Алексей Щербаков, заместитель генерального директора ПАО «ГТЛК»

ГТЛК АВТОМАТИЗИРОВАЛА ПРОЦЕСС УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ С ПОМОЩЬЮ MAXPATROL SIEM

«Успешное внедрение системы MaxPatrol SIEM создало дополнительный механизм для эффективного управления процессом обеспечения информационной безопасности, что показывает качественный подход к обеспечению поставленных задач».

Алексей Щербаков
заместитель генерального директора ПАО «ГТЛК»

«Внедрение комплекса Positive Technologies позволило создать гибкую систему выявления инцидентов информационной безопасности с работающими правилами корреляции. Ключевым достижением проекта является автоматизация существующих ИБ-процессов с минимальными временными затратами. Поддержка MaxPatrol SIEM актуальных для нас источников событий, в том числе российских СЗИ, и наличие эффективных правил корреляции "из коробки" позволили реализовать проект внедрения за полгода. Система запущена в промышленную эксплуатацию. Мы уже получили качественные результаты по автоматическому выявлению инцидентов информационной безопасности».

Сергей Рысин
советник директора по безопасности ПАО «ГТЛК»

ПРОФИЛЬ КОМПАНИИ

- **Отрасль:** государственный сектор
- **Название:** ПАО «Государственная транспортная лизинговая компания»
- **Источники событий:** MS SQL, Cisco IronPort, Cisco ASA, InfoWatch Traffic Monitor, Check Point Appliance, ERP-системы, сетевое оборудование, контроллеры доменов, почтовые серверы, серверы удаленного доступа и др.

- **Задача:** выстраивание и автоматизация комплексного процесса управления информационной безопасностью
- **Продукт:** MaxPatrol SIEM

ЗАДАЧА

ПАО «Государственная транспортная лизинговая компания» — многопрофильная лизинговая компания, входящая в пятерку крупнейших игроков лизингового рынка России по объему лизингового портфеля. Основными направлениями деятельности ГТЛК являются лизинг воздушного, водного и железнодорожного транспорта, грузовых автомобилей и специальной техники, а также городского пассажирского транспорта.

ГТЛК имеет 13 региональных представительств. Компания ведет деятельность во всех регионах России, реализует государственную политику управления и развития транспортной отрасли и сотрудничает с государственными ведомствами и агентствами, включая Министерство транспорта РФ и Федеральное дорожное агентство.

В рамках модернизации системы обеспечения информационной безопасности в ГТЛК был внедрен ряд систем для защиты от утечек данных, целенаправленных кибератак и вирусного заражения. Большое число систем, журналы которых необходимо анализировать для выявления инцидентов информационной безопасности, привело к низкой эффективности и ресурсозатратности ручной проверки событий ИБ. С помощью SIEM-системы компания планировала централизовать сбор данных из критически важных для бизнеса систем и автоматизировать обработку событий (порядка 3 тыс. событий ИБ в секунду).

РЕШЕНИЕ

Первым шагом к автоматизации обработки событий ИБ стал анализ существующих процессов ИБ. Специалисты ГТЛК проанализировали, какие процессы можно автоматизировать, и составили перечень требований к SIEM-системе.

В ходе поиска решения специалисты ГТЛК протестировали четыре системы класса SIEM российских и международных производителей — лидеров рынка. Ключевыми параметрами исследования были:

- наличие существующих коннекторов для источников событий, присутствующих в инфраструктуре ГТЛК;
- наличие актуальных правил корреляции «из коробки»;
- возможность подключения к системе собственных критически важных источников, в том числе «самописных»;
- возможность инвентаризации сети и поддержания данных о топологии в актуальном состоянии;
- достаточная простота работы с системой для самостоятельного создания новых правил корреляции;
- возможность масштабирования системы;
- русскоязычная техническая поддержка и возможность прямого взаимодействия с вендором.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- Автоматическое построение топологии сети организации на основе модели активов
- Мгновенная адаптация к изменениям в IT-инфраструктуре
- Выявление нарушений правил доступа между узлами и зонами сетевой безопасности
- Подключение актуальных источников данных без дополнительных затрат силами Positive Technologies
- Эффективные правила корреляции «из коробки»

В результате исследования функциональных возможностей продуктов был выбран MaxPatrol SIEM. В качестве системного интегратора выступила компания «Инфосекьюрити».

В ходе реализации проекта к MaxPatrol SIEM были подключены следующие источники: MS SQL, Cisco IronPort, Cisco ASA, InfoWatch Traffic Monitor, Check Point Appliance, ряд ERP-систем, а также сетевое оборудование, контроллеры доменов, почтовые серверы и серверы удаленного доступа. Благодаря наличию в базе нормализации широкого спектра систем, в том числе российских СЗИ, и готовым правилам корреляции «из коробки» специалисты «Инфосекьюрити» в короткие сроки осуществили внедрение MaxPatrol SIEM и его ввод в эксплуатацию.

Опираясь на данные источников, MaxPatrol SIEM формирует полную модель IT-инфраструктуры и отражает любые изменения в режиме реального времени, автоматически обновляя правила корреляции и тем самым обеспечивая их стойкость. Визуализация топологии сети и поиск связанных с инцидентами событий, который не требует знания языка сценариев, позволили MaxPatrol SIEM снизить требования к команде эксплуатации. Кроме того, визуализация топологии упростила процесс распределения задач по реагированию на инциденты ИБ между структурными подразделениями.

РЕЗУЛЬТАТ

Весь процесс внедрения продукта от старта предпроектного обследования до перевода в промышленную эксплуатацию занял всего 6 месяцев.

Столь краткие сроки внедрения были обеспечены серьезной подготовкой: в течение года специалисты ГТЛК определяли сценарии использования системы, а также проводили сравнение систем на основе разработанных критериев. Внедрение MaxPatrol SIEM позволило ГТЛК автоматизировать процессы информационной безопасности и объединить в комплекс узкоспециализированные ИБ-системы, а также выстроить удобный и эффективный процесс мониторинга и реагирования на инциденты ИБ. Уже в первые месяцы работы система неоднократно помогала выявить и предотвратить:

- несанкционированное подключение личного оборудования к корпоративной сети;
- несанкционированное получение доступа к конфиденциальной информации и ее распространение за периметром корпоративной сети;
- заражение рабочих станций вредоносным ПО;
- несвоевременное обновление программного обеспечения на рабочих станциях.

В текущий момент на базе MaxPatrol SIEM в ГТЛК тестируются корреляция событий со СКУД и данных об активности на рабочих станциях сотрудников для предотвращения передачи паролей и логинов третьим лицам, а также автоматизация управления политиками доступа к внешней сети.

В дальнейших планах сотрудничества ГТЛК, «Инфосекьюрити» и Positive Technologies — подключение к MaxPatrol SIEM новых источников событий и последовательное внедрение других продуктов (MaxPatrol 8, PT MultiScanner) для выстраивания всесторонней защиты корпоративной инфраструктуры от киберугроз.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays