SentinelOne™

SentinelOne
Антивирус и EDR нового поколения

Илья Осадчий
Тайгер Оптикс, дистрибьютор в России и СНГ
Email io@tiger-optics.ru

Давайте знакомиться, SentinelOne!
Антивирус и EDR нового поколения

900+
Сотрудников

5,500+
Заказчиков

$697M+
Инвестиции

$3B+
Капитализация

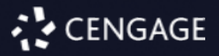
24/7

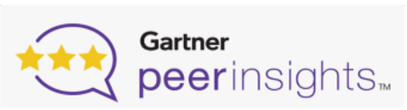
СЕРВИСЫ
MDR и DFIR

ПОДДЕРЖКА
Follow-the-Sun

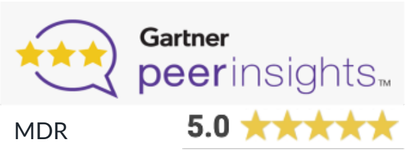
ЛОКАЦИИ
Тель Авив, Амстердам, Токио, Маунтин Вью

РОССИЯ И СНГ
Уже более 20 заказчиков в России и СНГ





Топ-вендор в категориях EDR и EPP



Топ-вендор в категории MDR

Рекомендовано 2019

Аттестации PCI DSS и HIPAA

EDR
Сильный игрок

Наибольшее число детектов в тесте APT29

Лучший новый продукт SE Labs

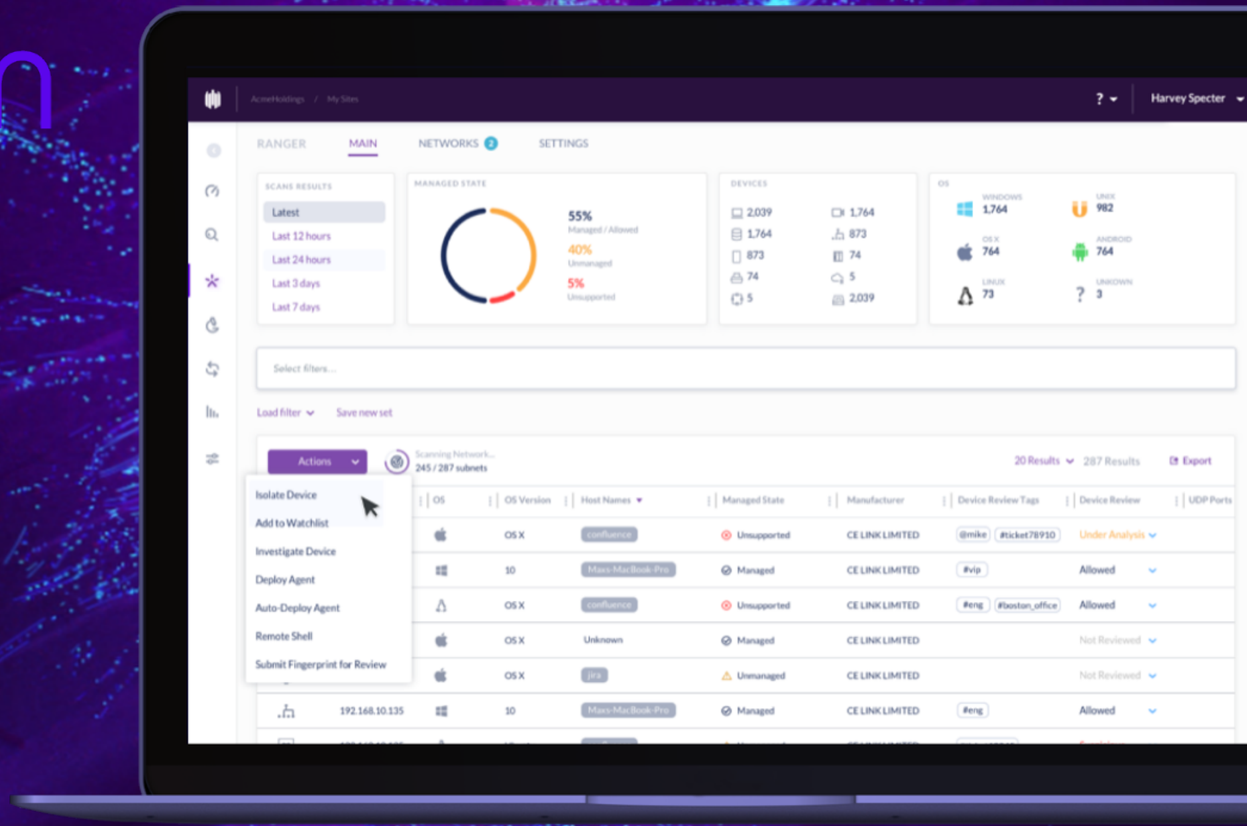
Singularity Platform

Антивирус и EDR нового поколения

Хосты

IoT

ЦОД и облако

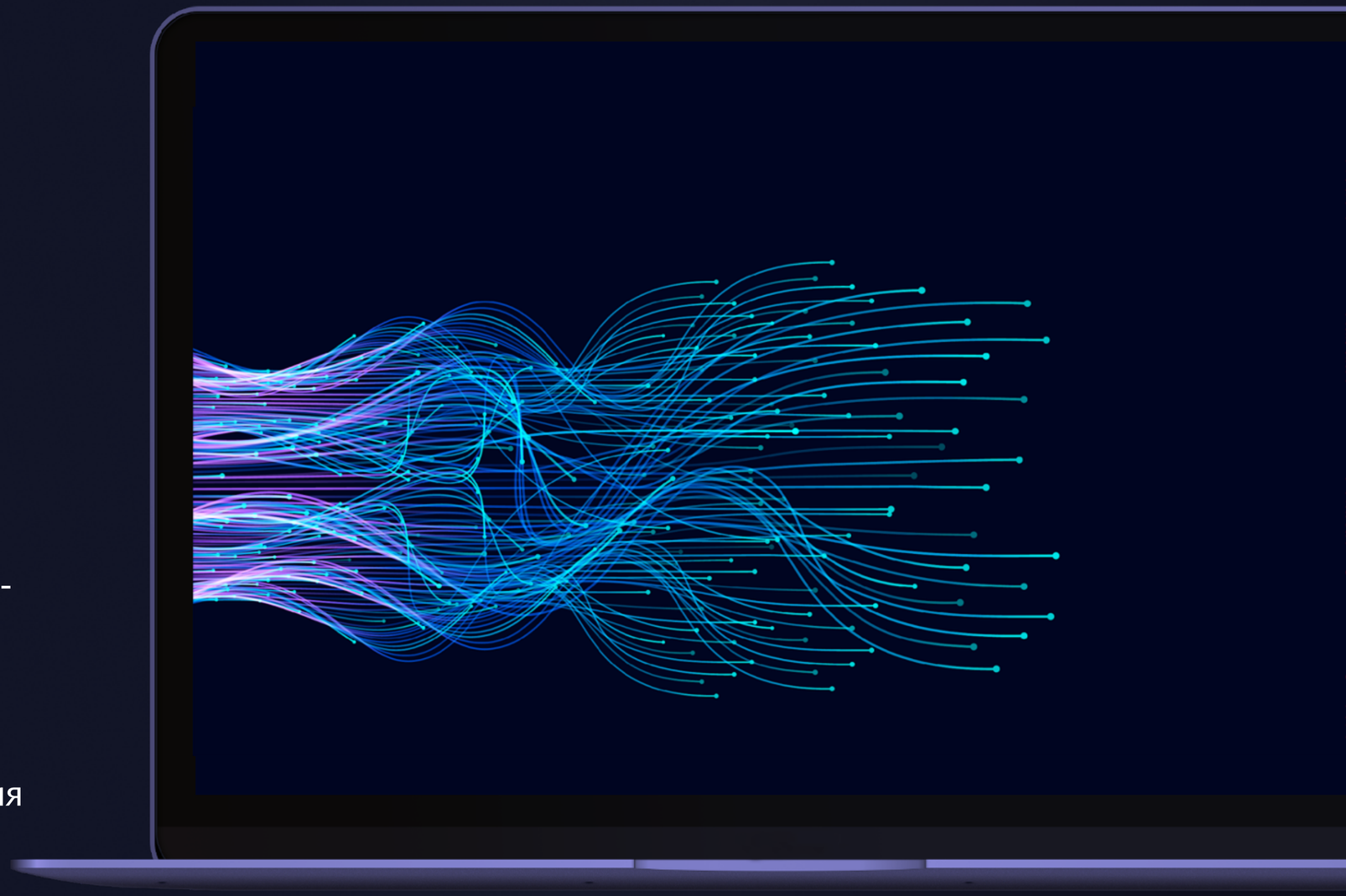


Singularity™ Platform

Storyline™

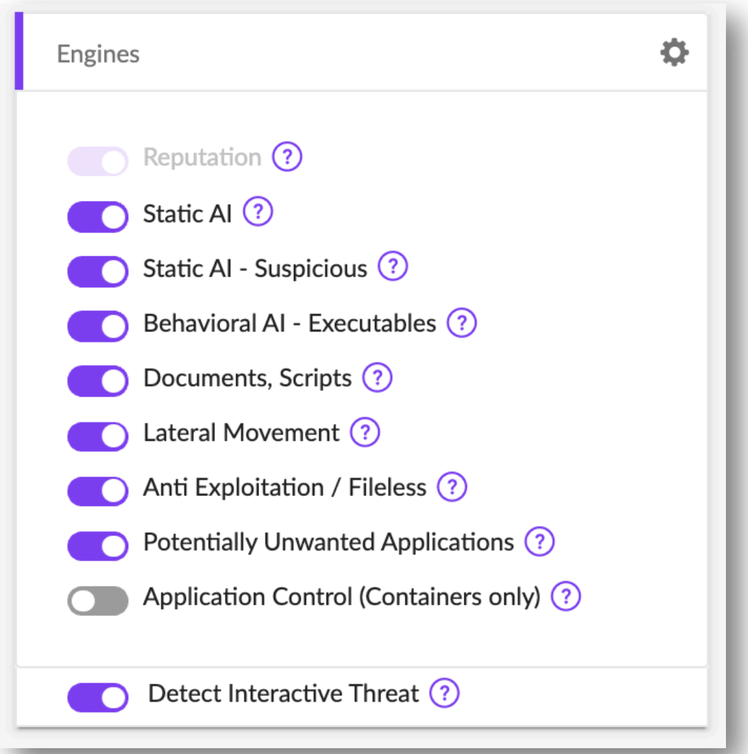
Автоматические сюжетные линии

- Запатентованный контекст в реальном времени для всех ОС
- Быстрое предотвращение на основе встроенного ИИ
- Долгосрочный горизонт хранения EDR-данных для любых запросов, хантинга по TTP MITRE, реагирования и т.п.
- Восстановление за один клик откатывает неавторизованные действия на всех хостах



9 движков в агенте

1. Репутация (хэши)
2. Статический ИИ при записи на диск и перед запуском
3. Поведенческий ИИ
4. Документы и скрипты
5. Латеральное движение (входящие подключения)
6. Антиэксплойт / бесфайловые атаки
7. Потенциально нежелательное ПО
8. Контроль приложений в контейнерах
