Fidelis Deception — продвинутая технология обмана злоумышленников для быстрого выявления атак и инсайдеров

Максим Прахов
Руководитель развития бизнеса в странах СНГ

Fidelis Cybersecurity

Oberig it

Краткая история Fidelis

2002

Основание Fidelis.
Network Security & DLP
Patented

2012

Поглощение General Dynamics. Отедел Advanced Information Systems.

2015

Новое видение рынка – интегрированная и автоматизированная сетевая безопасность и безопасность конечных точек в единой платформе.

2015

Fidelis становится частной компанией.

2015

Приобретение EDR.
Начало интеграции Network и Endpoint.
Добавление deep file analysis, deep session analysis, deep malware analysis, deep packet inspection, deep content inspection и ML

2017

Network & Endpoint.
Интеграция и автоматизация

Новое приобретение – TopSpin Deception

Founded

GD

Vision

Private

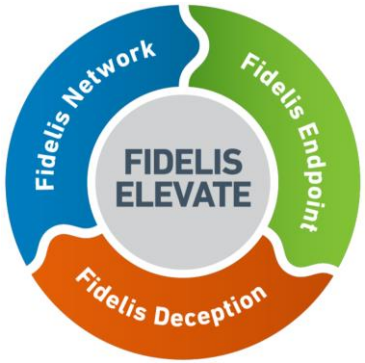
Endpoint

Integration

Security Value

Сегодня

ADR = **10 – 20X** повышение эффективности операций по обеспечению безопасности



Доверие крупнейших мировых брендов и правительств для защиты своих конфиденциальных данных

Лидер в Automating Detection and Response

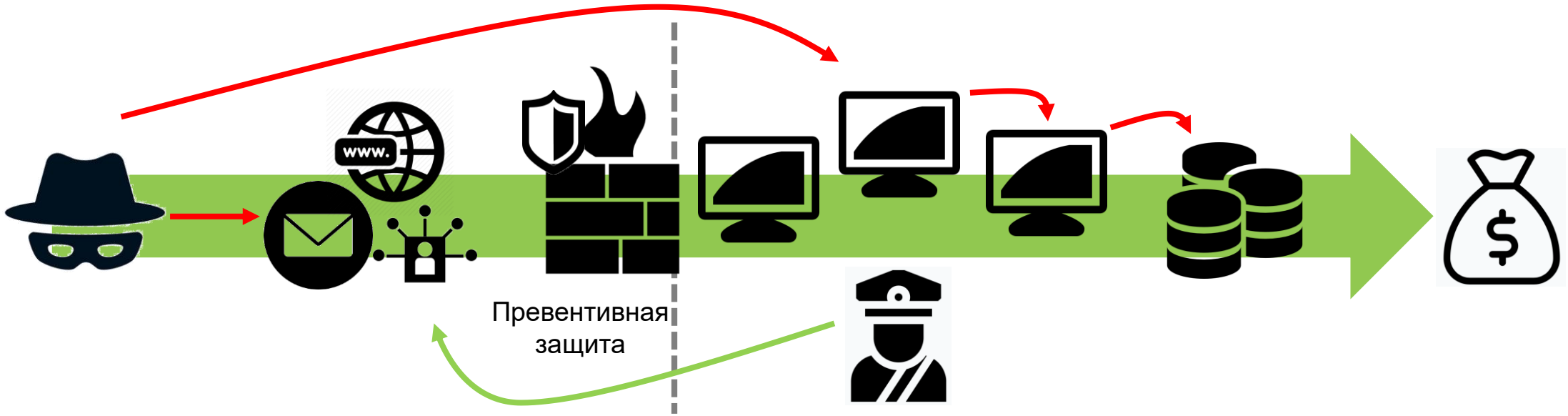
- Технологическое лидерство: Network Data Loss Prevention (DLP), Breach Detection, Deception, Endpoint Detection & Response (EDR), Asset Classification
- Эксперт «know-how» с 4000+ Incident Response (IR) кейсами и Оценками безопасности

Опираясь на:

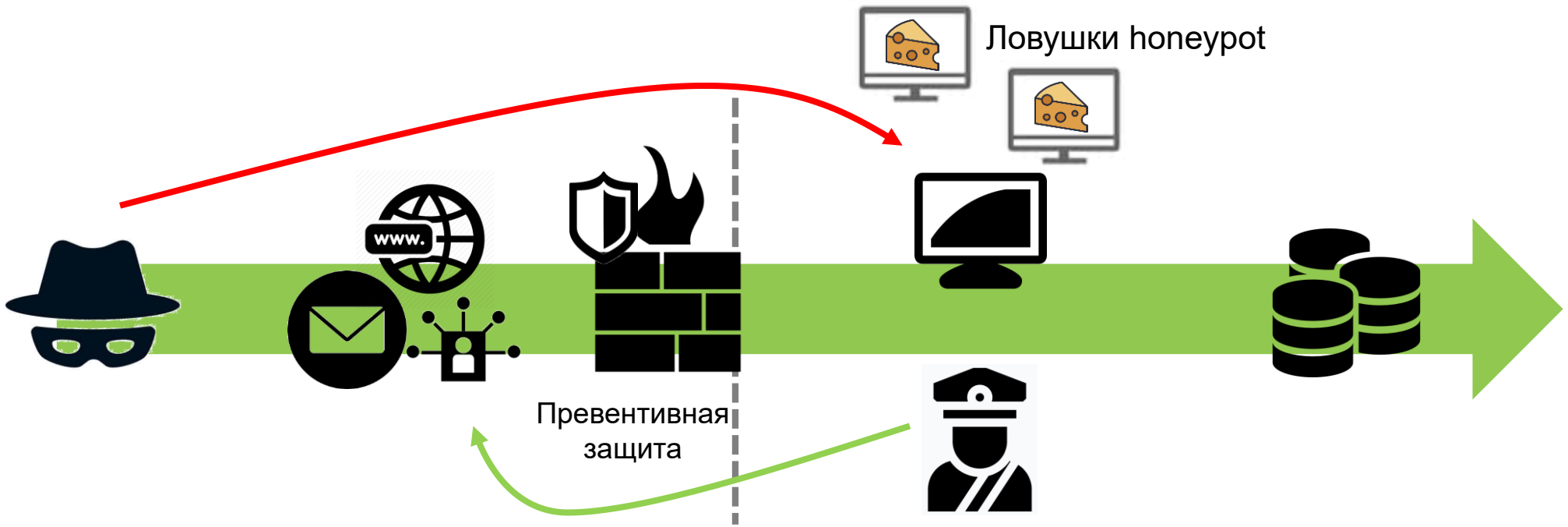
- 40 государственных учреждений и ведомств США
- Коммерческий бизнес по всему миру, включая:
  - 12 из Fortune 50
  - 24 из Fortune 100

