KASPERSKY lab

ПОДХОД ЛАБОРАТОРИИ КАСПЕРСКОГО К ПРОТИВОДЕЙСТВИЮ ЦЕЛЕВЫМ АТАКАМ

Владимир Даниленко

Менеджер по сопровождению корпоративных продаж

ДиалогНаука 2016

МАСШТАБ УГРОЗЫ

1994

1

НОВЫЙ ВИРУС КАЖДЫЙ ЧАС

2006

1

НОВЫЙ ВИРУС КАЖДУЮ МИНУТУ

2011

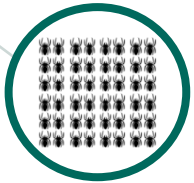
1

НОВЫЙ ВИРУС КАЖДУЮ СЕКУНДУ

2015

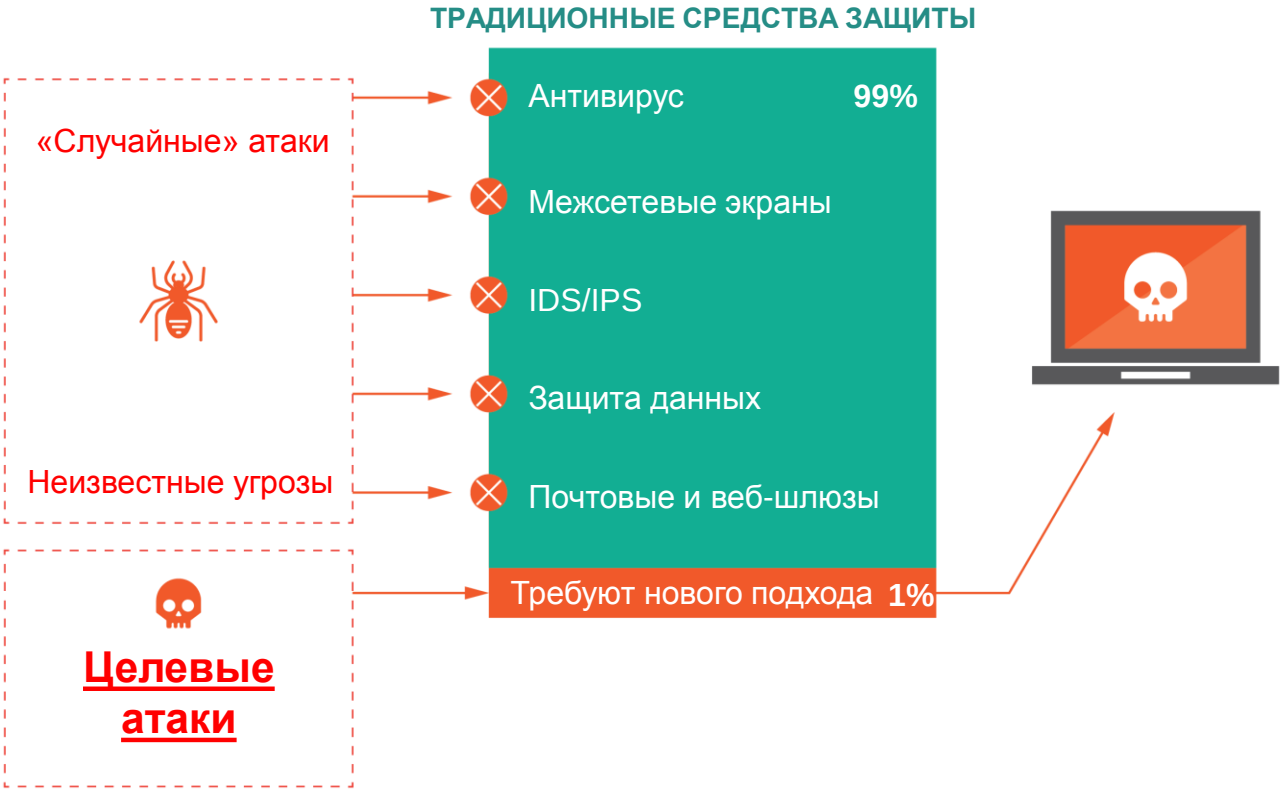
310000

НОВЫХ ВРЕДОНОСНЫХ ОБРАЗЦОВ В ДЕНЬ



KASPERSKY lab

1% атак

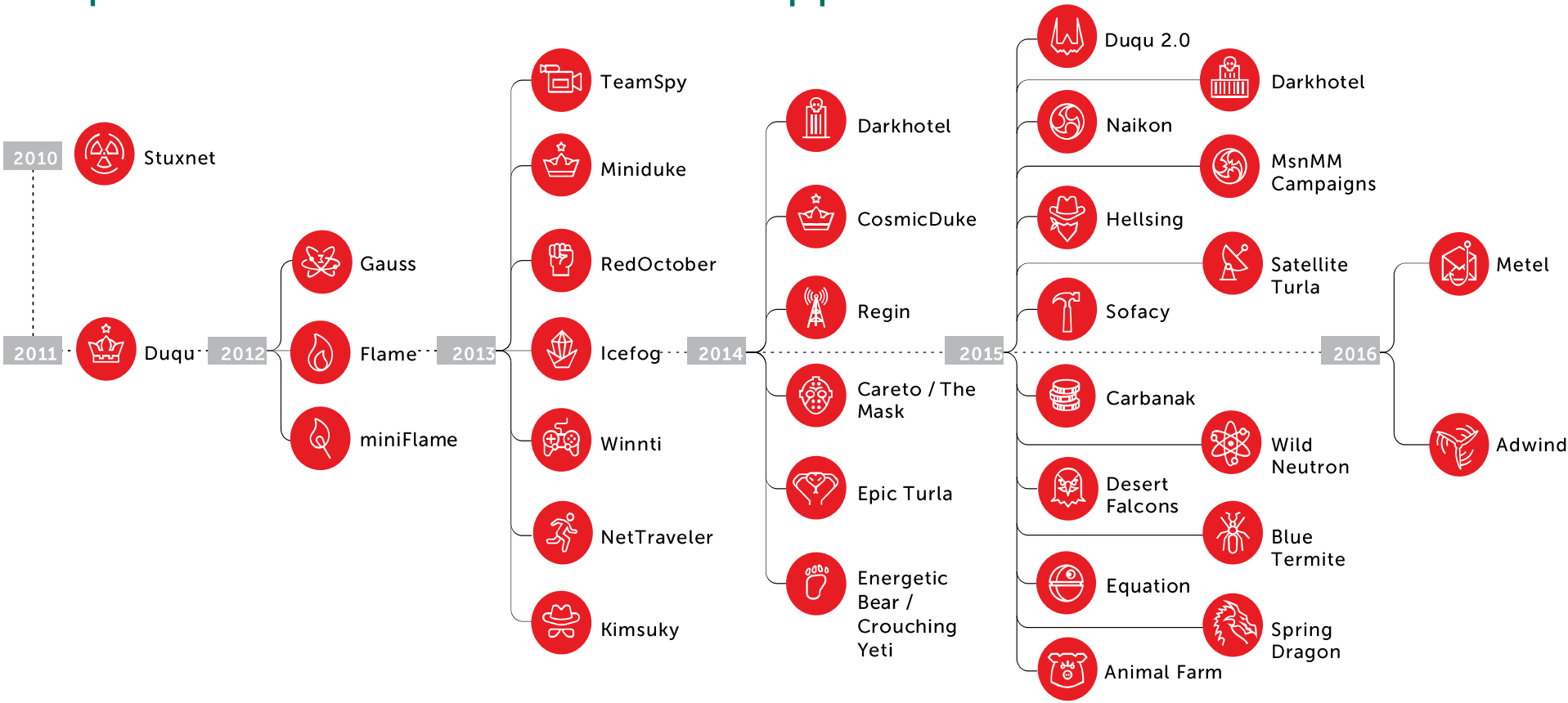

ТРАДИЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ
«Случайные» атаки
Неизвестные угрозы
Целевые атаки
Антивирус 99%
Межсетевые экраны
IDS/IPS
Защита данных
Почтовые и веб-шлюзы
Требуют нового подхода 1%

ОТ ЧЕГО ЖЕ ЗАЩИЩАТЬСЯ…

Целевая атака – это непрерывный процесс несанкционированной активности в инфраструктуре «цели» удаленно управляемый в реальном времени вручную

APT – это комбинация утилит, передового вредоносного ПО, уязвимостей нулевого дня и тд.