9. Интерактивные угрозы (расширение поведенческого ИИ для интерактивных сессий)

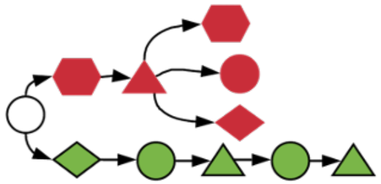


Логика работы агента

Статический анализ

ИИ для PE и документов

Поведенческий анализ



Динамические модели

Автоисправление

- Остановить и карантин
- Контроль приложений
- Отключить / изолировать
- Подчищение действий атаки
- Полный откат
- Работает онлайн и офлайн

Глубокий мониторинг

- Хантинг, в т.ч. на основе MITRE ATT&CK TTP
- Списки наблюдения STAR
- Быстрые запросы
- Полный сценарий атаки
- Трактовка цепочки как атаки
- Полный удаленный шел

ДЕТЕКТ И ПРЕДОТВРАЩЕНИЕ В РЕАЛЬНОМ ВРЕМЕНИ + ИСПРАВЛЕНИЕ И ВОССТАНОВЛЕНИЕ

РАССЛЕДОВАНИЯ ХАНТИНГ РЕАГИРОВАНИЕ

Длительность = Секунды
Единый легкий агент
Автономная работа агента + облако
Windows, Mac, Linux, VDI, облака, Kubernetes/Docker

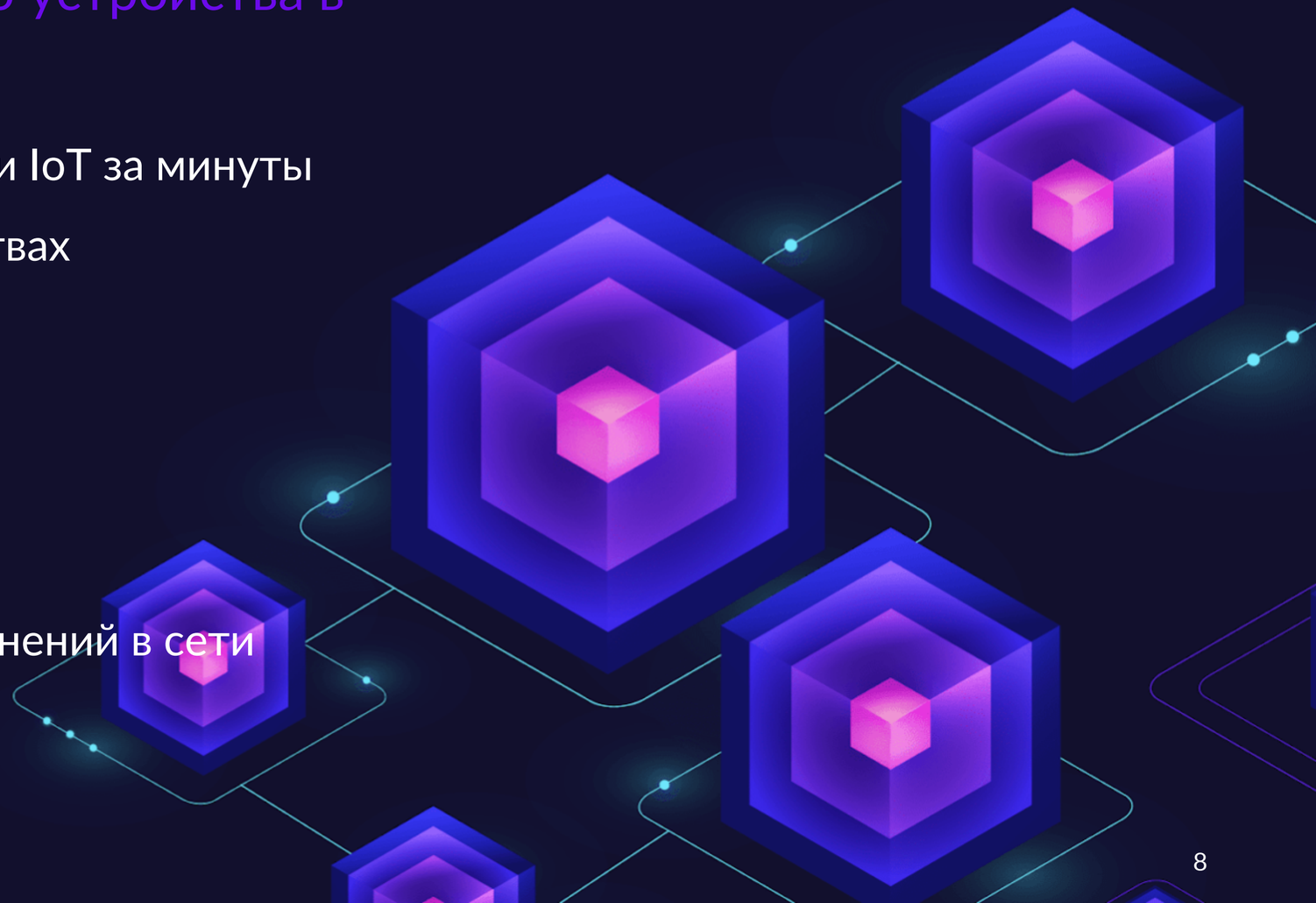
Хранение: 14 дней – 1 год
Полный контекст и корреляция
Встроенные процессы реагирования

Мониторинг и контроль сети

Singularity | RANGER

Обнаружение и отпечаток каждого устройства в сети

- Глобальная инвентаризация хостов и IoT за минуты
- Выявление уязвимостей на устройствах
- Изоляция чужаков за 1 клик
- Автоустановка агентов соседями
- Детальные политики контроля
- Не требует новых агентов или ПО
- Не требует нового железа или изменений в сети



И многие другие функции...

