CYBERBIT
PROTECTING A NEW DIMENSION

Cyberbit EDR

Обнаружение и реагирование на конечных устройствах

Обнаружение неизвестных атак и атак нулевого дня при помощи алгоритмов машинного обучения и анализа изменения моделей поведения

ЗАДАЧА

Отчет DBIR компании Verizon показывает ежегодный прирост кибератак, связанных с вредоносными программными средствами, на 30%. Несмотря на рост вложений в развитие технологий кибербезопасности, опытные хакеры могут обходить даже наиболее передовые системы обеспечения безопасности, включая системы защит следующего поколения на основе не сигнатурного анализа. Причина в том, что передовые угрозы разрабатываются таким образом, чтобы симулировать легитимное поведение. В силу этого их очень трудно обнаружить при помощи традиционных систем, и они могут беспрепятственно распространяться внутри целевых сетей. Традиционные системы обеспечения безопасности создают множество оповещений, требующих реакции специалистов по обеспечению безопасности, анализа, и ручного назначения приоритетов. Обнаружение и реагирование на неизвестные и целевые атаки требует использования новых подходов.

ОБНАРУЖЕНИЕ НА ОСНОВЕ IOC ЯВЛЯЕТСЯ НЕДОСТАТОЧНЫМ

Современные угрозы в киберпространстве являются настолько динамичными, что лишь 10% атак длятся более 90 секунд (Verizon DBIR 2016). Когда атакующей стороне удается создавать новые комбинации старых угроз в минуту, системы обеспечения безопасности не могут полагаться только на индикацию нарушения (IOC) для обнаружения. Такие малые изменения в коде известных угроз изменяют их атрибуты и позволяют вредоносному коду легко обходить механизмы обнаружения на основе IOC, и причинять ущерб.

Для обеспечения обнаружения и реагирования на современные, целенаправленные угрозы, организации должны применять передовые методы обнаружения, более эффективные, чем IOC.

Cyberbit EDR

Cyberbit EDR обеспечивает применение нового подхода к обнаружению и реагированию на современные угрозы на уровне конечных точек. Этот подход основан на системе с гибридным обнаружением, которое сочетает анализ поведения и алгоритмы машинного обучения, использующие статистические моделирование для обнаружения аномальных действий. Такой гибридный подход, используемый уникальной системой Cyberbit EDR, доказал свою способность обнаруживать более широкий спектр вредоносной деятельности, включая угрозы, неизвестные ранее, и является более эффективным в процессе различения нормальной и аномальной деятельности. В результате этот подход сводит к минимуму количество ложных оповещений без снижения высокого качества обнаружения.

