SentinelOne

ОБЗОР РЕШЕНИЯ

SentinelOne Singularity XDR

Ландшафт киберугроз растет и меняется быстрыми темпами. Векторов атаки становится все больше: они нацелены как на конечные точки, так и на сети, облака и контейнерные среды. Для защиты от конкретного вектора и связанных с ним уязвимостей многие организации выбирают отдельные решения, в идеале лучшие в своем классе. Однако эти точечные СЗИ не позволяют сопоставить информацию о безопасности со всех защитных решений компании. В результате данные собираются и анализируются по отдельности. Из-за отсутствия контекста и корреляции возникают пробелы в мониторинге и обнаружении угроз. Кроме того, расследования, которые проводятся вручную, могут занимать много времени и быть утомительными. В результате команды ИБ не успевают сдерживать и нейтрализовать угрозы.

Singularity XDR

SentinelOne Singularity XDR объединяет и расширяет возможности обнаружения и реагирования различных уровней защиты. Платформа предоставляет командам ИБ централизованный и полноценный мониторинг происходящего в масштабах всей организации, мощную аналитику и автоматическое реагирование с учетом всех СЗИ. Singularity XDR позволяет организациям решать проблемы кибербезопасности унифицированно и проактивно по всей сети. Благодаря этому аналитики ИБ могут легче выявлять и останавливать атаки до того, как они нанесут ущерб бизнесу.

Ключевые возможности

01 Ликвидируйте «слепые пятна» с помощью данных со во всей экосистемы ИБ

Платформа Singularity XDR позволяет организациям беспрепятственно собирать структурированные, неструктурированные и полуструктурированные данные в реальном времени с любых технологических продуктов или платформ, устраняя разрозненность данных и опасные слепые зоны. Благодаря Singularity XDR службы ИБ могут на едином дашборде просматривать данные, собранные СЗИ со всех платформ, включая конечные точки, облачные нагрузки, сетевые и IoT-устройства и т. д. Singularity XDR позволяет аналитикам пользоваться информацией, полученной в результате объединения данных из нескольких решений в один интегрированный инцидент. Платформа также предоставляет заказчикам возможность централизовать выявление инцидентов и их отработку, обеспечивая комплексный мониторинг, автономное выявление и предотвращение киберугроз, а также реагирование на них. Так организации могут решать проблемы кибербезопасности из единой консоли.

02 Выявляйте скрытые атаки благодаря корреляции данных со всех СЗИ

Запатентованная технология SentinelOne Storyline автоматически предоставляет в режиме реального времени контекст событий, собранных со всех СЗИ организации, а также их взаимосвязи, преобразуя разрозненные данные в информативные «сюжетные линии».

ПОЛЬЗА РЕШЕНИЯ

Повышает эффективность и продуктивность SOC

Реагирование на инциденты происходит без задержек благодаря тому, что не нужно переключаться между решениями или несколькими дашбордами. Единая платформа и рабочий процесс сокращают число алертов, устраняют «слепые пятна» и пробелы в данных, а команды ИБ видят всю необходимую для реагирования информацию в единой консоли.

Быстрая окупаемость

Встроенные интеграции со множеством разнообразных продуктов позволяет получить максимальную отдачу от уже развернутых в организации СЗИ.