Финансы	Правительство	Розница	Здравоохранение	Технологии	Индустрия	Энергетика	Медиа и Телеком
BARCLAYS	U.S. AIR FORCE	CARMAX	Allergan	Hewlett Packard Enterprise	CAT	Chevron	vodafone
FRANKLIN TEMPLETON INVESTMENTS		L.L.Bean	gsk	Microsoft	AECOM	AMERICAN ELECTRIC POWER	
INTERNATIONAL MONETARY FUND			ThermoFisher SCIENTIFIC		United Technologies		du add life to life
MORNINGSTAR	DISA	DOLLAR TREE	THE UNIVERSITY OF CHICAGO MEDICAL CENTER	SAMSUNG	PCC Precision Castparts Corp.	HALLIBURTON	
Fidelity INVESTMENTS			abbvie	Nintendo		ConocoPhillips	VIACOM

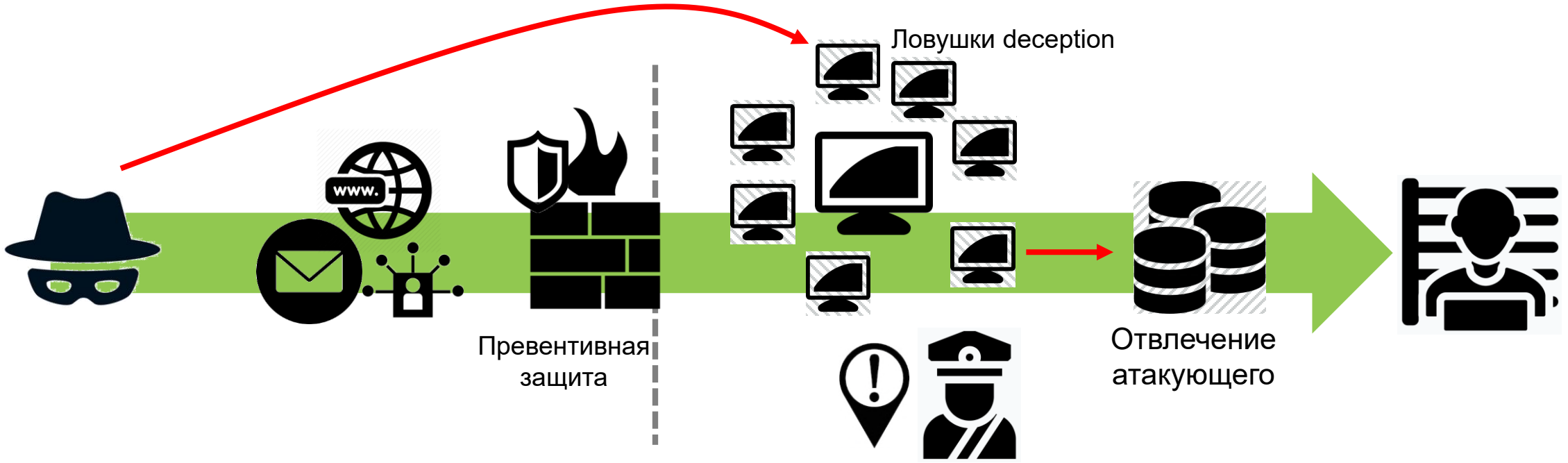
Сценарий кибератаки



Иллюзия обмана – технология honeypot

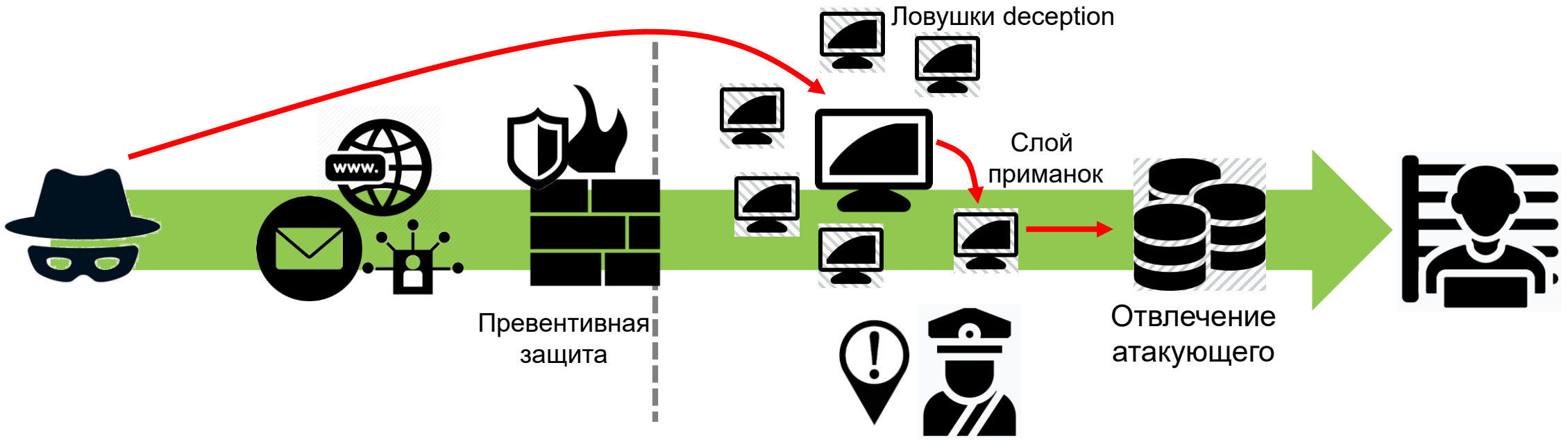


Fidelis – Distributed Deception Platform



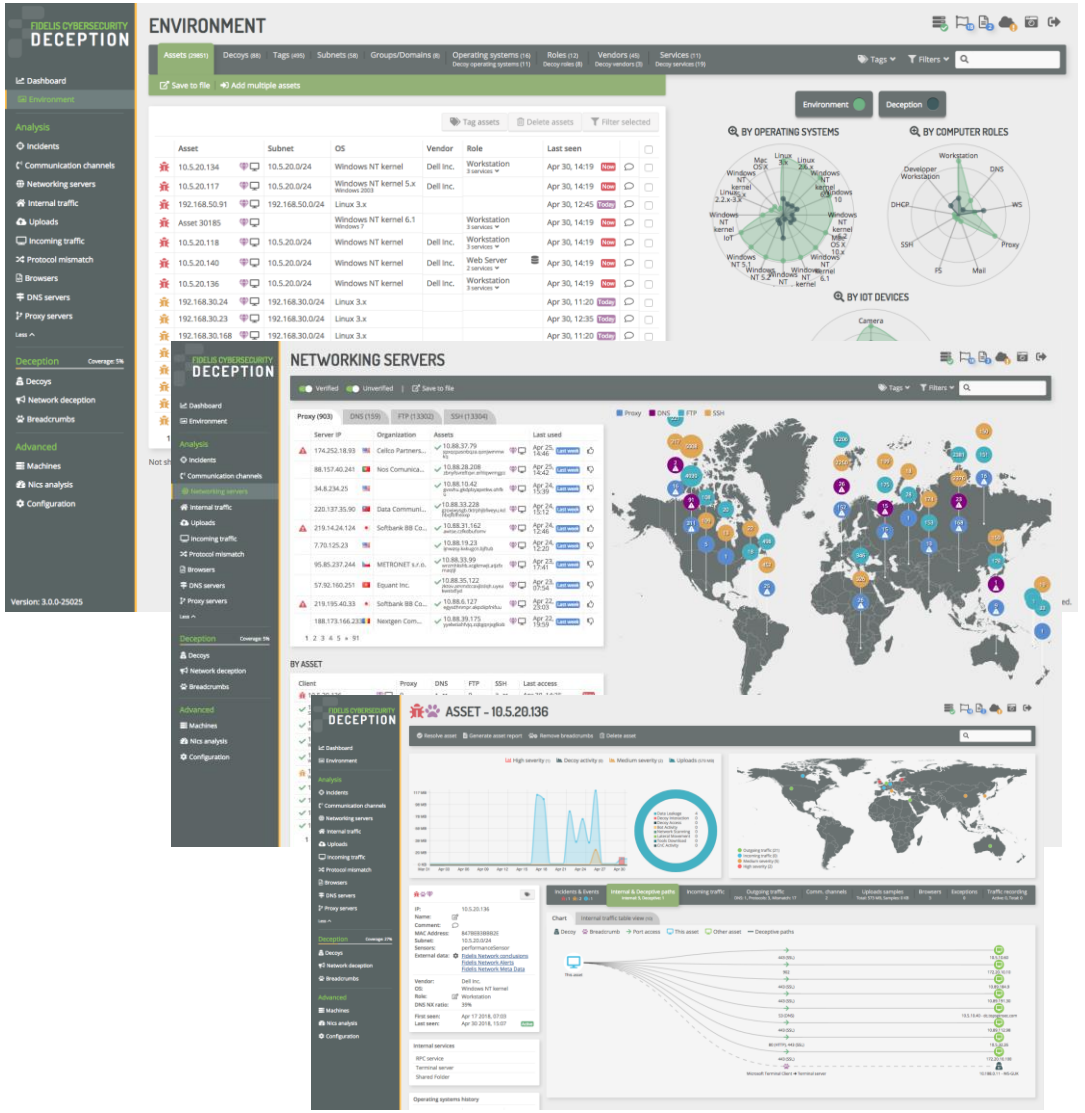
Fidelis – Distributed Deception Platform

