Система контроля защищенности и соответствия стандартам MaxPatrol 8 предназначена для решения большого количества задач безопасности SAP-систем, включая инвентаризацию, контроль обновлений и выявление уязвимостей, а также анализ настроек, конфигураций и прав доступа. Систему отличают:

- постоянно обновляемая база уязвимостей SAP с рекомендациями по их устранению;
- система рекомендаций по корректной настройке конфигураций SAP и необходимым обновлениям;
- поддержка со стороны известных экспертов по безопасности SAP;
- гибкий механизм отчетности и русскоязычный интерфейс.

MAXPATROL 8 ДЛЯ SAP: НОВЫЙ УРОВЕНЬ БЕЗОПАСНОСТИ ERP-СИСТЕМ

Бизнес-приложения класса ERP, часто построенные на решениях SAP, управляют ключевыми процессами крупных предприятий. Ежедневно эти системы обрабатывают большие объемы конфиденциальной информации, что делает их привлекательными для мошенников и недобросовестных конкурентов. Любая попытка проникновения в ERP-систему может обернуться остановкой производства, утечкой важных данных и финансовыми потерями. Безопасность SAP-систем у многих ассоциируется только с разграничением прав доступа, но этого явно недостаточно, поскольку злоумышленники активно используют и другие возможности:

- Уязвимости в компонентах SAP: их число за последние 5 лет выросло в несколько раз и составляет более 3000.
- Ошибки в настройке. Внедрение ERP — масштабный процесс, который требует значительных финансовых и организационных затрат, поэтому ERP-системы часто сдаются в эксплуатацию в небезопасных конфигурациях, с большим количеством стандартных настроек.
- Слабая парольная политика и отсутствие контроля действий пользователей ERP-системы, количество которых может исчисляться тысячами.
- Широкий охват технологических процессов и интеграция ERP-системы с большим количеством приложений, включая небезопасные.

Официальная интеграция с SAP NetWeaver®
Теперь вам не придется доверять свою SAP-систему посторонним. MaxPatrol официально поддерживает платформу SAP NetWeaver 7.0, совместим с CVE и имеет сертификат соответствия CIS Security Software Certification.

SAP® Certified
Integration with SAP NetWeaver®

КАК РАБОТАЕТ MAXPATROL 8 ДЛЯ SAP

+ **Инвентаризация:** MaxPatrol обеспечивает обнаружение и учет максимально широкого спектра ресурсов, в том числе серверов приложений SAP, серверов СУБД, рабочих станций и мобильных компьютеров, сетевого оборудования и специализированных средств защиты.
+ **Контроль обновлений и выявление уязвимостей:** система выполняет анализ компонентов SAP на платформе SAP R/3 и SAP NetWeaver, популярных операционных систем, СУБД и приложений сторонних разработчиков, а также веб-приложений собственной разработки.
+ **Анализ настроек и конфигураций SAP-системы** позволяет выявить небезопасные настройки, отсутствие шифрования при передаче данных, попытки отключения механизмов авторизации, а также повысить производительность систем.
+ **Анализ прав доступа** включает анализ привилегий пользователей системы SAP на наличие пересечений прав доступа в рамках матрицы segregation of duties (SoD) на основе рекомендаций SAP.
+ **Соответствие стандартам безопасности:** автоматизированная проверка соответствия стандартам ERP-систем (DSAG, ISACA), международным стандартам IT-индустрии (ISO 27001/27002, SOX, PCI DSS, NSA, NIST и CIS), а также требованиям государственных регуляторов (ФЗ-152, СТО Газпром, приказы ФСТЭК) и собственным политикам безопасности клиента.
+ **Контроль событий.** Совместно с системой мониторинга и корреляции событий безопасности MaxPatrol SIEM система контроля защищенности MaxPatrol 8 позволяет выявлять запуск критически важных транзакций и модулей, создание или удаление пользователей, попытки несанкционированного входа или получения доступа к конфиденциальным данным.
+ **Контроль изменений.** Система позволяет проводить регулярный контроль изменений по всем анализируемым объектам в SAP-системах, в том числе в части обнаружения новых уязвимостей, изменений прав доступа, ролей и профилей авторизации, создания или блокирования пользователей, изменения настроек системы.
+ **Генератор отчетов.** Набор интегрированных метрик позволяет наглядно представить текущий уровень защищенности системы или отдельных подразделений и активов, выявить наиболее слабые узлы и опасные уязвимости, а также оценить динамику решения задач безопасности в ретроспективе.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована ФСТЭК и «Газпромом». 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.ru
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays