



ИСТОРИЯ УСПЕХА

PT Sandbox обеспечивает кибербезопасность корпоративной почты группы «Солид»



ТПГ «Солид» — лидер в производстве отделочных материалов из полистирола и пенополистирола. Собственные производственные мощности завода, оснащенные высокотехнологичным оборудованием, располагаются на территории России и Беларуси.

По данным Positive Technologies [↗](#), в 2024–2025 годах промышленный сектор оказался в фокусе киберпреступников, подвергшись наибольшему числу успешных атак среди российских организаций. Для взлома инфраструктуры в большинстве случаев использовалось вредоносное ПО. Почти половина таких инцидентов начиналась [↗](#) с электронного письма. Стремясь защитить корпоративную почту от вредоносного ПО, в первую очередь от шифровальщиков, группа «Солид» решила внедрить проактивный анализ сообщений на базе песочницы.

500

специалистов
работают
в компании

>1500

позиций
в ассортименте
завода

>40%

продукции
экспортируется
в другие страны

Задача

Деятельность промышленного предприятия опирается на ключевые корпоративные ИТ-системы и сервисы («1С», CRM, корпоративную почту, файловые хранилища и сервисы доступа), а их остановка из-за кибератаки ведет к простоям, которые могут дорого обойтись компании. Корпоративная почта долгое время оставалась уязвимым сегментом инфраструктуры. До внедрения специализированного решения проверка подозрительных вложений осуществлялась вручную по запросу пользователей. Такой подход был не только трудоемким, но и рискованным — всегда существовала вероятность, что письмо с шифровальщиком или целевым вредоносом останется незамеченным.

ГЛАВНЫЙ ВОПРОС — КАК АВТОМАТИЗИРОВАТЬ ПРОВЕРКУ ПОЧТОВЫХ ВЛОЖЕНИЙ, ЧТОБЫ ИСКЛЮЧИТЬ ЧЕЛОВЕЧЕСКИЙ ФАКТОР И ЗАЩИТИТЬ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ ОТ УТЕЧКИ

Риски усугублялись регуляторными требованиями: компания обязана защищать коммерческую тайну и персональные данные в соответствии с законом № 152-ФЗ и рекомендациями ФСТЭК. Успешная атака могла привести не только к операционным, но и к репутационным и финансовым потерям из-за штрафов. Необходимо было найти российское решение, которое бы не просто обнаруживало угрозы, но и эффективно блокировало их до попадания к пользователю, интегрируясь в существующую ИТ-инфраструктуру без ущерба для бизнес-процессов.

Выбранное решение

После анализа рынка было принято решение внедрить песочницу PT Sandbox. Важным аргументом для заказчика стали экспертиза вендора, функциональная наполненность и удобство использования продукта. Песочница Positive Technologies обнаруживает угрозы за счет комбинации разных методов анализа, технологий машинного обучения и внешней экспертизы, а также блокирует ВПО, препятствуя его попаданию внутрь компании.

На этапе пилотного тестирования, организованного партнером вендора — компанией «Экстрим безопасность», PT Sandbox проанализировала около 40 000 объектов из почтового трафика и файловых хранилищ. Продукт показал высокую эффективность в обнаружении широкого спектра угроз: загрузчиков, троянов, стилеров, эксплойтов и потенциально нежелательных программ. По итогам испытаний было принято решение о полноценном внедрении.

Результаты

Благодаря PT Sandbox защита почтового трафика строится в режиме блокировки. Теперь каждое входящее письмо с вложением автоматически направляется в песочницу для глубокого поведенческого анализа. Если PT Sandbox обнаруживает признаки вредоносной активности, письмо блокируется, а система безопасности уведомляет администратора. Это полностью исключает возможность попадания опасного файла к конечному пользователю и прерывает цепочку атаки на самом раннем этапе.

Песочница PT Sandbox превратила почтовый канал из источника угроз в защищенный бизнес-инструмент.

Полная автоматизация анализа угроз.

Устранена необходимость в ручной проверке вложений. Процесс стал проактивным, непрерывным и не зависит от бдительности сотрудников.

Проактивное противодействие сложным угрозам.

Система эффективно выявляет и блокирует не только массовые, но и целевые атаки, направленные на кражу конфиденциальной информации.

Соответствие регуляторным требованиям.

Внедрение песочницы укрепило позиции компании в части выполнения требований закона № 152-ФЗ и рекомендаций ФСТЭК по защите информации.

Повышение киберустойчивости бизнеса.

Защита критически важных систем от простоя из-за кибератак обеспечивает непрерывность производственных и логистических процессов.

«Внедрение песочницы — часть стратегии кибербезопасности нашего предприятия. Нам нужен был российский продукт, удобный в использовании и имеющий более широкую функциональность по сравнению с аналогами, — рассказал Дмитрий Панов, директор ООО «ТПГ „Солид“». — Команда „Экстрим безопасности“ предложила рассмотреть PT Sandbox, и этот вариант оказался оптимальным для нас. Продукт автоматизировал анализ входящих писем и обеспечил проактивное обнаружение вредоносных и других сложных угроз. Песочница помогла повысить киберустойчивость завода и стала критически важным звеном в нашей системе ИБ»



← ПОДРОБНЕЕ ПРО ПРОДУКТ



← ОСТАВИТЬ ЗАЯВКУ НА ПИЛОТ