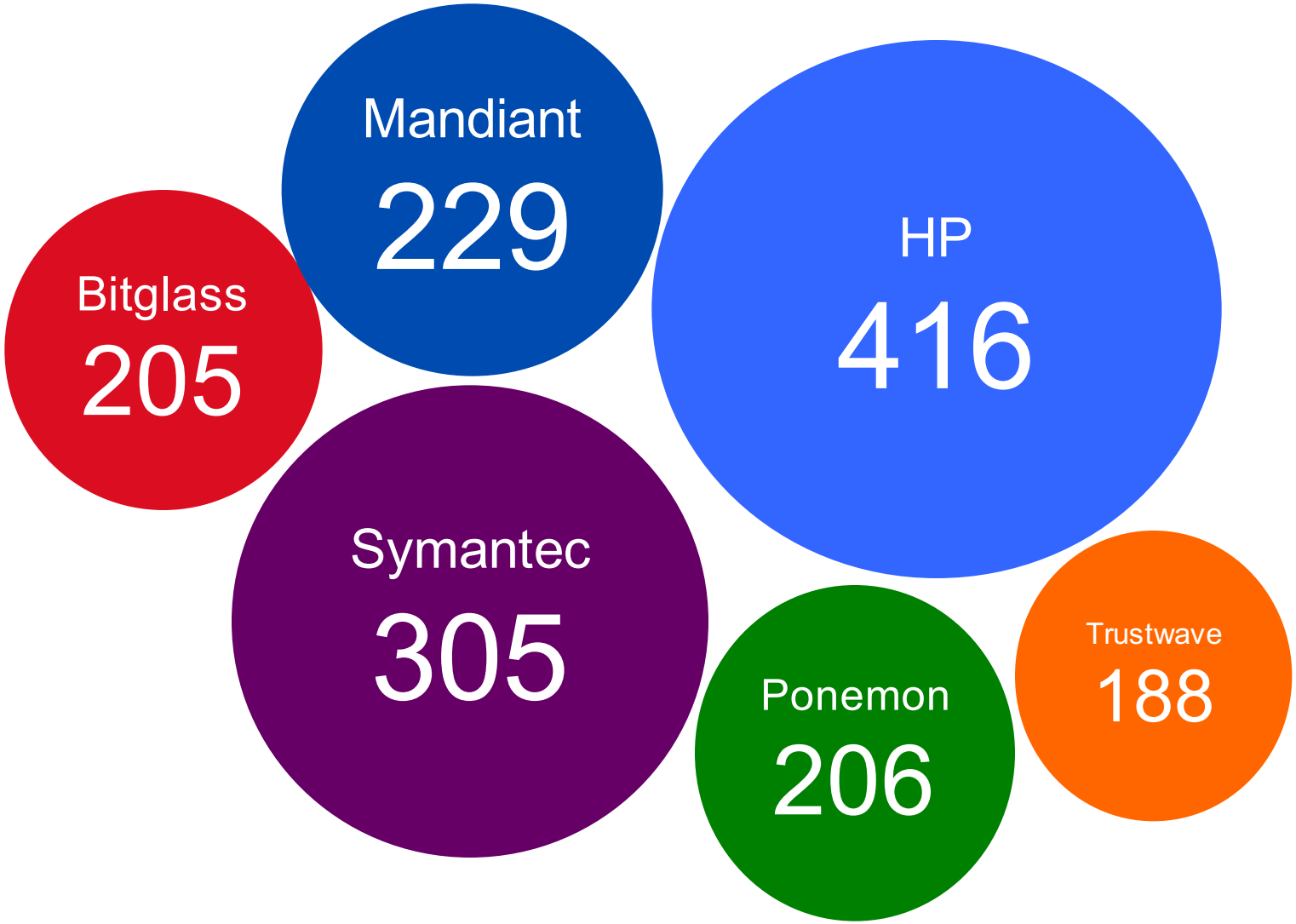
Аналитика угроз и противодействие вредоносному программному коду

Павел Родионов
Cisco CSE Security

18 мая 2016

Как хакеры зарабатывают деньги?

Время обнаружения вторжений очень велико



Один пример: эксплойт-кит Angler

Постоянные обновления увеличили уровень проникновения Angler до 40%

В два раза эффективнее, чем другие exploit kits в 2014

Теневая инфраструктура устойчива и скрытна

Базовая инфраструктура Angler

15000

Уникальных сайтов, перенаправляющих на Angler

99,8%

из них использовались менее 10 раз

Rombertik

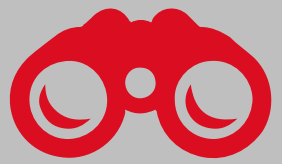
Вредоносное ПО эволюционирует не только в сторону кражи данных — если его обнаруживают и пытаются воздействовать на него, он может уничтожить зараженную систему.

Анти-анализ

Получение доступа

- Спам
- Фишинг
- Социальный инжиниринг

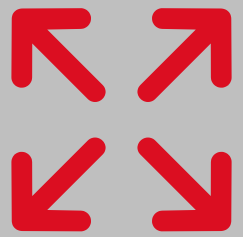
Стойкость



Уход от обнаружения

- Записать случайные данные в память 960 миллионов раз
- Засорение памяти в песочнице

Вредоносное поведение



Украсть данные пользователя

- Доставка данных пользователя обратно злоумышленникам
- Кража любых данных, а не только банковских

Уничтожение если обнаружено

- Уничтожение MBR
- После перезагрузки компьютер перестает работать

Обход «песочниц»

Вредоносное ПО эволюционирует в сторону защиты от исследования в песочницах, где вредоносный код запускается и анализируется. Данные методы не новы, но в 2015-м году они стали применяться все чаще.

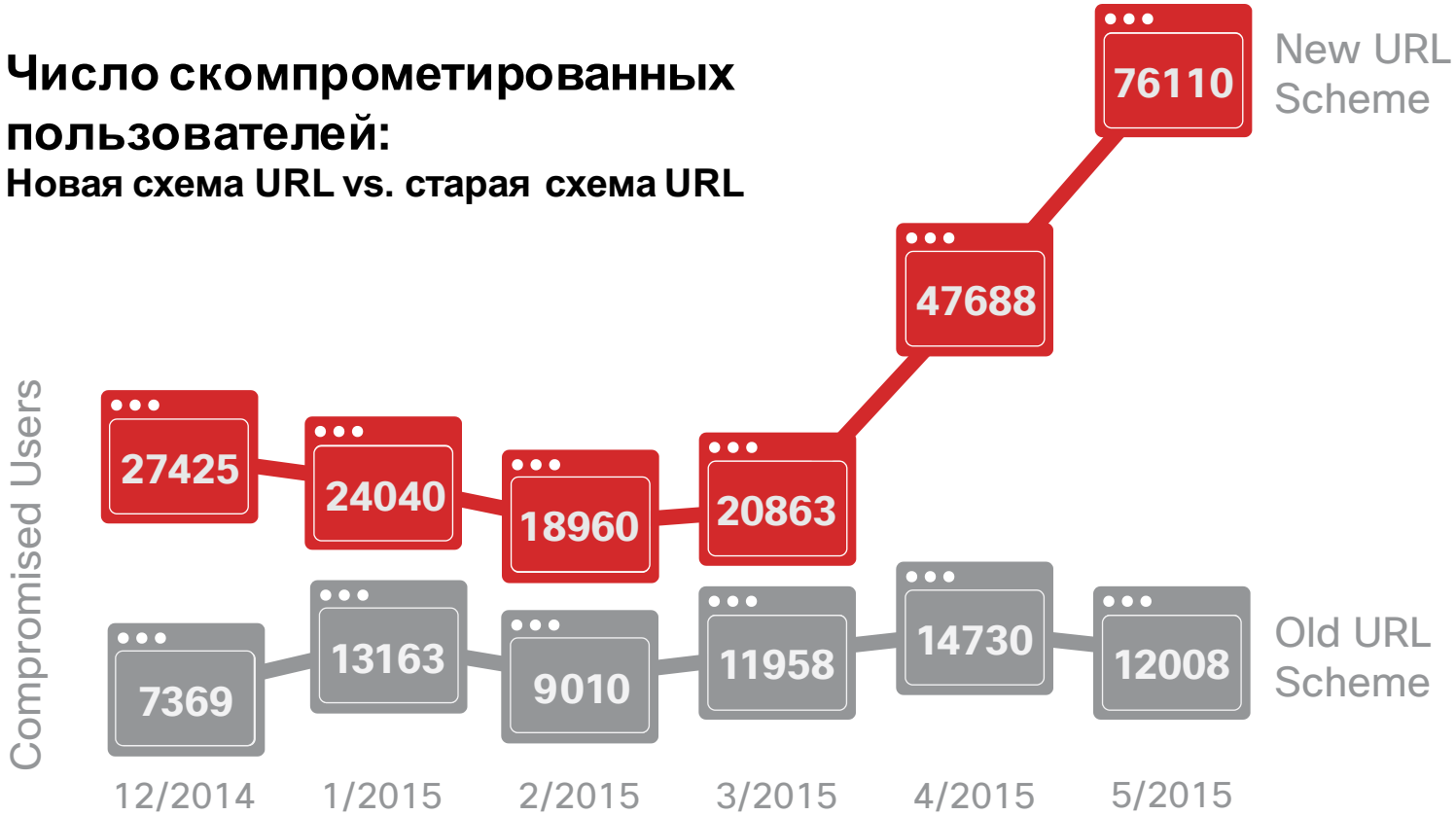
Постоянная модификация вредоносного кода

Adware MultiPlug использует собственную схему кодирования URL для обхода обнаружения, тем самым увеличивая «эффективность» по отношению к скомпрометированным пользователям

Изменение домена – раз в 3 месяца (уже 500 доменов)

Непрерывное изменение имен Add-On для браузера (уже 4000 имен)

Число скомпрометированных пользователей:
Новая схема URL vs. старая схема URL



Эволюция вымогателей: Цель – данные, а не системы

Фокусировка вымогателей – редкие языки (например, исландский) или группы пользователей (например, онлайн-геймеры)

Личные файлы

Финансовые данные

TOR

Вымогатели теперь полностью автоматизированы и работают через анонимные сети

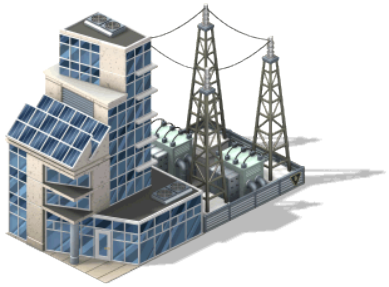
Фото

Email

$300-$500

Злоумышленники провели собственное исследование идеальной точки цены. Сумма выкупа не чрезмерна

Наша реальность! Кибератаки в Украине



Май 2014

Атака на предприятия Укрзалізниці

Август 2014

Blackenergy 0-Day атака на широкий спектр органов госвласти в Украине

Октябрь 2015

Blackenergy атака на медиакомпании. Уничтожение видеоматериалов, вывод из строя рабочих мест операторов

Декабрь 2015

Blackenergy атака на ряд облэнерго. Вывод из строя АСУТП электроподстанций, обесточена значительная территория на несколько часов

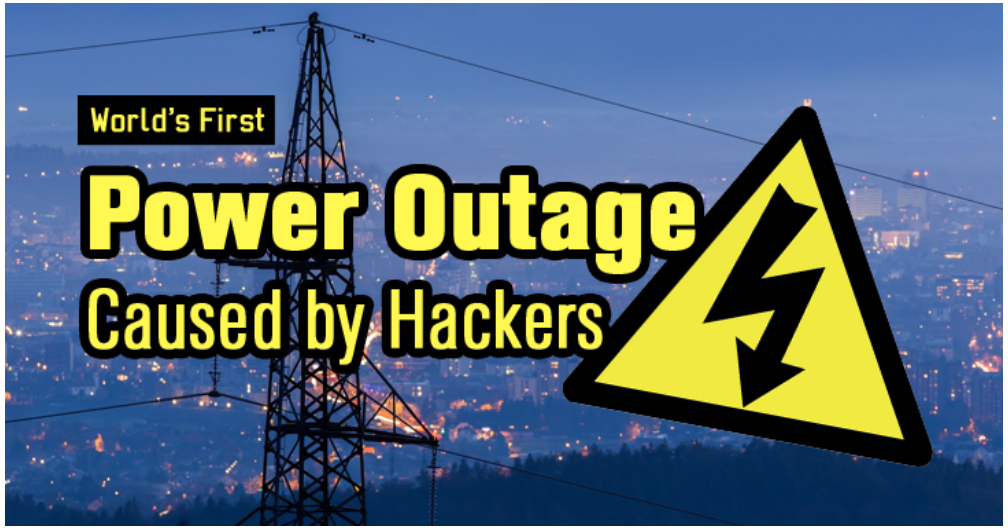
Декабрь 2015

Атака на АП Борисполь при помощи BlackEnergy

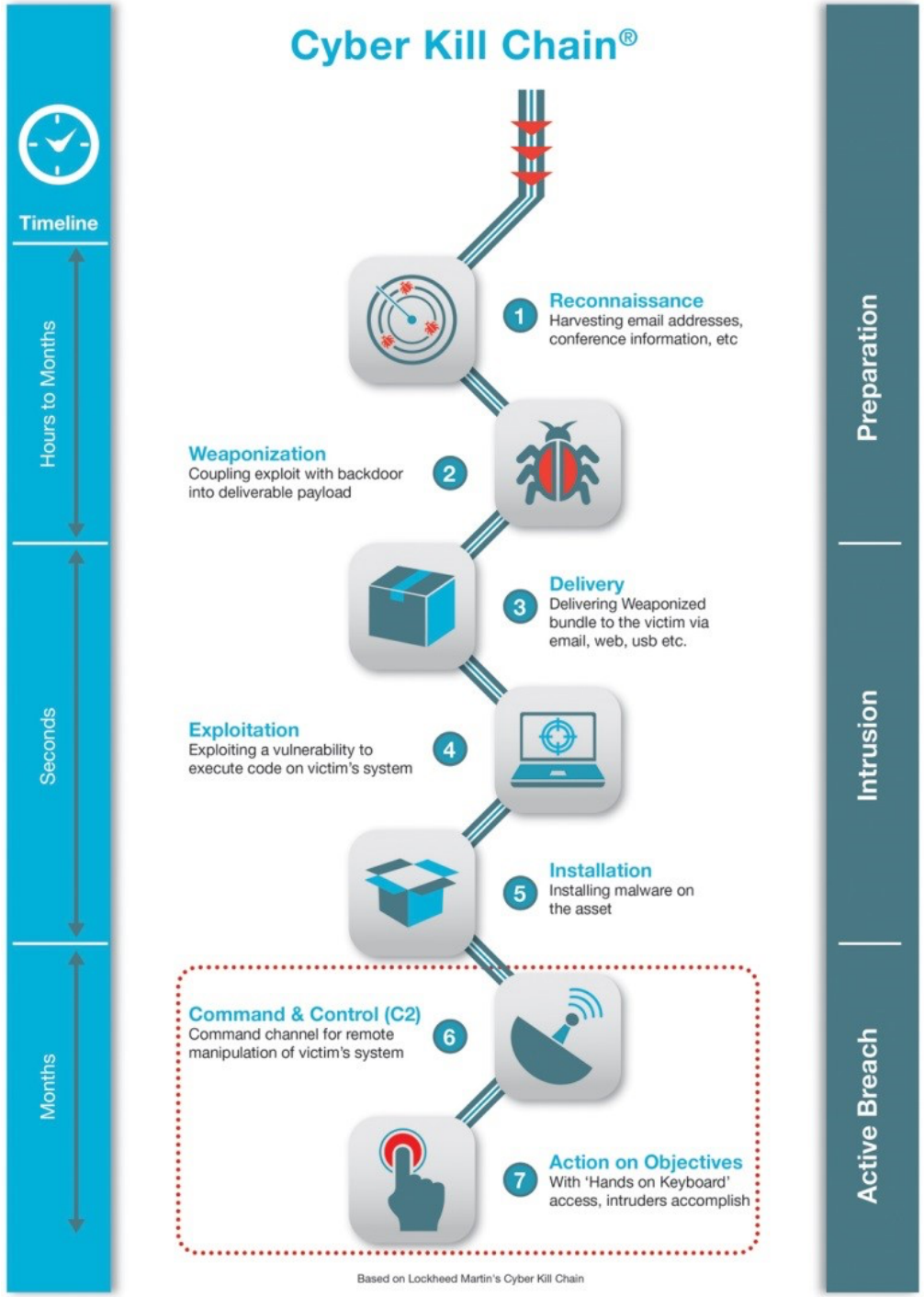
Time

Кибератаки в Украине

- Перед атакой следует стадия рекогносцировки
  - производится анализ email адресов компании, формирование соответствующих образом созданных писем, чтобы пользователь их открыл
- Атака включает рассылку электронных писем с вредоносным содержимым, который не обнаруживается традиционными средствами защиты
- Для включения базовых механизмов безопасности часто даже не надо менять оборудование
  - SPF, DKIM, DMARC, NIST 800-177 (общее описание)

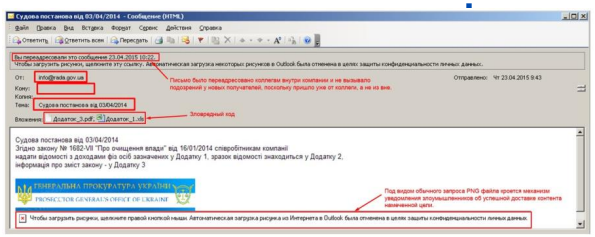


Cyber KillChain



Типичная атака. Starlight Media

1 Фишинговое письмо



2 Действия пользователя

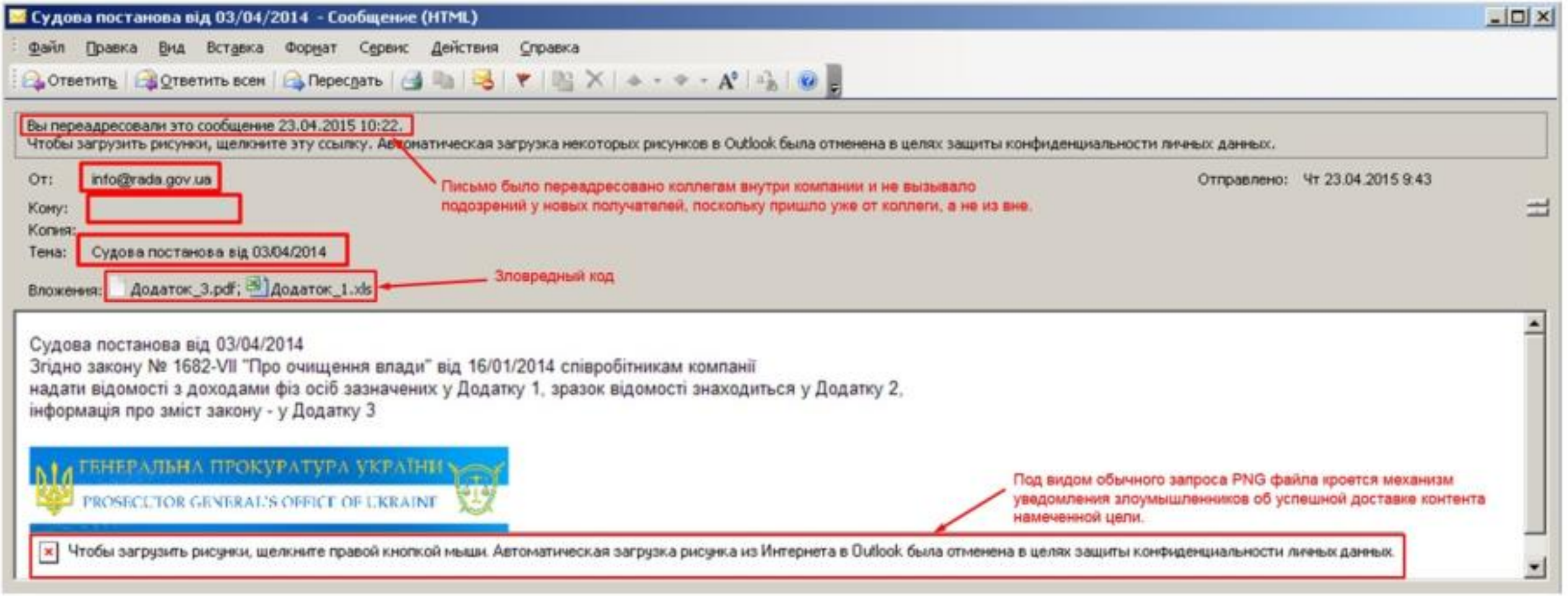
3 Эксплоит, загрузка основного тела, распространение

4 Вызов, CnC, дополнительный инструмент

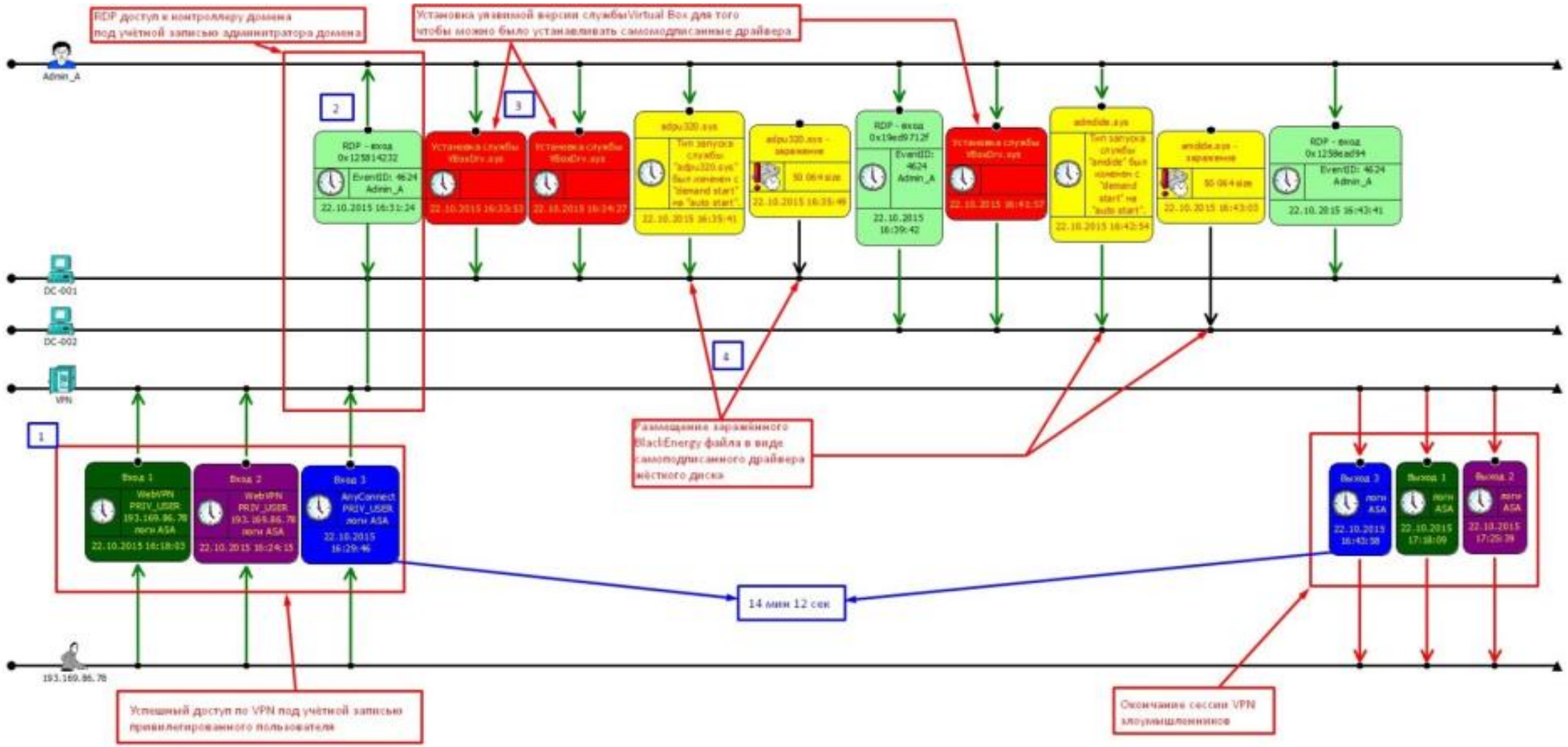
5 Распространение по сети

6 Хищение данных, ботнет, удаление…

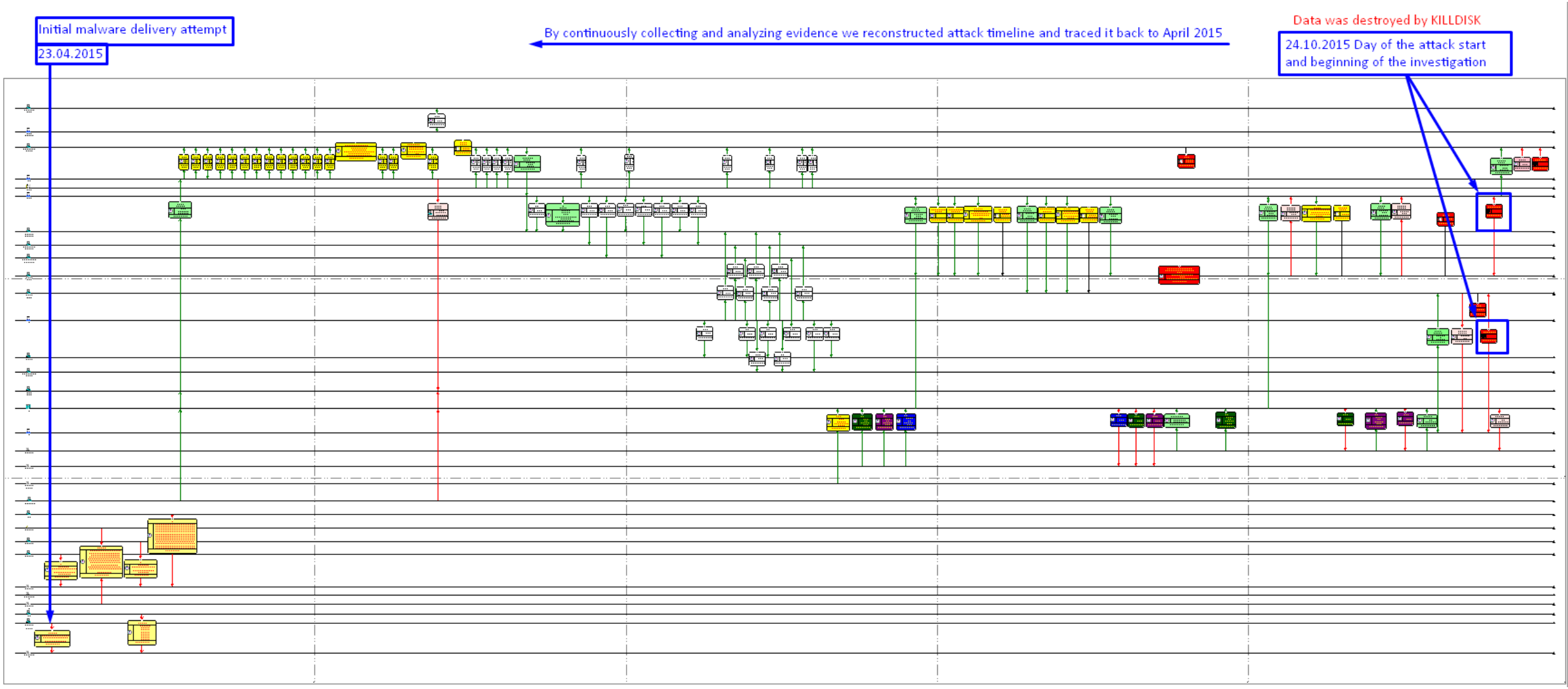
То самое письмо!



14 минут на установку инструментов



Продолжительность атаки и этапы её расследования

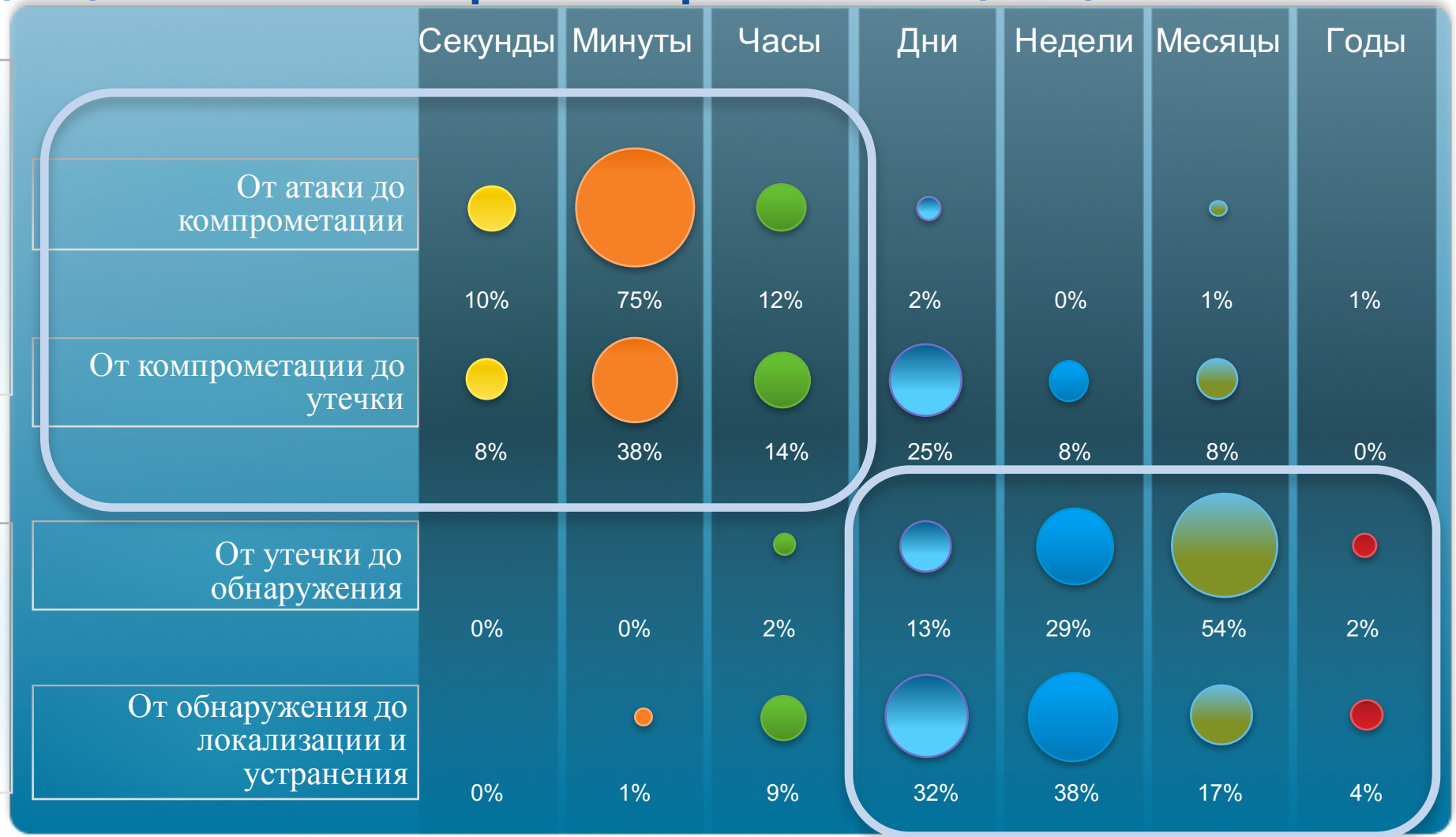


В центре внимания Cisco – анализ угроз

Почему традиционный периметр не защищает?

Взломы осуществляются за минуты

Обнаружение и устранение занимает недели и месяцы



А это подтверждение статистики

16 апреля 2015 года http://www.zdnet.com/article/palo-alto-networks-mcafee-websense-gateway-systems-allow-malicious-traffic-to-slip-through-the-net/

Дело COBCEM не в названиях компаний, проблема в методологии

В центре внимания Cisco — анализ угроз!

Приобретение компании Sourcefire Security

- Ведущие в отрасли СОПВ нового поколения
- Мониторинг сетевой активности
- Advanced Malware Protection
- Разработки отдела по исследованию уязвимостей (VRT)
- Инновации в ПО с открытым исходным кодом (технология OpenAppID)

Коллективные исследования Cisco – подразделение Talos по исследованию и анализу угроз

- Подразделение Sourcefire по исследованию уязвимостей — VRT
- Подразделене Cisco по исследованию и информированию об угрозах — TRAC
- Подразделение Cisco по безопасности приложений — SecApps

Приобретение компании Lancope

- Исследования угроз

AMP + FirePOWER
AMP > управляемая защита от угроз

Cognitive + AMP

Коллективный анализ вредоносного кода > Система коллективной информационной безопасности

Приобретение компании Cognitive Security

- Передовая служба исследований
- Улучшенные технологии поведенческого анализа в режиме реального времени

Приобретение компании ThreatGRID

- Коллективный анализ вредоносного кода
- Анализ угроз
- «Песочница»

Приобретение компании OpenDNS

- Анализ DNS/IP-трафика
- Анализ угроз

Гипотезы безопасности Cisco

Цифровая эволюция

+

Операционный фокус

+

Нехватка людей

Требуются изменения в ИБ

Видимость

Знание угроз

Платформы

Консалтинг

Интеграция

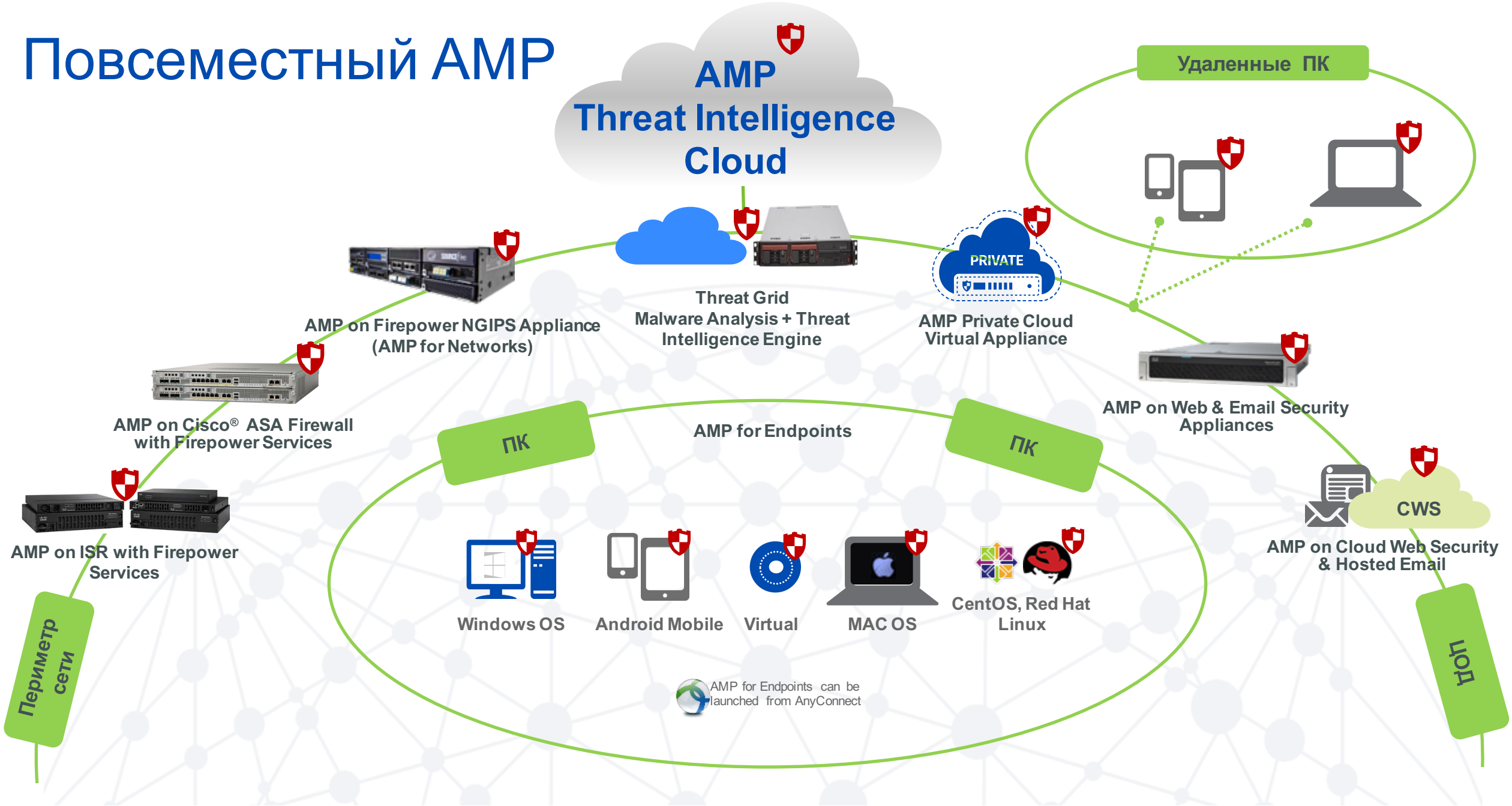
Управление

Cisco Advanced Malware Protection

Что мы знаем о современном вредоносном ПО?

