

В отличие от традиционных технологии анализа сетевого трафика решение SecBI позволяет использовать данные существующих сетевых журналов и не требует установки дополнительных программных или аппаратных средств, что ускоряет внедрение и снижает стоимость владения системой. Решение не требует длительного периода инсталляции, работа с системой понятна на интуитивном уровне, а результаты доступны практически сразу после установки без длительного периода обучения.

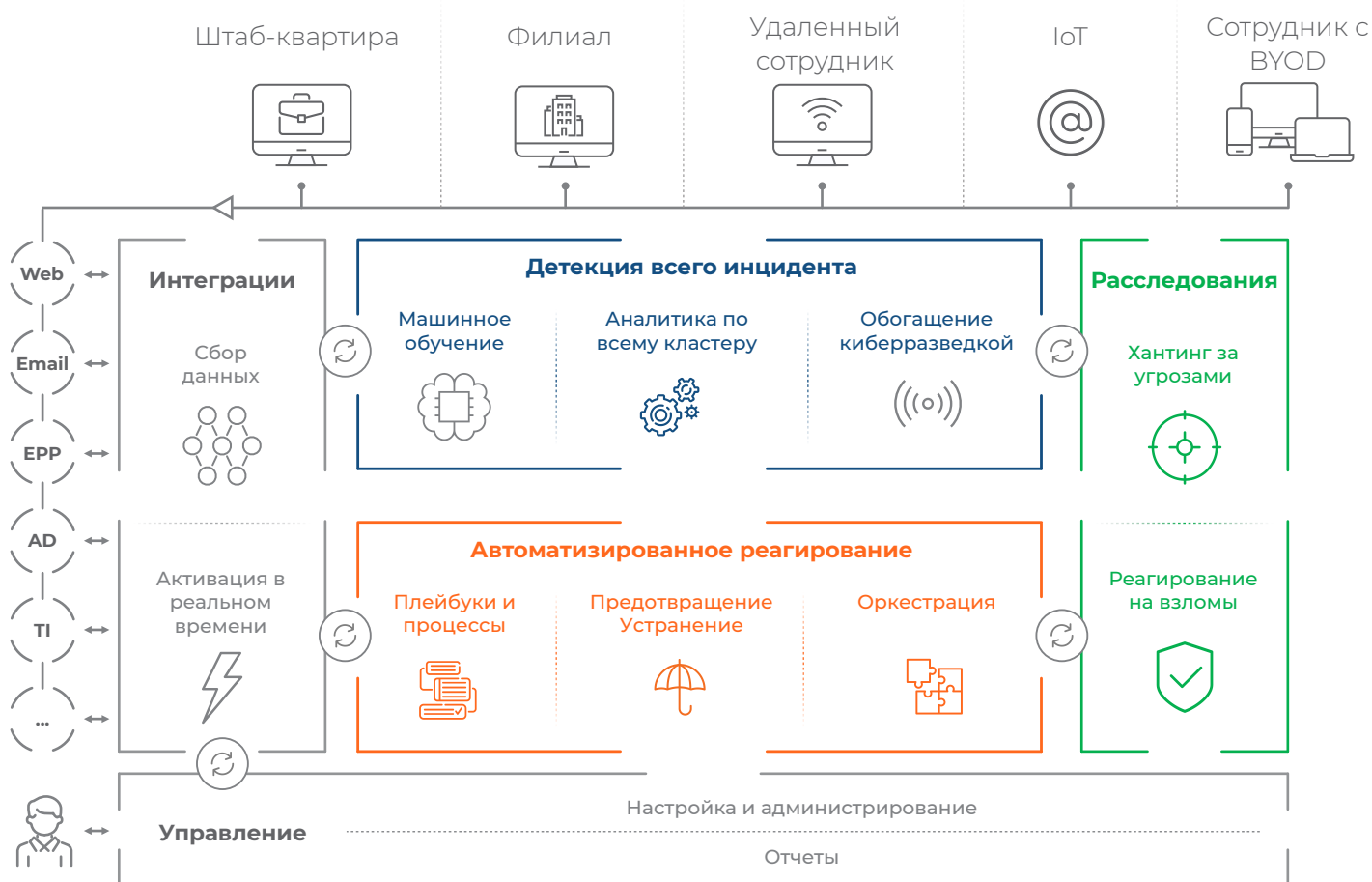
СПОСОБНОСТЬ ВЫЯВЛЯТЬ НЕИЗВЕСТНОЕ

Технология SecBI выявляет и объединяет в кластеры как внутренние сущности (например, пользователей и устройства), так и внешние (например, домены, IP-адреса, C2-серверы, точки сбора данных), коммуницирующие во взломанной сети. Выявление вредоносного кластера, а не отдельных аномалий или отдельных событий, позволяет быстрее и полнее обнаружить атаку. Из потока разрозненных алертов SecBI создает приоритизированный сценарий атаки, что облегчает анализ, проведение расследования и устранение последствий инцидента.

ГЛУБОКИЙ МОНИТОРИНГ БЕЗ УЩЕРБА ПРИВАТНОСТИ ДАННЫХ

SecBI анализирует сетевой трафик и данные существующей сетевой инфраструктуры, что позволяет выявлять угрозы и применять данные киберразведки, обеспечивая глубокий мониторинг вне зависимости от шифрования. Использование метаданных, а не сетевых пакетов, позволяет SecBI проводить глубокий анализ без нарушения требований защиты личных или конфиденциальных данных.