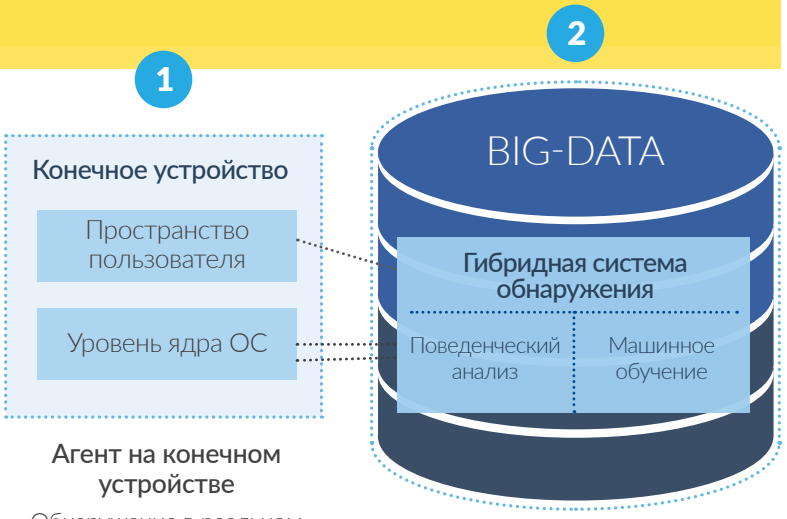
ПРЕИМУЩЕСТВА Cyberbit EDR

- **Обнаружение неизвестных угроз -** уникальная гибридная система обнаружения сочетает машинное обучение и анализ поведения для обнаружения неизвестных угроз в течение секунд и сводит к минимуму количество ложных оповещений.
- **Повышение эффективности анализа и снижение входного порога для нового анализа -** замена ручной аналитической работы на автоматизированные процессы. Ускорение расследований, анализа, и реагирования при помощи использования средств визуализации, которые отображают корреляцию несопоставимых источников данных в виде единого изображения жизненного цикла происшествия.
- **Быстрое опознание угроз с высоким приоритетом -** традиционные подходы требуют наличия специалистов по кибербезопасности для анализа большого количества потоков данных и ручного назначения приоритетов. Cyberbit EDR автоматизирует этот процесс, экономит драгоценное время, и обеспечивает обработку событий с высоким приоритетом.
- **Улучшение видимости угроз -** Cyberbit EDR непрерывно собирает данные на конечных точках, создавая легкий доступ и поиск в таких данных, таким образом, аналитик может исследовать угрозы на требуемом уровне.
- **Сочетание обнаружения и форензики -** Cyberbit EDR является мощной платформой для обнаружения, а также надежной платформой для форензики в наиболее полном объеме, в качестве единого продукта.
- **Устранение сбоя и реагирование по нажатию на кнопку -** выполнение реагирования, устранения сбоя, и профилактические меры на всех компьютерах в сети.
- **Масштабирование без нарушения качества обслуживания (QoS) -** Cyberbit EDR развертывается в крупномасштабных организациях правительственного и частного секторов, поддерживая сотни тысяч конечных точек.

КАК ЭТО РАБОТАЕТ

Cyberbit EDR обеспечивает выполнение анализа в несколько фаз - начиная от конечной точки, и до крупномасштабного хранилища данных. Такой подход ускоряет обнаружение угроз - как на одном компьютере, так и во всей сети, и обеспечивает быстрое реагирование и профилактику.

В отличие от традиционных решений по обеспечению кибербезопасности, в центре внимания которых находится либо обнаружение, либо экспертиза, Cyberbit EDR является уникальной системой в аспекте обеспечения обработки всего жизненного цикла угрозы от обнаружения до форензики в масштабе реального времени, отслеживания с упреждением, и реагирования. Графический пользовательский интерфейс системы упрощает и ускоряет комплексные расследования и осуществление реагирования.

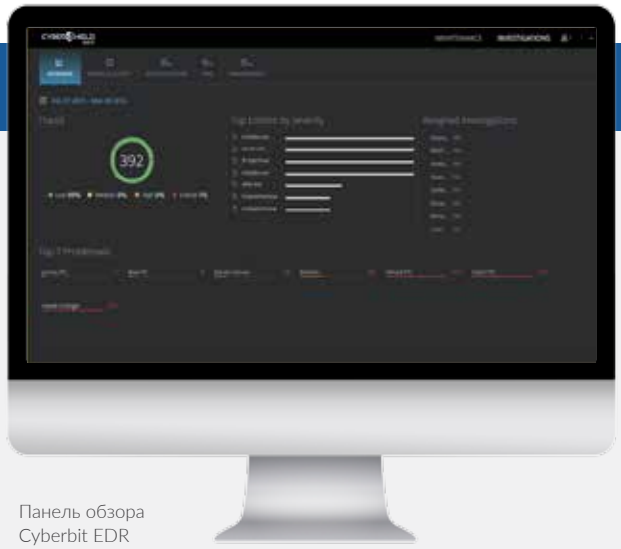


Агент на конечном устройстве

Обнаружение в реальном времени в активном и автономном режимах

Анализ Big Data

Основные возможности Cyberbit EDR



Панель обзора Cyberbit EDR

Обнаружение неизвестных угроз

Непрерывный мониторинг

Агенты Cyberbit EDR развертываются на всех конечных устройствах и серверах и осуществляют мониторинг всех объектов и действий в сети данной организации, как на уровне ядра, так и в пользовательском пространстве. Выполняется мониторинг памяти, файловой системы, реестра, процессов, и сети. Данные анализируются как на уровне агента, так и на уровне серверов Big Data. Этот процесс ускоряет обнаружение и обеспечивает должное качество обслуживания (QoS). Агент не нагружает конечное устройство, легко развертывается без нарушения текущих операций.

Гибридная система обнаружения

Гибридная система обнаружения является уникальным подходом к обнаружению комплексных угроз одновременно со снижением количества ложных тревог. Сочетание двух аналитических методов - алгоритмов машинного обучения и анализа поведения - обеспечивает надежное обнаружение и объявление тревог в порядке приоритета и с возможностью принятия действенных мер.

