



Positive Technologies

является одной из ведущих российских компаний в области информационной безопасности.

Основные направления деятельности компании - разработка системы контроля защищенности и соответствия стандартам MaxPatrol и сканера безопасности XSpider; предоставление консалтинговых и сервисных услуг в области информационной безопасности; развитие специализированного портала Securitylab.ru.

Компания имеет лицензии ФСТЭК России, ФСБ России и Минобороны России на деятельность в области защиты информации.

Заказчиками Positive Technologies являются более 40 государственных учреждений, более 50 банков и финансовых структур, 20 телекоммуникационных компаний, более 40 промышленных предприятий, компании ИТ-индустрии, сервисные и ритейловые компании России, стран СНГ, Балтии, а также Великобритании, Германии, Голландии, Израиля, Ирана, Китая, Мексики, США, Таиланда, Турции, Эквадора, ЮАР, Японии.

Positive Technologies - это команда высококвалифицированных разработчиков, консультантов и экспертов, которые обладают большим практическим опытом, имеют профессиональные звания и сертификаты, являются членами международных организаций и активно участвуют в развитии отрасли.

РОССИЯ / МОСКВА
ЩЕЛКОВСКОЕ ШОССЕ / 23А
ТЕЛ.: +7 (495) 744 01 44
ФАКС: +7 (495) 744 01 87
E-MAIL: PT@PTSECURITY.RU
WWW.PTSECURITY.RU
WWW.MAXPATROL.RU
WWW.SECURITYLAB.RU



MAXPATROL

СИСТЕМА КОНТРОЛЯ
ЗАЩИЩЕННОСТИ
И СООТВЕТСТВИЯ СТАНДАРТАМ
MAXPATROL

MAXPATROL

Система MaxPatrol - сертифицированное средство автоматизации процессов инвентаризации, управления уязвимостями, контроля соответствия стандартам и эффективности защиты распределенных гетерогенных информационных систем.



Ключевые возможности MaxPatrol

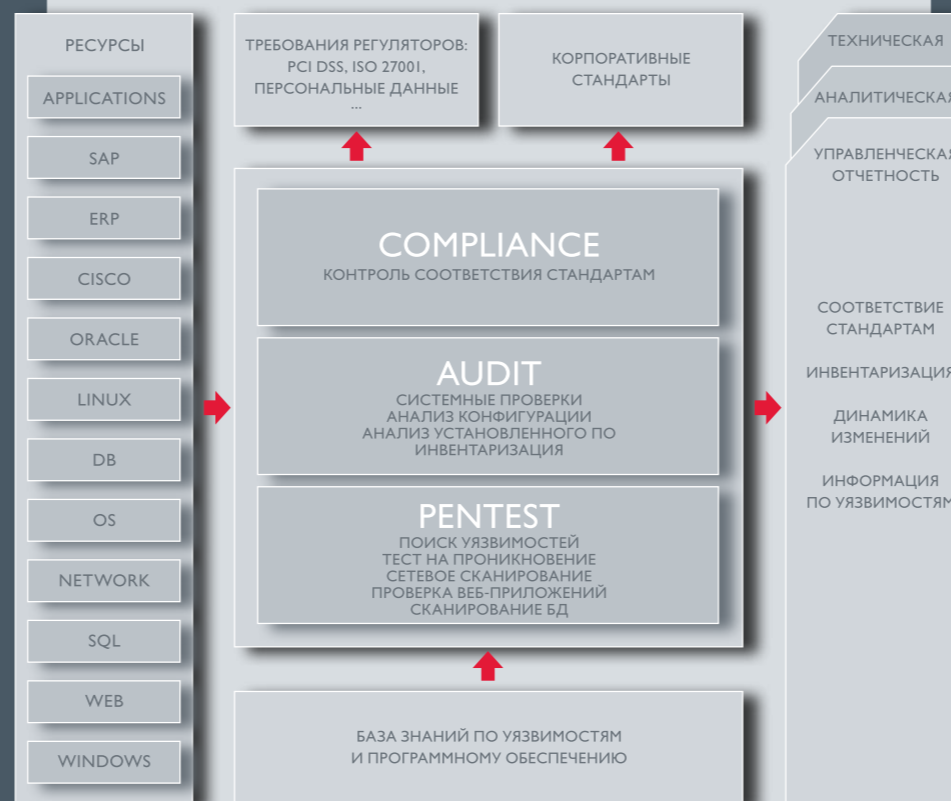
Основой для создания системы MaxPatrol послужил профессиональный сканер безопасности XSpider и десятилетний опыт экспертов компании Positive Technologies, полученный в ходе его разработки, внедрения и эксплуатации в ведущих российских и зарубежных компаниях.