АВТОМАТИЗИРОВАННЫЕ ДЕТЕКЦИЯ, РЕАГИРОВАНИЕ И РАССЛЕДОВАНИЯ



НЕДОСТАЮЩЕЕ ЗВЕНО СИСТЕМЫ ЗАЩИТЫ: АВТОМАТИЗИРОВАННОЕ РЕАГИРОВАНИЕ И ПОМОЩЬ В ПРЕДОТВРАЩЕНИИ АТАК

Несмотря на логичность желания автоматизировать ответные меры после выявления угрозы, на рынке практически отсутствуют решения, которые реализовали бы этот принцип. В отличие от продуктов, работающих на основе автоматизированных плейбуков, и подверженных частым ложным срабатываниям, SecBI повышает эффективность за счет полной автоматизации действий и уникальной технологии детекции угроз на основе спонтанного машинного обучения.

Широкий набор готовых автоматизированных процессов и плейбуков позволяет автоматически выявлять настоящий масштаб инцидента, и гибко добавлять необходимые действия по реагированию на инцидент на различных шагах процесса. Возможность добавлять коннекторы к различным СЗИ расширяет функционал платформы по формированию сложных процессов работы с инцидентами.

Пример использования: реагирование на инцидент

SecBI позволяет расставлять приоритеты и более эффективно расследовать инциденты. Аналитики любого уровня могут более эффективно решать задачи в любых расследованиях и сценариях реагирования. Решение помогает интерпретировать алерт в правильном контексте исходного инцидента и реагировать не на отдельные алерты, а на инцидент в целом.

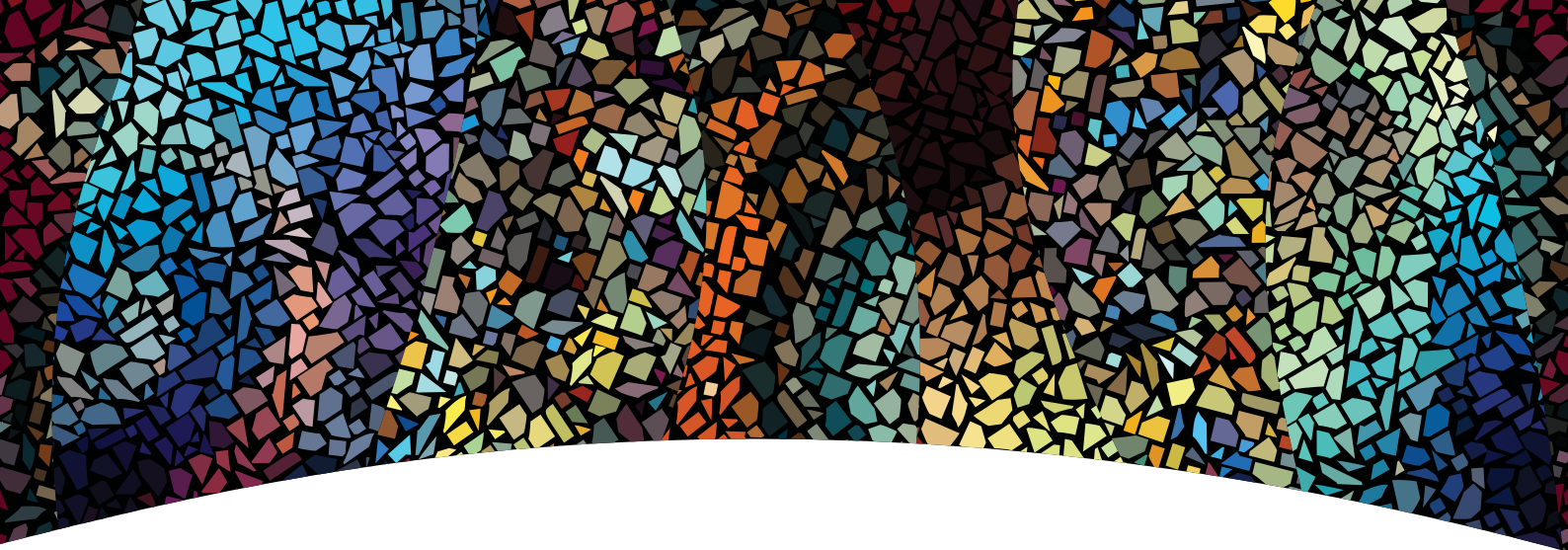
Пример использования: автоматизированный хантинг за угрозами