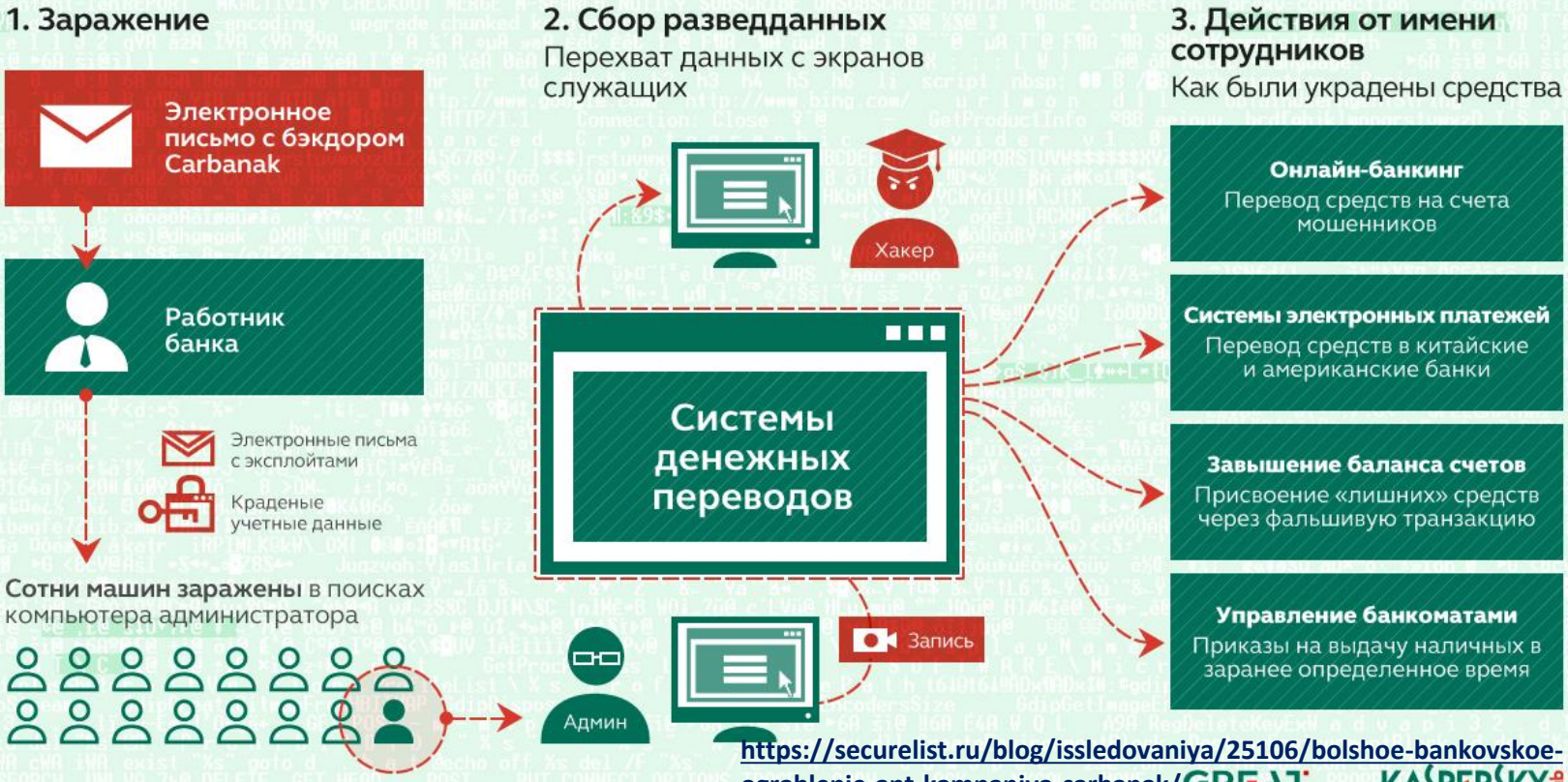
ЦЕЛЕВЫЕ АТАКИ: УЖЕ ПОВСЕДНЕВНОСТЬ



KASPERSKY lab

Как кибербанда Carbanak украла миллиард долларов

Целевая атака на банк



https://securelist.ru/blog/issledovaniya/25106/bolshoe-bankovskoe-ograblenie-apt-kampaniya-carbanak/

