SentinelOne®

Мини-антивирусная лаборатория у вас на каждом компьютере

Как работает SentinelOne EDR

Илья Осадчий, Talgar Systems

Давайте знакомиться, SentinelOne!

Антивирус, EDR, XDR и Deception нового поколения

2,000+
Сотрудников

9,000+
Заказчиков

$697M+
Инвестиции

$10B+
Капитализация

24/7

СЕРВИСЫ
MDR и DFIR

ПОДДЕРЖКА
Follow-the-Sun

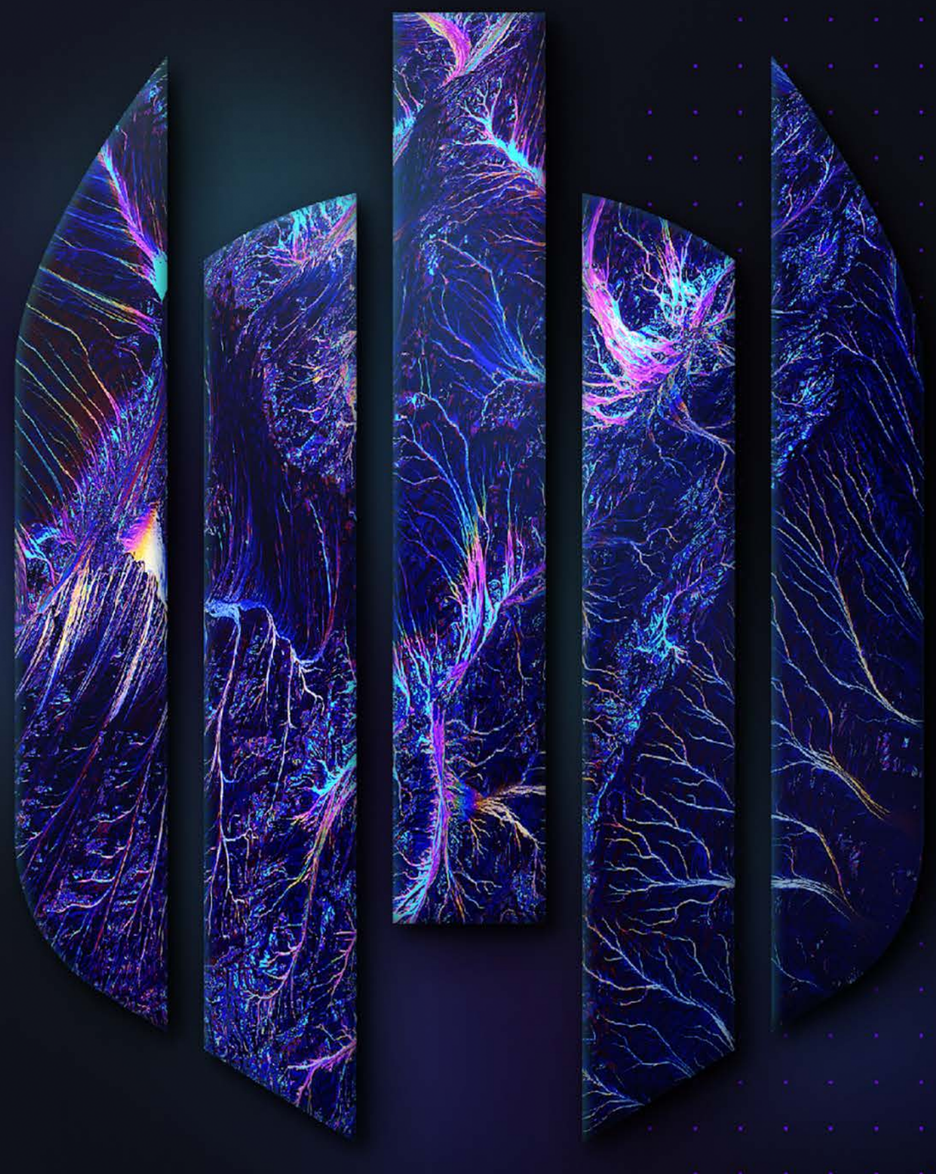
Лидер в Gartner Magic Quadrant

Лидер в MITRE ATT&CK Evaluations

SentinelOne

SentinelOne®

Как это все работает?