Зная, как действуют злоумышленники мы создаем возможности для активной обороны

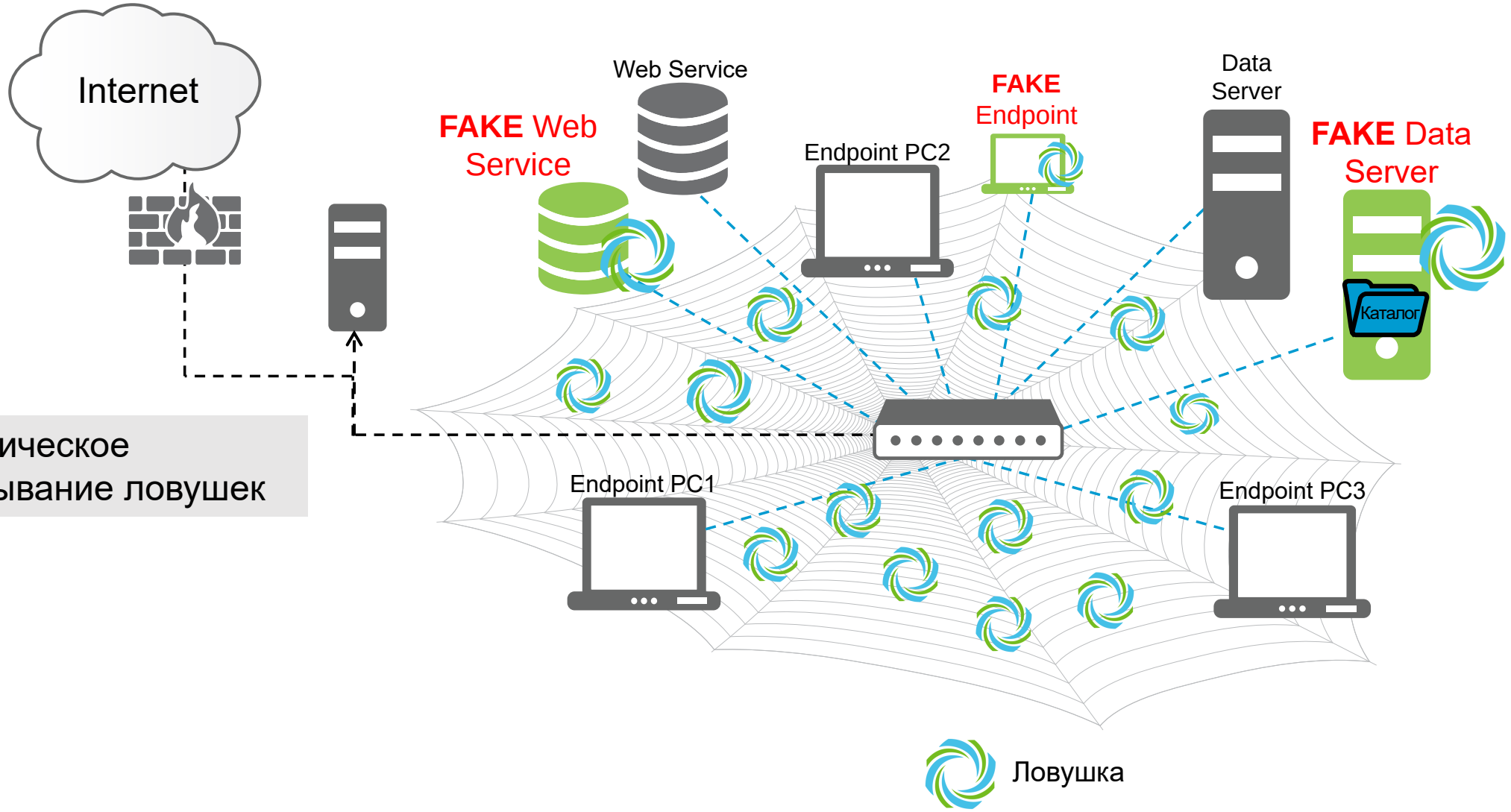


Шаг 1 – Автоматическая идентификация активов

- Предоставляет информацию о ресурсах организации
- Пассивная идентификация, профилирование, классификация
- Активы
  - Устройства (сервера, конечные точки, IoT, Shadow-IT)
- Данные
  - ОС, Приложения, Порты
- Использование каналов связи и сетевых ресурсов
  - Инструменты Shadow-IT, устаревшие приложения, сервера приложений, инструменты
  - Сервера: FTP, SSH, DNS, Proxy
- Обнаружение
  - Автоматический процесс VS работа в ручном режиме
  - Внутренняя и внешняя активность
- Графики визуализации взаимодействия активов