ТИПОВОЕ РАЗВИТИЕ ЦЕЛЕВОЙ АТАКИ

НЕГАТИВНОЕ ВОЗДЕЙСТВИЕ

- доступ к информации
- воздействие на бизнес процессы
- сокрытие следов
- тихий уход

ПОДГОТОВКА

- анализ цели
- подготовка стратегии
- создание/покупка тулсета

РАСПРОСТРАНЕНИЕ

- кража идентификационных данных
- повышение привилегий
- налаживание связей
- легитимизация действий
- получение контроля

ПРОНИКНОВЕНИЕ

- использование слабых мест
- проникновение внутрь инфраструктуры

АДАПТИВНАЯ МОДЕЛЬ ПРОТИВОДЕЙСТВИЯ ПЕРЕДОВЫМ УГРОЗАМ ИБ

ПРОГНОЗИРОВАНИЕ

Управление уязвимостями

Анализ потенциальных целей атакующего

Планирование развития стратегии защиты

ПРЕДОТВРАЩЕНИЕ

Снижение рисков проникновения

Повышение безопасности систем и процессов

РЕАГИРОВАНИЕ

Оперативное реагирование на инциденты

Расследование:
- реконструкция атак
- поиск затронутых активов

ОБНАРУЖЕНИЕ

Выявление попыток и фактов существующего проникновения

Подтверждение и приоритезация событий

KASPERSKY lab

KASPERSKY ANTI TARGETED ATTACK PLATFORM

АРХИТЕКТУРА РЕШЕНИЯ

Сбор данных

- Сенсоры
  - Сетевой
  - Web
  - Email
  - Рабочих мест

Анализ

- Движки
- Anti-malware
- Risk Engine
- Advanced Sandbox
- Targeted Attack Analyzer

Вердикт

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

Реагирование

- Сервисы оперативного реагирования экспертами ЛК
- Обучение

СБОР ДАННЫХ: РАБОЧИЕ МЕСТА, СЕТЕВЫЕ АКТИВНОСТИ, WEB И MAIL

Специализированные сенсоры сбора данных:

- Сетевой трафик
- Сессии пользователей (прокси)
- Почтовые сообщения
- Сетевая активность рабочих станций и серверов.

АНАЛИЗ ДАННЫХ

- **Anti-Malware.** Сканирует файловые объекты на предмет вредоносных составляющих и вирусов.
- **Intrusion Detection System.** Анализирует сетевые пакеты с помощью правил, разработанных специалистами Лаборатории Касперского на предмет вредоносной активности.
- Шаблоны детектирования на основе настраиваемых правил (**YARA**)
- Обнаружение попыток соединения с известными вредоносными хостами (**KSN**)
- **Репутационные данные** (**KSN**) для обнаружения подозрительного ПО и соединений
- **Targeted Attack Analyzer**. Технология производит статистический анализ трафика, поведения процессов и учетных записей на ПК и поиск аномальной активности.

АНАЛИЗ ДАННЫХ: ПЕРЕДОВАЯ ПЕСОЧНИЦА

- **Выявление вредоносной активности объектов на основе поведения**
- **Передовая Песочница**
  - На основе внутреннего решения ЛК
  - Доступ в интернет
  - 10+ лет разработки и развития
- **Поддерживаемые среды**
  - Windows XP, 7 (32/64)
  - Android