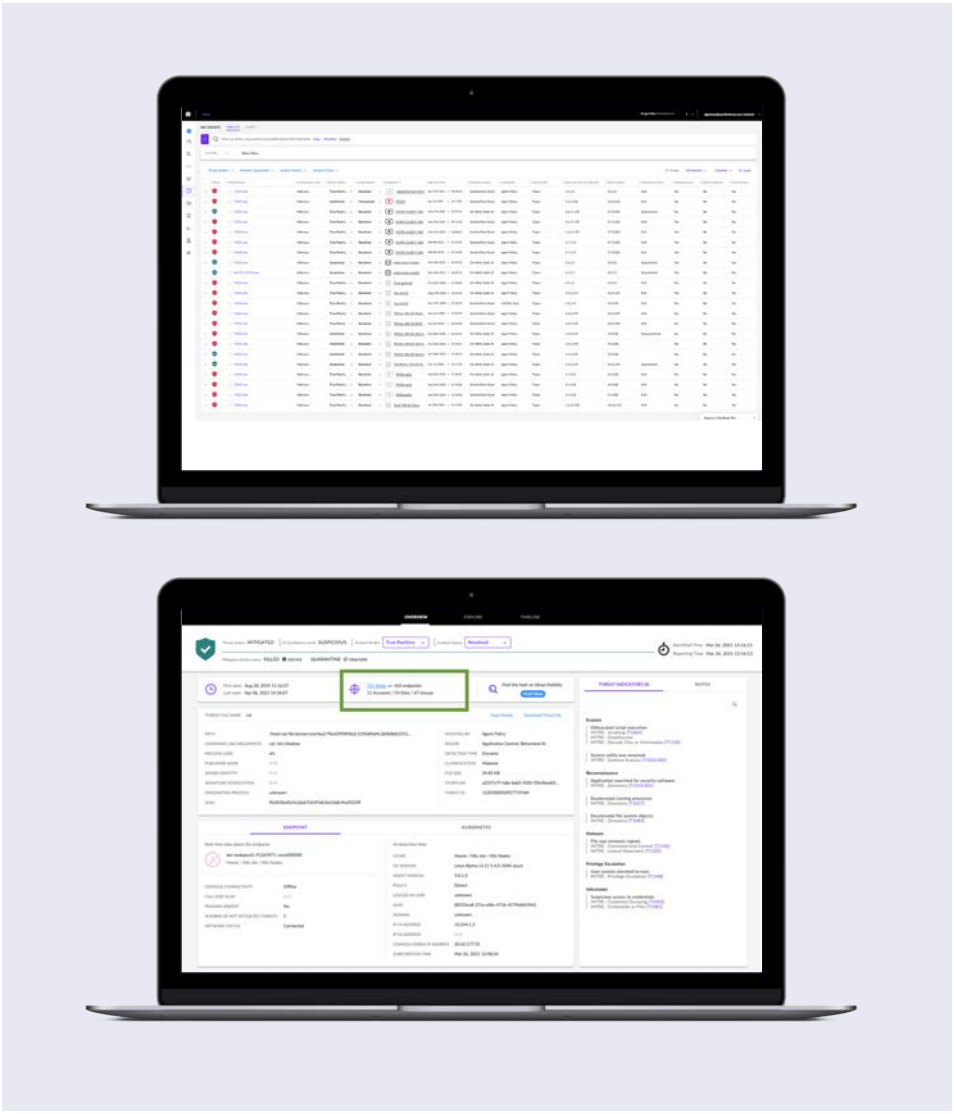
Оптимизация рабочих процессов

Просматривайте потоки разрозненных данных и аналитику по ним на единой панели управления.

Сниженная совокупная стоимость владения (TCO)

Сократите расходы, связанные с настройкой и интеграцией множества точечных СЗИ благодаря полностью интегрированной платформе кибербезопасности.

Это позволяет аналитикам ИБ понять, что произошло в их среде. Storyline автоматически соединяет все связанные между собой события и действия в одну цепочку развития атаки и присваивает ей уникальный идентификатор. Благодаря этому команды ИБ могут за несколько секунд увидеть полный контекст инцидента, а не тратить часы, дни или даже недели на корреляцию логов и поиск связей между событиями вручную. Поведенческий модуль SentinelOne отслеживает все действия в системе, включая изменения в файлах и реестре, запуск или остановку сервисов, межпроцессное взаимодействие и сетевую активность. Модуль выявляет техники и тактики атакующих, которые служат индикаторами компрометации. Это позволяет отслеживать скрытое вредоносное поведение и эффективно выявлять бесфайловые угрозы, латеральное движение, а также активное исполнение руткитов. Singularity XDR автоматически объединяет взаимосвязанные действия в единый алерт с анализом атаки на уровне вредоносной кампании. Это позволяет организациям коррелировать события с разных векторов атаки и приоритизировать разрозненные алерты как один инцидент.