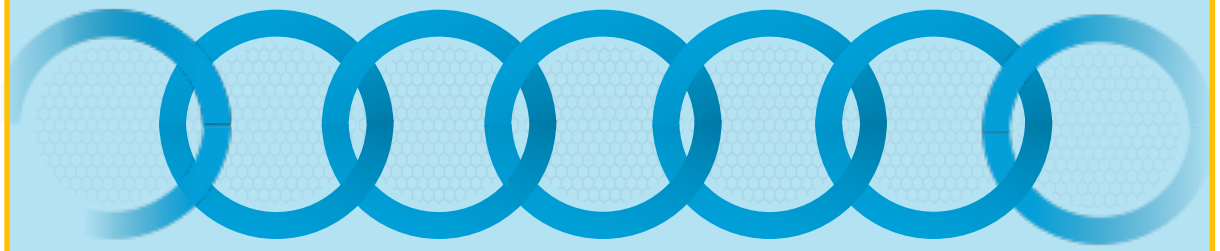
- Сложные программные продукты, созданные квалифицированными программистами и архитекторами (НЕ ОДИН .EXE файл, НЕ ОДИН вектор атаки)
- Высокий уровень доработки продуктов для очередной кампании
- Дропперы и даунлоудеры и иже с ними: внедрение одного модуля на 99% приведёт к внедрению следующих уникальных модулей
- Известно, что вредоносное ПО будут искать
- Известно про запуск в песочницах
- Развитая индустрия создания специфического ПО с неплохими бюджетами и высоким уровнем заинтересованности
- Все лучшие методологии разработки и отладки

Повсеместный AMP



Cisco AMP расширяет защиту NGFW и NGIPS

Точечное обнаружение



Репутация файла и анализ его поведения

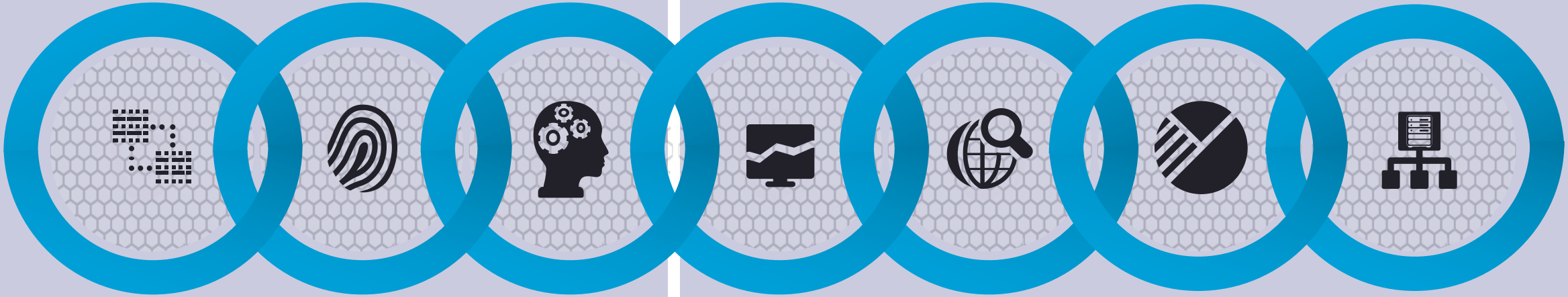
Ретроспективная безопасность

Непрерывная и постоянная защита

Cisco AMP защищает с помощью репутационной фильтрации и поведенческого анализа файлов

Фильтрация по репутации

Поведенческое обнаружение



Идентичная сигнатура

Нечеткие идентифицирующие метки

Машинное обучение

Признаки компрометации

Динамический анализ

Расширенная аналитика

Сопоставление потоков устройств

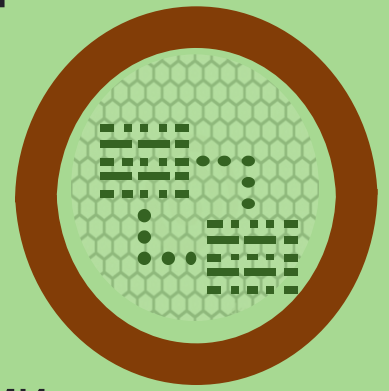
Фильтрация по репутации основывается на трех функциях

1. Сигнатура неизвестного файла анализируется и отправляется в облако
2. Сигнатура файла признана не вредоносной и принята
3. Сигнатура неизвестного файла анализируется и отправляется в облако
4. Известно, что сигнатура файла является вредоносной; ей запрещается доступ в систему

Техника: точные сигнатуры

- Так действуют традиционные антивирусы
- Отпечаток файла снимается с помощью SHA256 и отправляется в облако для сравнения с базой сигнатур
- Сам файл не отправляется в облако
- Быстро и аккуратно обнаруживается угроза
- Снижение нагрузки на другие механизмы обнаружения

Сигнатуры («точные»):
Очень простой подход, который наверняка реализован в любом решении любого поставщика

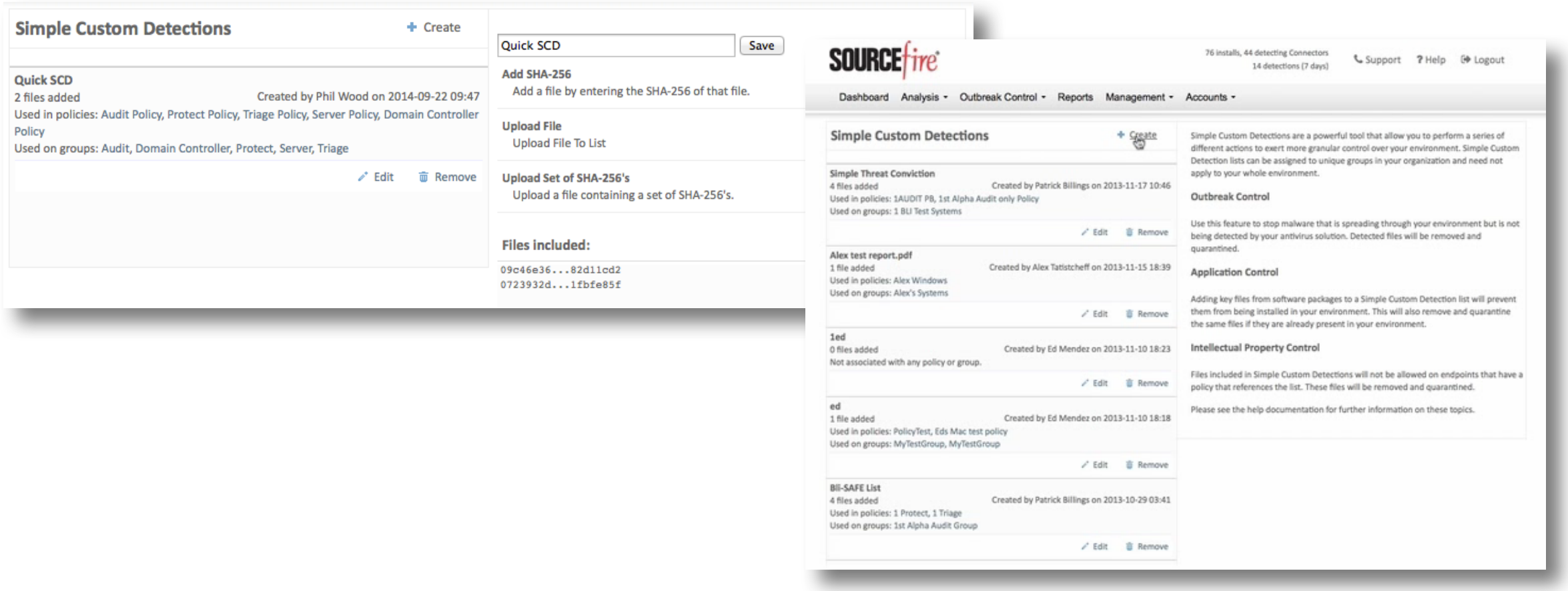


Точное соответствие файлу

Очень легко обходится простыми модификациями с файлом ☹

Возможность создания собственных сигнатур

- Создание собственных сигнатур, например, для контроля перемещения файлов с конфиденциальной информацией или полученных из внешних источников семплов вредоносного кода или даже приложений (для NGFW/NGIPS)



Фильтрация по репутации основывается на трех функциях

1. Сигнатура файла анализируется и определяется как вредоносная
2. Доступ вредоносному файлу запрещен
3. Полиморфная модификация того же файла пытается получить доступ в систему
4. Сигнатуры двух файлов сравниваются и оказываются аналогичными
5. Доступ полиморфной модификации запрещен на основании его сходства с известным вредоносным ПО

Техника: ядро Ethos

- ETHOS - ядро формирования нечетких отпечатков с помощью статической/пассивной эвристики
- Полиморфные варианты угрозы часто имеют общие структурные свойства
- Не всегда нужно анализировать все содержимое бинарного файла
- Повышение масштабируемости - обнаруживается и оригинал и модификации
- Традиционно создаются вручную

  Лучшие аналитики = несколько общих сигнатур в день
- У нас полная автоматизация = МАСШТАБИРОВАНИЕ

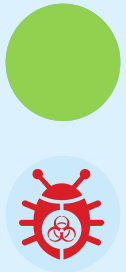
Ethos: создание обобщенных сигнатур, что опять же достаточно традиционно для отрасли

Адресуются семейства вредоносного кода

Потенциальное увеличение числа ложных срабатываний

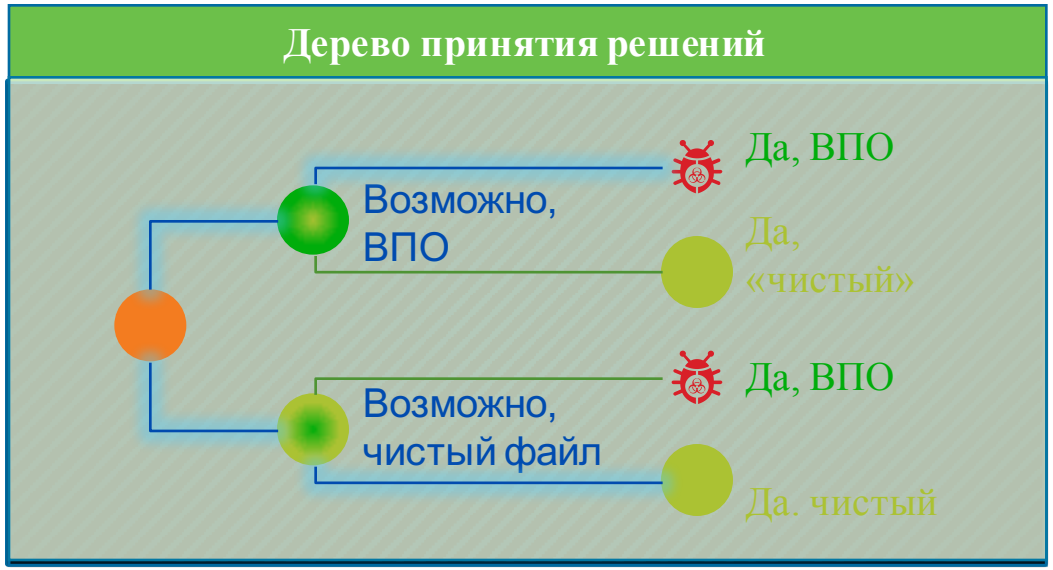
Фильтрация по репутации основывается на трех функциях

1	Метаданные неизвестного файла отправляются в облако для анализа
2	Метаданные признаются потенциально вредоносными
3	Файл сравнивается с известным вредоносным ПО и подтверждается как вредоносный
4	Метаданные второго неизвестного файла отправляются в облако для анализа
5	Метаданные аналогичны известному безопасному файлу, потенциально безопасны
6	Файл подтверждается как безопасный после сравнения с аналогичным безопасным файлом



Техника: ядро Spero

- Метки AMP = более 400 атрибутов, полученных в процессе выполнения
  - Сетевые подключения?
  - Нестандартные протоколы?
  - Использование интерфейсов API (каких)?
  - Изменения в файловой системе?
    - Самокопирование
    - Самоперенос
  - Запуск других процессов?
- Автоматизирует классификацию файлов на основе общих схожих признаков



- Машинное обучение позволяет находить и классифицировать то, что не под силу человеку – из-за возможности анализа больших объемов данных

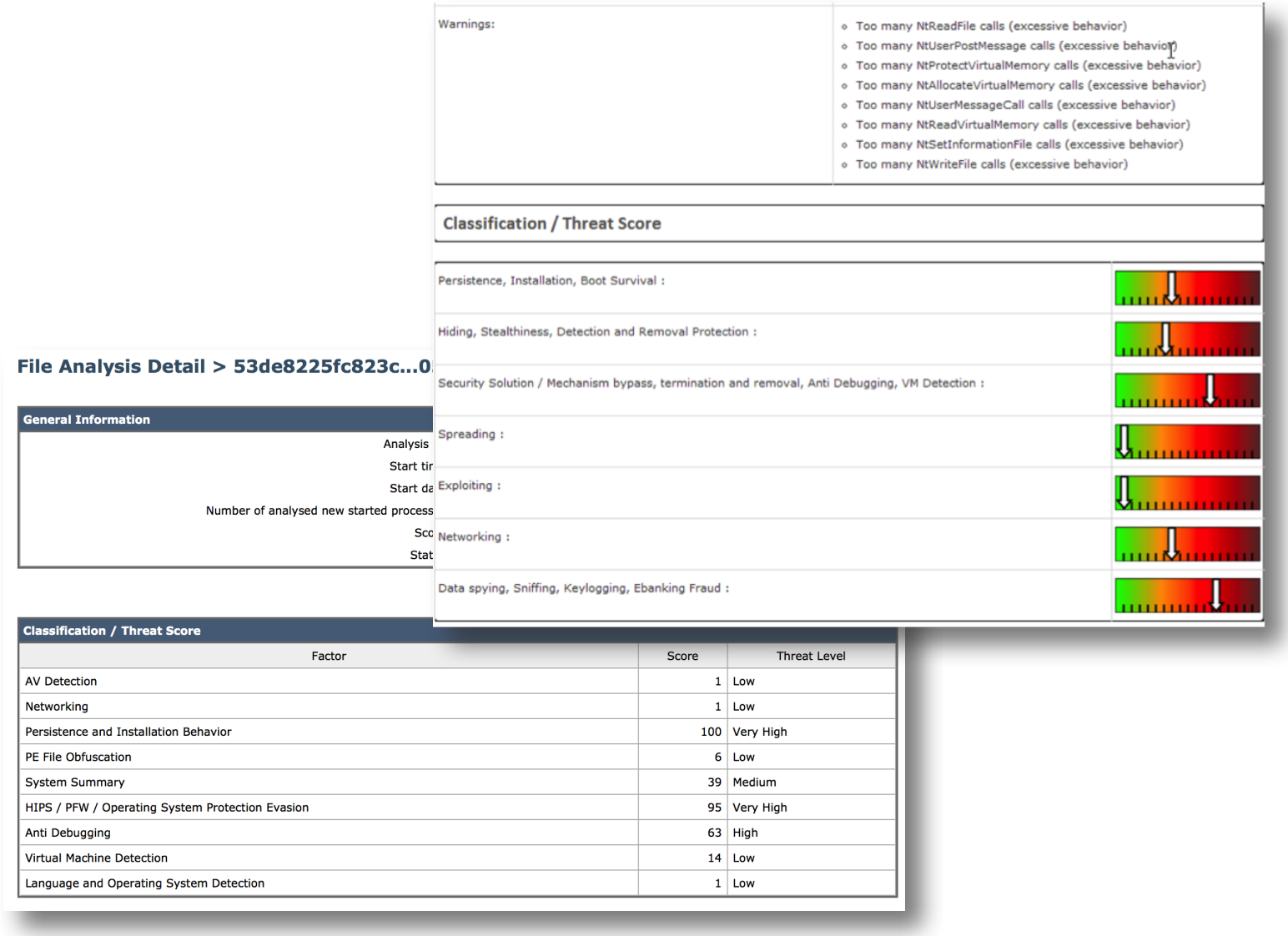
Поведенческое обнаружение основывается на четырех функциях

1. Неизвестный файл проанализирован, обнаружены признаки саморазмножения
2. Эти признаки саморазмножения передаются в облако
3. Неизвестный файл также производит независимые внешние передачи
4. Это поведение также отправляется в облако
5. Об этих действиях сообщается пользователю для идентификации файла как потенциально вредоносного

Bad Guys

Техника: анализ вредоносных признаков

- Анализ поведения файла – большое количество анализируемых параметров
- Требует большего времени на анализ, чем сигнатуры
- Потенциально ложные срабатывания
- Подробная информация о причинах принятия того или иного решения
- Выдача финального Threat Score



Warnings:	Too many NtReadFile calls (excessive behavior) Too many NtUserPostMessage calls (excessive behavior) Too many NtProtectVirtualMemory calls (excessive behavior) Too many NtAllocateVirtualMemory calls (excessive behavior) Too many NtUserMessageCall calls (excessive behavior) Too many NtReadVirtualMemory calls (excessive behavior) Too many NtSetInformationFile calls (excessive behavior) Too many NtWriteFile calls (excessive behavior)

Classification / Threat Score

Persistence, Installation, Boot Survival :
Hiding, Stealthiness, Detection and Removal Protection :
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection :
Spreading :
Exploiting :
Networking :
Data spying, Sniffing, Keylogging, Ebanking Fraud :

