ДРТ

ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ

BUSINESS SOLUTIONS AND TECHNOLOGIES

Создание централизованной системы мониторинга событий информационной безопасности систем SAP

Решение SAP Enterprise Threat Detection (SAP ETD)

Автоматизированные решения

Наш подход

Внедрение системы для централизованного мониторинга событий информационной безопасности (ИБ) SAP требует системного подхода. Подход ДРТ заключается в проведении **комплексного анализа архитектуры** системного ландшафта компании, выявлении **актуальных рисков ИБ в ходе оценки защищенности** и определении **детальных технических требований к мониторингу.** Это позволяет создать процессы и решения, которые дадут возможность **не только оперативно выявлять инциденты ИБ, но и отслеживать развитие событий по ним до устранения проблемы.**

Понимание бизнес-процессов компании и функционала решений SAP позволяет нам проводить риск-ориентированный мониторинг, направленный на покрытие областей высокого риска для компаний. Мы разрабатываем нестандартные, специфичные для бизнес-процессов и систем правила корреляции событий ИБ в системах SAP с учетом результатов проведения независимой оценки защищенности (penetration testing) и выявленных областей мониторинга событий ИБ, совместно с командой заказчика улучшаем правила для снижения числа ложных срабатываний и прорабатываем подход к устранению выявленных инцидентов ИБ.

Ключевыми результатами проекта по созданию системы для централизованного мониторинга событий ИБ в SAP являются:

- Настроенное и подключенное к системам-источникам решение для непрерывного мониторинга событий ИБ
- Описанные процессы по работе с решением, интегрированные с действующими процессами ИБ, а также нормативная документация
- Библиотека стандартных и нестандартных правил корреляции событий ИБ, учитывающих специфику процессов компании
- Сценарии реагирования на инциденты ИБ SAP-систем (incident response playbooks)

Правильно выстроенный процесс мониторинга событий ИБ на базе решения SAP ETD позволяет автоматически выявлять события ИБ в системах SAP без трудоемкой ручной проверки, минимизирует время выявления инцидентов и уязвимостей, обеспечивает создание доказательной базы длительного хранения для расследования неправомерных действий, категоризацию, унификацию и возможность глубокого анализа событий ИБ, а также снижает фактические и потенциальные потери в результате инцидентов ИБ в системах SAP.

Ключевые функции SAP ETD

Контроль событий ИБ

- Автоматизированное выявление событий ИБ на основе поступающих из систем-источников журнальных данных
- Наличие предустановленных правил корреляции с возможностью настройки и разработки нестандартных правил корреляции для выявления инцидентов ИБ систем SAP

Регистрация инцидентов ИБ

- Автоматизация регистрации и документирования инцидентов ИБ систем SAP
- Возможность оперативной передачи информации о выявленном инциденте в корпоративную SIEM-систему, а также ответственным лицам по электронной почте

Реагирование на инциденты ИБ

- Управление в SAP ETD расследованиями выявленных инцидентов, создание шаблонов расследования
- Возможность настройки правил для временного исключения повторной регистрации инцидента по выбранным критериям

Расследование инцидентов ИБ

- Анализ инцидентов ИБ SAP при помощи аналитических инструментов SAP ETD в рамках расследования
- Объединение идентичных инцидентов в одно расследование
- Возможность совместного ведения расследования пользователями

Контроль уязвимостей систем SAP

- Встроенные автоматические проверки работоспособности систем-источников и самой системы SAP ETD (health check)
- Мониторинг критичных инцидентов ИБ и статуса установки нот безопасности в подключенных системах SAP

Отчетность

- Формирование отчетов с результатами мониторинга событий ИБ систем SAP и количеством выявленных инцидентов
- Визуализация отчетности в виде дашбордов
- Интеграция отчетности ETD в регулярную корпоративную отчетность по ИБ

Что может предложить ДРТ?