Алгоритм выявления атаки

Уже известное ВПО
При записи на диск и перед запуском.
~30% атак

Статический AI
Выявление при записи на диск и перед запуском

Поведенческий AI
Выявление на основе ML и логических правил

Threat Hunting / IR
Работа SOC с исходными данными в терминах MITRE

- ✓ Шифровальщики
- ✓ Латеральное движение
- ✓ Документы и скрипты
- ✓ Интерактивные сессии
- ✓ Фреймворки
- ✓ Эксплойты
- ✓ Бесфайловые атаки

SentinelOne

SentinelOne®

Статический ML

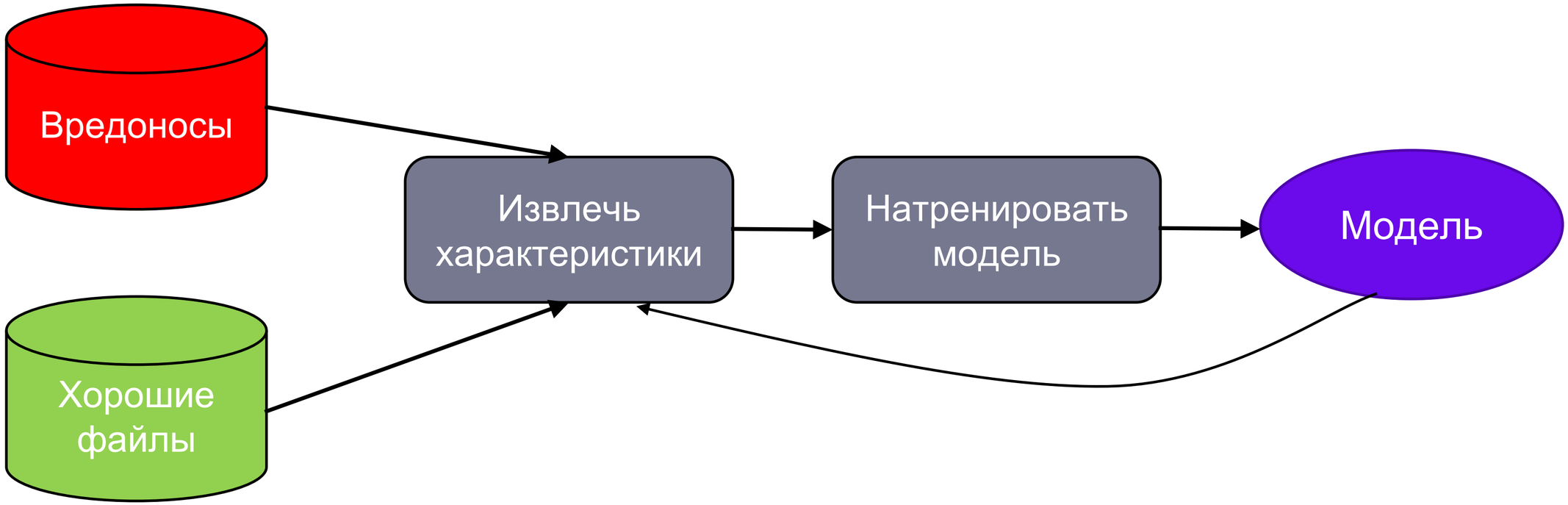
Проблема

Нужно классифицировать файл как вредонос, чистый или подозрительный

Сделать это быстро, до запуска, < 100 мс

Выявить ранее неизвестное ВПО, использующее новые техники

Обзор ML



Набор данных

Начальный сет из миллионов вредоносных и хороших файлов

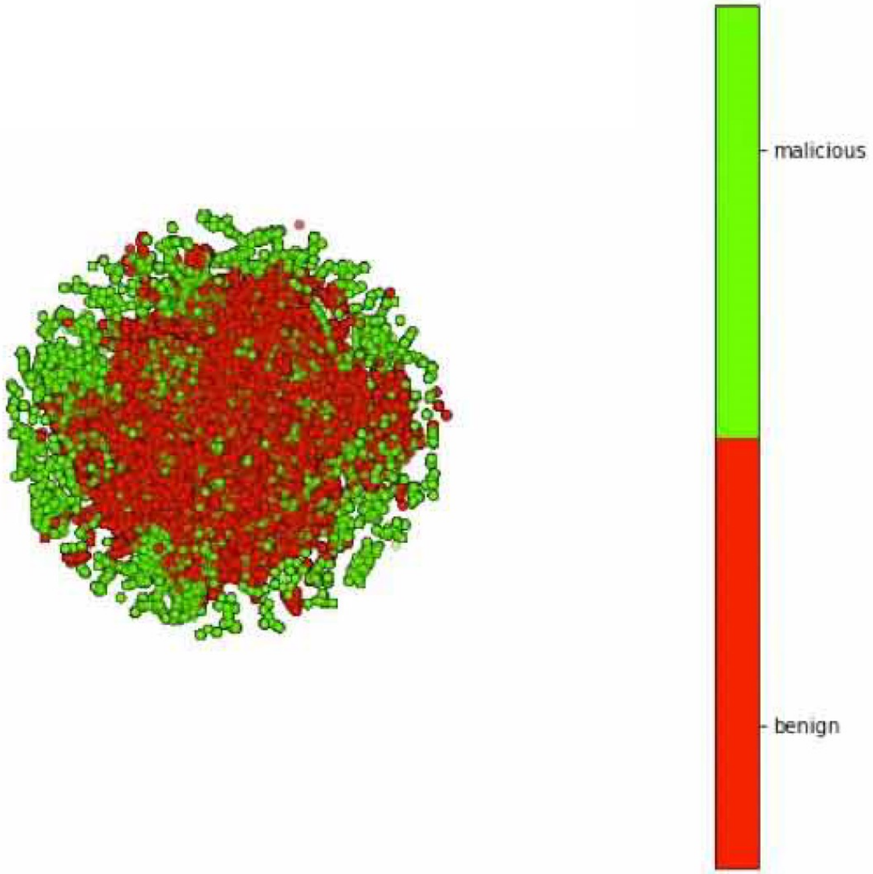
Постоянное получение новых из множества источников