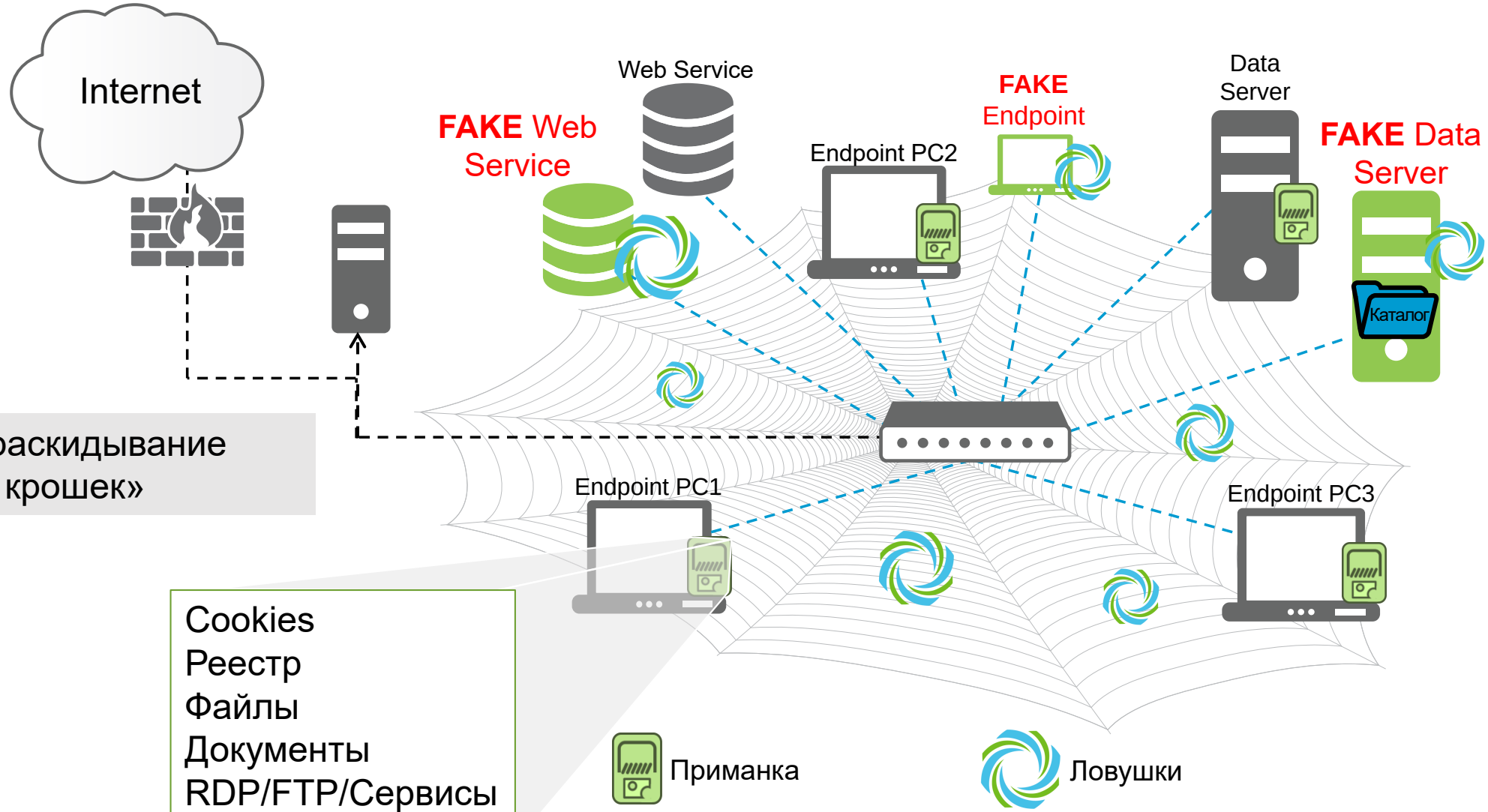


Шаг 2 – Автоматическое развертывание фальшивой инфраструктуры



Автоматическое развёртывание ловушек

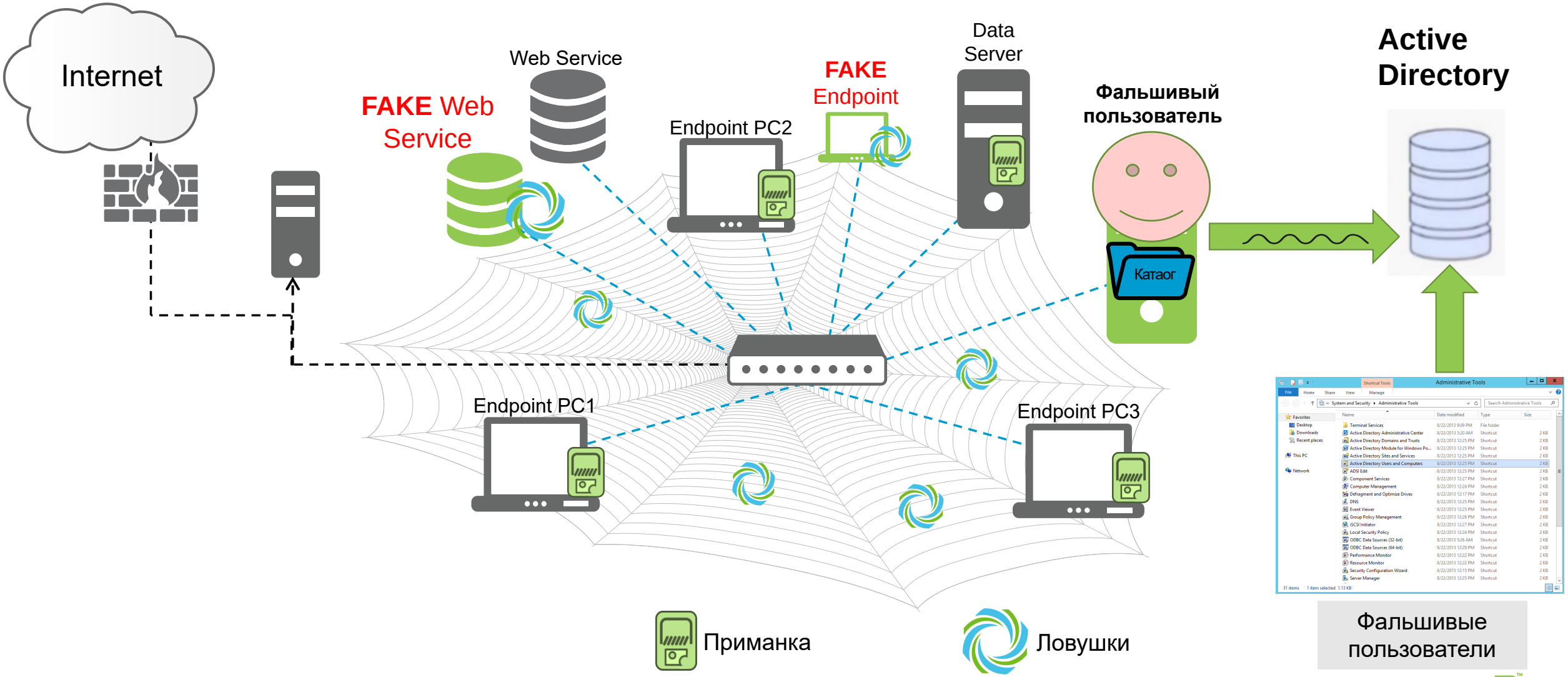
Шаг 3 – Распространение приманок



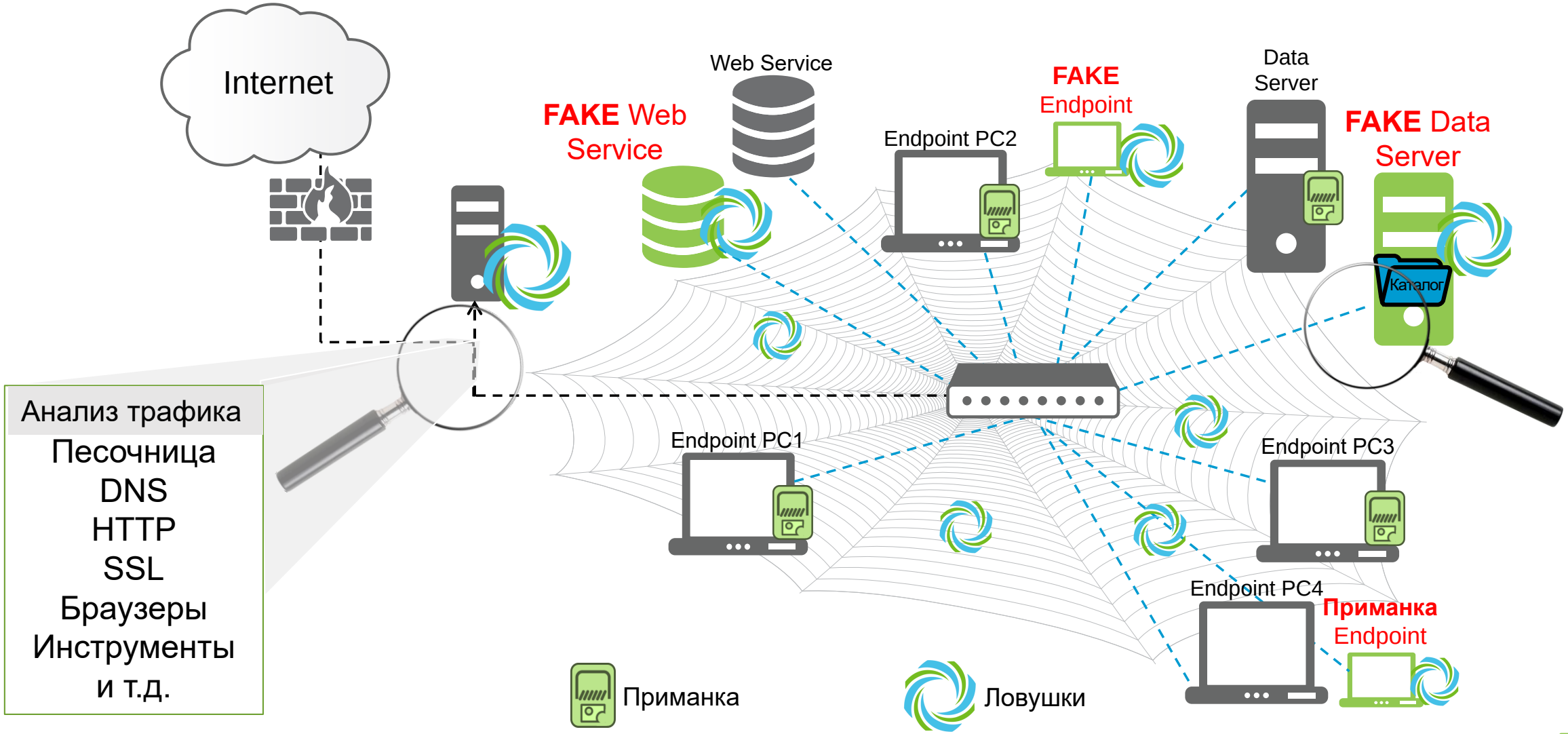
Целевое раскидывание «хлебных крошек»

Cookies
Реестр
Файлы
Документы
RDP/FTP/Сервисы

Шаг 4 – Active Directory Deception



Шаг 5 – Анализ трафика на ловушке и отвлечение атакующего

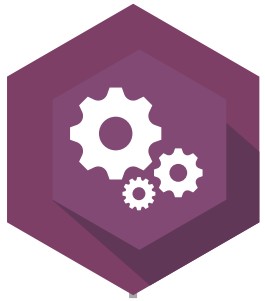


Как работает Fidelis Deception

Discover

- Построение карты сети и активов.
- Профили, создаются и обновляются с учетом использования, типа, местоположения и т. д.
- **Результат: уникальная основа, созданная для каждой приманки**

Decoys

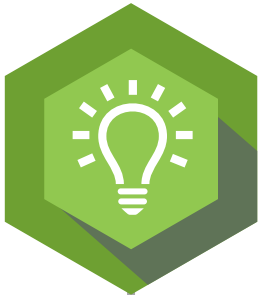


- Построение слоя обмана атакующего на основе данных профилирования.
- Автоматически создает сеть ловушек на основе реальных активов, услуг и процессов.
- **Результат: реалистичный слой фальшивой инфраструктуры**

Distribute

- Автоматически распространяет приманки.
- Размещает «хлебные крошки» в реальных активах и Active Directory
- **Результат: быстрое развертывание и мгновенная эффективность**

Detect



- Оповещения о доступе.
- Анализ использования отравленных данных (например, учетные данные).
- **Результат: обнаружение инсайдерских угроз, подмены учетных данных и побочных действий**

Adapt

- Распознает новые активы и сетевые топологии.
- Автоматическое обновление сети приманок.
- **Результат: Интеллектуальная и адаптивная защита**