SecBI позволяет аналитикам более эффективно осуществлять хантинг за угрозами и получать более полную картину происходящего в системе. Анализ данных можно коррелировать с форензикой, в том числе с метаданными для расследования пользователей или инцидентов, а также с исходными данными для тестирования гипотез аналитика. Архитектура на основе больших данных дает возможность SecBI легко и экономично масштабировать период поиска до нескольких месяцев или лет.

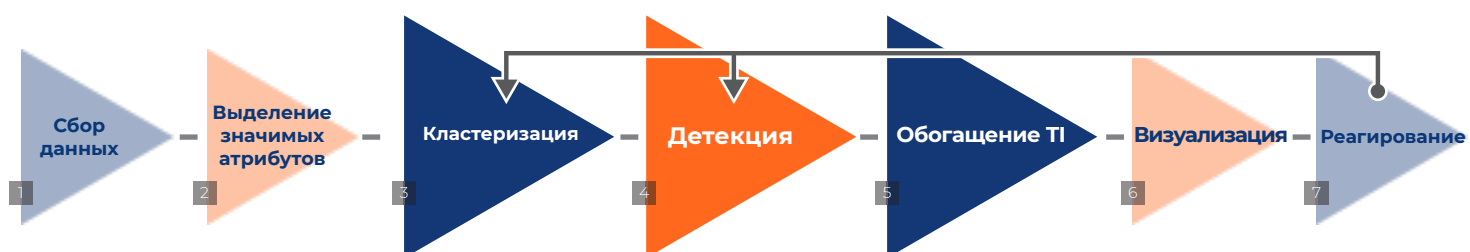
Преимущества технологии Автономных расследований

- ✓ Быстрое и точное реагирование на инциденты
- ✓ Сокращение потребности в высоко-квалифицированных сотрудниках
- ✓ Не требуется установка специализированных устройств или агентов
- ✓ Экономия времени аналитиков SOC благодаря автоматизации расследований и реагирования
- ✓ Защита от латерального движения после взлома





ПРОЦЕСС



ПРИЗНАКИ РЕАЛЬНОЙ ТРАНСФОРМАЦИИ SOC

- ✓ Значительное повышение производительности аналитиков
- ✓ Быстрый и эффективный хантинг угроз
- ✓ Обнаружение полного масштаба каждого инцидента
- ✓ Автоматизированное реагирование и предотвращение будущих схожих атак

ВНЕДРЕНИЕ И РЕЗУЛЬТАТЫ ЗА СЧИТАННЫЕ ДНИ

Решение SecBI легко и быстро разворачивается без использования дополнительных устройств или агентов. Установить решение можно как на площадке заказчика, так и в облаке. Эффективность SOC повышается моментально без изменений в сетевой инфраструктуре. Персонал SOC быстро обучается использованию решения. Не требуются дорогостоящие сервисы по внедрению.



www.secbi.com

info@secbi.com