- Фиды киберразведки
- Сайт распространения ПО
- Проблематичное ПО

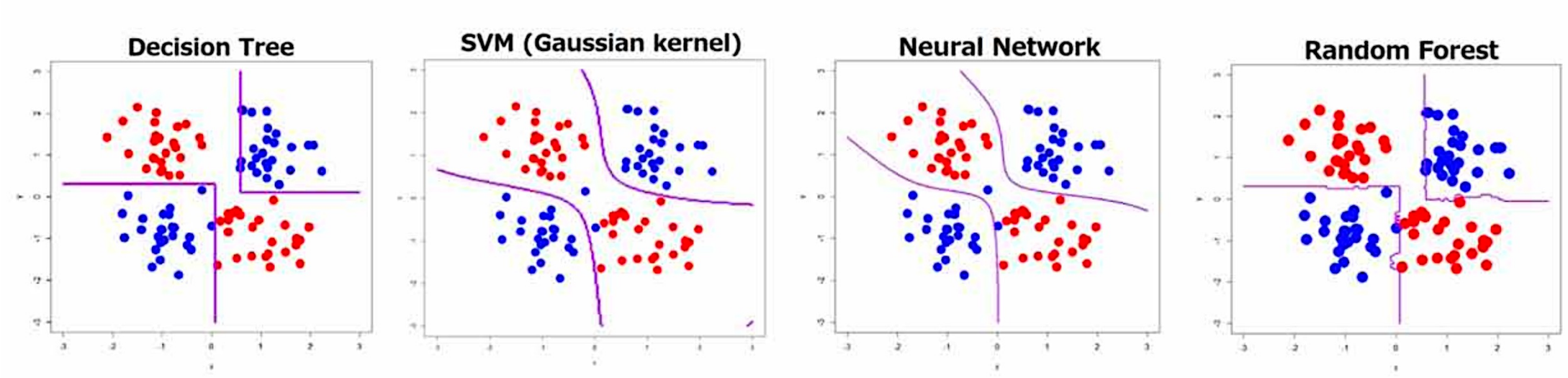
Извлечение характеристик

Характеристики PE	Характеристики макросов
Число секций	Энтропия кода
Что импортирет	Энтропия комментариев
Что экспортирует	Использует CallByName
Опкоды ассемблера	Использует XOR
Энтропия секций	Использует шелл
Крипто константы	Счетчик методов AutoExec
И многие другие …	И многие другие …

Тренируем модель – реальный пример



Битва классификаторов – вредонос или нет?



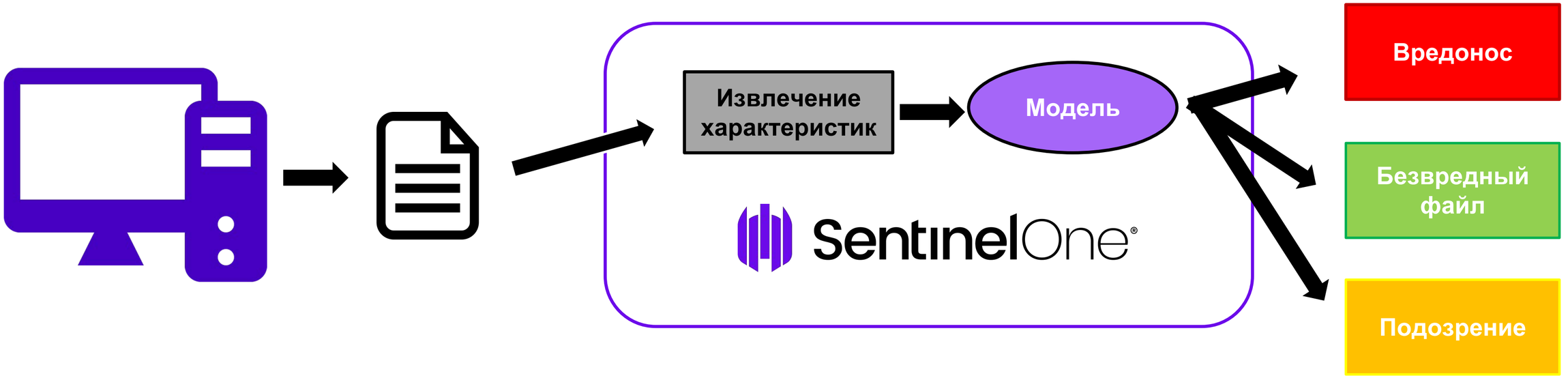
Дерево решений — классификация, основанная на вопросах о характеристиках, эмулирующая логику принятия решения

