Carbon Black

CB RESPONSE

Лидирующее решение в области Incident Response and Threat Hunting

Современные корпоративные службы безопасности отходят от стратегии пассивной защиты. Передовым методом сейчас является Threat Hunting (обнаружение и предотвращение кибератаки на ранней стадии). Но для проведения качественного расследования и точечной реакции именно на вредоносные аномалии, специалисты ИТ нуждаются в наиболее полных данных о состоянии конечных точек, которые зачастую им недоступны.

CB Response - это передовое решение в области реагирования на инциденты и поиска угроз, разработанное специально для команд центров информационной безопасности (SOC). CB Response непрерывно записывает и сохраняет нефильтрованные данные конечных точек, благодаря чему специалисты по безопасности в режиме реального времени могут отследить всю цепочку вредоносной активности и устранить ее до нанесения какого либо вреда. Решение усиливается информацией о выявленных угрозах из CB Predictive Security Cloud, которое применяется для распознавания и вычисления злонамеренной активности и подозрительных действий на конечных точках.

Лучшие команды SOC, IR и MSSP используют CB Response в качестве основного компонента в своих системах обнаружения и реагирования на инциденты.

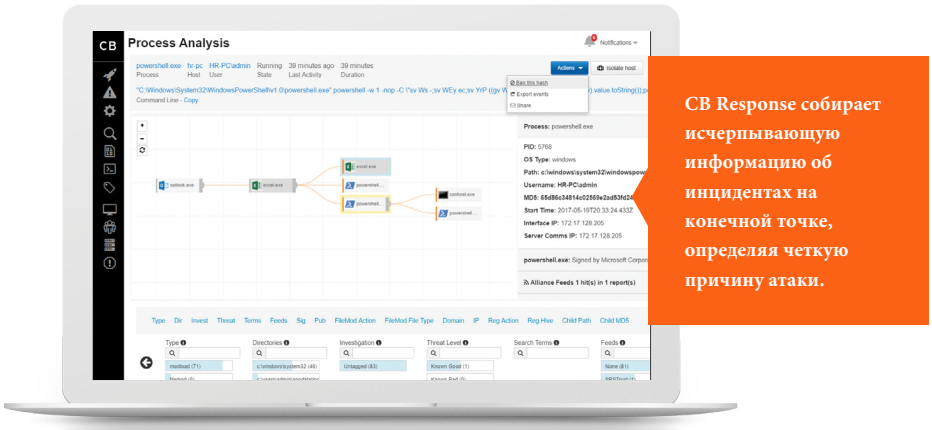
Клиенты, которые решают дополнить или заменить устаревшее антивирусное решение, выбирают CB Response из-за прозрачности и информативности в обеспечении безопасности их ИТ-среды, то, что не могли гарантировать предыдущие решения. Также традиционные антивирусы часто не дают возможность заметить надвигающиеся, а иногда и уже совершенные атаки.

CB Response доступно через MSSP, через локальное развертывание либо виртуальное частное облако, и как настраиваемое SaaS-решение.

«Использование CB Response дает уверенность в эффективности нашего поиска угроз - его результаты более достоверны, чем у традиционных антивирусов. Решение включает в себя обнаружение передовых вредоносных программ и выявления злонамеренного поведения, например - руткитов, а также предлагает поддержку изоляции хостов, запрета хэша или цепочки выполнения».

— МЕХАН КАЗИНАТ,
ДИРЕКТОР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В AT IAC

IAC



CB Response собирает исчерпывающую информацию об инцидентах на конечной точке, определяя четкую причину атаки.

ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ

- Поиск угроз
- Предотвращение взломов, нарушений
- Реагирование на инциденты
- Проверка и сортировка оповещений
- Анализ основных причин нарушения
- Расследования инцидентов безопасности
- Изоляция хостов

ПРЕИМУЩЕСТВА

- Быстрое реагирование и исправление
- Ускоренная реакция на инциденты и поиск угроз благодаря нефильтрованным данным конечных точек
- Мгновенное обнаружение действий злоумышленника и выявление их источников
- Безопасный удаленный доступ к зараженным конечным точкам для углубленного анализа
- Улучшенная защита от будущих атак на основе автоматического поиска
- Избавление ИТ-специалистов от повторной обработки заявок и обращений в службу поддержки

ПОИСК УГРОЗ НА CB PREDICTIVE SECURITY CLOUD

Все возможности CB Response по поиску угроз и реагированию на инциденты теперь доступны в CB ThreatHunter на новом облачном решении - CB Predictive Security Cloud!