File Analysis Detail > 53de8225fc823c...0

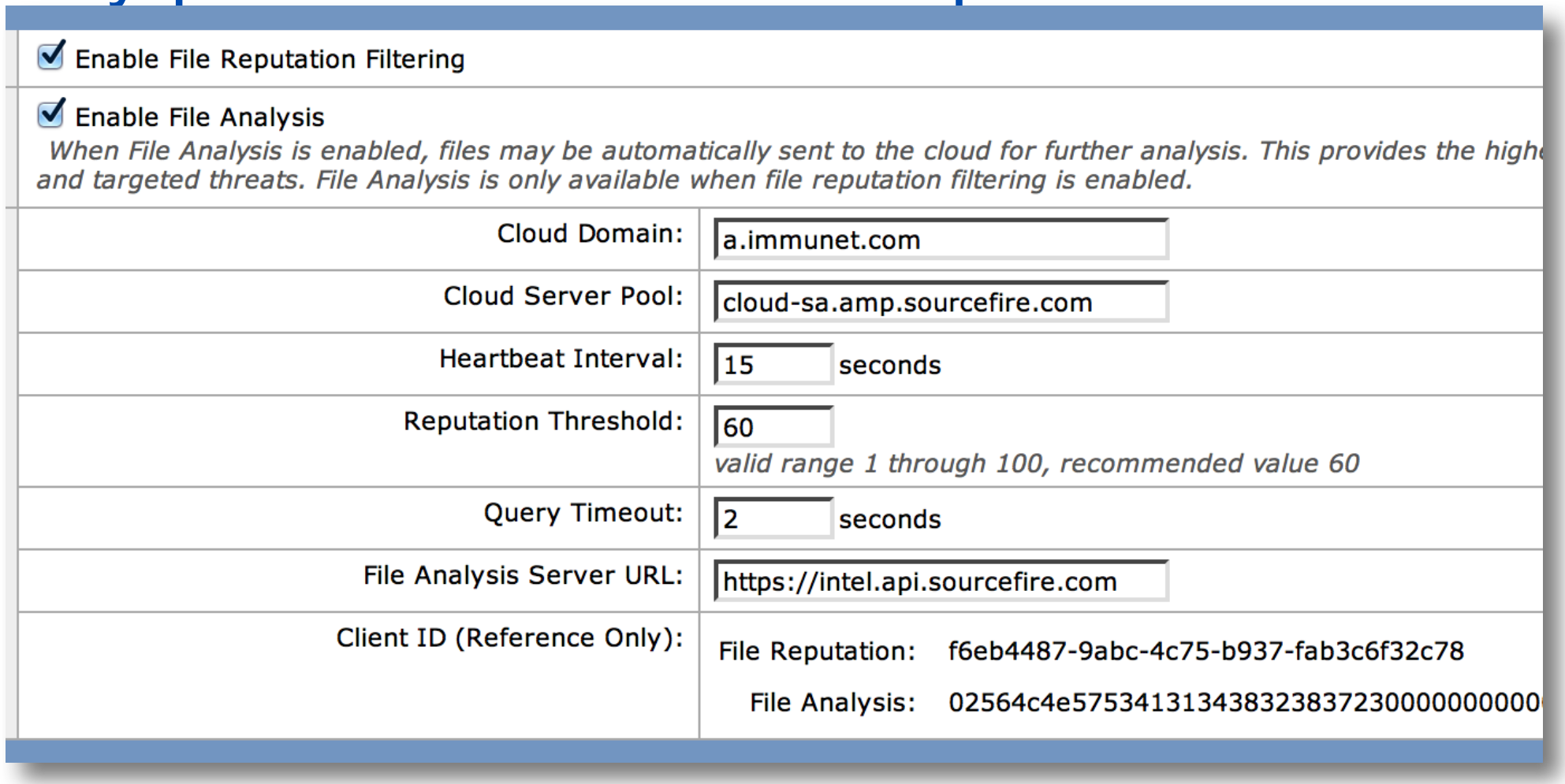
General Information

Analysis	
Start tir	
Start da	
Number of analysed new started process	
Sco	
Stat	

Classification / Threat Score

Factor	Score	Threat Level
AV Detection	1	Low
Networking	1	Low
Persistence and Installation Behavior	100	Very High
PE File Obfuscation	6	Low
System Summary	39	Medium
HIPS / PFW / Operating System Protection Evasion	95	Very High
Anti Debugging	63	High
Virtual Machine Detection	14	Low
Language and Operating System Detection	1	Low

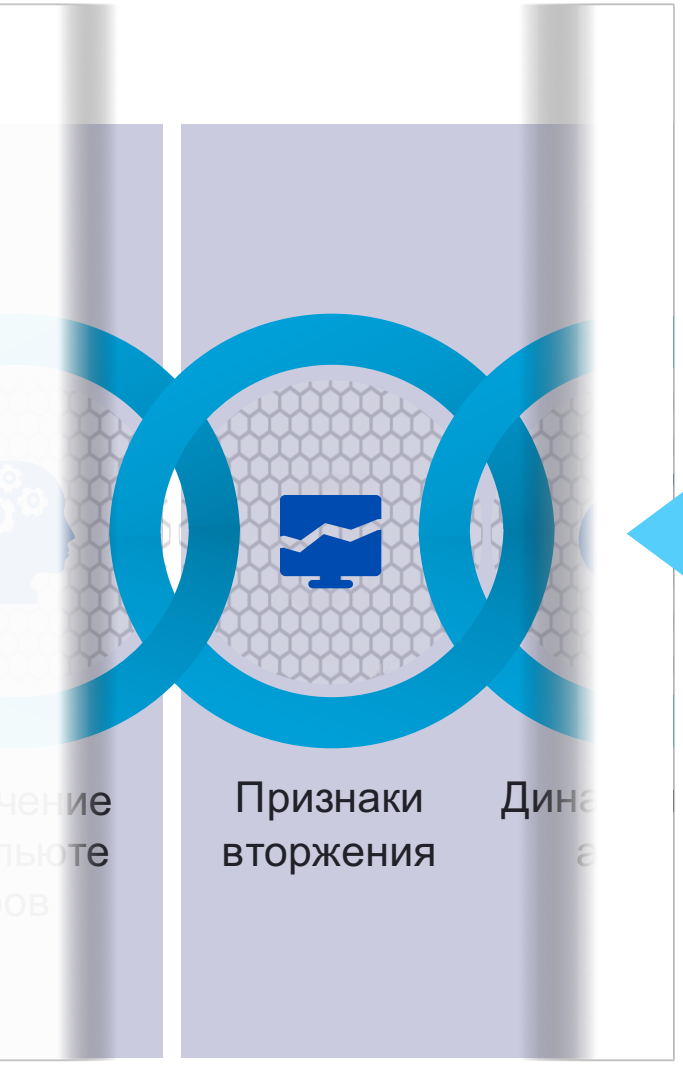
Уровень угрозы может быть настроен



На примере Cisco AMP for Content Security (WSA)

36

Поведенческое обнаружение основывается на четырех функциях



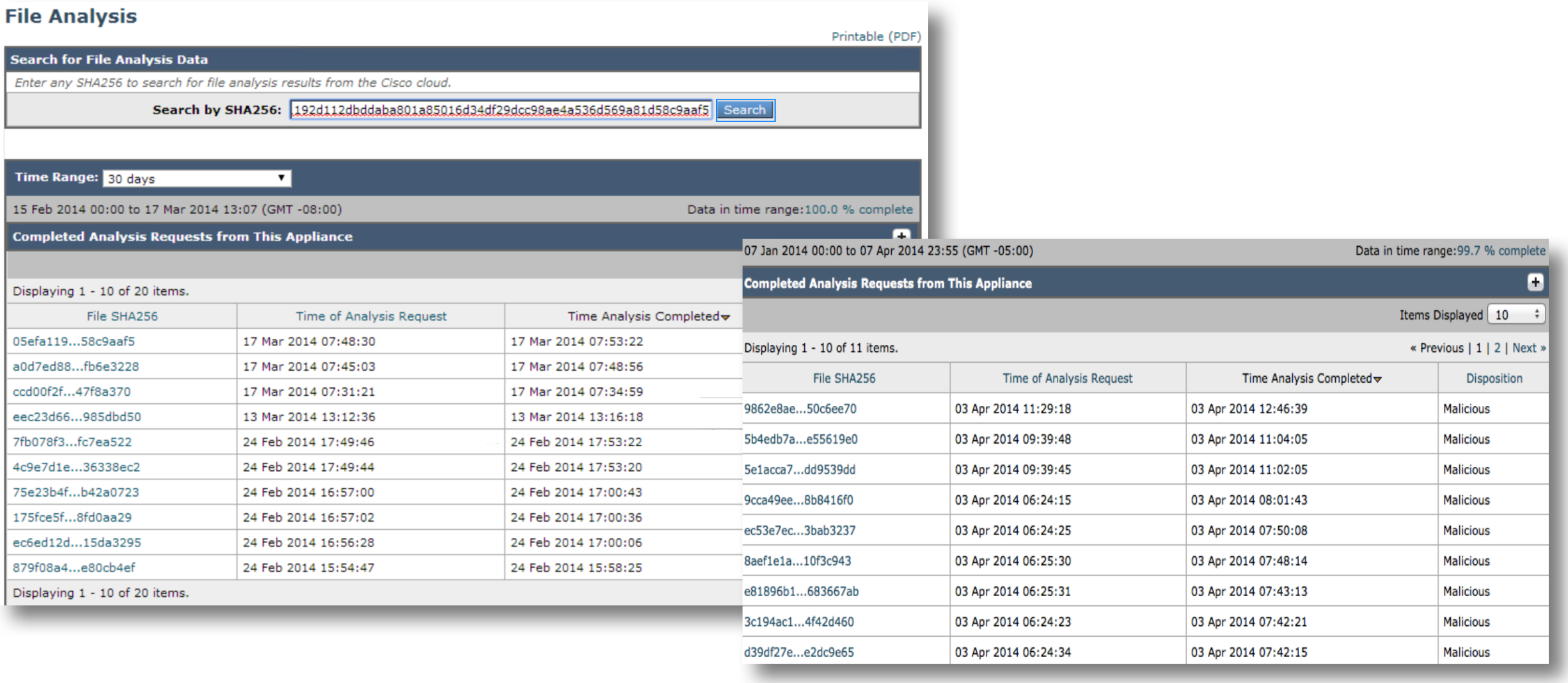
1. Неизвестные файлы загружаются в облако, где механизм динамического анализа запускает их в изолированной среде
2. Два файла определяются как вредоносные, один подтвержден как безопасный
3. Сигнатуры вредоносных файлов обновляются в облаке информации и добавляются в пользовательскую базу

Техника: динамический анализ

- Файлы для динамического анализа (песочница) могут быть загружены автоматически или в ручном режиме
- Загрузка файла осуществляется только в случае его неизвестности (неизвестен статус и Threat Score)

  «Чистые», уже проверенные ранее файлы или вредоносное ПО с вычисленным Threat Score в песочницу не загружаются, чтобы не снижать производительность решения
- Файлы можно загружать через прокси-сервера
- Результат представляется в виде обзора и детального анализа

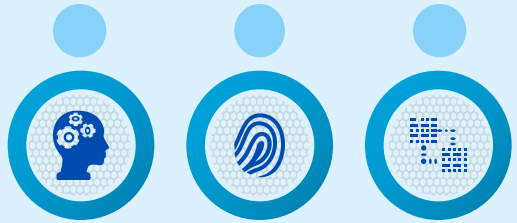
Анализ в облаке может занимать время



На примере Cisco AMP for Content Security (ESA)

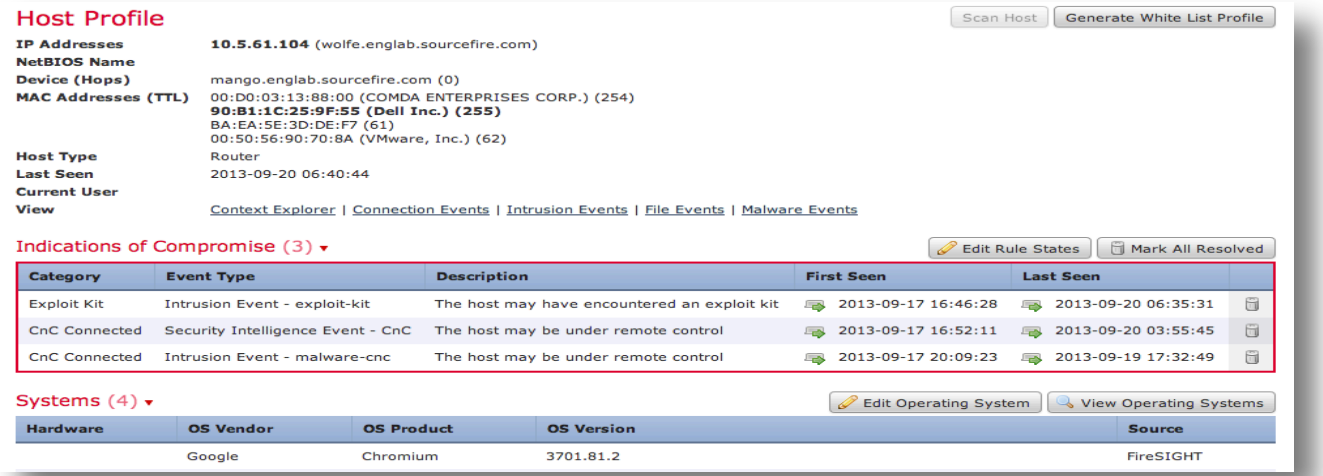
Поведенческое обнаружение основывается на четырех функциях

1. Получает информацию о неопознанном ПО от устройств фильтрации по репутации
2. Получает контекст для неизвестного ПО от коллективной пользовательской базы
3. Анализирует файл в свете полученной информации и контекста
4. Идентифицирует вредоносное ПО и добавляет новую сигнатуру в пользовательскую базу

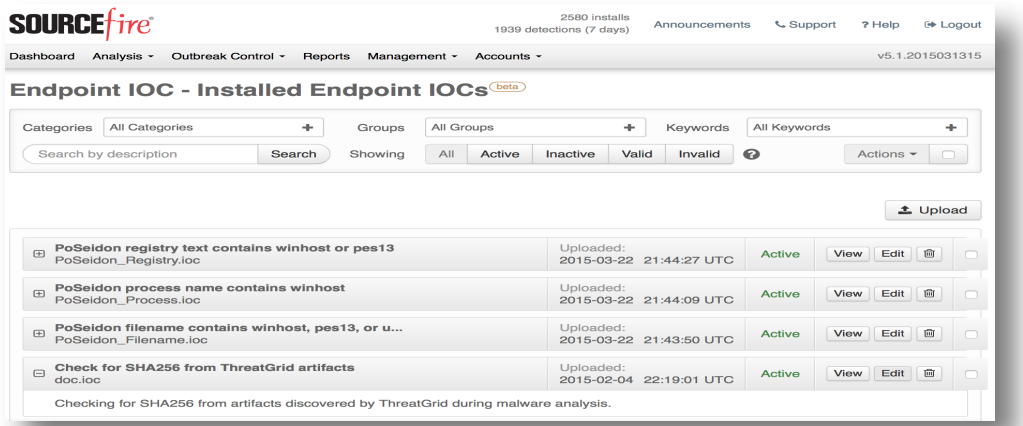


Индикаторы компрометации

- Индикатор компрометации – объединение нескольких связанных событий безопасности в единое мета-событие
- IOC “CNC Connected” (узел вероятно находится под чужим управлением)
  - Узел подключился к серверу C&C
  - Сработала система обнаружения вторжений по сигнатуре “Malware-CNC”
  - На узле запущено приложение, которое установило соединение с сервером C&C
- Встроенные и загружаемые индикаторы компрометации

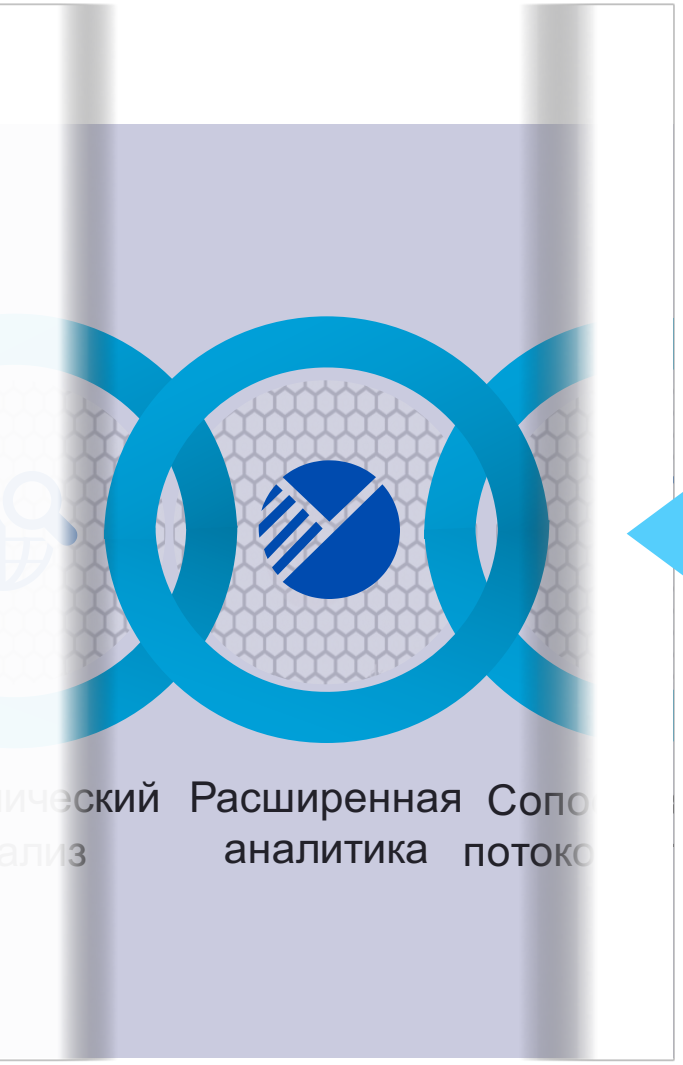


На примере Cisco AMP for Networks

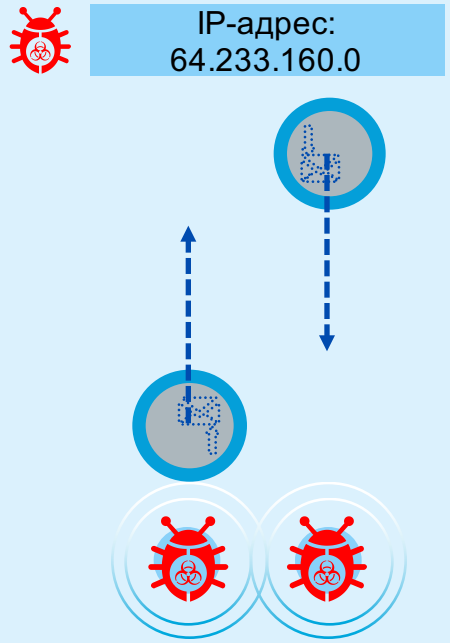


На примере Cisco AMP for Endpoint

Поведенческое обнаружение основывается на четырех функциях



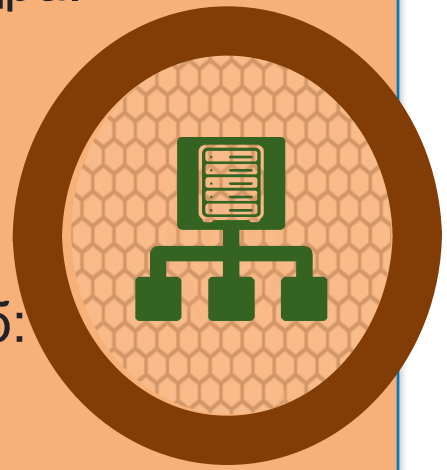
1. Сопоставление потоков устройств производит мониторинг источника и приемника входящего/исходящего трафика в сети
2. Обнаруживаются два неизвестных файла, связывающихся с определенным IP-адресом
3. Один передает информацию за пределы сети, другой получает команды с этого IP-адреса
4. Collective Security Intelligence Cloud распознает внешний IP-адрес как подтвержденный вредоносный сайт
5. Из-за этого неизвестные файлы идентифицируются как вредоносные



Техника: Анализ потоков данных с устройств

- Мониторятся внутренние и внешние сети
- Данные по репутации IP-адресов
- Регистрация URL / доменов
- Временные метки
- Передаваемые файлы

Корреляция потоков устройств: Анализ сетевых потоков на уровне ядра. Позволяет блокировать или предупреждать о любых сетевых действиях



В облаке есть информация об: известных серверах CnC, фишинговых сайтах, серверах ZeroAccess CnC, и т.д.

