ПОВЫШЕНИЕ ТОЧНОСТИ МОНИТОРИНГА И УСИЛЕНИЕ ПРОАКТИВНОЙ ЗАЩИТЫ В КРУПНОМ ПРОМЫШЛЕННОМ ХОЛДИНГЕ

Цитата эксперта заказчика

«Solar TI Feeds стал для нас одним из главных источников информации об актуальных угрозах. Он позволяет не просто реагировать на инциденты, а действовать на опережение, выявляя атаки и снижая риски их развития на самых ранних стадиях»

Профиль организации

Промышленная компания

Крупная компания с распределенной инфраструктурой, множеством офисов и дочерних организаций.

В компании функционирует зрелый SOC, выстроены процессы мониторинга и реагирования на инциденты ИБ, интеграции индикаторов компрометации (IoC) в межсетевые экраны и SIEM-систему для проактивного поиска угроз (Threat Hunting).

Данные о проекте

Solar TI Feeds

О сервисе: потоки данных (фидов) об актуальных киберугрозах

Внедрение: 2025 год

Выбор решения: В ходе всестороннего сравнения ключевых поставщиков данных об киберугрозах выбрано решение вендора «Солар», поставляющего самые актуальные фиды, напрямую пересекающиеся с реальными атаками на компанию.

Цель

Повышение точности мониторинга и усиление проактивной защиты

Задача

Развитие процессов Threat Intelligence:

Для достижения максимального баланса между широтой покрытия мониторингом и качеством детектирования при работе с коммерческими фидами перед департаментом ИБ стояла задача автоматизации процесса выявления актуальных угроз и получения уникальных данных, которые невозможно найти в открытых источниках.

Решение

Выбор решения и пилотное тестирование:

В ходе всестороннего сравнения ключевых поставщиков данных об киберугрозах основным критерием выбора для компании была актуальность данных для реального ландшафта киберугроз организации.

Максимальное пересечение с возможными угрозами:

Тестирование показало, что данные сервиса Solar TI Feeds имеют наиболее высокий процент совпадения с реальными атаками, которые компания фиксирует в своей инфраструктуре «в моменте».

Высокий уровень персонализации и клиентской поддержки:

Опыт и компетенции вендора при разработке индивидуальных коннекторов под конкретное техническое задание для SIEM, NGFW и внутренней TI-платформы заказчика позволили интегрировать фиды в существующий стек безопасности без необходимости разворачивать дополнительную инфраструктуру.

Внедрение и поддержка:

Процесс интеграции прошел бесшовно. Команда вендора обеспечила полную техническую поддержку: от разработки коннекторов до настройки потоков данных об угрозах. Выстроенное через оперативные каналы связи взаимодействие позволяет команде экспертов быстро реагировать на запросы по уточнению или корректировке индикаторов компрометации.

Результаты

Проактивное обнаружение:

Сервис усилил «первую линию обороны», позволив блокировать угрозы до их проникновения в сеть.

Улучшение процессов в команде:

Повышение качества данных позволило аналитикам SOC перераспределить ресурсы и высвободить время на развитие процессов Threat Hunting в режиме 24/7.

Ликвидация «слепых зон»:

Благодаря качеству и эксклюзивности фидов Solar 4RAYS команда ИБ получает наиболее полное представление о подозрительной активности, которую ранее не всегда было возможно обнаружить стандартными средствами.

Например, сервис позволил обнаружить факты массового использования сотрудниками VPN-расширений, запрещенных корпоративной политикой.