SECBI
AUTONOMOUS INVESTIGATION™

ХВАТИТ КОПАТЬСЯ В АНОМАЛИЯХ И ОПОВЕЩЕНИЯХ:

ОЦЕНИТЕ ПОЛНЫЙ МАСШТАБ АТАКИ

В сфере безопасности приходится сталкиваться с миллиардами событий, масштаб и характер которых постоянно меняется. Именно поэтому все сложнее обеспечивать безопасность. Задача сотрудников центра мониторинга информационной безопасности (ЦМИБ) – обнаружение инцидентов и одновременно поддержание заданного уровня обслуживания, что, учитывая ограниченность ресурсов и времени на принятие решений, является весьма сложной задачей. Аналитики ЦМИБ 1-го и 2-го уровня получают слишком большое количество ложно положительных сообщений об угрозах. А у аналитиков 3-го уровня и специалистов по поиску уязвимостей нет инструментов, позволяющих справляться с огромными массивами данных и успешно и своевременно выявлять угрозы. Менеджеры ЦМИБ также испытывают трудности с обеспечением требуемого уровня обслуживания при решении задач которые на это не ориентированы, например поиск угроз.

Кроме того, отсутствие комплексных средств обнаружения приводит к тому, что инциденты зачастую остаются либо полностью незамеченными, либо их масштаб остается не до конца ясен. Результат –частичное устранение инцидента и сохранение продолжительной вредоносной активности.

ЧТО МОЖНО ОБНАРУЖИТЬ ПРИ ОЦЕНКЕ ПОЛНОГО МАСШТАБА АТАКИ?

Можно узнать все детали инцидента, начиная от причины заражения и заканчивая полной картиной нанесенных повреждений, включая:

- ВСЕХ ПОДВЕРГШИХСЯ ЗАРАЖЕНИЮ ИЛИ ИНОМУ ВОЗДЕЙСТВИЮ УГРОЗЫ ПОЛЬЗОВАТЕЛЕЙ И ОКОНЕЧНЫЕ УСТРОЙСТВА
- ВСЕ ВРЕДОНОСНЫЕ ДОМЕНЫ И ХОСТЫ

ТЕХНОЛОГИЮ АВТОНОМНОГО АНАЛИЗА AUTONOMOUS INVESTIGATION™

Технология Autonomous Investigation™ основывается на принципах машинного обучения с учителем и без учителя, что позволяет обнаруживать сложные и скрытые угрозы путем анализа сетевого трафика. Она мгновенно определяет масштаб атаки, ускоряет поиск и обнаружение угроз, а также оптимизирует ответные действия и меры по устранению их последствий. Аналитики ЦМИБ получают полное описание атаки, благодаря чему им видны все затронутые пользователи и устройства, а также точки вторжения в рамках указанной атаки. Полное описание атаки содержит необходимую аналитикам информацию, на основе которой они могут принимать конкретные меры, например, блокировать узлы-источники вредоносного ПО.

РЕВОЛЮЦИОННАЯ ТЕХНОЛОГИЯ АНАЛИЗА СЕТЕВОГО ТРАФИКА

В процессе автономного анализа SecBI выявляется вредоносный кластер и его параметры, в том числе полное описание и отчет об инциденте. Это помогает быстрее и точнее обнаружить угрозу и существенно сократить количество ложно положительных срабатываний системы обнаружения.

В отличие от традиционной технологии перехвата пакетов, решение SecBI обрабатывает сетевой трафик без использования дополнительных решений или агентов, поэтому ее внедрение не требует значительных капиталовложений. В отличие от длительного процесса развертывания технологий перехвата пакетов, для которых требуются дополнительное оборудование, определенные точки интеграции и постоянное обслуживания для работы, технология SecBI позволяет достичь хороших результатов сразу после быстрого развертывания и настройки. Решение SecBI исключает непроизводительные затраты при настройке и установке, а в дальнейшем и при обслуживании, предоставляя лучшее понимание потенциальных киберугроз.

СПОСОБНОСТЬ ОБНАРУЖИТЬ НЕИЗВЕСТНОЕ

Технология SecBI обнаруживает и группирует все внутренние (например, пользователи, устройства) и внешние (например, домены, IP-адреса, серверы C&C, точки сброса) сущности, принимающие участие в обмене данными в поставленной под угрозу сети. Отслеживание вредоносных кластеров, а не отдельных аномалий или случайных оповещений, позволяет быстрее и точнее обнаружить угрозу и существенно сократить количество ложно положительных срабатываний системы оповещения.

SecBI создает из потока оповещений об инцидентах список с распределеными приоритетами, что облегчает приоритизацию, анализ и устранение последствий инцидента. Данное решение создает унифицированный обзор кибер-инцидентов, объединяя различные оповещения, события и журналы для создания полной картины текущих атак. Это позволяет отфильтровать лишнее и сосредоточиться на том, что поможет в проведении анализа киберугроз. В результате мы получаем автоматический анализ инцидентов, значительно сокращающий время реагирования группы кибербезопасности, повышающий общий уровень защиты и снижающий расходы.

ПРИМЕР ИСПОЛЬЗОВАНИЯ: РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

Технология автономного анализа SecBI позволяет аналитикам расставлять приоритеты и более эффективно изучать инциденты. SecBI обрабатывает сетевой трафик и данные безопасности одновременно с анализом угроз, что обеспечивает непревзойденную осведомленность. Решение SecBI помогает аналитикам с любым опытом более эффективно достигать поставленных задач, анализировать и правильно реагировать на инциденты при любых условиях. Оно помогает аналитикам интерпретировать уведомления в правильном контексте, а также анализировать уведомления с высоким приоритетом в соответствующем контексте и минимизировать риски.

ПРИМЕР ИСПОЛЬЗОВАНИЯ: АВТОМАТИЧЕСКИЙ ПОИСК УГРОЗ

Технология автономного анализа SecBI позволяет аналитикам более эффективно выявлять угрозы и составлять более полную картину происходящего в системе. Аналитические инструменты SecBI включают неконтролируемое, контролируемое и адаптивное машинное обучение, а также статистические методы для создания комплексных поведенческих профилей. Аналитика объединена с высокоточной, многоуровневой фильтрацией от самых полезных метаданных, помогающих в поддержке пользователей или изучении инцидентов, до необработанных данных, позволяющих аналитикам по безопасности проверять свои гипотезы. Архитектура на основе больших данных дает возможность SecBI легко и экономично расширять период поиска до нескольких месяцев или лет.