Пользовательские списки

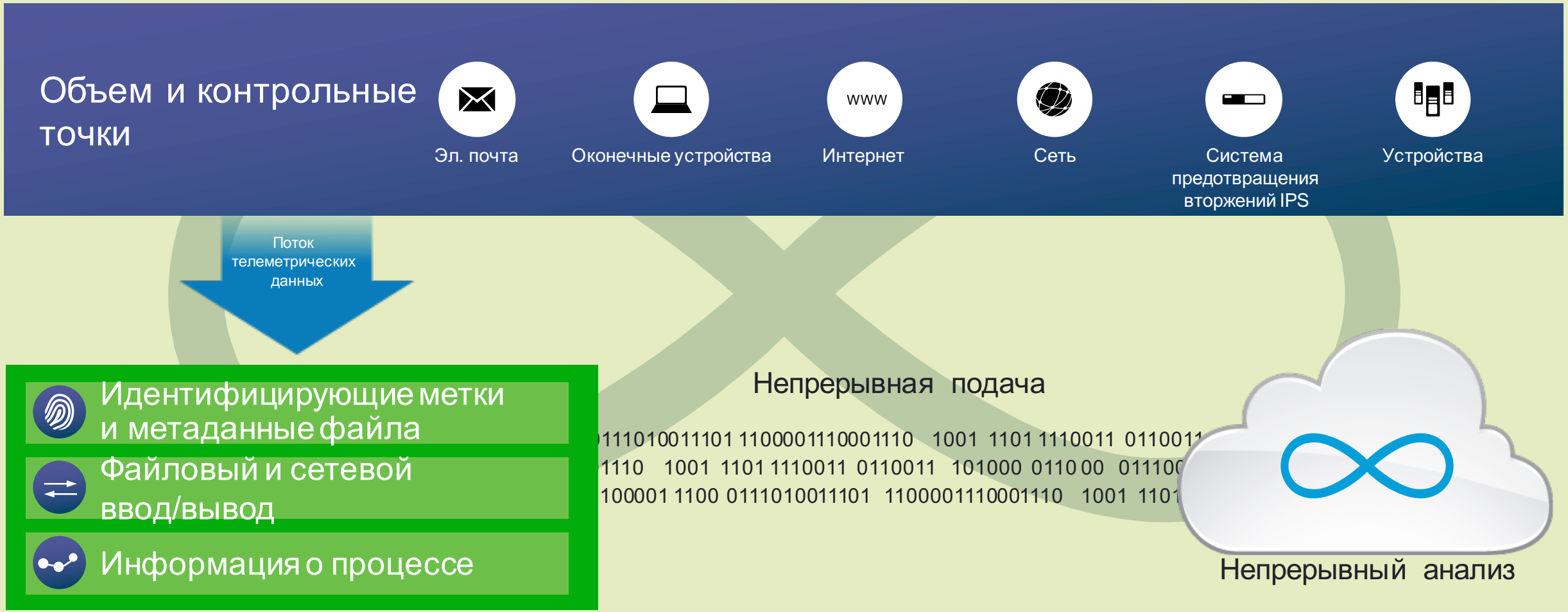
43

Сила в комбинации методов обнаружения

- На оконечных узлах не хватает ресурсов для анализа все усложняющегося вредоносного кода
- Не существует универсального метода обнаружения вредоносного кода – у каждого метода есть своя область применения, свою достоинства и недостатки
- Каждый метод может быть обойден вредоносным кодом; особенно специально подготовленным

7 методов обнаружения в Cisco AMP повышают эффективность защиты!!!

Почему необходима непрерывная защита?

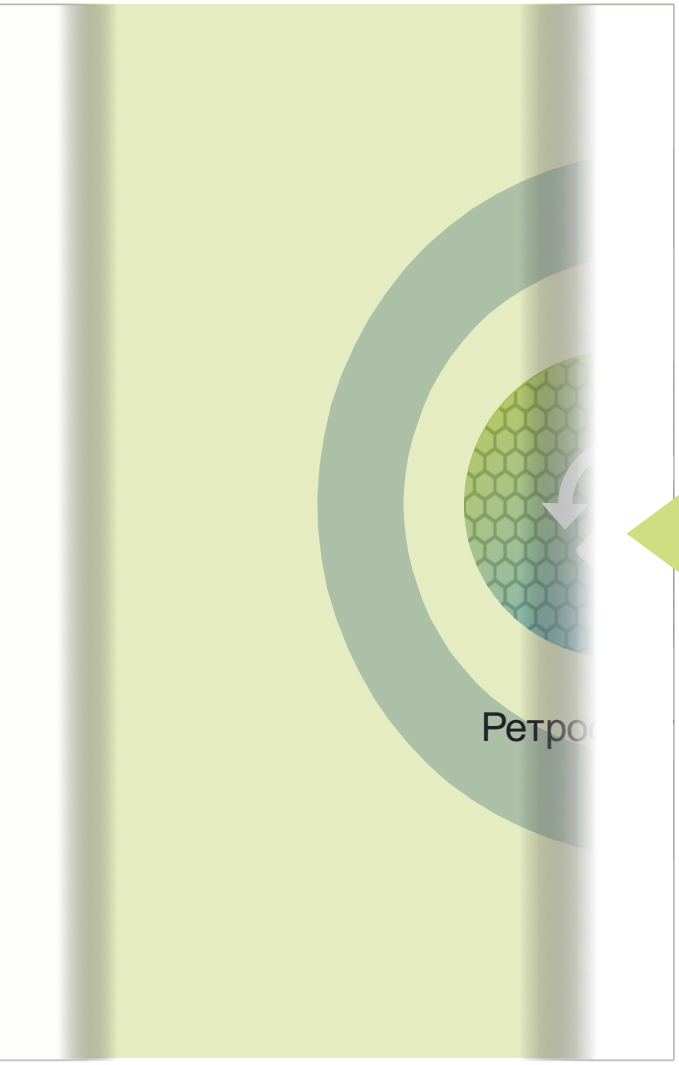


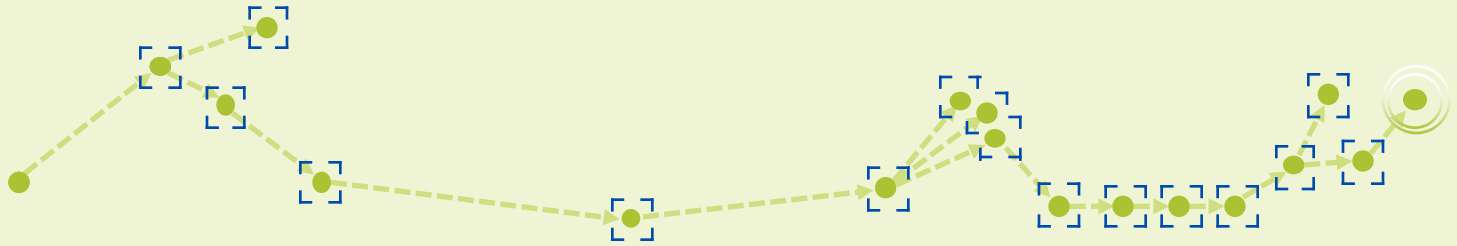
Почему необходима непрерывная защита?

Контекст | Применение | Непрерывный анализ

Cisco AMP обеспечивает ретроспективную защиту

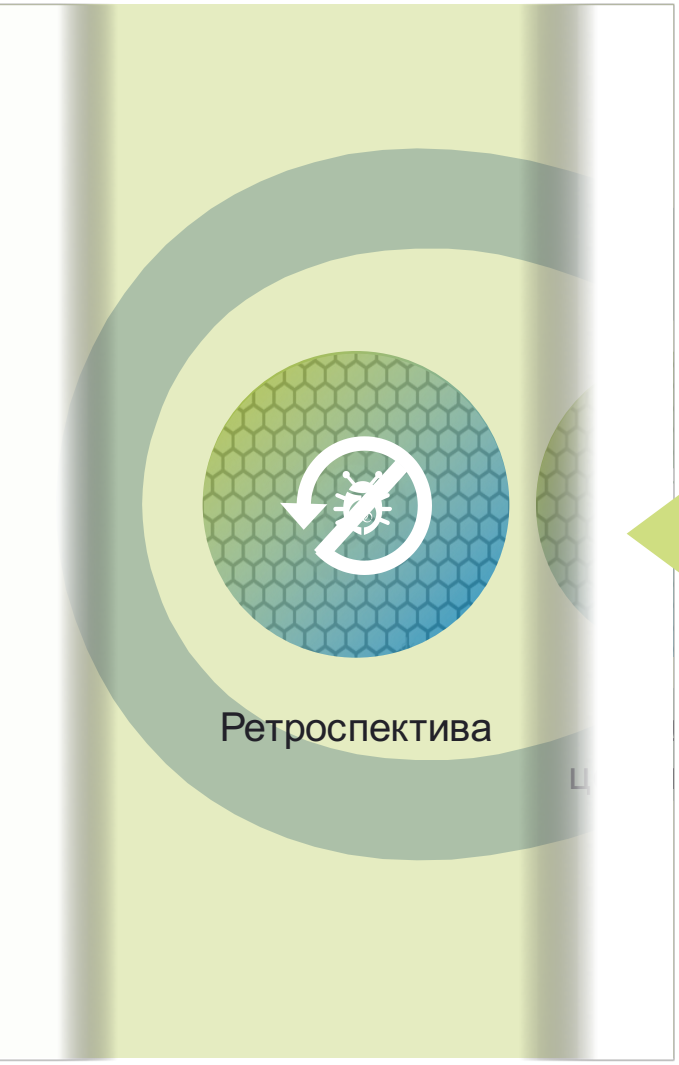
Ретроспективная безопасность основана на…





1	Выполняет анализ при первом обнаружении файлов
2	Постоянно анализирует файл с течением времени, чтобы видеть изменения ситуации
3	Обеспечивает контроль перемещений, действий или связей, касающихся конкретного элемента ПО

Ретроспективная безопасность основана на…

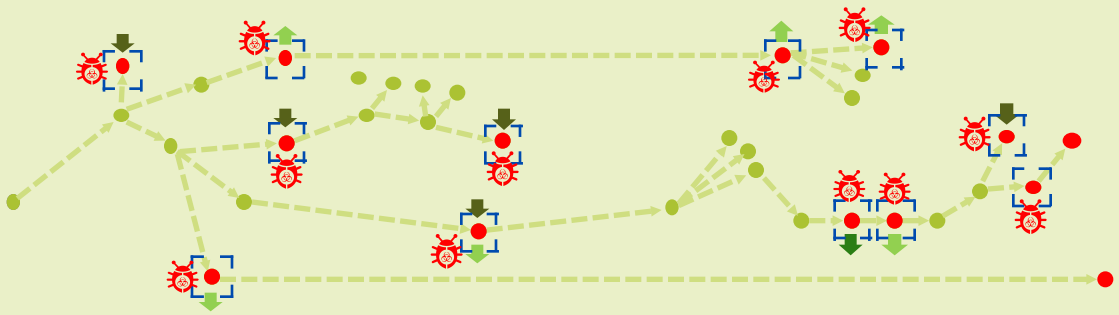


Использует ретроспективные возможности тремя способами:

1. Ретроспективный анализ файлов
2. Ретроспектива процесса
3. Ретроспектива связи

Создание цепочки атак

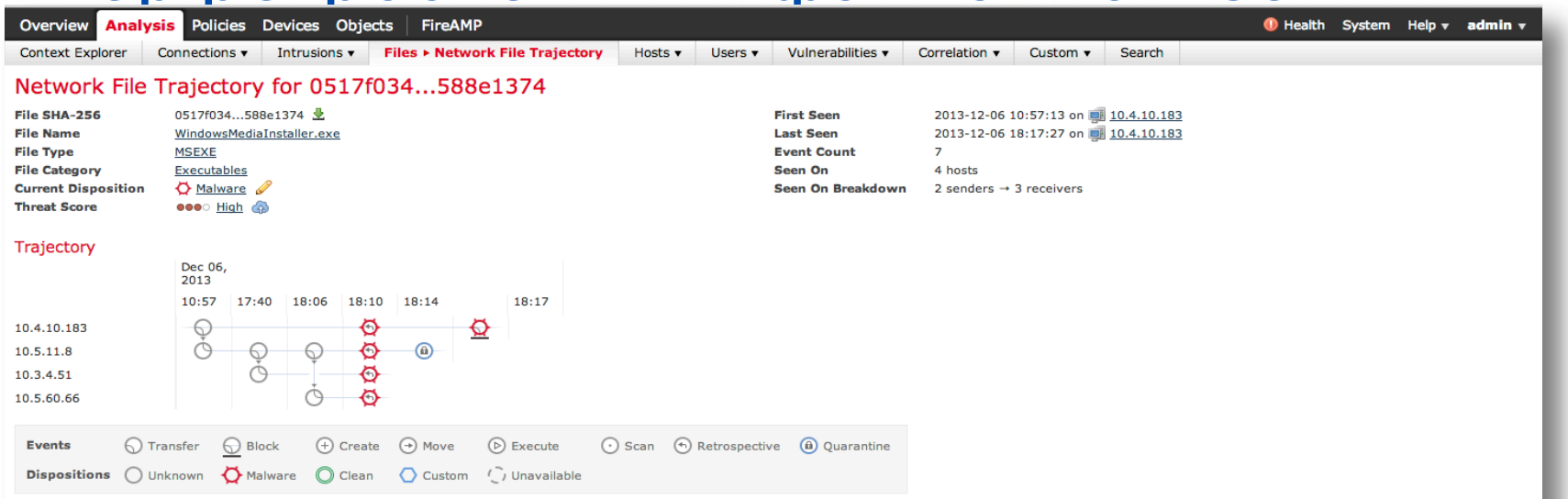
Анализирует данные, собранные ретроспекцией файлов, процессов и связи для обеспечения нового уровня интеллектуальных средств мониторинга угроз