MaxPatrol - единственный продукт на мировом рынке, в котором объединены механизмы системных проверок, тестирования на проникновение, контроля соответствия стандартам в сочетании с поддержкой анализа сетевого оборудования, операционных систем, ERP-систем, веб-приложений.

При разработке MaxPatrol учтены особенности российского рынка, в частности: используется русскоязычный интерфейс, реализована возможность работы модулей системы по узким каналам связи, учтены требования российского законодательства в области информационной безопасности.

Основные характеристики системы MaxPatrol

- Реализация всех активных механизмов оценки защищенности в одном продукте. В системе MaxPatrol используются модули сетевого сканирования, тестирования на проникновение (PenTest), оценки защищенности веб-систем и системного сканирования ОС, СУБД и приложений. Это позволяет проводить комплексный анализ безопасности всей информационной инфраструктуры.
- Гибкая система отчетности (техническая, аналитическая, управленческая). Техническая отчетность с подробным описанием найденных уязвимостей и указаниями по их устранению. Аналитическая отчетность по соответствию информационных систем техническим политикам. Управленческая отчетность по состоянию защищенности подразделений/филиалов/департаментов с указанием динамики изменений метрик эффективности за период времени. Отчеты формируются на русском и английском языках.
- Трехуровневая архитектура системы. Система построена на основе трехуровневой архитектуры (сканер-сервер-консолидатор), что обеспечивает высокое масштабирование и позволяет производить внедрения в организациях любых масштабов.
- Безагентные технологии. Все проверки ресурсов проводятся удаленно, без установки на них дополнительных агентов, что позволяет упростить установку и эксплуатацию системы.
- Уникальные методы поиска уязвимостей. В базе знаний системы содержится больше 20 000 уязвимостей. Используются уникальные эвристические методы, позволяющие обнаруживать еще неопубликованные уязвимости. Поддержкой базы знаний занимается специализированная лаборатория, выпускающая ежедневные обновления.
- Интеграция с системами управления обновлениями и системами консолидации и корреляции событий ИБ (netForensics, ArcSight, Cisco MARS).



Комплексный подход и интеллектуальные средства автоматизации, реализованные в системе MaxPatrol, обеспечивают минимизацию трудозатрат, необходимых для решения задач оценки защищенности и контроля соответствия стандартам, что позволяет оперативно контролировать состояние защищенности информационной системы.



Основные возможности системы MaxPatrol

- Оценка защищенности информационных систем. Выявление брешей в защите ИТ системы, формирование задания на их устранение, отслеживание эффективности и своевременности устранения найденных уязвимостей.
- Отслеживание текущего состояния информационных ресурсов. Проведение инвентаризации корпоративных ресурсов и своевременное обнаружение изменений в ИТ системе.
- Контроль соответствия ИТ системы техническим политикам. Формирование технических стандартов с использованием имеющейся в системе базы знаний, включающей комплексные стандарты для сетевого оборудования Cisco, Nortel, Juniper, Huawei, платформ Windows, Linux, Unix, СУБД Microsoft SQL, Oracle, приложений Active Directory, Microsoft Exchange, Lotus, SAP/R3 и веб-служб собственной разработки. Автоматическое проведение мониторинга соответствия ИТ системы сформированным техническим политикам безопасности.
- Измерение эффективности процессов ИБ в организации. На основе постоянно пополняемой информации, система формирует расширяемый набор метрик безопасности (KPI), по которым оценивается эффективность процессов обеспечения ИБ. Метрики рассчитываются на основе реальных количественных данных, собранных модулями оценки защищенности, инвентаризации, контроля соответствия.
- Управление соответствием отраслевым и международным стандартам, таким как ГОСТ ИСО/МЭК 17799, ГОСТ ИСО/МЭК 27001, SOX (Sarbanes-Oxley Act), PCI DSS (Payment Card Industry Data Security Standard), NSA (National Security Agency), NIST (National Institute of Standards and Technologies), CIS (Center for Internet Security).