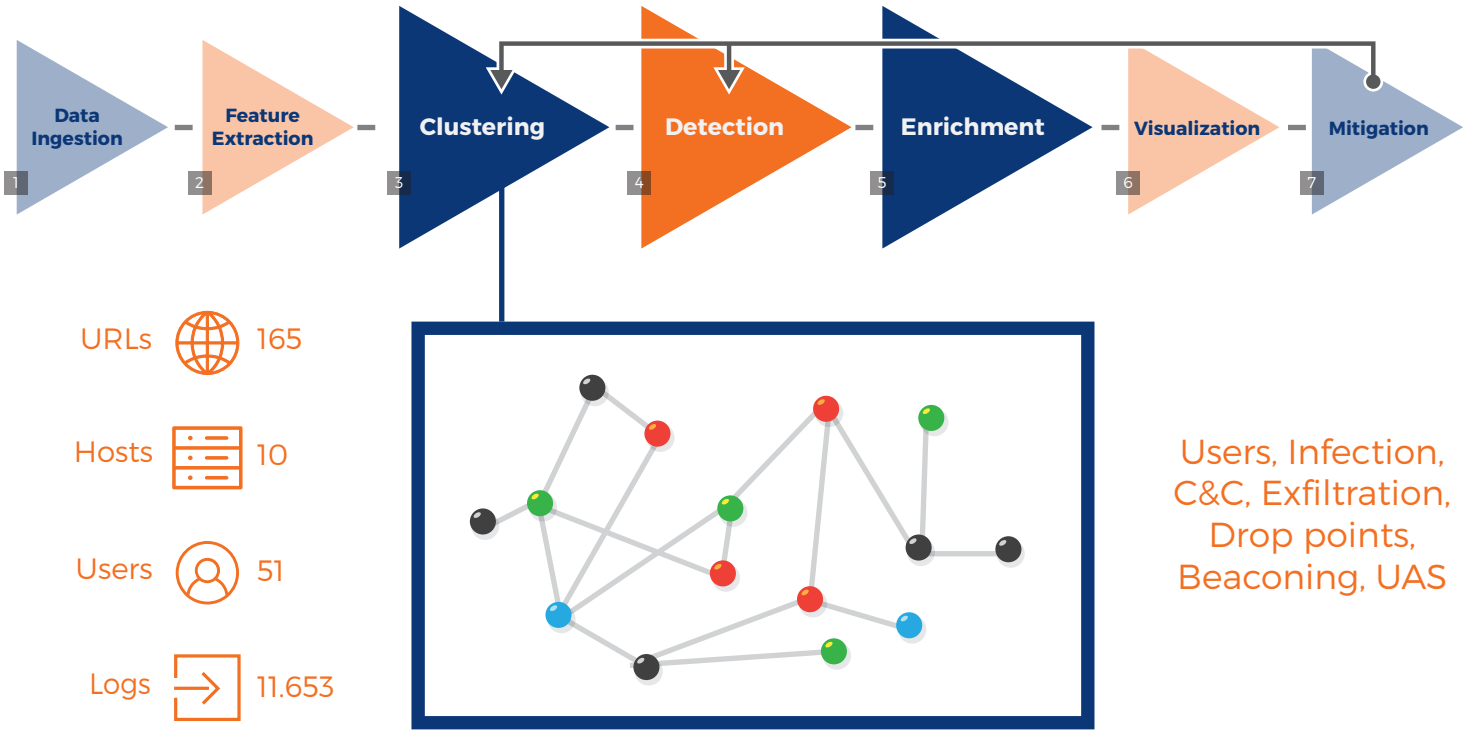
ПРИМЕР ИСПОЛЬЗОВАНИЯ: ДЛЯ ПОСТАВЩИКОВ УСЛУГ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (MSSP)

Используя технологию SecBI, поставщики услуг по управлению информационной безопасностью могут предлагать продвинутые услуги по обнаружению угроз, реагированию на несанкционированный доступ, анализу недоработок, а также улучшить инструменты для поиска угроз. Расширенный портфель услуг позволяет увеличить доход провайдеров.

ПРЕИМУЩЕСТВА ТЕХНОЛОГИИ AUTONOMOUS INVESTIGATION™

- ☑ Позволяет быстрее и эффективнее реагировать на инциденты
- ☑ Облегчает составление точного плана действий
- ☑ Не требует дополнительного оборудования (устройств и агентов)
- ☑ Экономит время аналитиков ЦМИБ, снижая количество ложно положительных срабатываний
- ☑ Сокращает время задержки

THE PROCESS



СОТРУДНИКИ ЦМИБ: ПОМОЩЬ УЖЕ В ПУТИ!

SecBI освобождает сотрудников ЦМИБ от отслеживания случайных уведомлений и утомительных изыскательных задач для сбора фактов проникновения. Наш комплексный инструмент обнаружения позволяет аналитикам тщательно оценивать информацию об инцидентах благодаря быстрому реагированию и малому количеству ложно положительных срабатываний, а также значительно сокращает время задержки.

Решение SecBI легко и быстро развертывается без использования дополнительных устройств и агентов. Развернуть решение можно как на месте, так и в облаке. Ваш ЦМИБ сразу станет эффективнее без каких-либо изменений сетевой инфраструктуры.

О КОМПАНИИ SECBI

Компания SecBI сделала прорыв в области автоматизированного обнаружении кибер-угроз и анализа сетевого трафика. В технологии автономного анализа Autonomous Investigation™ используется неконтролируемое машинное обучение, позволяющее распознать полный масштаб кибератак, включая все подвергшиеся воздействию сущности и вредоносные действия. SecBI обнаруживает сложные угрозы, которые могут пропустить другие системы, создает комплексную картину инцидента и позволяет быстро и эффективно устранить последствия. На сегодняшний день технологией SecBI пользуются финансовые учреждения, телекоммуникационные компании, ритейлеры и производственные предприятия по всему миру.

SECBI
AUTONOMOUS INVESTIGATION™

www.secbi.com

info@secbi.com