Мы предлагаем следующие услуги в области создания систем мониторинга событий ИБ для систем SAP:

Создание централизованного комплексного решения, обеспечивающего непрерывный мониторинга событий ИБ в системах SAP на базе решения SAP ETD

Разработка методологии контроля и мониторинга событий ИБ и сценариев реагирования на инциденты, интеграция с действующими процессами управления безопасностью

Анализ и разработка требований заказчика, создание решения, учитывающего специфичные требования в рамках внедрения SAP ETD

Риск-ориентированный подход к созданию специфичных для компании правил корреляции, калибровка работы стандартных правил SAP ETD, минимизация ложных срабатываний

Обучение сотрудников заказчика работе с решением SAP ETD, содействие в проведении расследований инцидентов ИБ, развитие навыков для сопровождения и развития решения

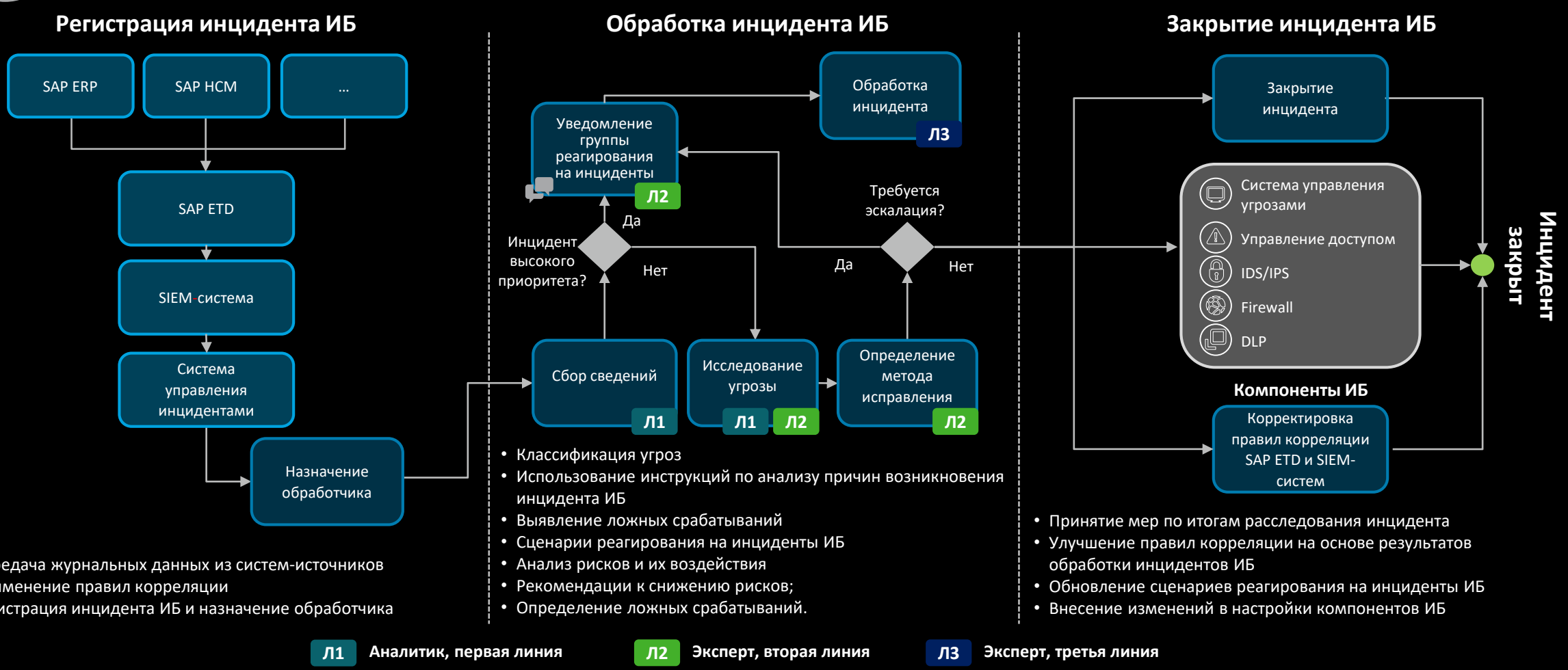
Пример архитектуры межсистемной интеграции

* Приведенная на слайде схема является примером. Архитектура может быть устроена иначе с учетом специфики требований и особенностей ландшафта заказчика.