АНАЛИЗ ДАННЫХ: АНАЛИЗАТОР ЦЕЛЕВЫХ АТАК

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

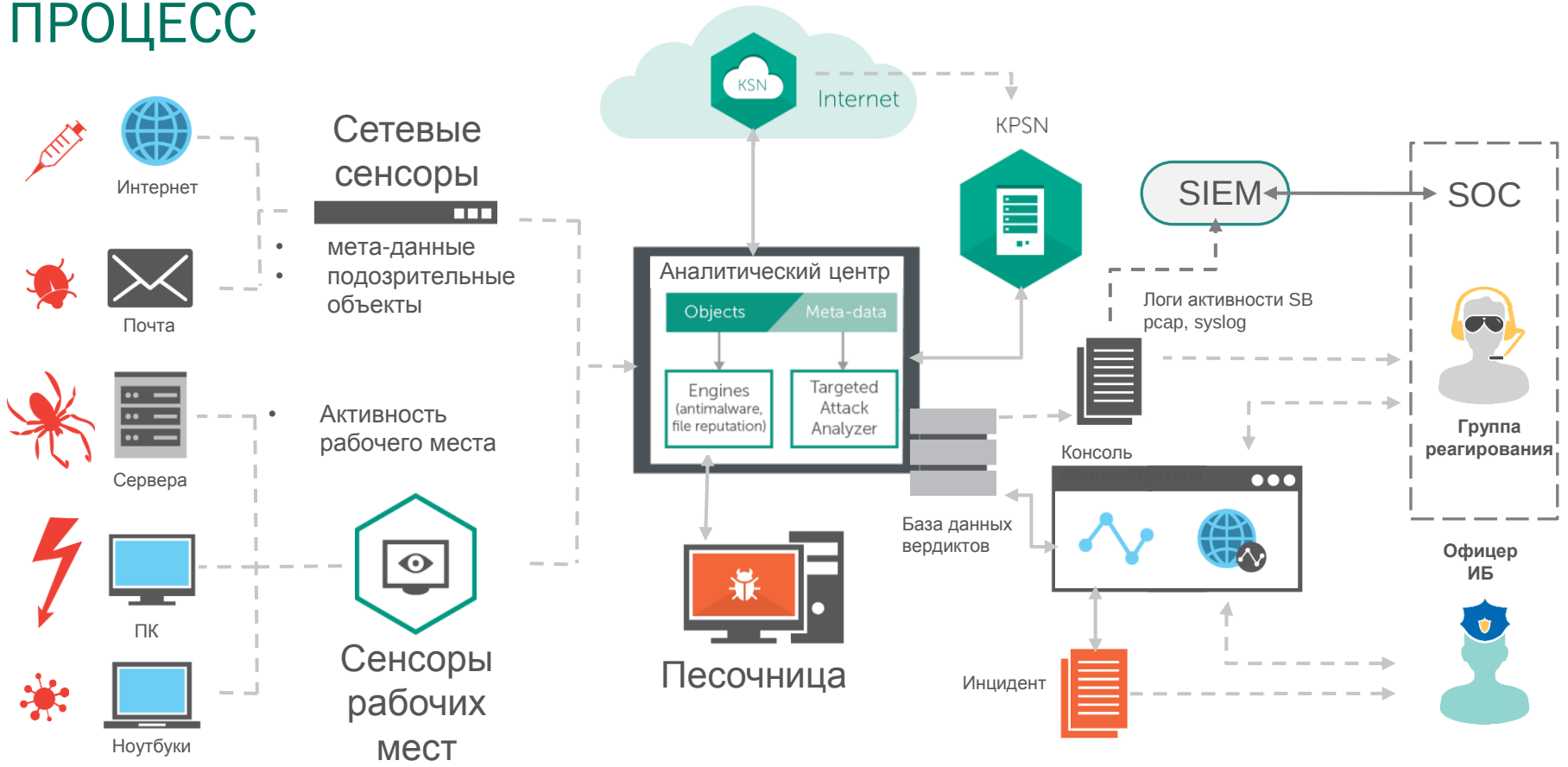
- Подход:
  - Обнаружение аномалий путем анализа мета-данных
  - Корреляция данных сетевого уровня, рабочих станций и серверов
  - Связка разноплановых событий в единый инцидент или в привязке к пользователю

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 (Syslog)