- Антивирус
- Отчеты по течению атаки
- Откат и восстановление в 1 клик
- Изоляция от сети, карантин файла
- Хостовой МСЭ
- Управление съемными устройствами
- Инвентаризация ПО и уязвимостей
- Выявление устройств без агентов
- ActiveEDR и Storyline
- Интеграция с MITRE ATT&CK
- Удаленный полноценный шел
- FIM
- Списки наблюдения в EDR
- Функции для серверов (соответствие CIS, App Control, метаданные облаков)
- Локер двоичных файлов
- Кастомные правила хантинга
- Стримминг данных в свое озеро
- Многотенантность
- Мониторинг и защита от IoT-атак, изоляция устройств
- Автоустановка агентов на устройства без них
- IoT-хантинг
- Ролевая модель доступа
- Дашборды
- API
- Windows, Linux, Mac, K8s / Docker, в т.ч. старые версии

SentinelOne™

Испытания MITRE ATT&CK Phase 2: APT29

Качество детекта по методике MITRE ATT&CK
Контекст + корреляция событий атаки

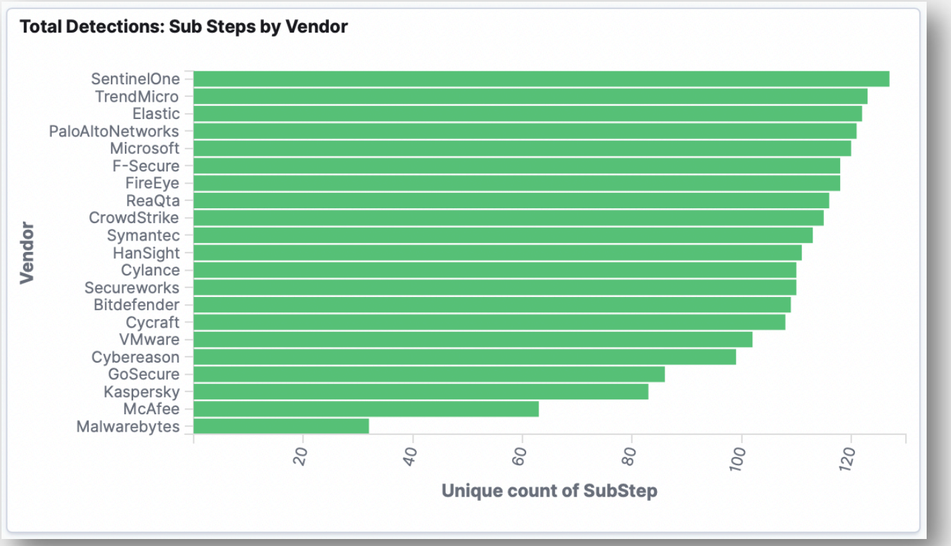
Корреляция

Связывает разрозненные алерты и события в единую причинно-следственную связь цепочки атаки

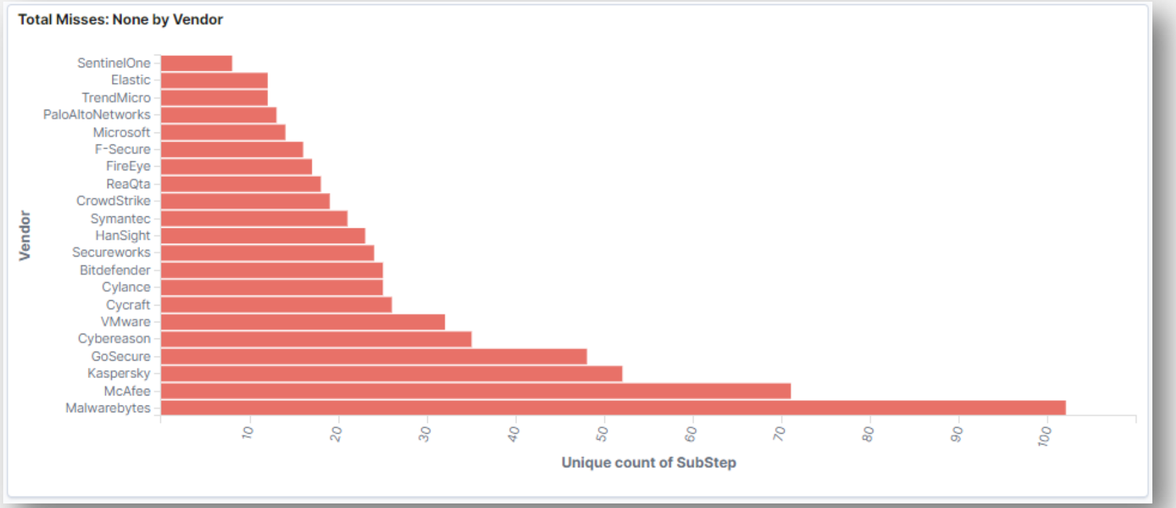
Детальное описание концепций: attackevals.mitre.org/APT29/detection-categories

