Cisco Umbrella

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

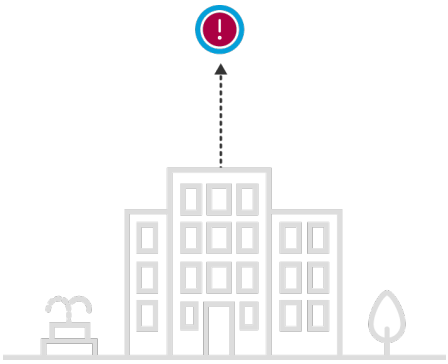
Беспрецедентные возможности расследования атак

Злоумышленники вторгаются в вашу сеть. А что если бы вы могли получать представление об их инфраструктуре?

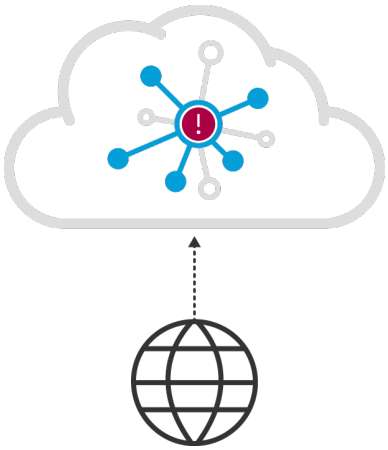
Многие средства обеспечения безопасности позволяют вам контролировать собственную сеть. Но знаете ли вы, что происходит в Интернете в целом, за пределами периметра вашей сети? Именно там киберпреступники создают инфраструктуру для подготовки к атакам.

Cisco Umbrella Investigate обеспечивает наиболее полный обзор инфраструктуры злоумышленников и позволяет специалистам по безопасности обнаруживать вредоносные домены, IP-адреса, хеш-суммы файлов и даже прогнозировать появление новых угроз.

Изучение событий безопасности с помощью Investigate



Доступная вам картина локального трафика, направляемого в подозрительный домен или на IP-адрес



Созданная средствами Investigate картина глобального трафика, направляемого в связанные домены и на IP-адреса

В цифрах

- 65 млн активных корпоративных и обычных пользователей ежедневно
- Пользователи из более чем 160 стран
- 100 млрд DNS-запросов ежедневно
- Более 500 пиринг-партнеров обмениваются с нами BGP-маршрутами, что улучшает для нас обзор интернет-трафика

Как это работает

Отправная точка – огромный массив разнородных данных

В 2006 г. мы начали создавать крупнейшую в мире сеть интернет-безопасности для накопления глобальных аналитических данных. На сегодняшний день свыше 65 млн активных пользователей из более чем 160 стран ежедневно направляют свой DNS-трафик в нашу глобальную сеть. Это позволяет нам отслеживать более 100 млрд интернет-запросов в день. Кроме того, более 500 пиринг-партнеров обмениваются с нами BGP-маршрутами. В результате мы получаем полную картину связей и отношений между различными сетями в Интернете. Этот огромный массив разнородных данных обеспечивает нам беспрецедентный обзор всего Интернета.

Применение статистических моделей

Чтобы выявлять шаблоны и обнаруживать аномалии в данных, мы разработали статистические модели для категоризации и оценки. Несколько примеров перечислено ниже.

- Многие модели анализируют пространственные отношения; пример – графическое отображение отношений между сетями в Интернете.
- Некоторые модели анализируют временные отношения; пример – выявление причинно-следственной связи перехода между доменами в результате последовательных DNS-запросов, которые многократно отправляют тысячи пользователей за очень короткие интервалы времени.
- Другие модели анализируют статистические отклонения от нормальной активности; пример – оценка географического распределения IP-сетей, запрашивающих доменное имя.
- Используя обработку естественного языка, модель NLP Rank выявляет фишинговые домены, которые имитируют фирменные наименования, анализируя их лексическую структуру и расположение в Интернете.

Использование опыта и знаний специалистов
Перечисленные модели созданы и отлажены группой Cisco Umbrella, в которую входят специалисты по обработке и анализу данных, инженеры, математики и аналитики по информационной безопасности. С помощью 3D-визуализации, многочисленных методов интеллектуального анализа данных и экспертных знаний в области информационной безопасности аналитики Umbrella совершенствуют модели и добавляют дополнительный контекст к результатам их применения. Специалисты постоянно находят новые способы анализа данных для выявления новых взаимосвязей и шаблонов.

Результат: прогнозная аналитика
Результаты этого анализа позволяют нам точно обнаруживать вредоносные домены, IP-адреса, сети и хеш-суммы файлов в Интернете и даже прогнозировать источники будущих атак.

Преимущества для вас

- **Беспрецедентные возможности обнаружения атак благодаря мониторингу всего Интернета.** Отслеживание запросов в масштабах всего Интернета позволяет понять, где злоумышленники организуют свою инфраструктуру и как связаны вредоносные, безопасные и неизвестные домены, IP-адреса, номера автономных систем и хеш-суммы файлов.
- **Ускорение реагирования на инциденты.** Когда на раннем этапе расследования у специалистов по безопасности нет нужного контекста или доступа к актуальной информации, реагирование на инциденты замедляется. Ускорив расследование инцидента, вы можете более оперативно принять меры и сократить время нахождения злоумышленника в вашей среде.
- **Приоритизация расследований инцидентов.** Чтобы правильно расставить инциденты по приоритету, необходимо быстро получить точную информацию и соответствующий контекст. Глобальный контекст, полученный благодаря нашему уникальному обзору Интернета, дополняет ваши собственные данные о событиях безопасности и аналитику угроз, помогая точнее приоритизировать расследования.
- **Более эффективное использование аналитики угроз.** Дополните свои устаревшие стандартные каналы информации об угрозах нашей актуальной аналитикой, охватывающей весь Интернет.

Сценарии использования

- Ускорение расследований
- Опережение атак
- Приоритизация расследований и ответных мер
- Передача данных реального времени в системы безопасности

Варианты использования Investigate

Динамическая поисковая система
Наша веб-консоль обеспечивает доступ ко всей аналитике в режиме реального времени и возможность интерактивной комбинации различных элементов данных во время расследований. В Investigate можно создать запрос на точные совпадения доменных имен, IP-адресов, адресов электронной почты, номеров ASN и хеш-сумм файлов либо использовать поиск по шаблону, формируя более гибкие запросы определенных терминов, фирменных наименований, образцов и неточных совпадений.

REST API-интерфейс
Investigate предоставляет доступ к API-интерфейсу для передачи контекстных данных в систему управления событиями и данными безопасности, платформу аналитики угроз или процесс обработки инцидентов. Это ускоряет обнаружение серьезных нарушений безопасности.

Возможности продукта

- Связывание атак с определенными доменами, IP-адресами, номерами ASN и вредоносным ПО для определения плана инфраструктуры злоумышленников.
- Отображение подозрительных пиков в количестве глобальных DNS-запросов к определенному домену.
- Прогнозирование источников будущих атак путем выявления доменов и IP-адресов, связанных с вредоносным ПО.
- Исследование поведенческих индикаторов и сетевых подключений образцов вредоносного ПО с использованием данных от Cisco AMP Threat Grid.
- Использование данных WHOIS для определения владельцев доменов и обнаружения вредоносных доменов, зарегистрированных с одинаковыми контактными данными.
- Применение нашей системы оценки риска к различным атрибутам доменов с целью выявить среди них подозрительные.
- Обнаружение доменов, использующих Fast Flux, и доменов, созданных с помощью алгоритмов генерации доменных имен.
- Доступ к крупнейшей пассивной базе данных DNS и WHOIS для просмотра ретроспективных данных о доменах.