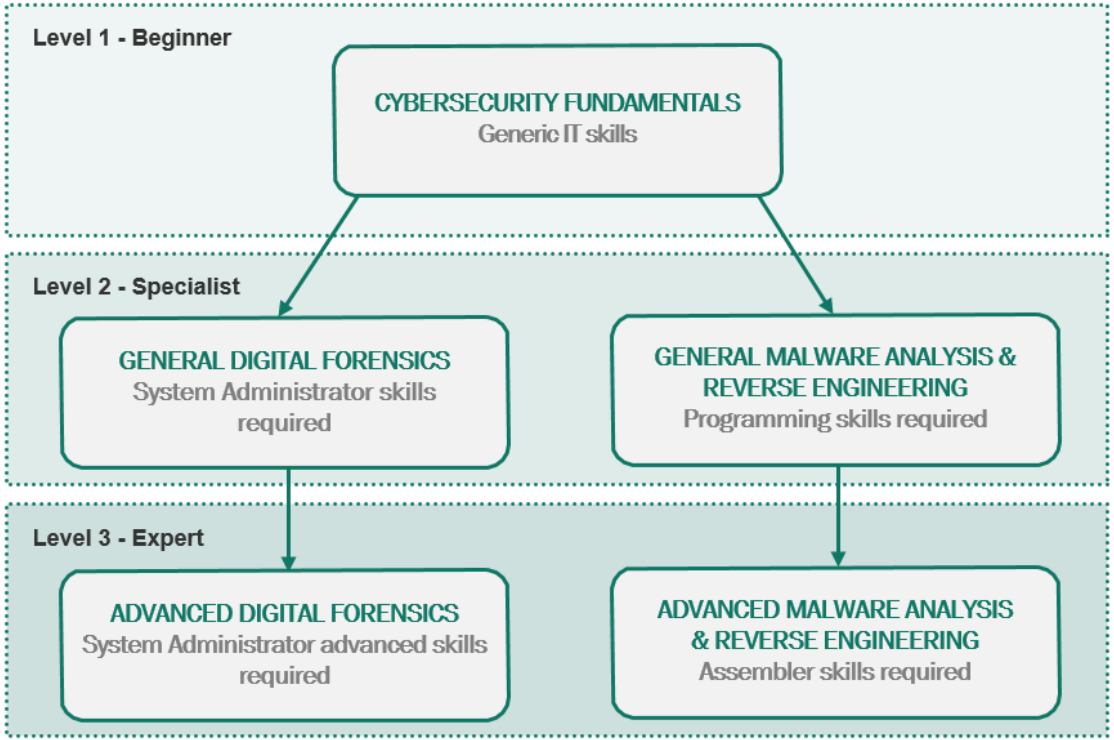


Расследовать как инцидент произошел

Обучение правильному построению процесса реагирования – это ключевая задача эффективного использования ЛЮБОГО анти-APT решения

ОБУЧЕНИЕ В ОБЛАСТИ ИБ

- Интерактивная платформа
- Экспертные курсы
  - Цифровая криминалистика
  - Анализ ВПО
  - Расследование инцидентов



СЕРВИСЫ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

- Анализ вредоносного ПО
- Цифровая криминалистика
- Реагирование на инциденты
- Выявление целевых атак

No	Investigation phases	Malware Analysis	Digital Forensics	Incident Response
1	Incident assessment • Rapid response to the incident • Minimization of the consequences • Initial analysis of the incident, that can be done onsite if required, to establish a full understanding of the issue and determine how to collect the necessary evidence			X
2	Collecting evidence Depending on the situation, gather HDD images, memory dumps, network traces etc related to the incident under investigation			X
3	Performing forensic analysis • Establishing a clear, detailed picture of the incident: – What happened – Who was targeted – When it happened – Where it happened – Why it happened – How it happened • Analyzing the evidence to find the malware that caused the incident		X	X
4	Performing malware analysis Analyzing the malware to understand how it works, including its: • Classification • Functions • Related vulnerability and exploits • Means of propagation • Destructive activity • Means of installation	X	X	X
5	Creating a remediation plan • Understanding the objective of the malware binary • Developing ways to stop its propagation • Developing uninstallation plans	X	X	X
6	Creating an investigation report Upon the completion of their analysis Kaspersky Lab experts provide a detailed report, including investigation details and a remediation scenario	X	X	X

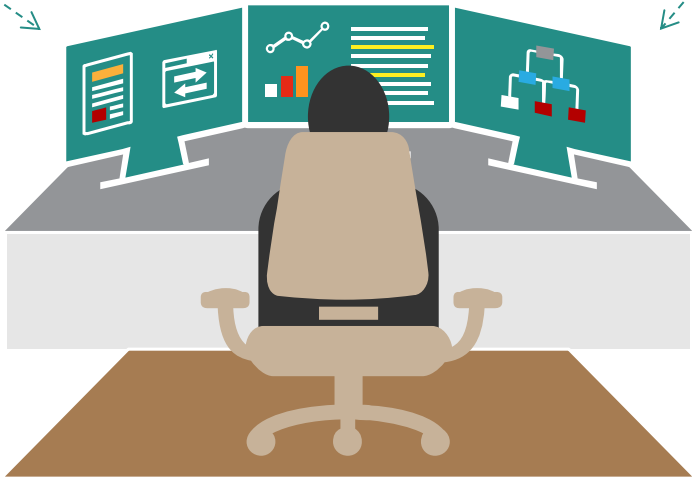
ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СУЩЕСТВУЮЩИХ РЕШЕНИЙ

Проактивное оповещение об угрозах безопасности

Повышение эффективности существующей SIEM-системы

- Malicious URLs
- Phishing URLs
- Botnet C&C URLs
- Malware Hashes
- Mobile Malware Hashes
- P-SMS Trojan Feed
- Mobile Botnet C&C URLs

splunk> Radar® ArcSight An HP Company



Оперативная информация о новых целевых атаках

- Детальная информация как обнаружить угрозу внутри сети
- Обновление новой информацией по угрозе со временем
- Подписка на все выявленные целевые атаки ЛК (Global Targeted Attacks)

ОТЧЕТЫ О УГРОЗАХ APT

- Раннее предупреждение целевых атаках
- Детальное описание атак
- Используемые техники и процедуры

- Дополнительные артефакты
  - Индикаторы компрометации
  - Open IOC/yara/STIX

Month	Report
Feb	Animal farm private report
March	EquationDrug IOC's
March	Hawkeye
March	Gloog waterholering campaign
April	Dyre private report
May	Sofacy 0-day
June	Naikon private report
June	Sofacy AZZY backdoor
June	Duqu 2 private report
July	Wild [redacted]
July	Blue [redacted]
August	[redacted]

СПАСИБО!

ВЕБ-САЙТ
www.kaspersky.ru

БЛОГ
blog.kaspersky.ru

FACEBOOK
facebook.com/KasperskyLabRussia

TWITTER
twitter.com/Kaspersky_ru

KASPERSKY lab