Преимущества Fidelis Deception

Точная информация
Меньше ложных срабатываний

Простота использования
Корпоративний масштаб

Автоматизация и адаптация

Без риска
Без влияния

Исследование безопасности*

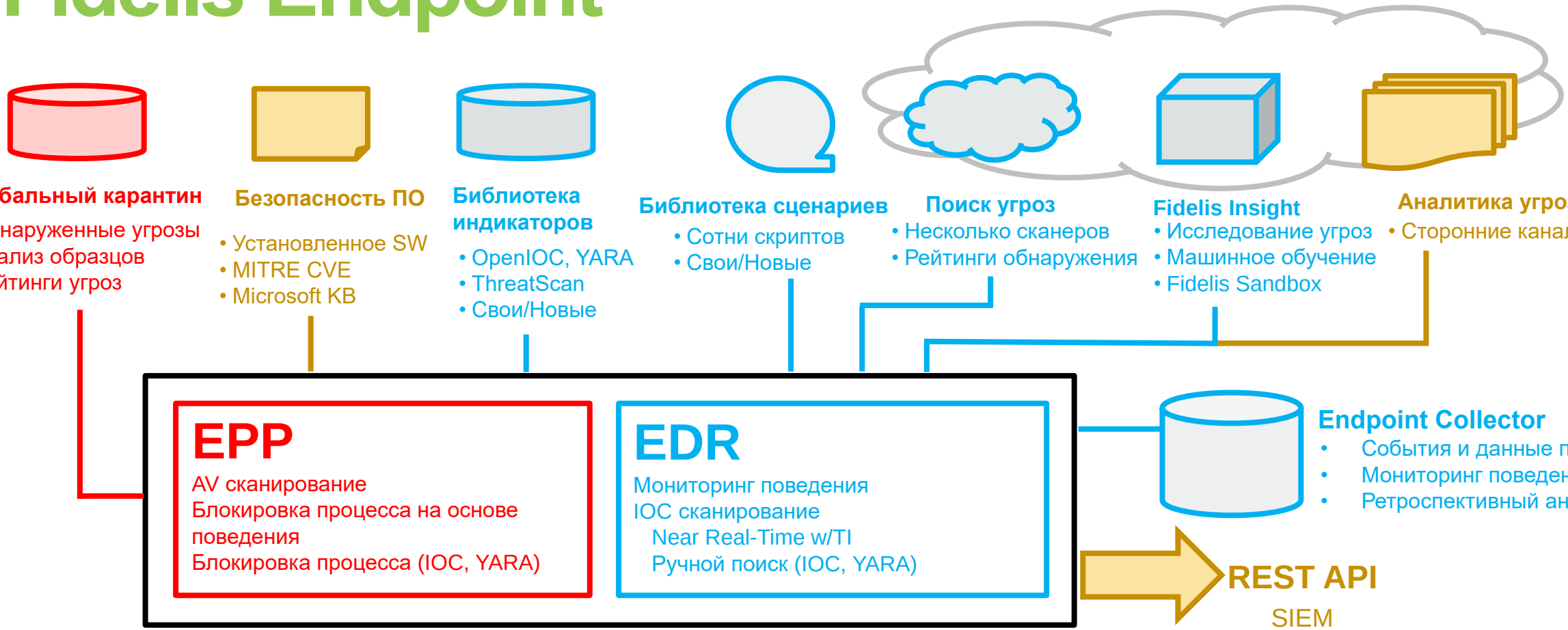
Умные оповещения

IoT Устройства

Нестандартные устройства*

* Fidelis Deception v9.2

Fidelis Endpoint



- Один агент,
- EDR+EPP, или EDR
- Windows, Mac, Linux

- Управление локально или в облаке
- Full Disk Imaging, File Collection
- Full Memory Capture & Analysis

Платформа Fidelis Elevate

Unified Security Platform

Network

Полная видимость сети по всему трафику, всем портам и всем протоколам, обнаружение угроз и предотвращение потери данных

Endpoint

Automate Endpoint Detection and Response (EDR) и защита конечных точек – все в одном агенте

Deception

Обнаружение и классификация сетевых ресурсов. Обнаружение атак после взлома с помощью автоматизированных слоев обмана

Информация перехватывается и хранится для анализа в режиме реального времени и ретроспективного анализа:

Сетевые активы | Метаданные | Содержимое сеансов | Данные для расследований | События на конечных точках

Агенты Endpoint

Приманки и ловушки

Сетевые сенсоры

Песочница

Обнаружение вредоносных программ на основе их выполнения и анализа

Глобальная аналитика угроз

Обнаружение угроз через Threat Intelligence Feeds, определения AV, поведенческие правила