КЛЮЧЕВЫЕ ИНТЕГРАЦИИ

КОНЕЧНЫЕ ТОЧКИ

IOT

ОБЛАКА

КИБЕРРАЗВЕДКА

СИСТЕМЫ УПРАВЛЕНИЯ УЗ

ЭЛЕКТРОННАЯ ПОЧТА

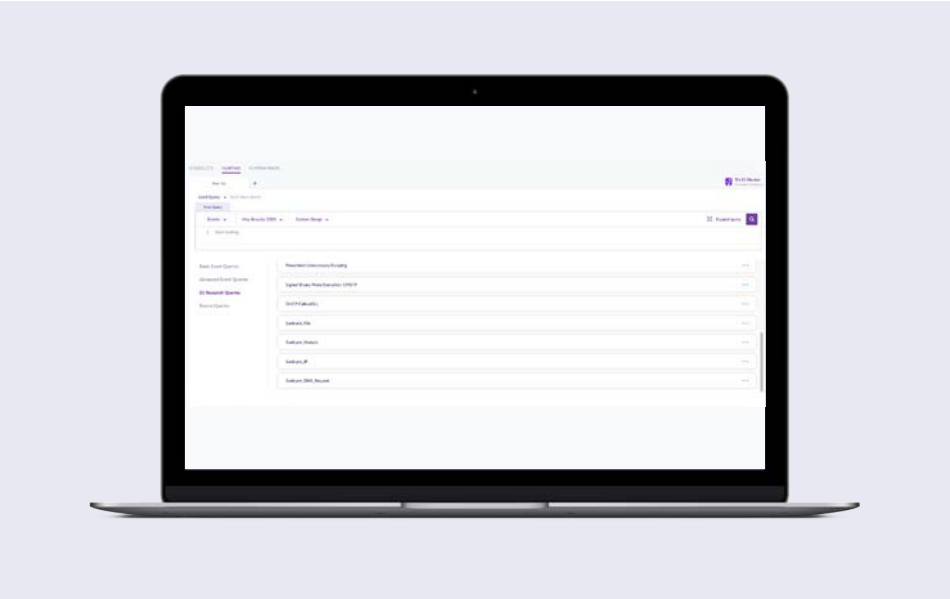
СЕТЕВЫЕ УСТРОЙСТВА

SASE

03 Автоматическое обогащение инцидентов данными кибер разведки

Встроенная кибер разведка Singularity позволяет обнаруживать угрозы и автоматически обогащает данные о них в реальном времени из сторонних фидов ведущих вендоров, а также из собственных проприетарных источников SentinelOne. Благодаря этому команды ИБ могут дополнительно оценивать риски в контексте индикаторов компрометации (IoC), таких как IP-адреса, хэши, уязвимости и домены. Например, интеграция с решением Recorded Future позволяет автоматически обогащать данные об угрозах, используя более 800 000 источников, что ускоряет расследование инцидентов и их приоритизацию.

Заказчики также могут использовать библиотеку хантинговых запросов, подобранную аналитиками SentinelOne, которые непрерывно проверяют последние методики выявления новых индикаторов угроз (IOC), а также техник, тактик и процедур (TTP) злоумышленников.



04 Автоматическое реагирование на угрозы на разных эшелонах защиты

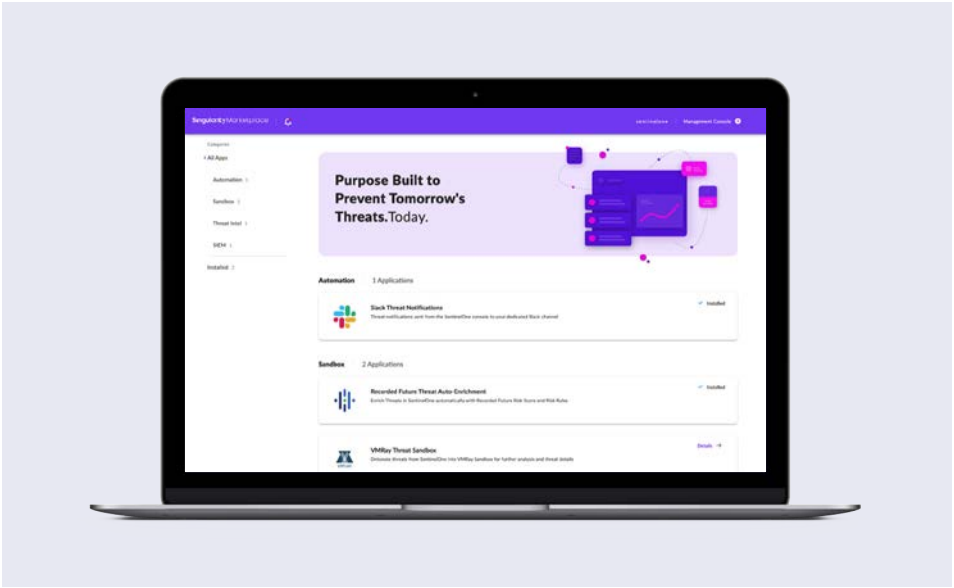
Singularity XDR позволяет аналитикам ИБ выполнять все необходимые действия для автоматического устранения угроз одним щелчком мыши на одном, нескольких или всех устройствах в сети – все это без использования скриптов. Одним кликом аналитик ИБ может принять такие меры реагирования на угрозу, как изоляция устройства от сети, автоматическая установка агента на незащищенной рабочей станции или автоматическое применение политик в облачных средах.