Метод опорных векторов – классификация элементов на основе поиска такого набора характеристик, который максимально разделяет элементы

Нейронные сети эмулируют работу мозга в принятии решений и частично комбинируют в себе идеи деревьев решений и метода опорных векторов

Случайный лес использует множество деревьев принятия решений при обучении и выбирает классификацию на основе решения большинства деревьев

Итог работы – в каждом агенте SentinelOne



SentinelOne®

Поведенческий ML

Проблема

Классификация запущенного процесса как **вредоносного**, **хорошего** или **подозрительного** на основе его поведения и сопутствующей информации

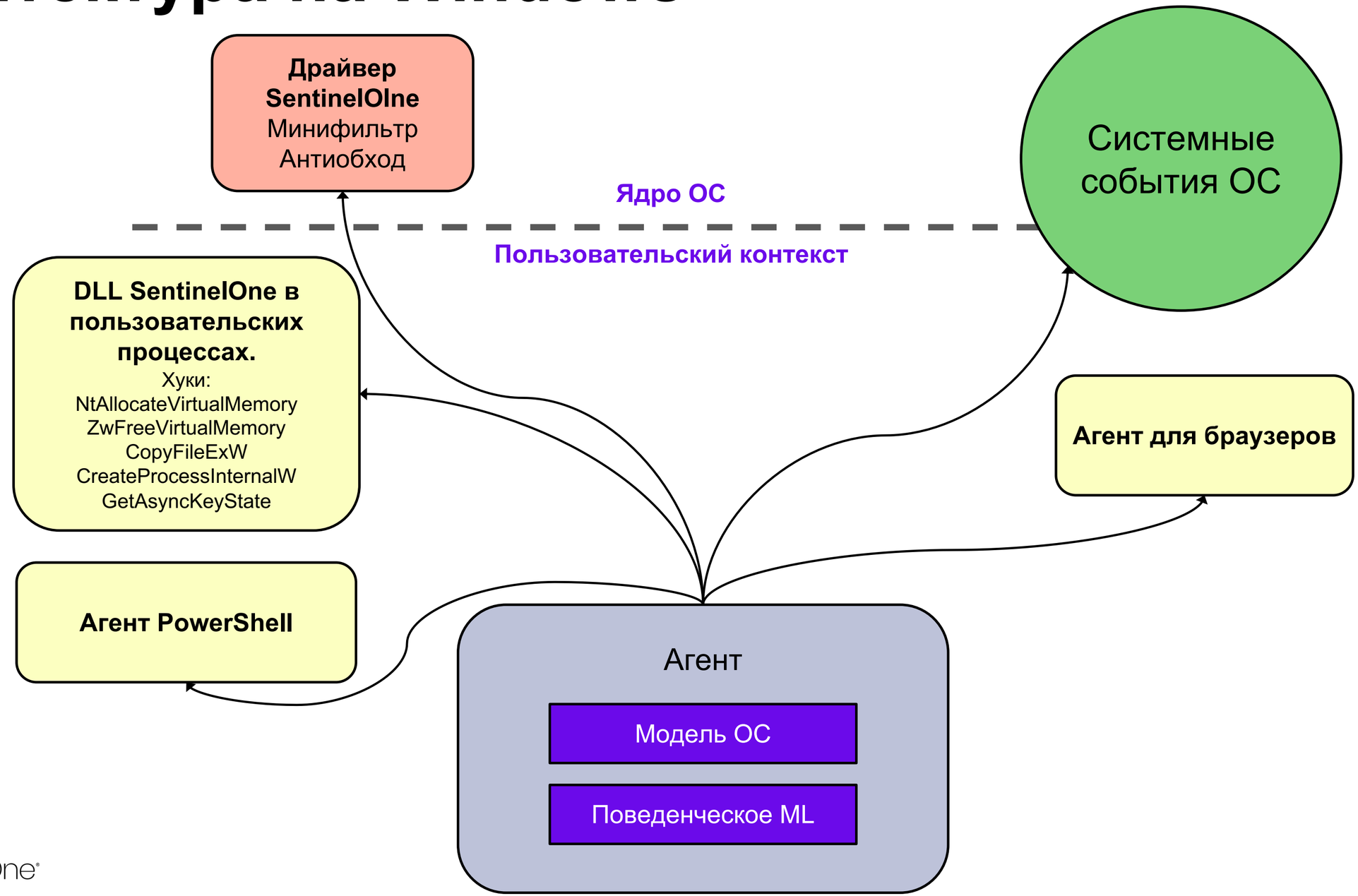
Мониторинг событий ОС

- Сотни типов
- Внутренние для Windows
- Некоторые недокументированные, но полезные маркеры

Корреляция поведения и вредоносности

Движок поведенческого ML

Архитектура на Windows

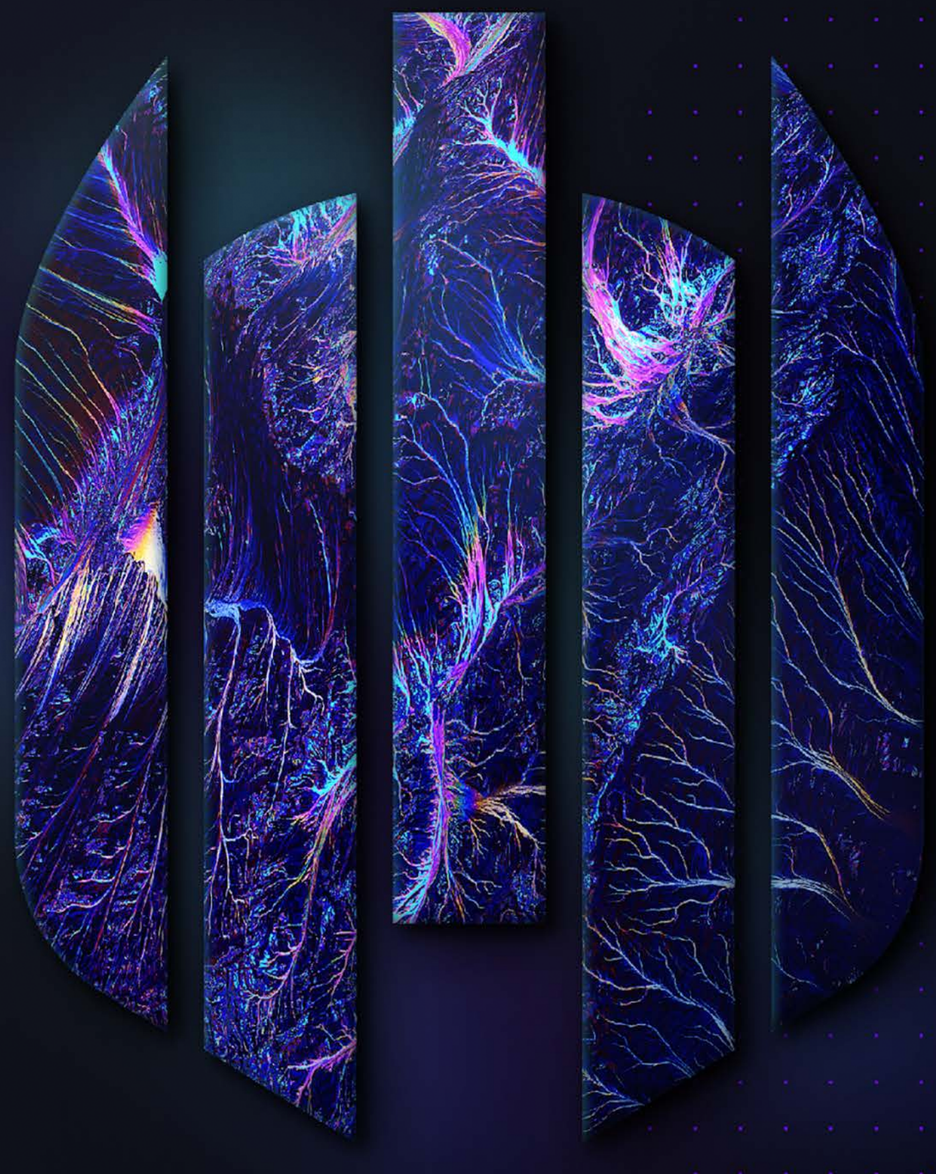


Возможности детекта

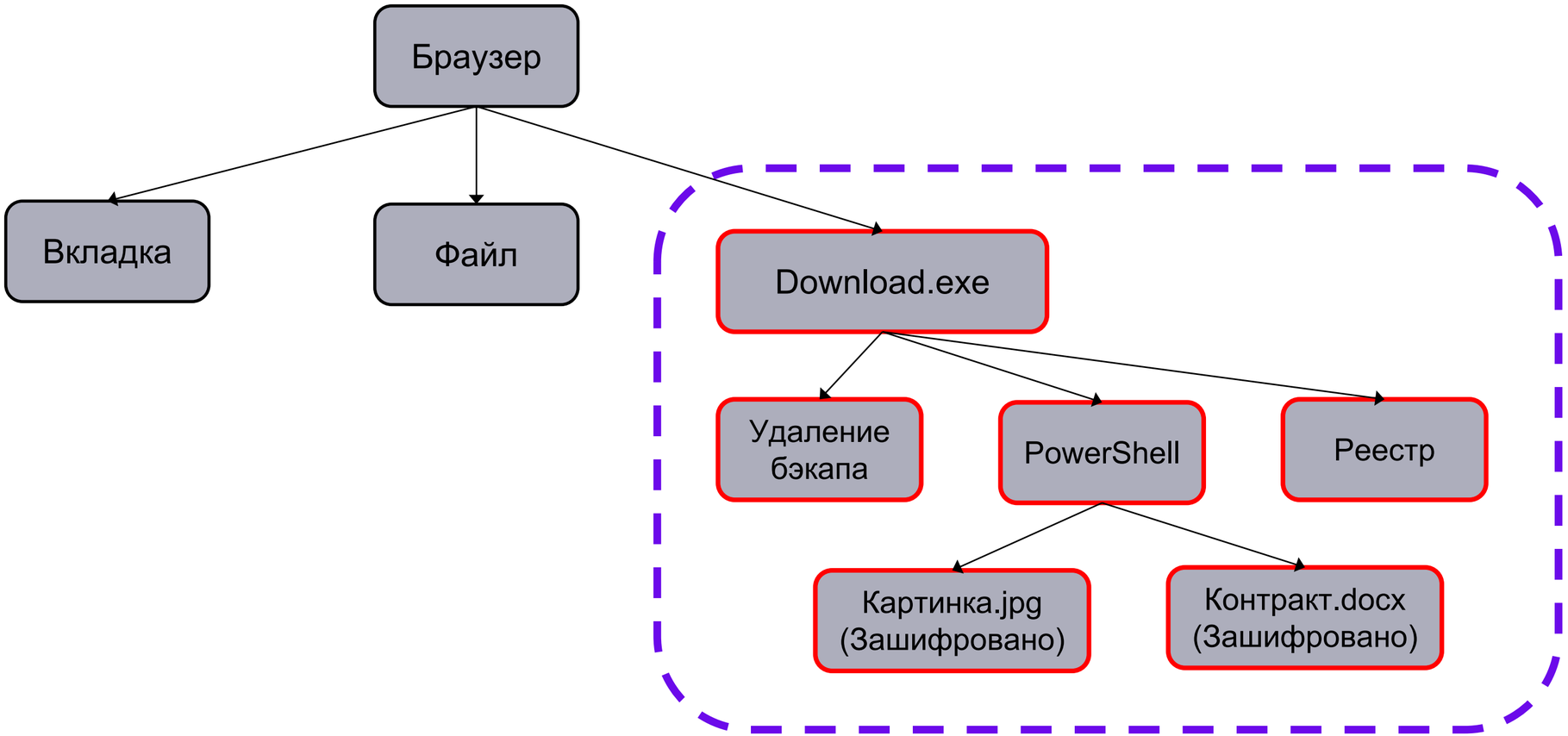
Манипуляции с ОС	Известные фреймворки	Техники эксплуатации
• Обход UAC • Инъекции кода • Персистетность • Шифровальшики • Кража информации • Кража паролей • Кейлоггеры • Удаленный шелл • Латеральные движения • Process hollowing • дебаг / Анти-ВМ • Doppelganger • Попытки скрытия	• Meterpreter • Empire • Shinobot • Koadic • Mimikatz • Powersploit • PowerUp	• Stack Pivot • Java-эксплойты • Shellcodes • Обход песочницы • Документы и скрипты • Эксплойты сс эскалацией привилегий • ROP

SentinelOne®

Реагирование и защита



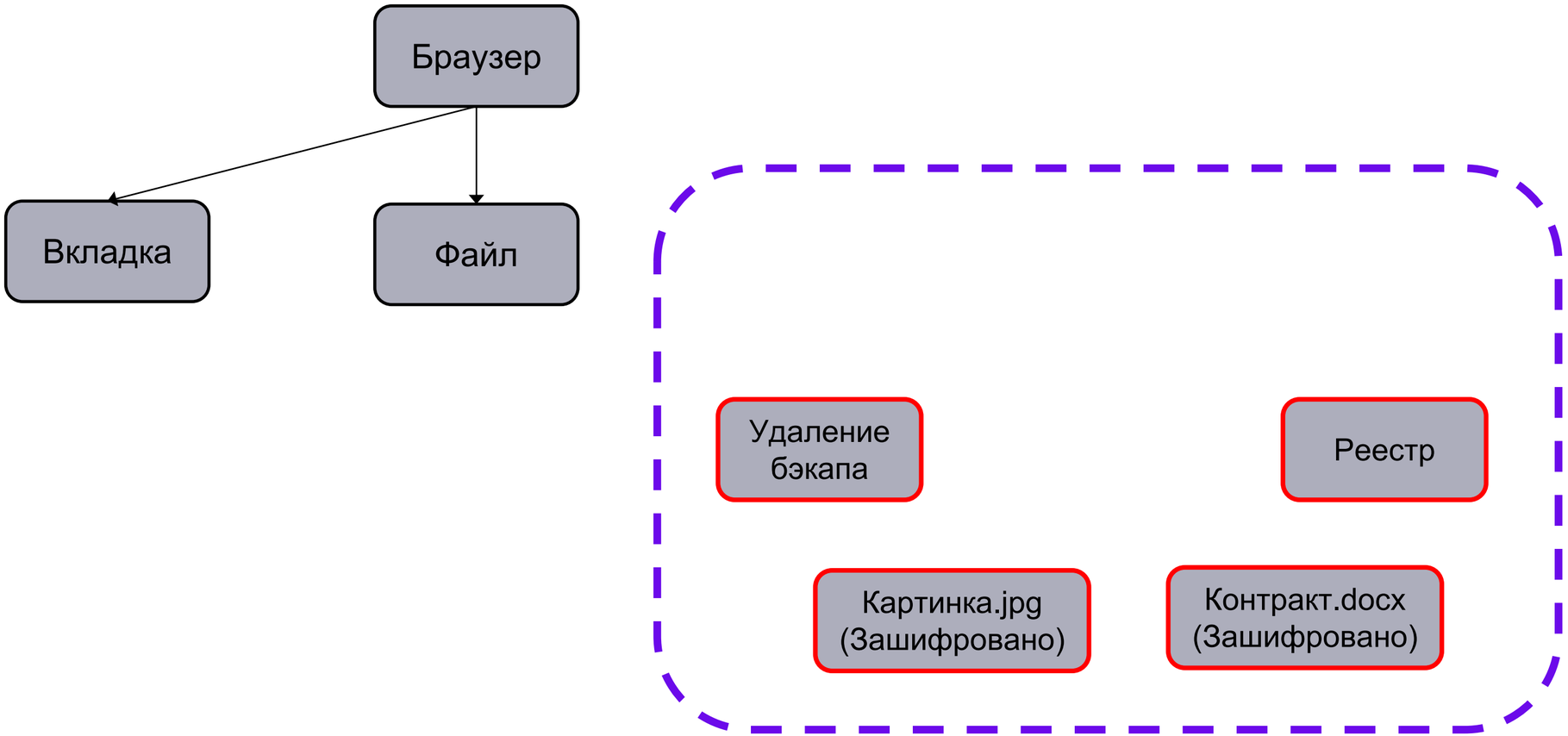
Реагирование и защита



Уникальная модель данных SentinelOne
позволяет работать со сложными потоками событий ОС (APC, RPC, Remote Threads и т.д.)

Реагирование и защита

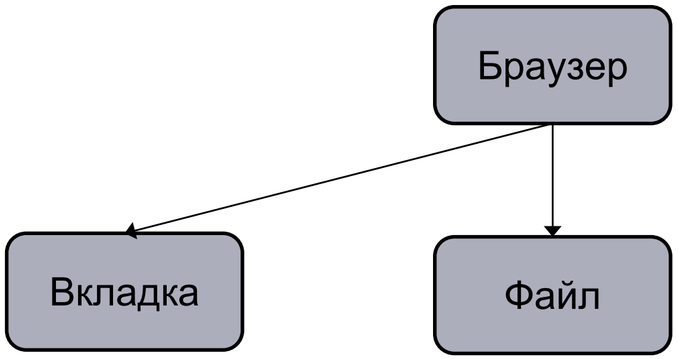
Download.exe и скрипт PowerShell терминированы и помещены в карантин

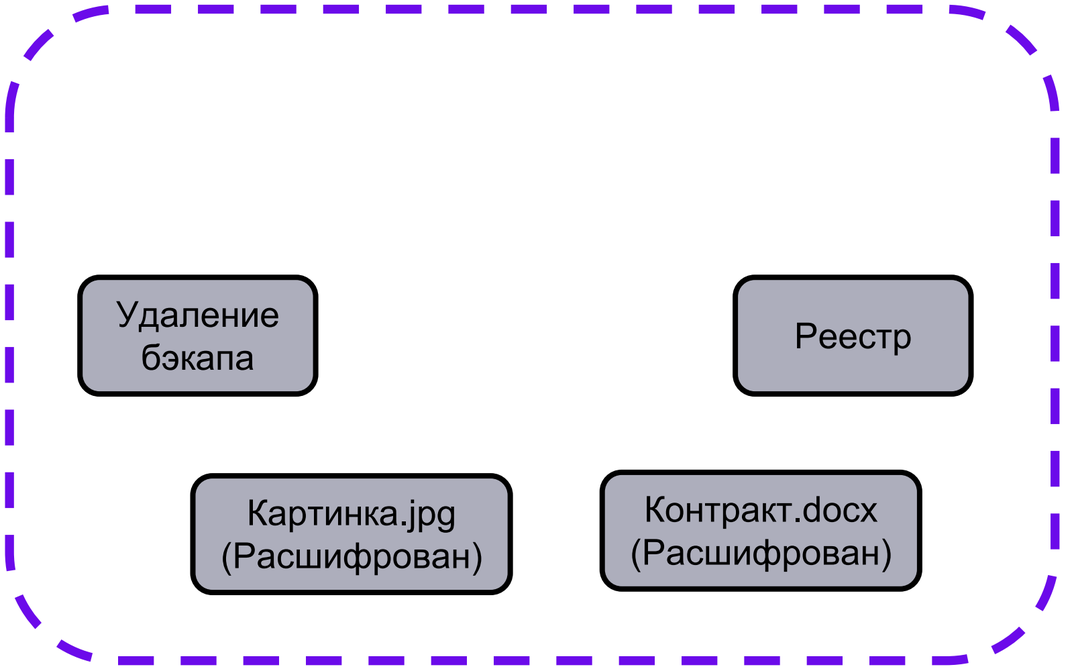


Уникальная модель данных SentinelOne
позволяет работать со сложными потоками событий ОС (APC, RPC, Remote Threads и т.д.)

