MAXPATROL SIEM ОБЕСПЕЧИВАЕТ НЕПРЕРЫВНОСТЬ РАБОТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВЛАСТИ РЕСПУБЛИКИ КОМИ

«На ГАУ РК "ЦИТ" лежит ответственность за бесперебойную работу значимых для Республики Коми информационных систем. Для нас обеспечение их информационной безопасности и оперативное реагирование на киберугрозы — задачи номер один. Внедрение MaxPatrol SIEM позволило нам в кратчайшие сроки создать эффективную систему выявления инцидентов и уже за первую неделю эксплуатации выявить и предотвратить серьезные угрозы».

Денис Рычков, начальник отдела технической защиты информации управления по безопасности ГАУ РК «ЦИТ»

ПРОФИЛЬ ОРГАНИЗАЦИИ

Название:
государственное автономное учреждение Республики Коми «Центр информационных технологий»

Деятельность:
развитие информационного общества и формирование электронного правительства в регионе

IT-инфраструктура — 3200 сетевых узлов

Сайт: cit.rkomi.ru

ЗАДАЧА:

выявление инцидентов для обеспечения непрерывной работы региональных информационных систем и ресурсов

РЕШЕНИЕ:

MaxPatrol SIEM

ГАУ РК «Центр информационных технологий» — крупнейшая IT-организация на территории Коми. Центр отвечает за техническое обеспечение эксплуатации региональных информационных систем, техническую поддержку компьютерных систем органов исполнительной власти Республики Коми и формирование электронного правительства в регионе. Ключевые клиенты ГАУ РК «ЦИТ» — государственные структуры и бизнес-сообщество.

Задача

В задачи ГАУ РК «ЦИТ» входят организация электронного взаимодействия, выстраивание политики ИБ в органах государственной власти республики и местного самоуправления, аттестация рабочих мест и информационных систем.

Инфраструктура организации включает 2600 рабочих станций, 600 серверов и средства защиты информации. На серверах обрабатываются государственные информационные системы Республики Коми с 1-го по 3-й класс защищенности, система обращения граждан в органы государственной власти.

Чтобы оперативно выявлять атаки и подозрительные действия в инфраструктуре, а также 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.

Ранее организация использовала SIEM-систему зарубежного производства, но из-за сложностей при получении технической поддержки и требований законодательства руководство ГАУ РК «ЦИТ» решило заменить систему.

Решение

Специалисты по безопасности ГАУ РК «ЦИТ» оценили возможности отечественных SIEM-систем. Сравнивались возможности интеграции и взаимодействия с инфраструктурой, а также ценовая политика производителей. В результате конкурса победило предложение о поставке одного из лидирующих решений на рынке — MaxPatrol SIEM. Продукт поддерживает большое количество источников и включен в реестр отечественного ПО, что особенно значимо для государственных учреждений.

Подразделение ИБ самостоятельно внедрило и настроило MaxPatrol SIEM за три недели. За это время были определены источники событий для мониторинга, выстроены процессы взаимодействия с IT-службой, настроен регулярный аудит инфраструктуры, прием сетевого трафика для его комплексного анализа. Кроме того, специалисты ГАУ РК «ЦИТ» самостоятельно написали правила корреляции для выявления инцидентов, опираясь на обучающие материалы на портале технической поддержки.

К SIEM-системе были подключены рабочие станции и источники с наибольшим количеством событий, среди них система обнаружения вторжений Snort, системы обнаружения вторжений ViPNet IDS, антивирусное решение Kaspersky Endpoint Security, межсетевые экраны FortiGate. Служба технической поддержки Positive Technologies оперативно реагировала на запросы ГАУ РК «ЦИТ» и помогала настраивать источники событий.

Результат

Установив MaxPatrol SIEM, ГАУ РК «ЦИТ» владеет полной информацией об инфраструктуре, отслеживает события ИБ и сетевой трафик, в режиме реального времени выявляет критически опасные инциденты; за первую неделю в государственных системах республики были выявлены и локализованы семь вредоносных программ.

В планах развития проекта расширение области мониторинга MaxPatrol SIEM — подключение рабочих станций и серверов на Windows. Также MaxPatrol SIEM станет ядром системы безопасности в региональном центре ГосСОПКА, который будет построен на базе ГАУ РК «ЦИТ». Выявленные им инциденты будут передаваться в Национальный координационный центр по компьютерным инцидентам.

MAXPATROL SIEM

Система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз

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

Более 150 проектов внедрения MaxPatrol SIEM реализовано с 2015 года

Более 250 источников событий преднастроено, подключение любых других бизнес-систем бесплатно

От 30 дней занимает ввод продукта в промышленную эксплуатацию

О компании

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.

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

CIT KOMI_CS_A4.RUS.0001.02.JUN.17.2019