ИСТОРИЯ УСПЕХА

Внедрение системы мониторинга и управления событиями информационной безопасности в компании Тройка Диалог

Тройка Диалог – ведущая инвестиционная компания, работающая на рынках стран СНГ. Ключевыми направлениями деятельности компании, основанной в 1991 г., являются торговые операции с ценными бумагами, инвестиционно-банковские услуги, доверительное управление активами, прямые и венчурные инвестиции, персональные инвестиции и финансы.

Помимо Москвы Тройка Диалог представлена в 20 городах России, а также в Нью-Йорке, Лондоне, Никосии, Киеве и Алматы. Среди клиентов Тройки Диалог ведущие российские и международные компании, финансовые институты, государственные учреждения, а также состоятельные частные лица.

ЗАДАЧИ

Компания Тройка Диалог уделяет повышенное внимание безопасности бизнес-процессов и регулярно принимает необходимые организационно-технические меры по ее обеспечению. Для автоматизации процесса управления событиями ИБ руководство отдела информационной безопасности компании Тройка Диалог приняло решение о внедрении специализированной системы, осуществляющей мониторинг событий, их автоматизированную обработку и выявление инцидентов.

К новой системе были предъявлены следующие требования:

- обеспечить постоянный анализ событий и инцидентов ИБ;
- автоматизировать процесс выяснения причин их возникновения;
- оптимизировать работу специалистов, осуществляющих мониторинг состояния ИБ;
- сократить издержки по накоплению, классификации, анализу и разбору инцидентов;
- свести к минимуму рутинные ручные операции при оценке эффективности текущих мер защиты и процессов ИБ.

Исполнителем проекта была выбрана компания «Инфосистемы Джет», имеющая в портфолио различные проекты, начиная от внедрения отдельных компонентов систем ИБ до разворачивания Центров оперативного управления ИБ «под ключ».

«В настоящее время задачи по мониторингу событий информационной безопасности и оперативному реагированию на инциденты выходят на первый план, и большинство наших заказчиков концентрирует усилия на автоматизации этих задач, – комментирует **Евгений Акимов, заместитель директора Центра информационной безопасности компании «Инфосистемы Джет».** *– Для такой крупной компании, как Тройка Диалог, оперативный доступ к данным мониторинга безопасности, своевременное отслеживание и разрешение инцидентов в режиме реального времени – неоценимый вклад в повышение эффективности и управляемости системы ИБ в целом».*

РЕШЕНИЕ

Система мониторинга и управления событиями ИБ класса SIEM (Security Information and Event Management) реализует комплексный подход к решению задач сбора, анализа и контроля событий, поступающих от различных средств защиты. Она помогает решить следующие задачи:

- управление большим объемом событий ИБ;
- получение полной картины происходящего в информационной системе с точки зрения ИБ;
- мониторинг текущего уровня обеспечения безопасности (контроль достижения заданных показателей эффективности (KPI);
- своевременное обнаружение инцидентов ИБ;
- получение реальных данных для анализа и оценки рисков;
- принятие обоснованных решений по управлению безопасностью;
- выполнение отдельных требований законодательства и нормативных актов в области мониторинга событий ИБ (ISO/IEC 27001:2005, PCI DSS, СТО БР ИББС, Федеральный закон № 152-ФЗ «О персональных данных» и др.).

127015 Россия, г. Москва,
ул. Б. Новодмитровская, д. 14, стр.1
Телефон: +7 (495) 411-7601
Факс: +7 (495) 411-7602
info@jet.su
www.jet.su



Благодаря четкой постановке задач со стороны компании Тройка Диалог специалистам компании «Инфосистемы Джет» удалось в кратчайшие сроки создать систему мониторинга и управления событиями информационной безопасности – с момента старта проекта до его окончания прошло всего два месяца. В ходе пошаговой проработки деталей проекта достигалось выполнение всех ключевых показателей и метрик, заданных заказчиком.

Одним из ключевых этапов проекта стало подключение источников событий: настроен сбор информации с различных систем, образовывающих периметр безопасности, и установлены серверы корреляции событий. Далее в соответствии с требованиями компании Тройка Диалог специалисты компании «Инфосистемы Джет» провели работы по настройке правил обработки, нормализации, агрегации и приоритизации событий информационной безопасности.

РЕЗУЛЬТАТ

Система позволяет сотрудникам отдела информационной безопасности Тройки Диалог получать оперативный доступ к данным аудита критичных систем, за счет чего более эффективно отслеживать события ИБ в режиме реального времени. В то же время она дает возможность хранить историю событий, откуда можно получать данные для оценки и последующего анализа рисков и принятия обоснованных решений по обеспечению информационной безопасности.

В настоящее время система находится на технической поддержке специалистов компании «Инфосистемы Джет». Привлечение интегратора может потребоваться для оперативного реагирования в случае возникновения нештатных ситуаций. Кроме того, по запросу заказчика специалисты компании оказывают поддержку при написании новых правил корреляции событий. В дальнейшем планируется масштабирование системы и подключение к ней новых источников.

«В нашей компании применяется комплексный подход к обеспечению информационной безопасности. Использование системы класса SIEM позволяет автоматизировать и систематизировать процесс сбора, анализа и обработки информации о событиях безопасности, что в конечном итоге приводит к повышению эффективности работы всей системы безопасности, – комментирует **начальник отдела информационной безопасности компании Тройка Диалог Михаил Иванов**. *– Своевременное получение и реакция на события безопасности позволяют перейти на качественно новый уровень в поддержке бизнес-процессов компании. Мы удовлетворены сотрудничеством с компанией «Инфосистемы Джет» и планируем продолжить совместную работу по совершенствованию и оптимизации системы».*

«Сегодня одной из основных задач системы безопасности, помимо отражения атак, является их уверенное, своевременное обнаружение, предоставление максимума информации для разбора инцидентов, – резюмирует **Эльман Бейбутов, заместитель руководителя по работе с финансовыми организациями Центра информационной безопасности компании «Инфосистемы Джет».** *– Поэтому компания Тройка Диалог концентрирует свои усилия на повышении именно управляемости системы, её прозрачности и «аудируемости». Такой подход позволяет не только более эффективно распоряжаться информационными и материальными ресурсами, но также взаимодействовать с персоналом – отслеживать лояльность, выявлять скрытые потребности сотрудников, повышать мотивацию, что значительно снижает риски появления внутренних инцидентов».*

Эльман Бейбутов, заместитель руководителя по работе с финансовыми организациями Центра информационной безопасности компании «Инфосистемы Джет»:

«На наш взгляд, в качестве средства выявления угроз, финансовых рисков и утечки информации наиболее интересны функции и отчеты по отслеживанию использования «чужих» учетных записей для аутентификации в системе. Также важным показателем для индикации нарушения могут быть изменения конфигурации систем, создание пользователей с административными привилегиями на короткий промежуток времени и отчеты по удалению/копированию пользователями данных. Поэтому мы выбрали в качестве технологической платформы HP ArcSight как технически наиболее совершенный и законченный продукт для решения подобных задач».

Михаил Иванов, начальник отдела информационной безопасности Тройки Диалог:

«Сегодня понятие информационной безопасности гораздо шире, чем борьба с утечками. Для обеспечения требуемого уровня информационной защищенности уже недостаточно одного мониторинга нарушений политик информационной безопасности. Для этого необходимо выявлять, аккумулировать, анализировать и связывать между собой множество самых разнообразных данных и событий, связанных с процессами компании. Реализация данного проекта позволила нам получить прозрачную и предсказуемую систему управления рисками и ИТ-безопасностью».