Базовое сравнение

Выявлено подшагов (продукт + MSSP)

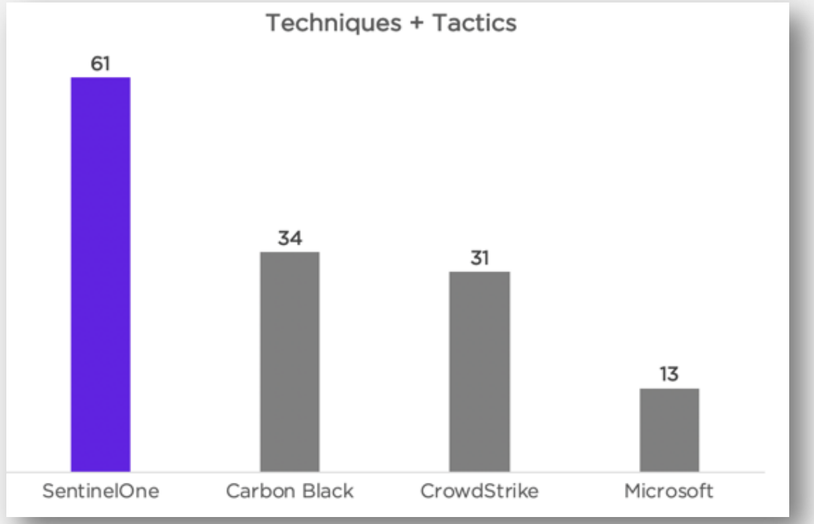


Пропущено подшагов



Выявлено подшагов (только продукт, без MSSP)