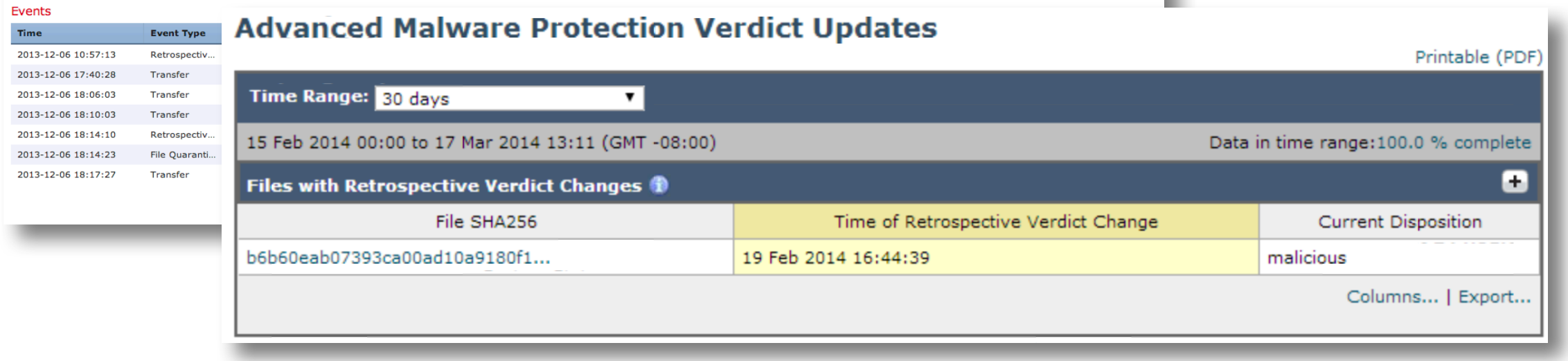
Ретроспектива связей

Производит мониторинг, какие приложения выполняют действия

Пример ретроспективы файла и связей

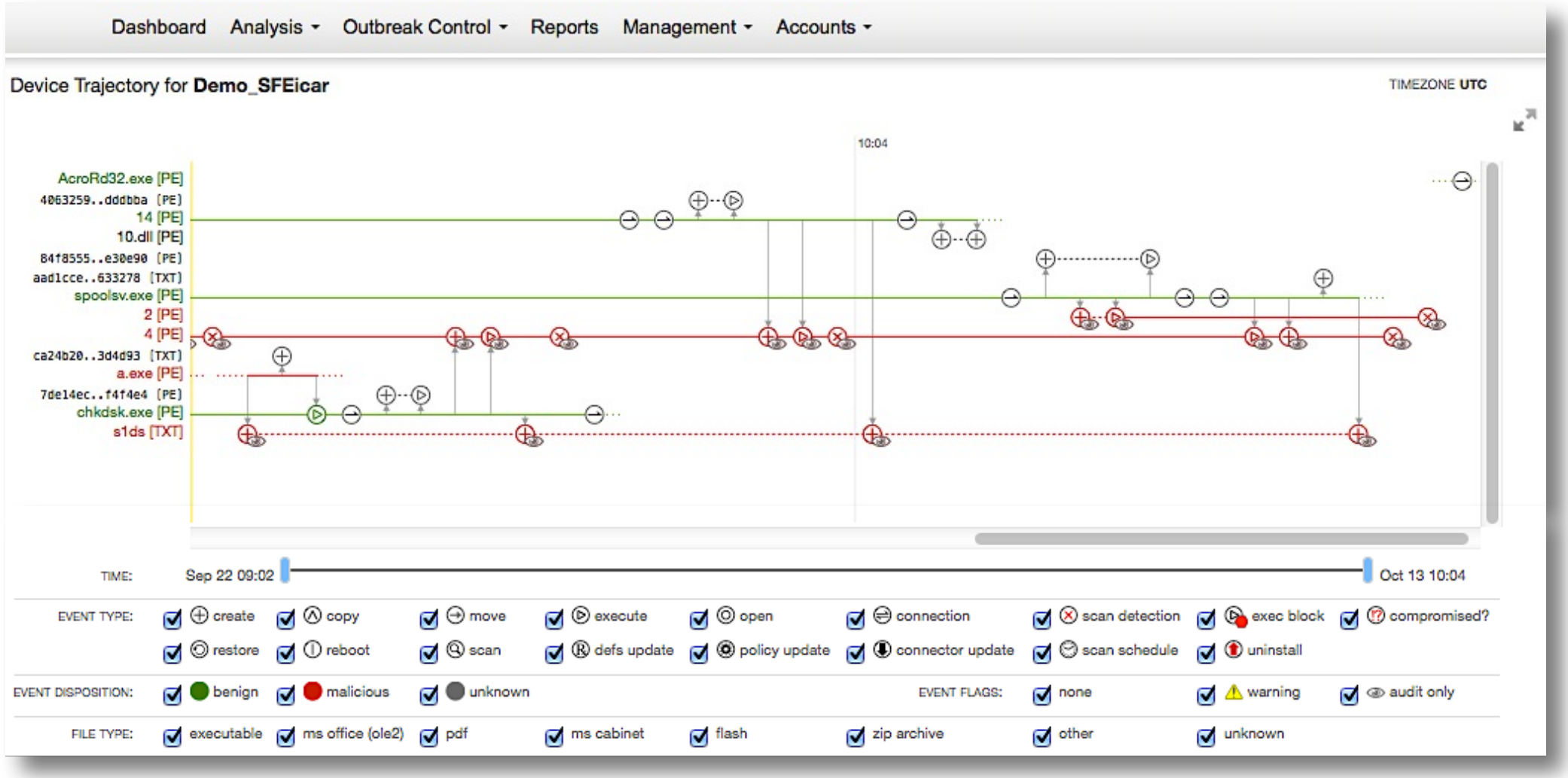


На примере Cisco AMP for Networks



На примере Cisco AMP for Content Security (ESA)

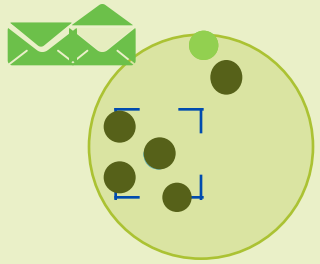
Пример ретроспективы процессов



На примере Cisco AMP for Endpoints

Ретроспективная безопасность основана на…

Поведенческие признаки вторжения используют ретроспективу для мониторинга систем на наличие подозрительной и неожиданной активности

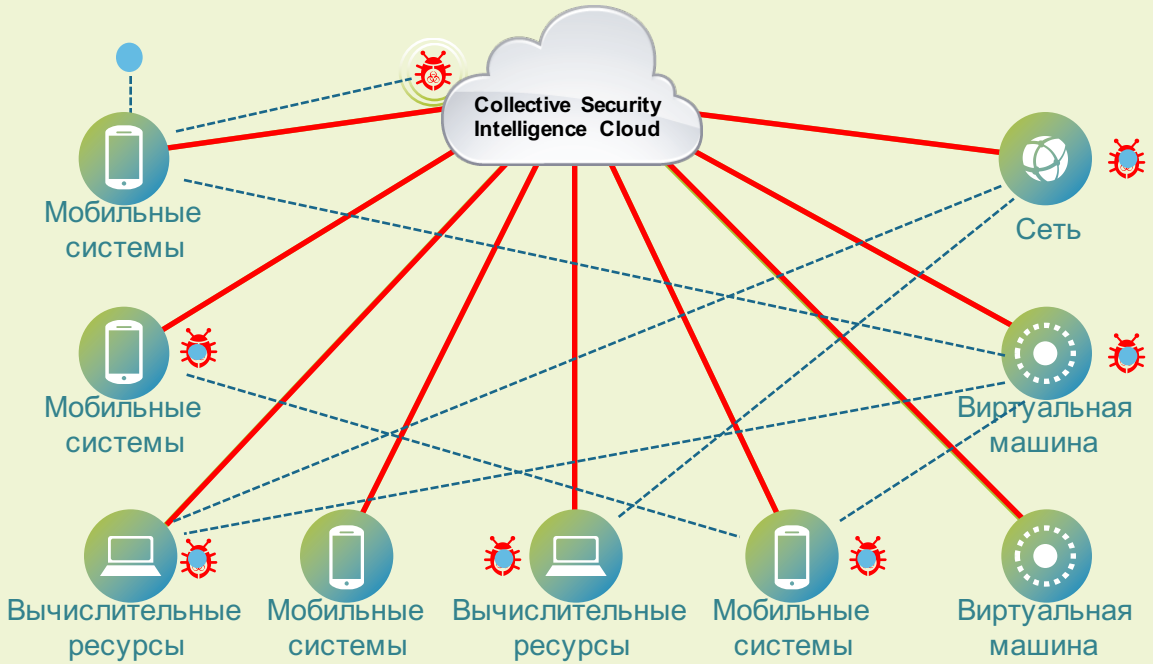


1	Неизвестный файл допущен в сеть
2	Неизвестный файл копирует себя на несколько машин
3	Копирует содержимое с жесткого диска
4	Отправляет скопированное содержимое на неизвестный IP-адрес

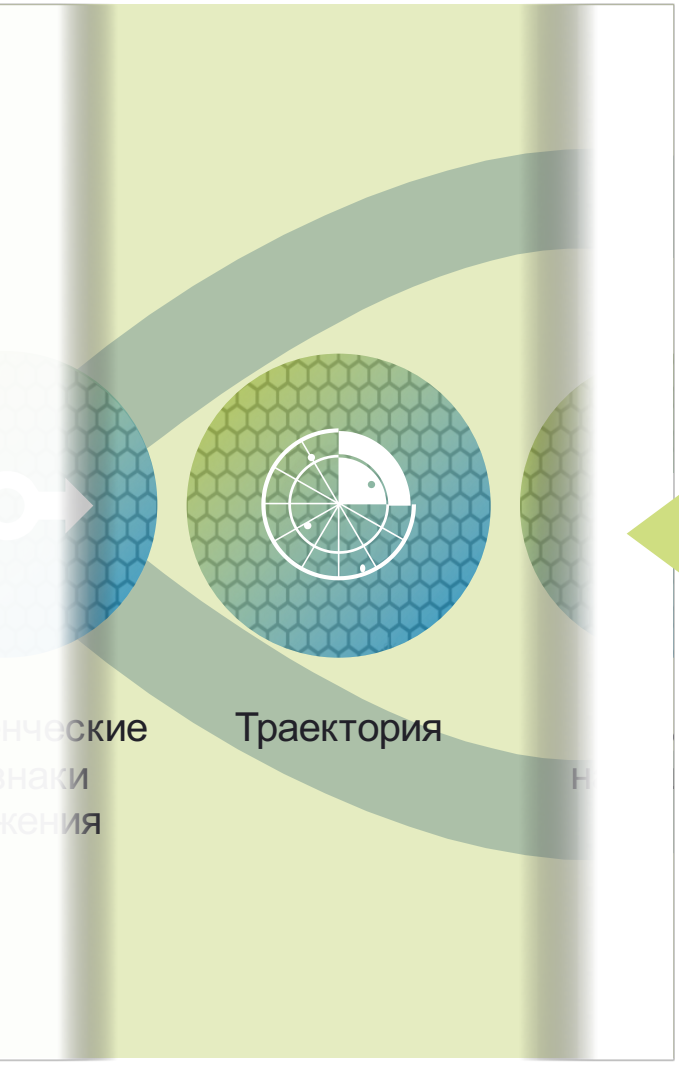
С помощью связывания в цепочки действий при атаке, Cisco® AMP способен распознать характерные шаблоны поведения для указанного файла и идентифицировать его, не производя поиск по меткам или сигнатурам файлов

Ретроспективная безопасность основана на…

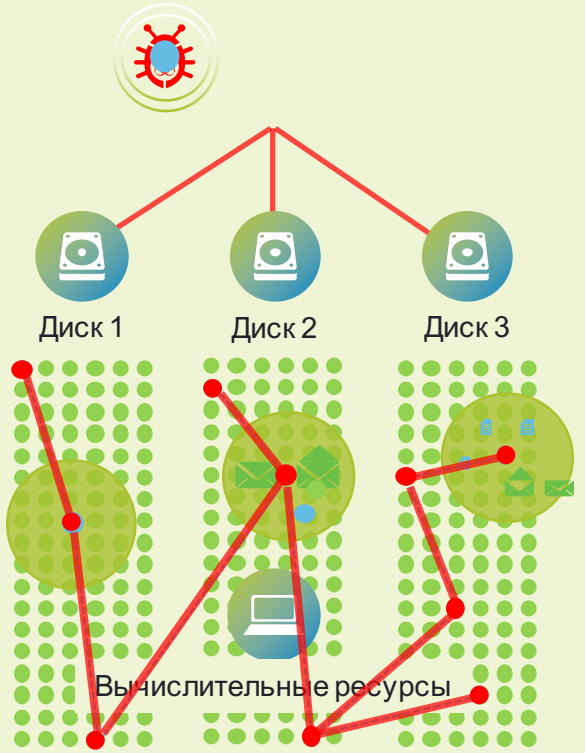
1	Неизвестный файл загружается на устройство
2	Сигнатура записывается и отправляется в облако для анализа
3	Неизвестный файл перемещается по сети на разные устройства Траектория файла автоматически записывает время, способ, входную точку, затронутые системы и распространение файла
4	Аналитики в изолированной зоне определяют, что файл вредоносный, и уведомляют все устройства
5	Траектория файла обеспечивает улучшенную наглядность масштаба заражения



Ретроспективная безопасность основана на…



1	Неизвестный файл загружается на конкретное устройство
2	Файл перемещается на устройстве, выполняя различные операции
3	При этом траектория устройства записывает основную причину, происхождение и действия файлов на машине
4	Эти данные указывают точную причину и масштаб вторжения на устройство



Что делать в случае обнаружения вредоносного кода?

- Вариант реагирования на обнаруженный вредоносный код зависит от варианта реализации AMP
- AMP for Endpoints

  Режим аудита – разрешить запускать вредоносный код

  Пассивный режим – не ждать ответа из облака и запустить вредоносный код (блокировать после)

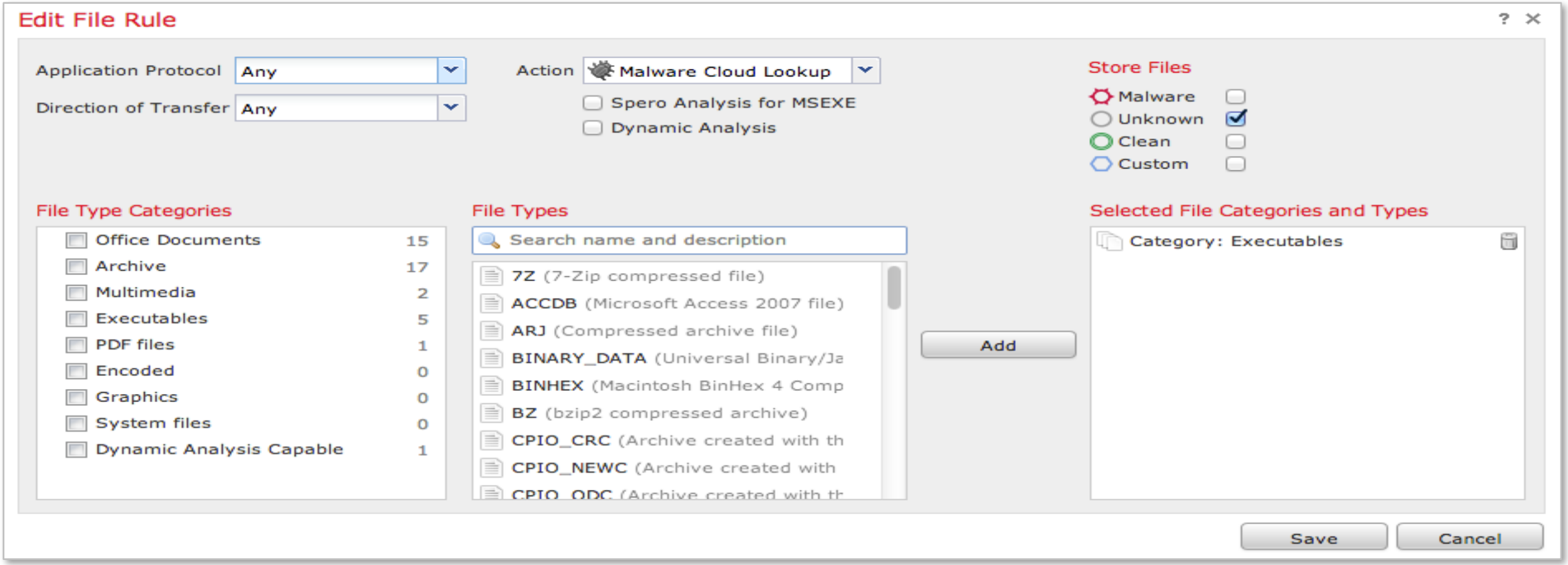
  Активный режим – ждать ответа из облака, не запуская файл
- AMP for Content Security

  Пропустить, заблокировать или поместить в карантин (для ESA)
- AMP for Networks

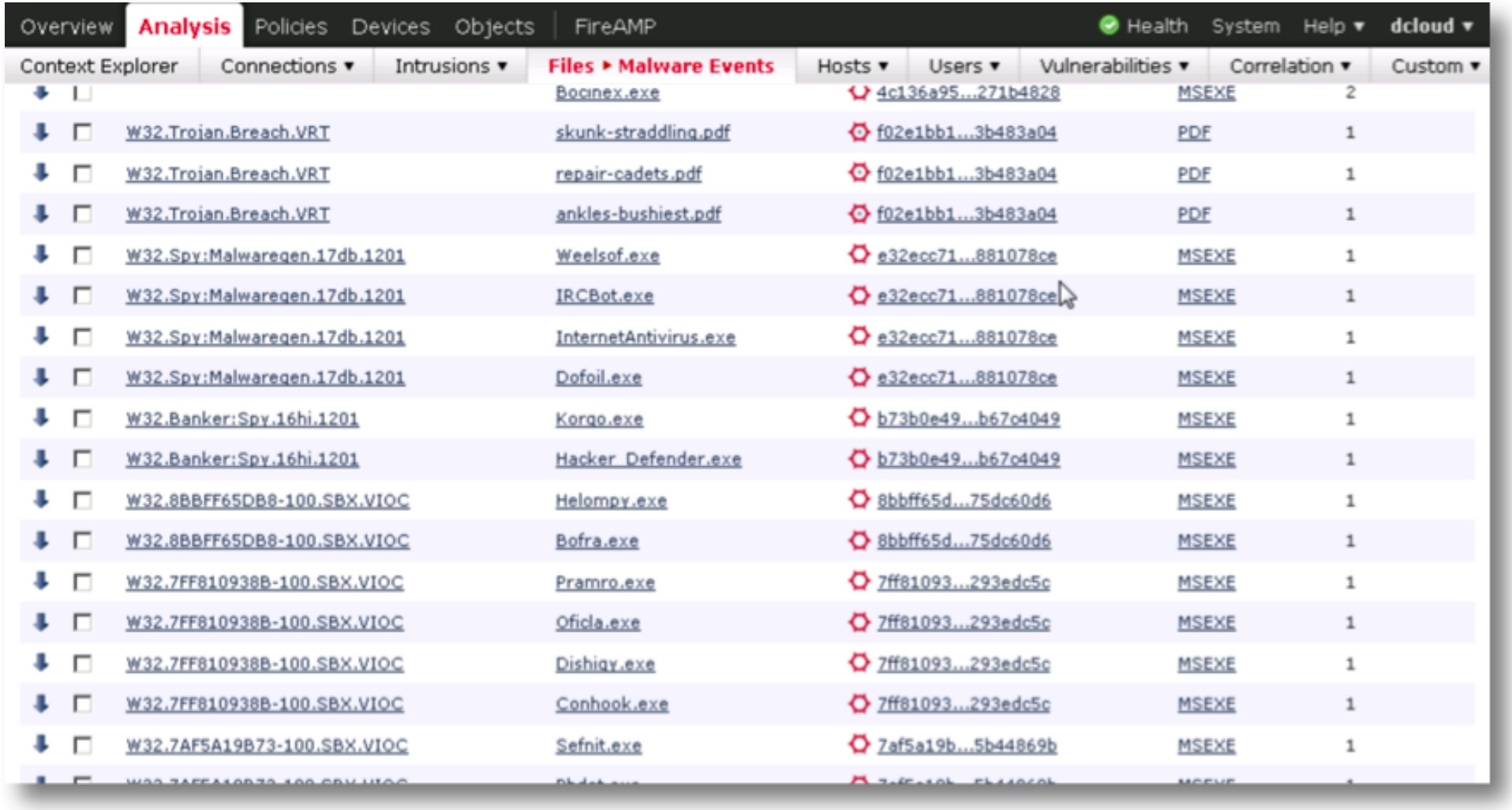
  Пропустить, заблокировать или сохранить вредоносный код

Какие файлы можно анализировать?