Проверка и расследование инцидентов без Fidelis

Типичный день в офисе

Лучший сценарий 4 – 5 дней

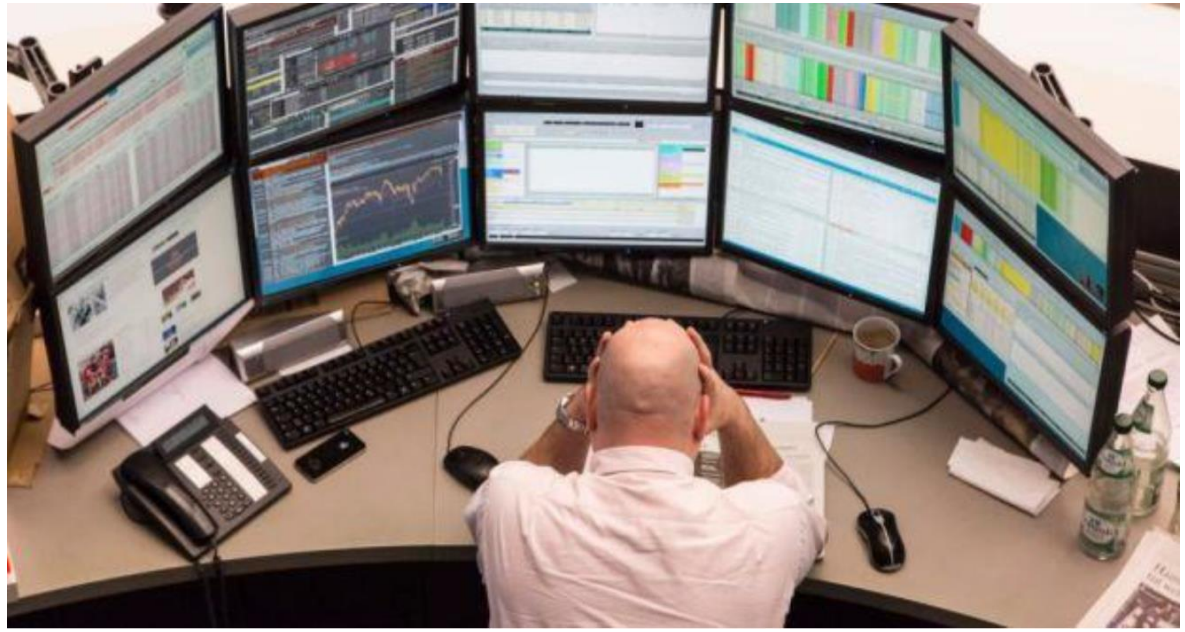
Будни SOC без Fidelis

Бесконечные ложные срабатывания и «инциденты»

Слабая приоритезация - с чего начать?

Затруднены ретроспективный анализ и форензика

Синдром «Alt + Tab» - слишком много инструментов
= слишком много экранов



Необходимость постоянной доработки правил корреляции для учета новых сценариев атак

Постоянная нехватка экспертов по безопасности с навыками и опытом

SIEM

Проверка и расследование инцидентов вместе с Fidelis

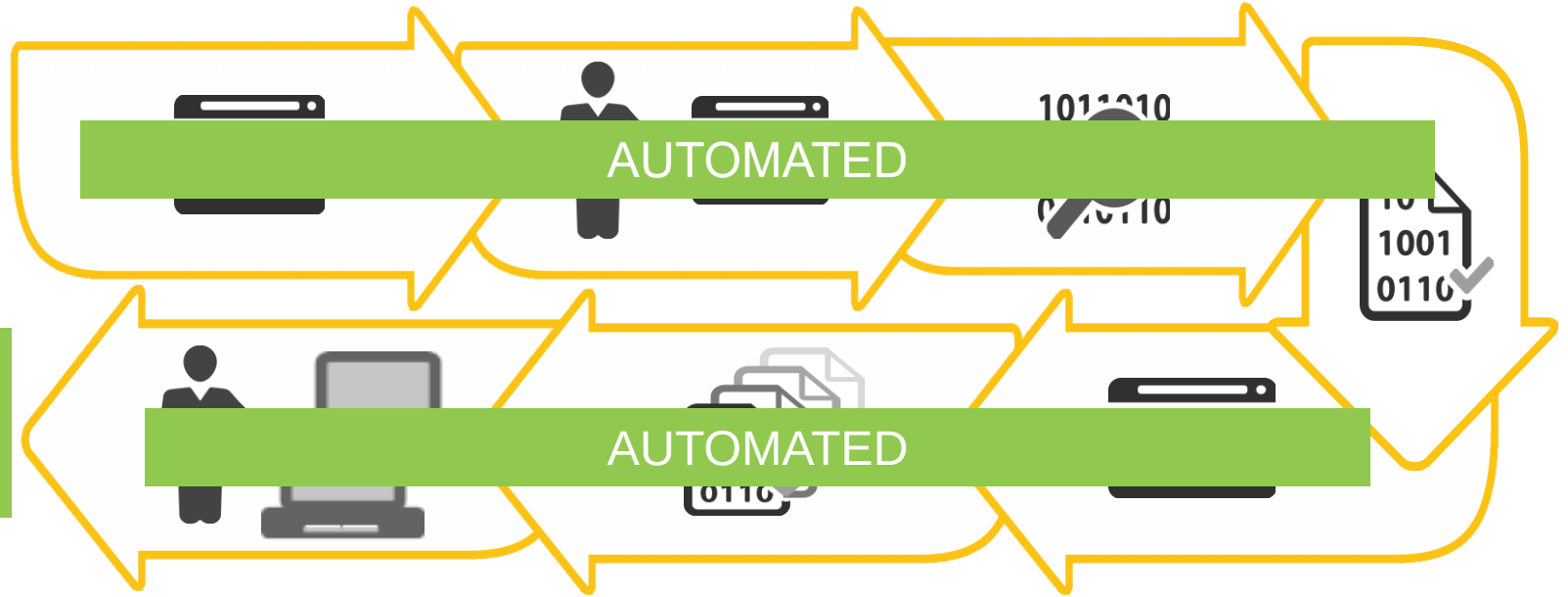
Типичный день в офисе

Типичный случай – в минутах (не дней!!)

Просмотр происшествия в SIEM

Определение диапазона событий и их важности

Поиск и определение подозрительных сетевых подключений или процессов которые выполняются



Анализ дампов памяти

Ручное восстановление системы

Выполнение более глубокого реагирования на происшествия – сбор ключевых артефактов (журналы событий/история Интернета)

Система потенциально скомпрометирована, Выполнить изоляцию

Fidelis Cybersecurity

Как найти злоумышленников в Вашей ИТ-инфраструктуре?

ОБМАНУТЬ. ОБНАРУЖИТЬ. УДЕРЖАТЬ. ОТРАЗИТЬ.

Платформа Fidelis Elevate - автоматическое обнаружение целенаправленных атак и действий инсайдеров без ложных срабатываний: на конечных точках, сетевом оборудовании, устройствах IoT и в облачных средах!

FIDELISSECURITY.COM

Oberig it

Компания Oberig IT
официальный дистрибьютор решений Fidelis
на территории Украины, Грузии и стран СНГ
oberig-it.com

Максим Прахов
Руководитель развития бизнеса в странах СНГ
m.prakhov@oberig-it.com
+7 (917) 570-87-38