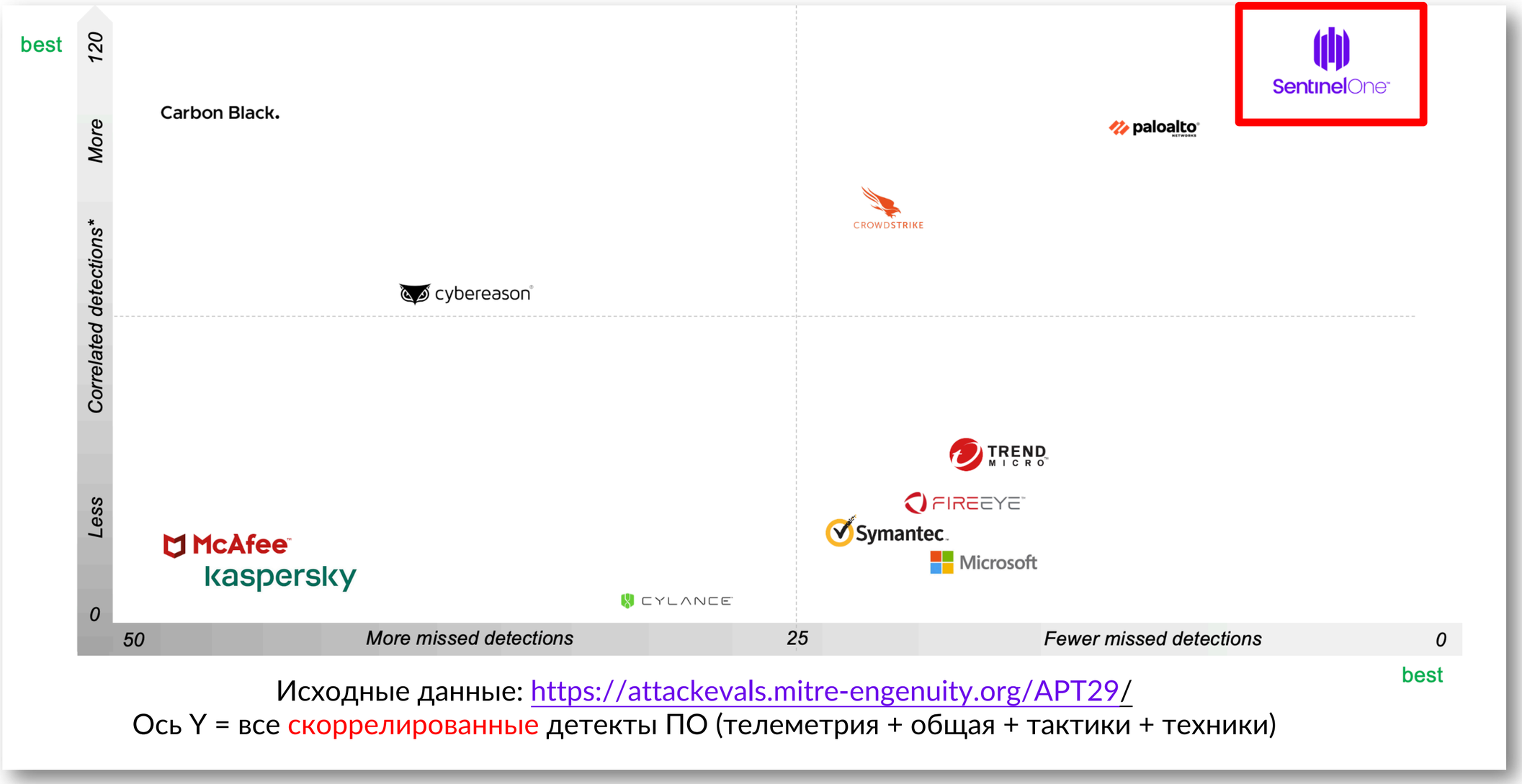
Выявлено техник + тактик



SentinelOne

Исходные данные: https://ela.st/mitre-eval-rd2 и https://www.sentinelone.com/blog/coverage-and-context-the-key-measures-of-mitre-attck-

Сравнение по качественным детектам + пропускам



Исходные данные: https://attackevals.mitre-engenuity.org/APT29/
Ось Y = все скоррелированные детекты ПО (телеметрия + общая + тактики + техники)