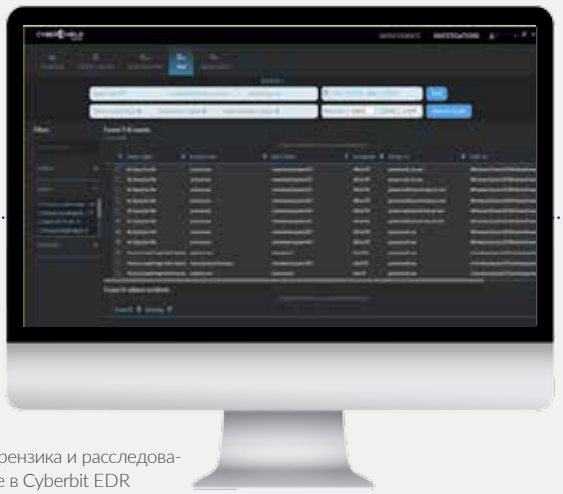
- **Анализ поведения**
  Аналитические алгоритмы компании Cyberbit распознают схемы поведения сконфигурированные экспертом, а также модели поведений, которые несут индикацию потенциально аномальной деятельности, в совокупности называемых «след». При помощи анализа вредоносного кода на основе графов, все поведение, объекты, и события, относящиеся к такому следу, автоматически отображаются в качестве визуальной схемы. Это позволяет аналитикам просматривать полный контекст и последовательность поведения, вызывающего подозрение как угроза. Корреляция данных с несопоставимых источников и понимание контекста таких данных в составе единой угрозы обычно требует часов и даже дней работы аналитика. Анализ поведения, предоставляемый Cyberbit EDR, устраняет необходимость ручного выполнения такой работы, путем автоматического добавления контекста к подозрительному поведению.

- **Алгоритмы машинного самообучения**
  Cyberbit EDR использует статистические модели для обнаружения аномалий. Алгоритмы системы включают сотни сценариев угроз и обучаются опознавать типовое угрожающее поведение в различных измеряемых пространствах, таких, как время и причинная зависимость. После обучения основным аспектам деятельности в организации, алгоритмы машинного обучения генерируют сигнал оповещения при обнаружении подозрительной деятельности с высокой статистической значимостью. В силу наличия обширной базы образцов, которая постоянно пополняется новыми угрозами, а также благодаря специфике анализируемых и моделируемых измерений, машинное обучение компании Cyberbit способно обнаруживать ранее неизвестные схемы проведения атак и понижать количество ложных оповещений.

Основные возможности Cyberbit EDR

Активное отслеживание

При помощи удобного пользовательского интерфейса и модуля расследований Cyberbit EDR обеспечивает возможность активного отслеживания с поиском и идентификацией событий по всей сети, с целью предоставления аналитикам возможности обнаружения и упреждения.



форензика и расследование в Cyberbit EDR

Удобные расследования в масштабе реального времени

Экспертиза в масштабе реального времени

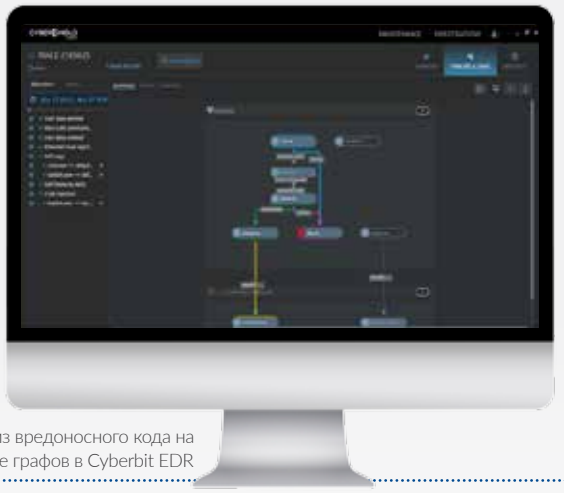
Используя платформу на основе Big Data, Cyberbit EDR обеспечивает выполнение форензики в масштабе реального времени и доступ ко всем данным в течение секунд. Имея быстрый доступ ко всем данным, аналитики могут выполнять комплексные расследования и анализ источников угроз, а также вести архив для использования в решении будущих задач.

Полноценный просмотр

Централизованное хранилище большого объема данных содержит данные по всем конечным устройствам. Это обеспечивает уникальную возможность просмотра всех конечных устройств и серверов, а также позволяет аналитикам контролировать операции в сети.