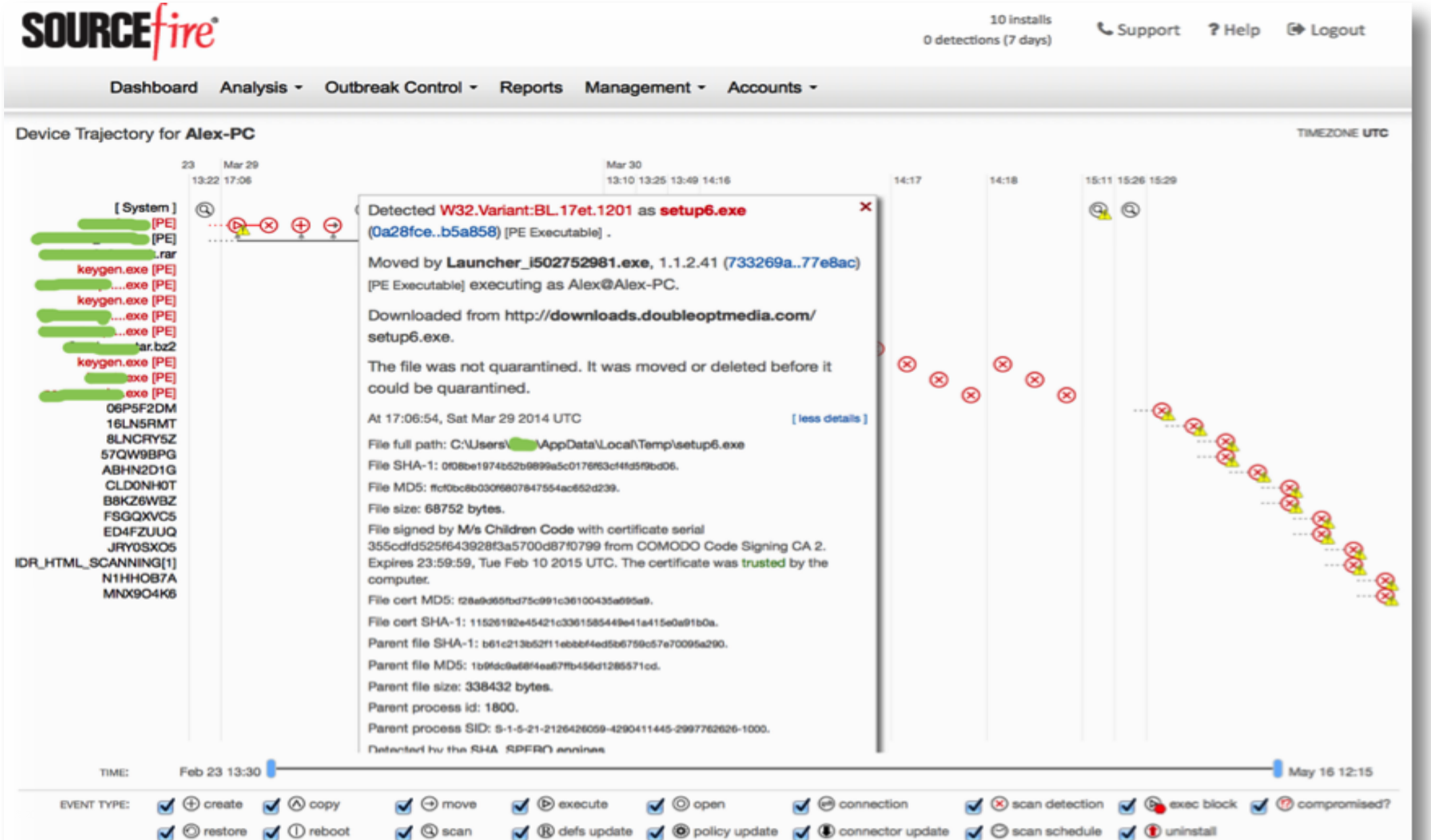
- Файлы, передаваемые по сети (HTTP, SMTP, POP3, IMAP, SMB, FTP), можно захватывать и сохранять для дальнейшего анализа



Обнаружение известного вредоносного кода

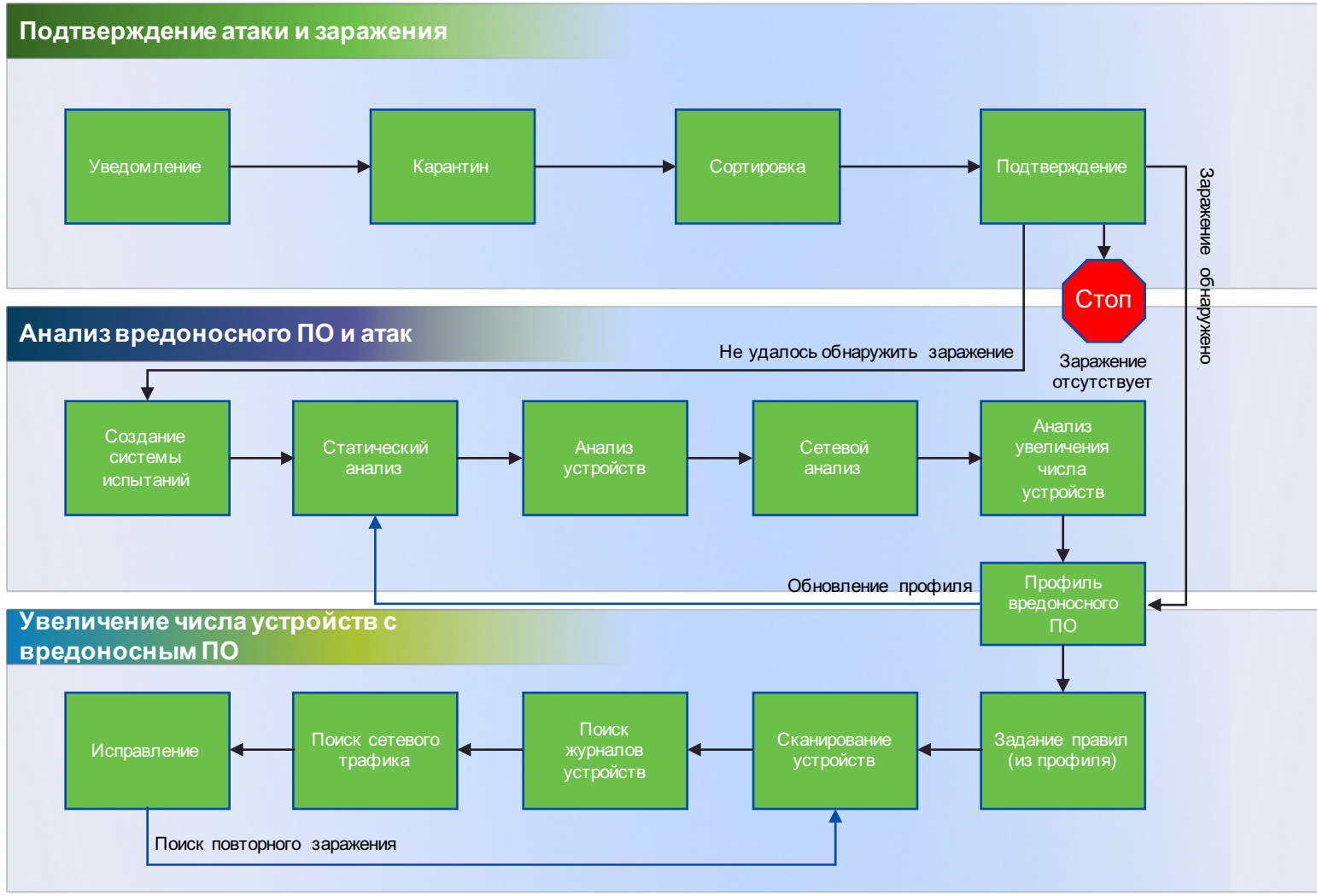


Полная информация о вредоносном коде



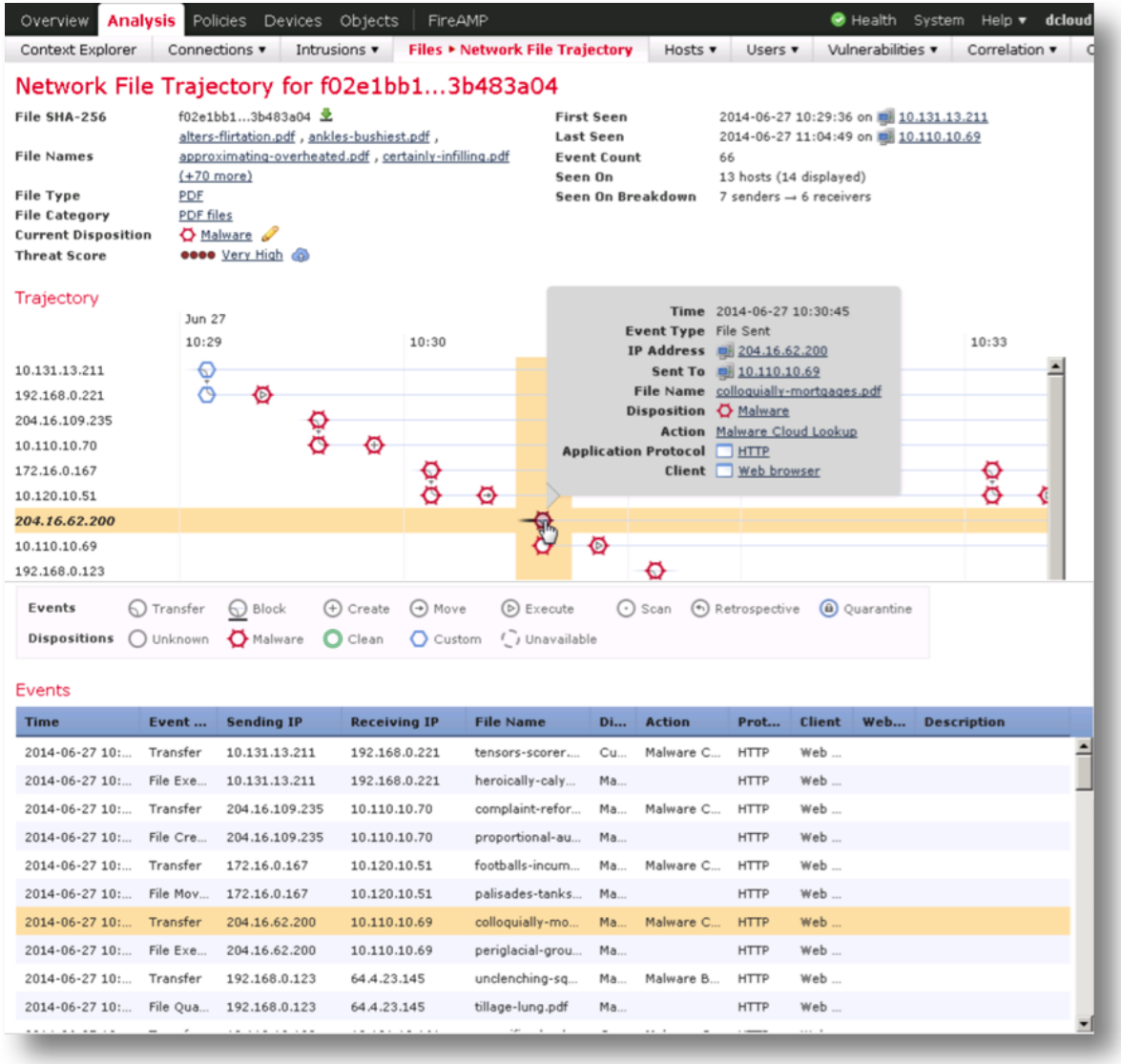
Вопрос не в том, произойдет ли заражение, а как скоро мы его обнаружим, устраним и поймем причины?

- С чего начать?
- Насколько тяжела ситуация?
- Какие системы были затронуты?
- Что сделала угроза?
- Как можно восстановить?
- Как можно предотвратить ее повторение?



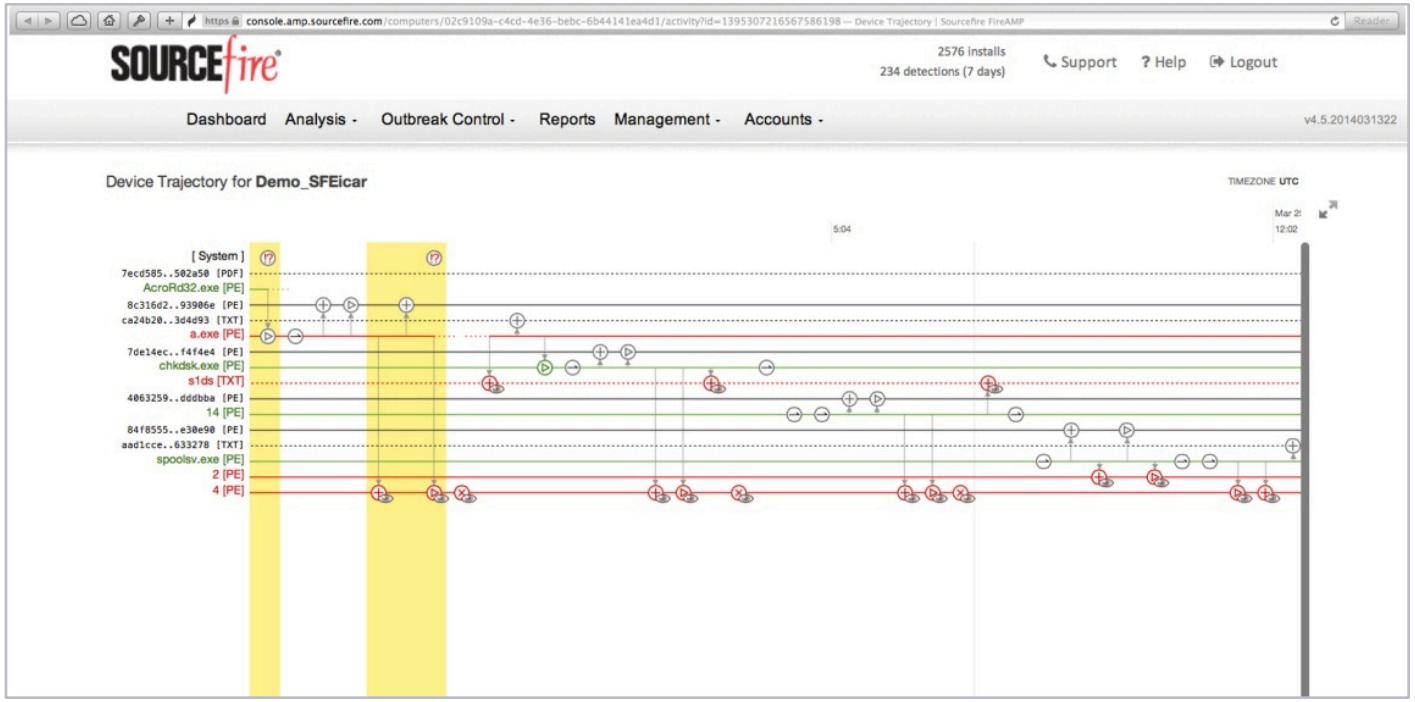
Ретроспективный анализ файлов позволяет определить

- Какие системы были инфицированы?
- Кто был инфицирован?
- Когда это произошло?
- Какой процесс был отправной точкой?
- Почему это произошло?
- Что еще произошло?

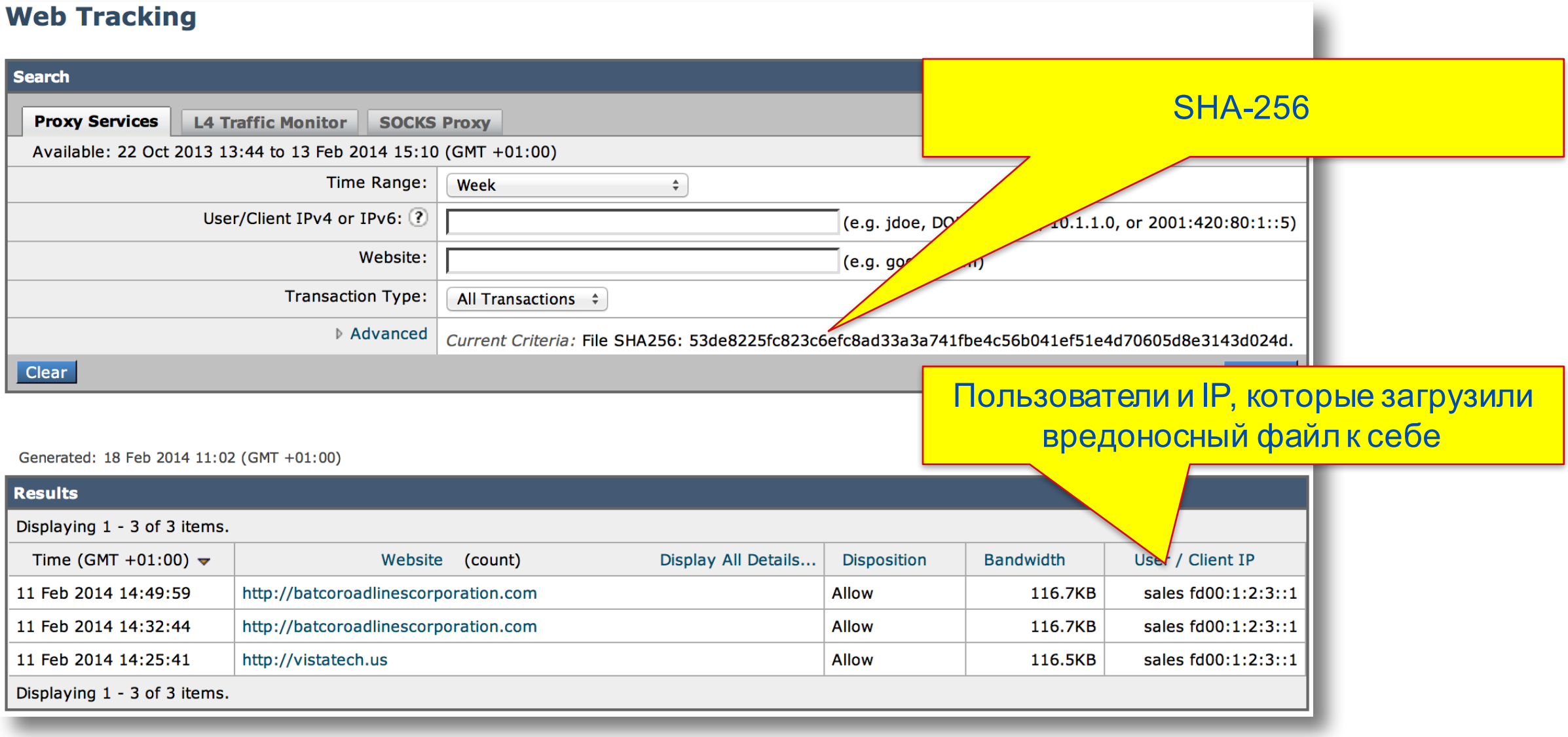


Ретроспективный анализ процессов позволяет определить

- Как угроза попала на узел?
- Что плохого происходит на моем узле?
- Как угроза взаимодействует с внешними узлами?
- Чего я не знаю на своем узле?
- Какова последовательность событий?