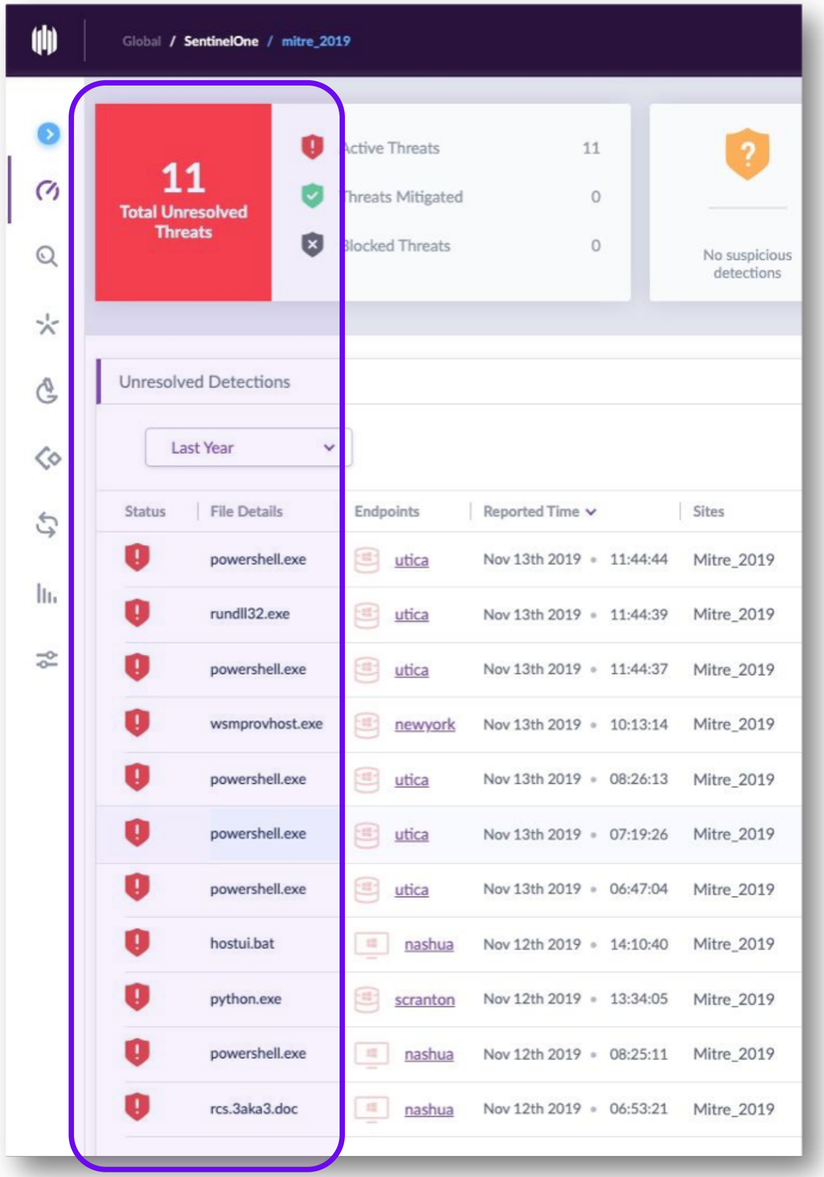
3 дня атак = 11 алертов в консоли

«Покрытие техник MITRE ATT&CK» важно, но также важно, дает ли вам продукт сырые данные, **или решает за вас проблемы:**

- **72 часа атак автоматически сгруппированы в 11 инцидентов в консоли**
- **Наибольшее число детектов *Тактик и Техник*, а не сырых логов (которые НИКТО не смотрит)**
- **Наименьшее число пропущенных шагов**

Это и есть реальная польза S1 для заказчиков и сила Storyline:

- Снижение усталости от отдельных алертов
- Повышение скиллов аналитиков благодаря автоматизации и простоте использования
- Снижение времени реагирования (MTTR)



SentinelOne™

Истории успеха в России и СНГ

Разработчик ПО

Что продали:
6.000 хостов CMP

Проблемы и задачи

- Повысить уровень ИБ → нужен EDR
- Более сильная защита Mac и Linux
- Локальная инсталляция усложняла архитектуру / не хотели тратить время
- Конкуренты: CRWD, CB

Почему S1

Наибольшее количество взаимосвязанных событий и заблокированных угроз в сочетании с лучшей видимостью

Заменили локальную инсталляцию Касперского на более гибкое решение с одним агентом

Сниженная сложность и более быстрое развертывание на новых устройствах с помощью интегрированного решения на основе AWS

Разработчик ПО

Что продали:
501 хост CTL

Проблемы и задачи

- Унификация защиты
- Нет защиты от «современных» атак
- Конкуренты: CB и CRWD

Почему S1

Качественный понятный детект

Заменили MS и ESET на более автоматизированное решение → ActiveEDR

Более простое внедрение и управление

Страховая компания

Что продали:
350 хостов CMP

Проблемы и задачи:

- Повысить уровень ИБ → нужен EDR
- Проблемы с ESET
- Ручные процессы
- Конкуренты: CB, Cortex XDR

Почему S1

Более сильная защита, особенно против критолокеров

Заменили ESET на автоматизированное единое решение

Снижение сложности и более быстрое исправление проблем, функционал отката впечатлил

SentinelOne™

Лицензирование, опции и сервисы

Редакции и опции

Редакции ПО	Функции
Core	Антивирус, откат и восстановление в 1 клик, сетевая изоляция, карантин файлов, отчеты по атакам с индикаторами MITRE ATT&CK, API, поддержка 8x5
Control	+ МСЭ, управление съемными устройствами, инвентаризация ПО и уязвимости, выявление устройств без агентов
Complete	+ ActiveEDR, Storyline, интеграция с MITRE ATT&CK, удаленный шел, FIM, списки наблюдения, хранение данных 14 дней

Дополнительные варианты и опции	
Ranger	Мониторинг и защита от IoT-атак, авто-установка агентов на устройства без них, IoT-хантинг
Дополнительные опции	Хранения EDR-данных до 30/90/365 дней, функции для серверов (соответствие CIS, App Control, метаданные облаков), локер двоичных файлов, кастомные правила, стримминг данных в свое озеро
Сервисы	Поддержка 24x7, TAM, установка и ведение инсталляции, Vigilance MDR

Минимальный заказ – 100 агентов

Детальный список https://www.sentinelone.com/platform-packages/

SentinelOne™

Спасибо!
Вопросы и ответы

Илья Осадчий
Тайгер Оптикс, дистрибьютор в России и СНГ
Email io@tiger-optics.ru