Узнайте больше на **carbonblack.com/products/CB-threathunter**

Carbon Black

Ключевые возможности

Ведение непрерывной и централизованной записи

Централизованный доступ к нефильтрованным данным конечных точек означает, что специалисты по безопасности обладают информацией, необходимой для поиска угроз в режиме реального времени и проведения углубленных расследований после инцидентов информационной безопасности.

Live Response для удаленного исправления

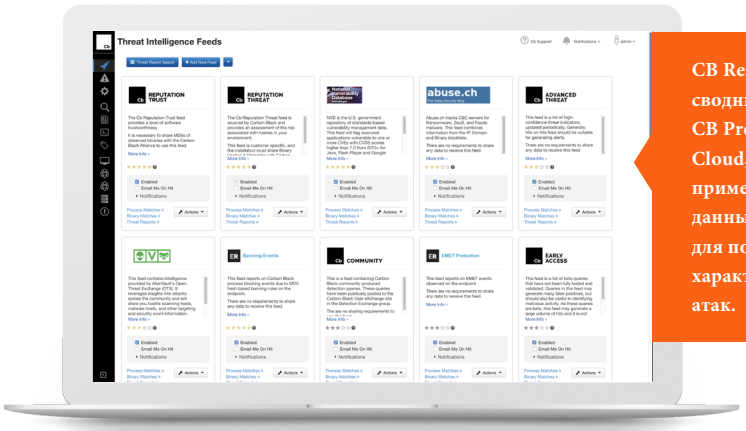
С помощью Live Response, сотрудники, реагирующие на инциденты, могут создавать безопасное соединение с зараженными хостами, чтобы дистанционно извлекать из них данные или отправлять туда файлы, завершать процессы, производить дампы памяти и быстро исправлять ошибки.

Визуализация цепочки атак и их поиск

CB Response обеспечивает интуитивно понятную визуализацию цепочки атак, что гарантирует быстрое определение первопричины нарушения. Аналитики могут оперативно переключаться между стадиями вредоносных атак, понимая тактику поведения злоумышленника. Это не только помогает моментально устранять пробелы в безопасности, но и дает возможность избежать повторения атак в будущем.

Автоматизация с помощью интеграций и OpenAPI

Carbon Black может похвастаться надежной партнерской экосистемой и доступной платформой, позволяющей группам безопасности легко интегрировать продукты в свою существующую систему безопасности.



CB Response использует сводный анализ угроз CB Predictive Security Cloud, который применяется ко всем данным конечных точек для понимания характера вредоносных атак.

О CARBON BLACK

Carbon Black (NASDAQ: CBLK) - ведущий поставщик облачных средств защиты конечных точек следующего поколения. Используя облачную платформу big data и аналитики, Predictive Security Cloud (PSC), Carbon Black объединяет средства предотвращения, обнаружения, реагирования, поиска угроз и управляемые сервисы в единую платформу с одним агентом и единой консолью управления. Такое решение упрощает консолидацию комплекса безопасности для организаций и позволяет добиться наилучшей защиты.

Новатор в области кибербезопасности, Carbon Black был и является первопроходцем в категориях безопасности конечных точек, включая контроль над приложениями, обнаружение конечных точек и реагирование (EDR), антивирус следующего поколения (NGAV). Более 4300 клиентов по всему миру, в том числе 35 из списка Fortune 100, доверяют Carbon Black безопасность своих организаций.

ХАРАКТЕРИСТИКИ

- Полностью готовое или настраиваемое функциональное обнаружение
- Множество настраиваемых поисков по информационным каналам
- Автоматизированные списки собранной информации
- Обработка и бинарный поиск централизованных данных
- Интерактивная визуализация цепочки атак
- Live Response для быстрого исправления и восстановления
- OpenAPI и более 120 готовых средств интеграции
- Доступно для установки на локальном или виртуальном частном облаке, как настраиваемое SaaS-решение или MSSP

ПЛАТФОРМЫ

- Windows
- MacOS
- Red Hat Linux
- CentOS (Linux)
- Oracle RHCK

Варианты установки:

- Облака или на вышеуказанных платформах

ЗАПРОСИТЬ ДЕМО

Свяжитесь с нами сегодня, чтобы запланировать демонстрацию.

INFO@SOFTPROM.COM

Carbon Black.

1100 Winter Street
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.CarbonBlack.com