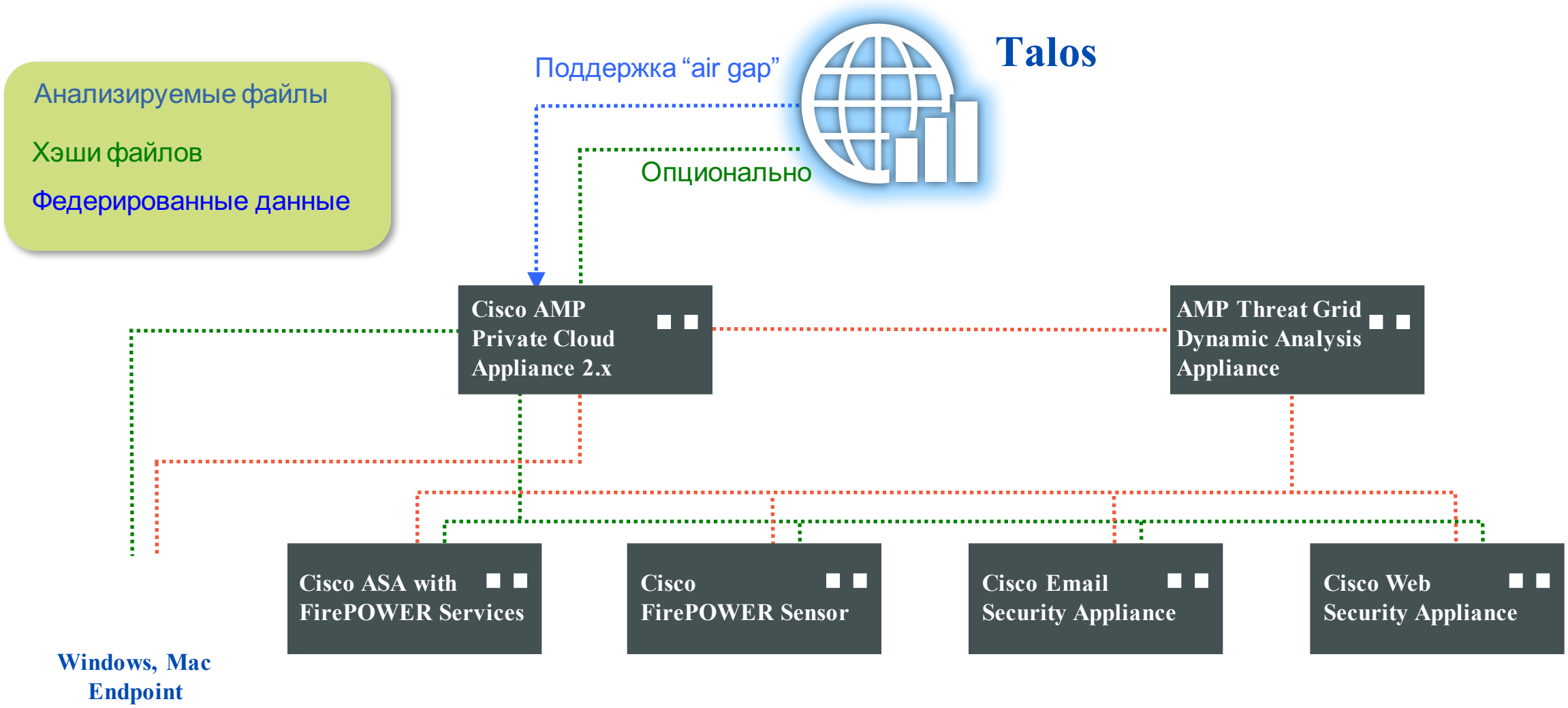


Трекинг каждого вредоносного файла



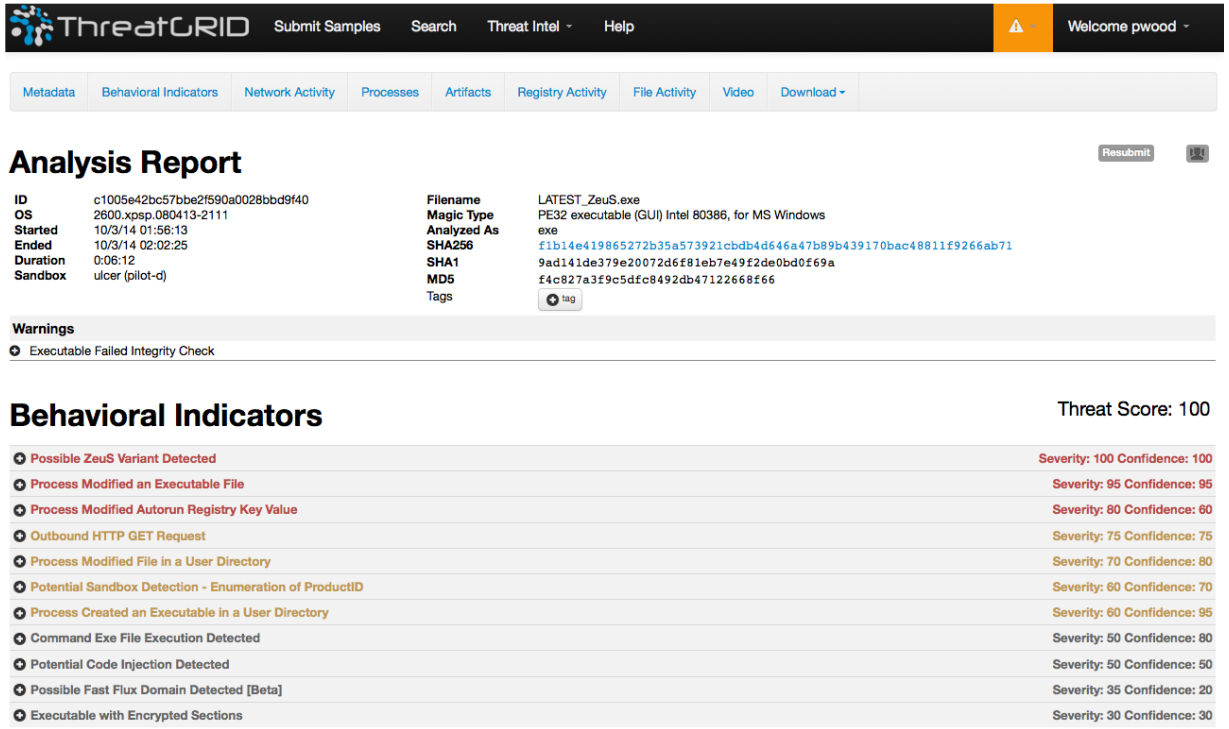
Вопросы конфиденциальности

AMP Private Cloud 2.0



А можно анализировать вручную?

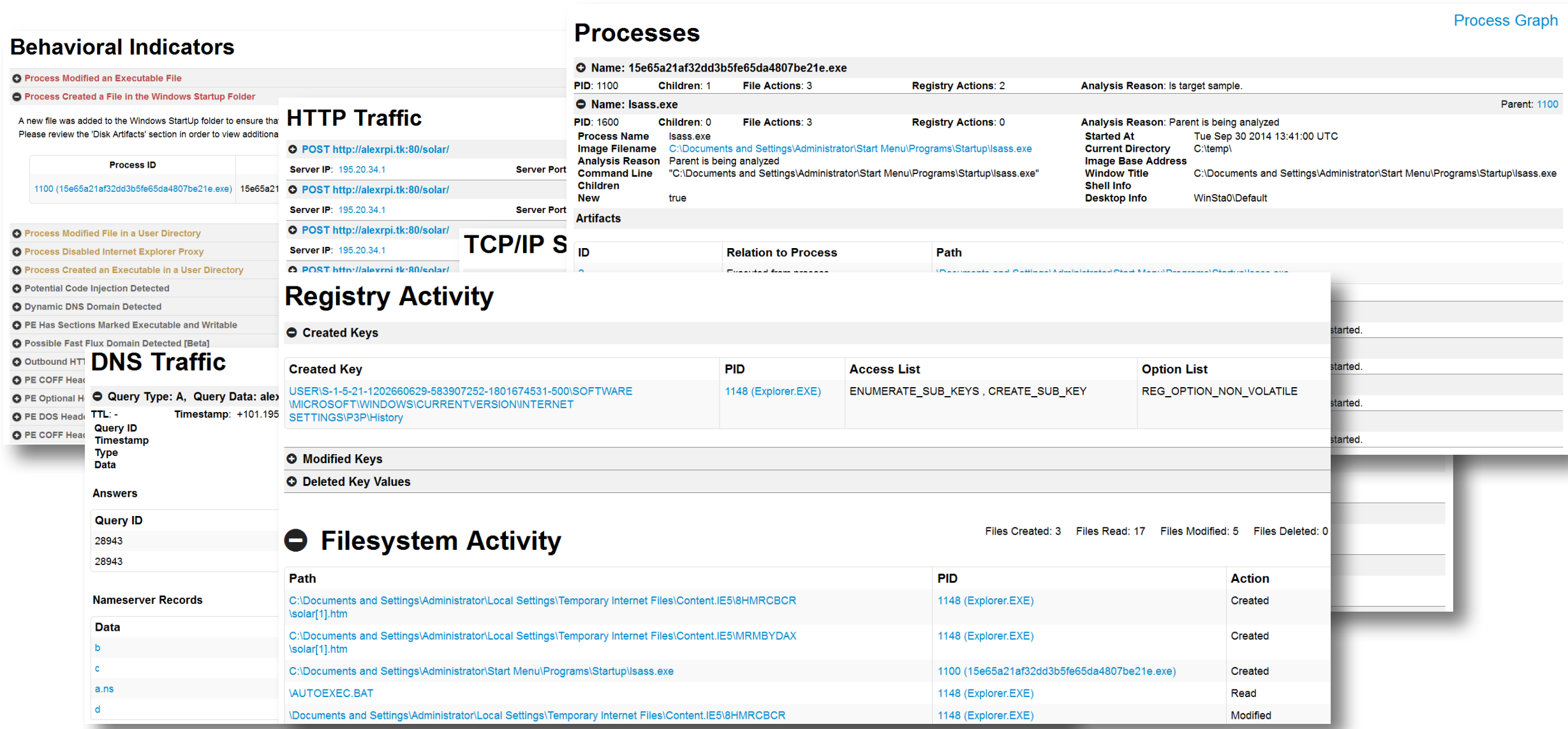
- Нередко бывает необходимость анализировать файлы, попавшие в службу безопасности на USB-носителях или иных носителях, а также проводить более глубокий анализ обнаруженных с помощью Cisco AMP вредоносных программ
- Не у всех бывает реализована автоматическая защита с помощью Cisco AMP
- Организация может захотеть создать собственную службу Threat Intelligence или Security Operations Center



Cisco AMP Threat Grid

- Платформа для глубокого анализа вредоносного кода
  - Доступ через портал, выделенное устройство или с помощью API
- Может применяться при построении собственных систем Threat Intelligence или SOC
- Уже используется многими компаниями при проведении расследований – EnCase, Maltego и т.п.

Детальный анализ вредоносного ПО в AMP Threat Grid



Типовые сценарии использования AMP Threat Grid

- Доступ к порталу
  - Зависит от числа аналитиков и ежедневно загружаемых образцов вредоносного кода
  - Приватная маркировка загружаемых семплов (опционально)
  - Устройство Threat Grid (опционально) позволяет загружать образцы на него, без загрузки в облако
- Интеграция с решениями Cisco
  - AMP for Endpoints
  - AMP for Networks (FP / ASA)
  - AMP for WSA / CWS
  - AMP for ESA / CES
- API для автоматизации передачи образцов в Threat Grid включен во все лицензии с подпиской

Вариант развёртывания внутри сети, без прямого доступа в Интернет

- Локальный анализ вредоносного ПО с полной поддержкой облака Cisco® AMP Threat Grid
- В целях соблюдения нормативных требований все данные остаются на территории заказчика
- Непрерывный однонаправленный поток данных из облака Cisco AMP Threat Grid для актуализации контекста
- Ощущения пользователя не меняются при переходе от облака к устройству (UI, API, ….)

- TG5000:
  - Анализ до 1500 образцов в день
  - Cisco UCS C220 M3 Chasis (1U)
  - 6 x 1TB SAS HDD (аппаратный RAID)
- TG5500:
  - Анализ до 5000 образцов в день
  - Cisco UCS C220 M3 Chasis (1U)
  - 6 x 1TB SAS HDD (аппаратный RAID)

Отличия портала от локального устройства AMP Threat Grid

- Масштабируемость
  - Отсутствуют ограничения на число загружаемых для анализа образцов (в устройстве – до 5000 в день)
- Скорость обработки образцов
  - Обработка 1000 образцов занимает около 30 минут. На устройстве такое же количество обрабатывается за 4 часа
- Стоимость
  - Устройство стоит дороже доступа к порталу
- Анализ угроз
  - Сопоставление угроз в облаке осуществляется со всеми образцами, загруженными в него и помеченными как публичные. На устройстве сопоставление осуществляется только с локальными образцами
- Обновления для поведенческих индикаторов
  - Обновления для устройства выпускаются каждый квартал, а для портала – каждые 2 недели

Преимущества и недостатки локального устройства

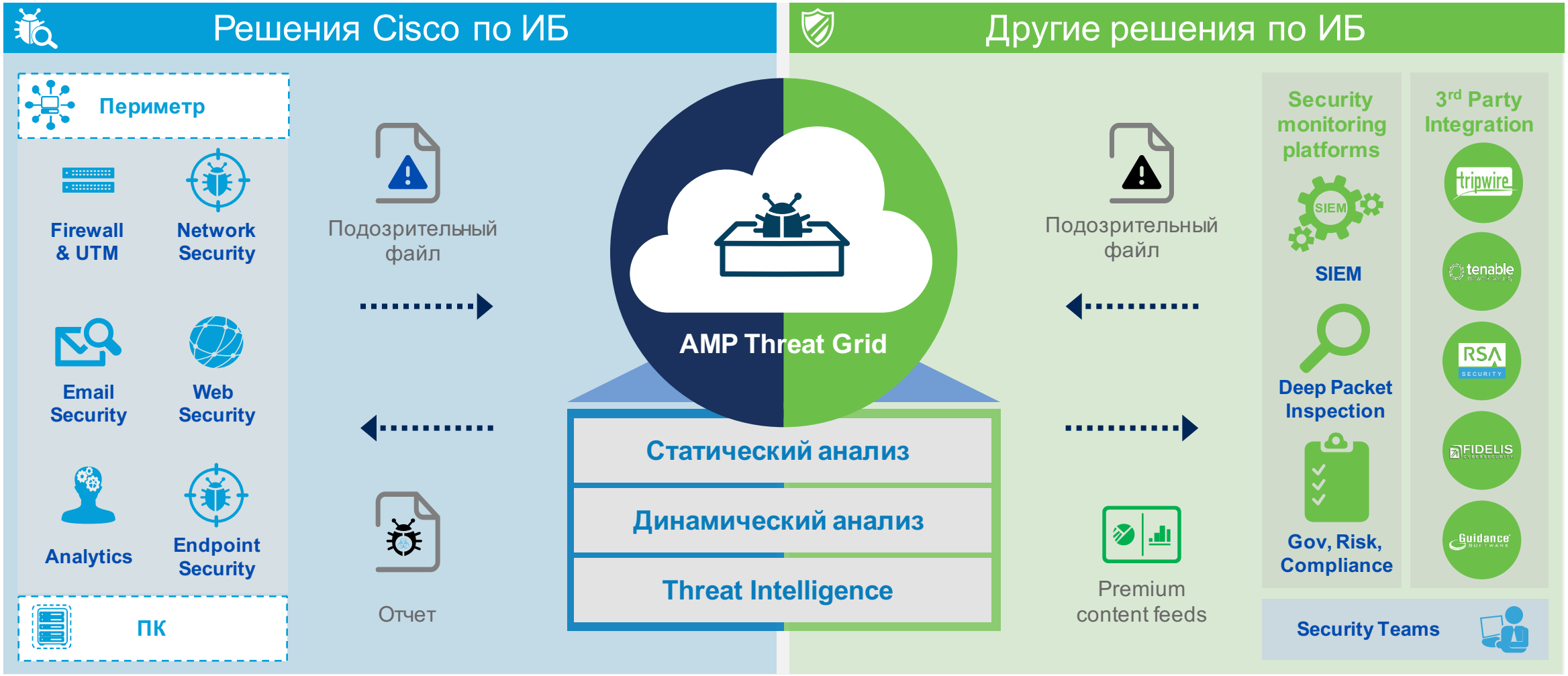
Преимущества

- Конфиденциальность данных
- Возможность работы в изолированной сети
- Независимость от наличия Интернет-канала

Недостатки

- Обновления поведенческих индикаторов приходят с задержкой
- Невозможность полного анализа Интернет-активности вредоносного ПО
- Невозможность сопоставления данных с другими публичными семплами

Повсеместный AMP Threat Grid



Cisco Advanced Malware Protection
Gartner Endpoint Detection and Response (EDR)

- Обнаружение инцидентов безопасности.

  С помощью мониторинга активности хостов и объектов, нарушения политик или же с помощью набора внешних индикаторов компрометации

- Сдерживание инцидента на хосте

  Блокирование сетевого трафика или же выполнения файла. Удаленно контролируется

- Расследование инцидентов безопасности

  Функция расследования должна включать исторические данные всех основных событий на хосте для того, чтобы определить как технические изменения (активности файлов, реестра, сети, драйверов) и их влияние на бизнес (обход, эскалация привилегий, распространение, эксфильтрация, геолокация, подключение к CnC и подозрительное авторство)

- Восстановление узла до первоначального состояния

  В идеале решение должно удалять вредоносные файлы, делать откат к предыдущему состоянию и восстанавливать другие изменения. Решение должно создавать инструкции по предотвращению, должно быть доступно для других инструментов, особенно для организаций, которые имеют разделение обязанностей и жесткие процедуры контроля изменений

  В реальности проще всего восстановить систему из предыдущего snapshot, или же полностью реинициализировать систему и восстановить данные из резервной копии. Это может оказаться менее затратно по времени по сравнению с детальным анализом состояния и восстановлением изменений

Thank you.