Визуализация с обнаружением причин и взаимосвязей

Уникальный анализ вредоносного кода на основе графов, разработанный компанией Cyberbit, отображает полный след атаки, включая все связанные объекты и события, вместе со значительным обнаружением причин и взаимосвязей, автоматически предоставляемым системой, позволяя аналитикам быстро опознавать и понимать угрозу и ее метод действия.



Анализ вредоносного кода на основе графов в Cyberbit EDR

Реагирование и профилактика

Используя единого агента на конечном устройстве, Cyberbit EDR поддерживает многовариантное реагирование и профилактические действия, обеспечивая контроль на протяжении всего жизненного цикла угрозы, снижая тем самым время до начала реагирования. Ответные меры включают удаление работающих процессов, карантин файлов или компьютеров, удаленные операции с файлами и реестром, захват сброса памяти, и предотвращение исполнения вредоносного кода.

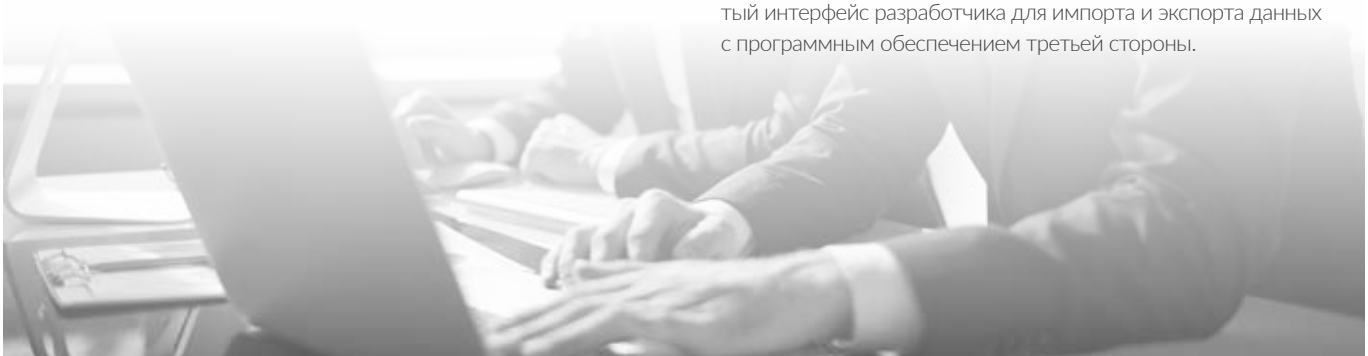
Оптимизированная архитектура

Высокая надежность и безопасность

Cyberbit EDR была разработана с соблюдением строгих требований по безопасности, и включает механизмы противодействия вмешательству, шифрование кода и данных, а также самоконтроль, с целью обеспечения безопасности, надежности, и доступности, не имеющий аналогов.

Открытая и масштабируемая архитектура

SDK для добавления специфического анализа как на стороне агента, так и на стороне алгоритмов анализа Big Data, открытый интерфейс разработчика для импорта и экспорта данных с программным обеспечением третьей стороны.



О КОМПАНИИ CYBERBIT™

Cyberbit предлагает передовые решения в области кибербезопасности для финансовых организаций, предприятий критической инфраструктуры, военных и правительственных организаций. Портфолио компании предоставляет полный набор продуктов для обнаружения и митигации кибератак, а также помогает нашим Заказчикам решать оперативные задачи управления кибербезопасностью. Портфолио Cyberbit включает в себя решения по обнаружению и реагированию для конечных устройств (EDR), по кибербезопасности и контроля бесперебойной работы SCADA (SCADAShield), по автоматизации процессов управления SOC (SOC 3D), а также по подготовке персонала для обеспечения кибербезопасности на базе полнофункционального симулятора (Range). Продукты компании Cyberbit были выбраны крупными международными корпорациями по всему миру для обеспечения кибербезопасности своих сетей.

Cyberbit является стопроцентной дочерней компанией Elbit Systems Ltd. (NASDAQ и TASE: ESLT)

sales@cyberbit.net | www.cyberbit.net

Офис в Израиле:

CYBERBIT Commercial Solutions Ltd.
22 Zarhin St. Ra'anana
Israel 4310602
Тел.: +972-9-7799800 | E-mail: sales@cyberbit.net

CYBERBIT
PROTECTING A NEW DIMENSION