Кроме того, Singularity позволяет клиентам использовать сведения Storyline и создавать собственные правила автоматического обнаружения для своей среды благодаря Storyline Active Response (STAR). С помощью STAR организации могут настраивать XDR-решение с учетом бизнес-контекста в соответствии со своими потребностями. Настраиваемые правила обнаружения Storyline Active Response (STAR) позволяют превратить запросы Deep Visibility в автоматизированные правила хантинга, которые при обнаружении совпадений будут запускать систему алертинга и реагирования. STAR позволяет гибко настраивать алерты и меры реагирования в соответствии со спецификой корпоративной инфрастуктуры для оперативного автоматического обнаружения и сдерживания угроз.

05 Органичная интеграция с ведущими SOAR-инструментами

Поскольку в SOC большинства организаций уже развернуты другие СЗИ и технологии, SentinelOne предлагает растущий набор интеграций со сторонними системами, такими как SIEM и SOAR, на площадке Singularity Marketplace. Приложения Singularity размещаются на масштабируемой бессерверной платформе FaaS (Function-as-a-Service). Они интегрируются с СЗИ и средствами управления ИТ-инфраструктурой по API за пару кликов. Singularity Marketplace — часть платформы Singularity, поэтому эффективность продуктов очевидна сразу после их настройки. Маркетплейс устраняет барьеры, связанные с написанием сложного кода, упрощая и масштабируя автоматизацию между СЗИ различных вендоров. Команды ИБ могут легко определить наиболее оптимальный план для устранения быстро развивающихся угроз, т. к. реагирование унифицировано и оркестрировано между СЗИ различного класса.

> “
>
> Сбор данных — большая проблема для большинства вендоров СЗИ. Чтобы современное XDR-решение успешно справлялось со скоростью поступления разнообразных данных, в его основе должен лежать современный конвейер обработки данных, который может собирать и обрабатывать данные в масштабе всей гибридной ИТ-инфраструктуры.
>
> Кроме того, XDR-решения должны автоматически предоставлять контекст событий и их взаимосвязи. Так команды ИБ могут видеть данные со всего корпоративного стека СЗИ.
>
> **Дэйв Грубер**
>
> СТАРШИЙ АНАЛИТИК, ENTERPRISE STRATEGY GROUP



06 | Повышение эффективности команды ИБ и SOC

Singularity XDR предоставляет единую унифицированную платформу для расширенного обнаружения угроз и реагирования на них, расследования инцидентов и хантинга благодаря:

- Единому источнику приоритизированных алертов, который собирает и стандартизирует данные из нескольких источников.
- Единой панели управления, которая позволяет оперативно отслеживать развитие атаки на разных уровнях защиты.
- Единой платформе, предоставляющей возможности проактивного хантинга и оперативного реагирования на атаки.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

Легкий сбор данных из множества источников

Собирайте структурированные, неструктурированные и полуструктурированные данные в реальном времени с любых технологических решений или платформ.

Выявление атак по всей экосистеме ИБ

Автоматически получайте контекст и корреляцию событий, собранных со всех СЗИ организации в режиме реального времени, преобразуя точечные данные в информативные «сюжетные линии».

Оперативное сдерживание атак благодаря активному автоматическому реагированию на угрозы

Устраняйте угрозы одним щелчком мыши на одном, нескольких или всех устройствах в сети без использования скриптов.

Ускоренное расследование инцидентов и хантинг

Проактивно вычисляйте продвинутых злоумышленников благодаря общим запросам к центральному репозиторию данных.

Инновации. Надежность. Признание.

Gartner

Лидер в волшебном квадранте Gartner по оценке EPP-платформ за 2021 год

Наивысшие оценки во всех сценариях использования в отчете о критических возможностях

MITRE ENGENUITY

Рекордные результаты в испытании ATT&CK

- Ни одной пропущенной угрозы – детект 100%
- Больше всего аналитических детектов 2 года подряд
- Без задержек и изменений конфигурации

Gartner peerinsights 4.9 ★★★★★

98% положительных отзывов о SentinelOne

в отчете Gartner Peer Insights «Голос клиента»

FedRAMP · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS · TEVORA PCI DSS Attestation HIPAA Attestation

О компании SentinelOne

Больше возможностей. Меньше сложностей. SentinelOne в числе первых ведет кибербезопасность в будущее с автономным ИИ, аналитическое ядро которого находится не в облаке, а на конечной точке. Цель компании — упростить стек технологий безопасности, не снижая функциональные возможности организации. Наша технология разработана для того, чтобы дать людям больше возможностей для масштабирования благодаря автоматизации и удобному блокированию угроз. Вы готовы?

Тайгер Оптикс — авторизованный дистрибьютор SentinelOne в России и СНГ
sales@tiger-optics.ru
https://www.tiger-optics.ru