«ТАМОЖЕННАЯ КАРТА» КОНТРОЛИРУЕТ IT-ИНФРАСТРУКТУРУ С MAXPATROL SIEM ALL-IN-ONE

«MaxPatrol SIEM All-In-One — это быстрый способ получить работающую SIEM-систему. За три месяца с помощью консультаций специалистов Positive Technologies нам самостоятельно удалось внедрить систему и настроить необходимые источники. Благодаря этому мы получили подробную картину IT-инфраструктуры и отслеживаем инциденты ИБ».

Сергей Горчаков,
директор по информационной безопасности
«Таможенной карты»

Таможенная Карта

«Таможенная карта» — национально значимая платежная система, позволяющая проводить все виды таможенных платежей на территории России. Услугами «Таможенной карты» пользуются около трех тысяч клиентов — от транспортных компаний до ведущих промышленных предприятий.

ПРОФИЛЬ ОРГАНИЗАЦИИ

Название:
ООО «Таможенная карта»

Деятельность:
организация расчетов по таможенным платежам

Клиенты: компании пищевой промышленности, нефтяного и энергетического комплекса, авиаперевозчики, импортеры медикаментов

73 банка в России — эмитенты «Таможенной карты»

IT-инфраструктура — небольшая: 200 сетевых узлов

Сайт: customscard.ru

ЗАДАЧА:

сбор и анализ событий ИБ для выявления инцидентов в небольшой организации

РЕШЕНИЕ:

MaxPatrol SIEM All-In-One

Задача

Вопрос информационной безопасности имеет высокий приоритет для компании, так как финансовая отрасль по-прежнему остается одной из популярных целей для кибератак.

Для «Таможенной карты» важна непрерывность бизнеса, чтобы проводить операции в рамках установленного SLA. В месяц через платежную систему проходит операций на сумму от 50 до 70 млрд рублей.

Чтобы оперативно выявлять атаки и предотвращать сбои в работе, необходимо анализировать события ИБ из всех значимых источников в инфраструктуре. Необходимость регистрации и анализа событий безопасности прописана и в приказах ФСТЭК России № 17 и 21.

Инфраструктура «Таможенной карты» включает 200 сетевых узлов. Анализ событий проводился вручную, что не позволяло оперативно реагировать на обнаруженные угрозы. При регулярно меняющихся конфигурациях сетевых узлов, отсутствие актуальных знаний об инфраструктуре мешало выявлять инциденты.

Руководство «Таможенной карты» приняло решение внедрить SIEM-систему для автоматического анализа событий ИБ и выявления атак, аномалий и подозрительных действий в инфраструктуре. Департамент информационной безопасности оценил возможности трех самых популярных систем в России — IBM QRadar, ArcSight и MaxPatrol SIEM All-In-One. Сравнивались их ценовая политика, возможности интеграции и взаимодействия с инфраструктурой.

По итогам тестирования «Таможенная карта» выбрала SIEM-систему компании Positive Technologies, так как она соответствовала всем заявленным требованиям:

- MaxPatrol SIEM All-In-One — законченное коробочное решение для небольших инфраструктур;
- дополнительные источники событий подключаются бесплатно в рамках техподдержки;
- доступная цена — от 3,5 млн рублей;
- входит в реестр отечественно ПО.

Решение

Пилотный проект длился три месяца. Подразделение ИБ самостоятельно внедрило и настроило MaxPatrol SIEM All-In-One. За это время к SIEM-системе были подключены рабочие станции и источники с наибольшим количеством событий — контроллеры домена, прокси-серверы и межсетевой экран Cisco. На основе поступающих из источников данных MaxPatrol SIEM All-In-One формирует базу активов и по правилам корреляции выявляет инциденты. По итогам пилота «Таможенная карта» получила полностью работающий продукт, готовый к промышленной эксплуатации.

Внедрить систему в короткие сроки получилось за счет бесплатного обучения специалистов компании и оперативного реагирования службой технической поддержки Positive Technologies на запросы заказчика. Специалисты «Таможенной службы» научились писать правила корреляции для выявления инцидентов, подключать источники, писать запросы к системе для поиска конкретных событий.

Результат

MaxPatrol SIEM All-In-One поддерживает непрерывность деятельности «Таможенной карты». Теперь подразделение ИБ владеет полной информацией об инфраструктуре, выявляет проблемные и новые активы, следит за аномалиями и подозрительными активностями. Все это стало возможным благодаря сбору и анализу событий ИБ в единой точке — MaxPatrol SIEM All-In-One.

За время эксплуатации к источникам событий добавились:

- инфраструктурные серверы: почта, система контроля и управления доступом, система видеонаблюдения, системы учета аппаратных средств, сетевых адресов, мест в серверных стойках;
- системы защиты: антивирус, средство криптографической защиты информации для создания электронной подписи JINN;
- бизнес-системы: центр обработки данных процессинга, 1С;
- критически значимые файловые серверы.

В планах подключение к источникам событий серверов собственного удостоверяющего центра.

MAXPATROL SIEM ALL-IN-ONE

Система выявления инцидентов ИБ для IT-инфраструктур малого и среднего масштаба

Коробочное решение: поставляется в виде программно-аппаратного комплекса

В 2017 году MaxPatrol SIEM занял 25% рынка SIEM в России (исследование IDC)

Подходит организациям с общим количеством сетевых узлов 250, 500 или 1000

80+ проектов внедрения MaxPatrol SIEM и MaxPatrol SIEM All-In-One реализовано с 2015 года

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. 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.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.