1. Активация необходимых логов на стороне систем-источников (SAP и других систем). Оперативное получение данных. Для каждого источника может быть настроено отдельное расписание получения логов системой SAP ETD.
2. Применение правил нормализации и настроенных правил корреляции, выявление инцидентов ИБ на различных уровнях подключенных систем-источников (уровень приложения, ОС, БД). Устранение ложных срабатываний. Хранение журнальных данных на время проведения расследования
3. Передача выявленных инцидентов ИБ в корпоративные системы противодействия злоупотреблениям для дальнейшей обработки и длительного хранения (опционально)
4. Передача выявленного инцидента ИБ в систему управления инцидентами для назначения ответственного за обработку и принятие мер по реагированию

Иллюстративный пример процесса реагирования на инциденты ИБ

Перечень действий по реагированию на инциденты ИБ систем SAP прописывается и детализируется для каждого из корреляционных сценариев, а также отражается в инструкциях по реагированию на инциденты.



Результаты внедрения системы SAP ETD

Ключевыми результатами внедрения системы SAP ETD являются:

01 Охват автоматическим мониторингом критически важных систем SAP и других систем за счет подключения необходимого количества журнальных данных систем-источников

02 Повышение точности выявления инцидентов ИБ в системах SAP за счет корреляции событий ИБ на разных уровнях ИТ-инфраструктуры, поддерживающей системы SAP

03 Снижение фактических и потенциальных потерь в результате инцидентов ИБ в системах SAP с помощью формализации процесса реагирования и увеличения количества обрабатываемых инцидентов

04 Минимизация времени выявления инцидентов и уязвимостей за счет быстрой передачи журнальных данных из источников в SAP ETD

05 Сокращение времени реагирования на инциденты ИБ в системах SAP за счет организации процесса, применения аналитических инструментов SAP ETD и гибкой работы с событиями ИБ

06 Увеличение уровня контроля за процессами ИТ-направлений и SAP Basis, пользователями и несанкционированным использованием полномочий и, как следствие, повышение дисциплины пользователей систем SAP

О компании ДРТ

ДРТ имеет значительный опыт в сфере кибербезопасности, включая реализацию одного из крупнейших проектов централизации мониторинга событий ИБ с помощью решения SAP Enterprise Threat Detection в СНГ.

Специалисты компании ДРТ хорошо знакомы со спецификой внедрения решения SAP ETD, жизненным циклом таких проектов, а также возможными рисками, особенностями подключения источников данных и создания новых правил корреляции событий ИБ. Это позволяет нам эффективно реализовывать проекты и достигать поставленных целей, используя накопленный опыт и отработанную практику.

ДРТ может оказать вам поддержку в области автоматизации процессов сбора, контроля и мониторинга событий ИБ в системах SAP на базе решения SAP ETD. Наши услуги включают:

- создание комплексного решения для централизованного мониторинга событий ИБ в системах SAP в режиме реального времени, которое учитывает специфику бизнеса заказчика и интегрировано с корпоративными процессами управления ИБ;
- использование риск-ориентированного подхода к разработке специфичных правил корреляции событий ИБ в системах SAP с учетом результатов проведения независимой оценки защищенности систем SAP (penetration testing);
- разработку методологии контроля и мониторинга событий ИБ;
- организацию процесса реагирования на инциденты ИБ систем SAP, при необходимости предполагающего передачу выявленных инцидентов во внешнюю корпоративную систему для централизованной обработки;
- подключение к SAP ETD источников, не имеющих стандартного интерфейса подключения к SAP ETD и преднастроенных правил нормализации данных, а также интеграция с системой управления инцидентами ИБ (SIEM).

Выбирая сотрудничество с ДРТ, вы получаете доступ к команде сертифицированных SAP-специалистов, готовой разработать действенные варианты решений и предоставить рекомендации по интересующим вас вопросам.

Нам доверяет большое количество клиентов. Мы оказываем профессиональные услуги в самых различных областях, и это позволяет нам продуктивно использовать накопленный опыт.

Контакты

Алексей Яковлев

Директор

+7 (495) 787 06 00

доб. 5219

ayakovlev@delret.ru

Михаил Следков

Директор

+7 (495) 787 06 00

доб. 1210

msledkov@delret.ru

ДРТ

ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ

BUSINESS SOLUTIONS AND TECHNOLOGIES

АО ДРТ