MAXPATROL SIEM АНАЛИЗИРУЕТ БОЛЬШИЕ ДАННЫЕ ИБ-ПОДРАЗДЕЛЕНИЯ ФНС РОССИИ

«MaxPatrol SIEM предоставляет необходимые инструменты для решения задач управления инцидентами и событиями ИБ в рамках распределенной IT-инфраструктуры. Продукт также обеспечил централизованную обработку отчетов антивирусной системы, которая не имеет собственных механизмов передачи событий ИБ с регионального уровня на федеральный. С MaxPatrol SIEM мы получили возможность автоматизировать работу с большими данными в ИБ-подразделении ФНС России и в результате сократили время на эскалацию инцидентов и реагирование на них».

Юшков Дмитрий Юрьевич,
Заместитель начальника Межрегиональной инспекции
Федеральной налоговой службы
по централизованной обработке данных

ПРОФИЛЬ ОРГАНИЗАЦИИ

- **Название:** Федеральная налоговая служба (ФНС России)
- **Отрасль:** государственное учреждение, ФОИВ
- **География:** более 100 площадок регионального и межрегионального уровней, более 800 инспекций и более 150 000 узлов сети, распределенные по территории России
- **Источники событий:** автоматизированная система ФНС России и российские средства защиты: система антивирусной защиты, DLP-система, криптомаршрутизаторы, средства межсетевого экранирования и обнаружения сетевых вторжений, система контроля и управления доступом

- **Решение:** централизованный анализ больших данных ИБ-подразделения, управление инцидентами информационной безопасности
- **Продукт:** MaxPatrol SIEM

ЗАДАЧА

Федеральная налоговая служба (ФНС России) состоит из более чем 800 инспекций по всей России, 84 подразделений регионального уровня, 20 межрегиональных подразделений и центрального аппарата, которые составляют единую систему налоговых органов. В ходе совершенствования процессов защиты информации встала задача создать систему централизованного мониторинга инцидентов информационной безопасности инфраструктуры ФНС России, а также автоматизировать процессы реагирования на основе организационной структуры службы. Ее решение было возложено на Межрегиональную инспекцию ФНС России по централизованной обработке данных (МИ ФНС России по ЦОД).

Одним из ключевых источников информации о событиях безопасности в ФНС России является система антивирусной защиты, поэтому к оперативности ее подключения стояли наиболее высокие требования. Однако установленное средство защиты не могло передавать события ИБ с регионального уровня в централизованную систему. В МИ ФНС России по ЦОД приняли решение внедрить новый механизм подъема данных и обработки событий безопасности.

РЕШЕНИЕ

Сотрудничество ФНС с компанией Positive Technologies началось в 2009 году с проекта по внедрению системы контроля защищенности и соответствия стандартам MaxPatrol. В службе реализована крупнейшая инсталляция продукта — более 1000 лицензий, развернутых на федеральном, региональном и местном уровнях и управляемых из единого центра обработки данных. На сегодняшний день MaxPatrol — одна из ключевых систем обеспечения информационной безопасности ФНС России.

Задача централизованного анализа данных антивирусной системы возникла в момент расширения сотрудничества между ФНС России и Positive Technologies — внедрения системы выявления инцидентов информационной безопасности в реальном времени MaxPatrol SIEM. MaxPatrol SIEM — новое поколение MaxPatrol. SIEM-система автоматически строит модель IT-инфраструктуры, выявляет угрозы и маршруты потенциальных атак даже при изменениях IT-ландшафта. Positive Technologies обеспечивает поддержку продукта на всех стадиях внедрения, непрерывно анализирует актуальные угрозы и предоставляет проактивные способы их выявления и локализации через обновляемую базу знаний Positive Technologies Knowledge Base.

РЕЗУЛЬТАТЫ ОЦЕНКИ:

MaxPatrol SIEM — инновационная платформа для выявления инцидентов ИБ и новых угроз в реальном времени.

- Система автоматически строит топологию сети организации на основе модели активов
- Адаптируется к изменяющейся инфраструктуре
- Выявляет нарушения правил доступа между узлами и зонами сетевой безопасности
- Positive Technologies обеспечивает подключение актуальных источников данных без дополнительных затрат
- В MaxPatrol SIEM реализован механизм передачи в продукт экспертизы исследовательского центра Positive Research, основанный на базе знаний Positive Technologies Knowledge Base (PT KB)

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Создание механизма централизованного сбора и обработки событий ИБ на федеральном уровне при отсутствии единого центра передачи журналов в СЗИ
- Поддержка производителем актуальных источников, в том числе российских ИБ-продуктов, «из коробки»
- Повышение оперативности расследования инцидентов

Чтобы организовать централизованный сбор и обработку событий антивирусного средства защиты, специалисты службы и Positive Technologies разработали способ передачи информации о событиях с антивирусной системы из региональных центров в МИ ФНС России по ЦОД и включения этих данных в MaxPatrol SIEM. Для его реализации использовались те же принципы, что были применены ранее при автоматизации защиты от фрода в АИС ФНС «Налог-2». Специалисты Positive Technologies и компании «ЭЛВИС-ПЛЮС» разработали коннектор для антивирусной системы и правила корреляции для выявления инцидентов ИБ.

Помимо мониторинга, в МИ ФНС России по ЦОД требовалось организовать оперативное реагирование на инциденты посредством разграничения прав доступа к событиям на основе организационной структуры ФНС России. На данном этапе внедрения сканеры MaxPatrol SIEM не были установлены в региональных подразделениях ФНС России, поэтому IT-активы выявлялись не только собственными механизмами SIEM-системы, но и с помощью событий антивирусного средства. События информационной безопасности в системе MaxPatrol SIEM привязаны к динамическим группам IT-активов, поэтому каждое новое событие ИБ автоматически относится к определенному элементу организационной структуры. Благодаря разграничению доступа к событиям в MaxPatrol SIEM специалисты из МИ ФНС России по ЦОД получили возможность делегировать реагирование и расследование инцидентов инженерам по безопасности регионального уровня и получать от них уведомления о результатах.

РЕЗУЛЬТАТЫ

В рамках проекта построения системы управления инцидентами и событиями информационной безопасности в ФНС России MaxPatrol SIEM обеспечил централизованный сбор и обработку данных антивирусной системы в масштабах всей инфраструктуры службы.

Кроме того, с помощью MaxPatrol SIEM был выстроен процесс, который позволяет оперативно реагировать на инциденты ИБ на федеральном, региональном и местном уровнях. Это означает, что система может назначить ответственных за реагирование в соответствии с оргструктурой ФНС России, а также разграничить права доступа сотрудников к событиям согласно зонам ответственности.

В результате использования MaxPatrol SIEM удалось автоматизировать работу с большими данными в ИБ-подразделении ФНС России, сократить время на эскалацию инцидентов и реагирование на них.

В планах работы по масштабированию MaxPatrol SIEM почти на 1000 подразделений ФНС России на всей территории Российской Федерации и подключение новых источников, а также упрощение обновления версии продукта и доставки правил нормализации, корреляции и агрегации для выявления атак и расследования инцидентов.

О компании

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