ПРОЦЕСС

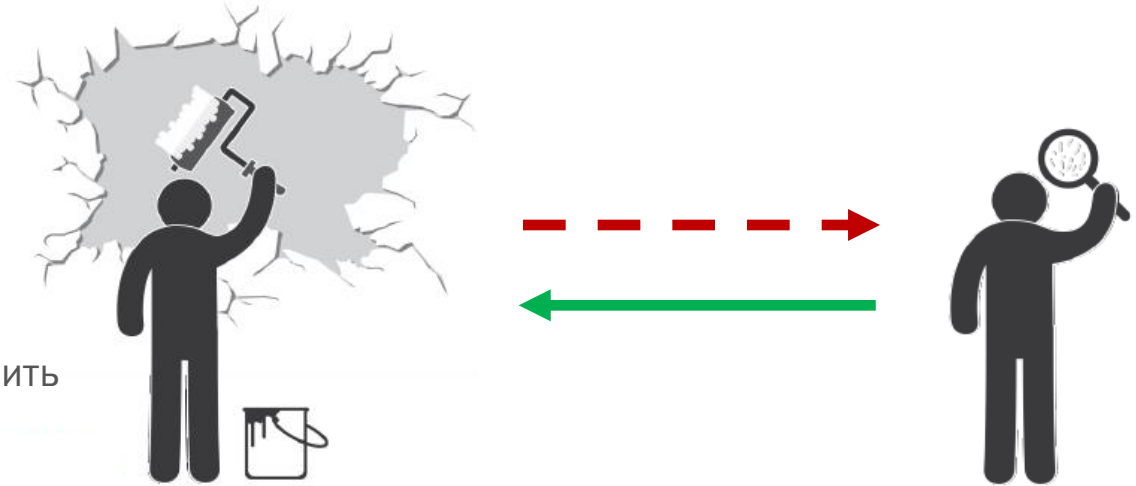


Вектора угроз | Сбор данных | Анализ данных | Приоритезация | Реагирование

KASPERSKY lab

ОБУЧЕНИЕ РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

- Семинар по расследованию инцидентов
- Тренинги ЛК



Быстро восстановить системы

Расследовать как инцидент произошел

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

АДАПТИВНАЯ МОДЕЛЬ ПРОТИВОДЕЙСТВИЯ ПЕРЕДОВЫМ УГРОЗАМ ИБ

ПРОГНОЗИРОВАНИЕ

Управление уязвимостями

Анализ потенциальных целей атакующего

Планирование развития стратегии защиты

ПРЕДОТВРАЩЕНИЕ

Снижение рисков проникновения

Повышение безопасности систем и процессов

РЕАГИРОВАНИЕ

Оперативное реагирование на инциденты

Расследование:

- реконструкция атак
- поиск затронутых активов

ОБНАРУЖЕНИЕ

Выявление попыток и фактов существующего проникновения

Подтверждение и приоритезация событий

СТРАТЕГИЯ АДАПТИВНОЙ КОРПОРАТИВНОЙ ИБ

ПРОГНОЗИРОВАНИЕ

САМОАНАЛИЗ:

- Penetration testing service
- Security assessment service
- Targeted Attack Discovery Service

ПРЕДОТВРАЩЕНИЕ

ОБУЧЕНИЕ:

- Cybersecurity training

ЗАЩИТА:

- Kaspersky Lab Enterprise security solutions

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ:

- Cyber safety Games
- Threat simulation

ОБНАРУЖЕНИЕ

ЭКСПЕРТИЗА:

- Targeted Attack Investigation Training

ЛАНДШАФТ УГРОЗ:

- APT reporting
- Botnet tracking
- Threat data feeds

РЕШЕНИЕ:

- Kaspersky Anti Targeted Attack Platform

РЕАГИРОВАНИЕ

РАССЛЕДОВАНИЕ:

- Incident response service
- Malware analysis service
- Digital forensics services

ВОПРОСЫ?

Владимир Даниленко
Менеджер по сопровождению
корпоративных продаж
Enterprise Security Division

Vladimir.Danilenko@kaspersky.com
D: +7 495 797 87 00 x2092

KASPERSKY lab