Реагирование и защита

Бэкап и файлы восстановлены
Конфигурация, изменения реестра и пр. отменены
Все это за секунды!

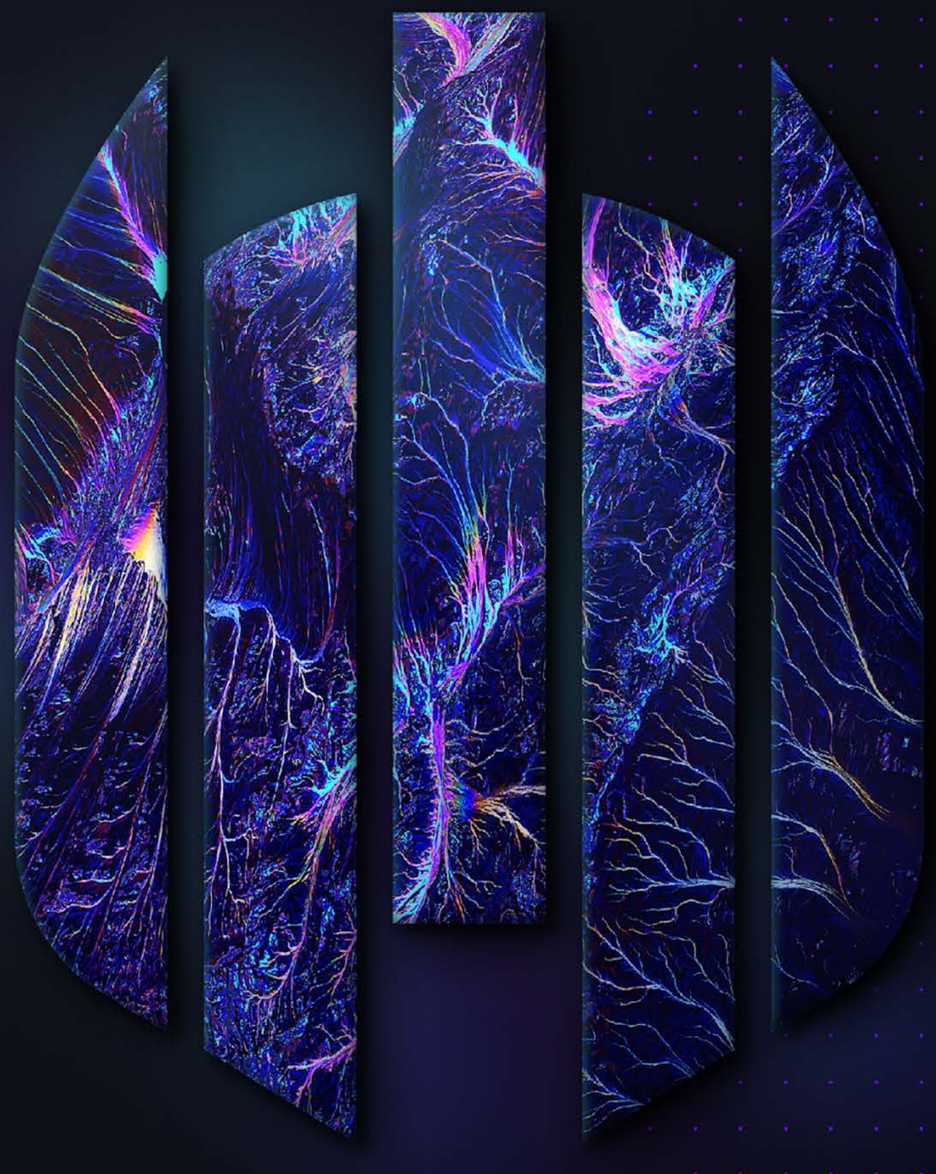




Уникальная модель данных SentinelOne
позволяет работать со сложными потоками событий ОС (APC, RPC, Remote Threads и т.д.)

SentinelOne®

Комплексный подход SentinelOne



Пирамида SentinelOne

SentinelOne Hologram

SentinelOne Identity

SentinelOne Ranger AD

SentinelOne Singularity

SentinelOne®

Уникальное предложение!

Бесплатный аудит Active Directory
на 90 признаков атак, рисков, ошибок
конфигурации с помощью
SentinelOne Ranger AD

hello@talgarsystems.com