«Абсолют Банк» контролирует IT-инфраструктуру с помощью MaxPatrol SIEM

ПРОФИЛЬ ОРГАНИЗАЦИИ

- **Название:** АКБ «Абсолют Банк»
- **Деятельность:** банковские услуги для физических и юридических лиц
- **Т-инфраструктура:** более 4000 сетевых узлов
- **Сайт:** absolutbank.ru
- **Задача:** развитие собственного SOC в рамках стратегической трансформации подходов к информационной безопасности
- **Решение:** MaxPatrol SIEM

Задача

В 2018 году Абсолют Банк приступил к реализации своей новой стратегии с фокусом на высокотехнологичное развитие приоритетных направлений бизнеса. Одним из условий глобальной цифровизации стало изменение подходов к информационной безопасности: построение процессов ИБ в соответствии с лучшими мировыми практиками и современными российскими нормативами, развитие собственного SOC, переход от защиты периметра к всеобъемлющей защите данных.

При выборе SIEM-системы Абсолют Банк рассматривал решения, на которых можно выстроить экосистему безопасности, а SIEM будет частью такой экосистемы. Решение должно было интегрироваться в выстраиваемую банком современную экосистему защиты, а также легко взаимодействовать с ИТ- и ИБ-продуктами разных классов, в том числе vulnerability management. Абсолют Банк выбирал решение отечественного производства.

Решение

Эксперты Абсолют Банка протестировали и оценили четыре SIEM-системы. В приоритете рассматривались вендоры SIEM, которые обладают экспертизой в исследовании уязвимостей, угроз и таргетированных атак, и регулярно переносят эти знания в свой продукт. По итогам данного тестирования был выбран MaxPatrol SIEM.

Абсолют Банк — крупный федеральный банк с фокусом на высокотехнологичное развитие в приоритетных направлениях бизнеса. Банк специализируется на работе в сегментах с высоким уровнем экспертизы и уникальными IT-решениями: ипотеке, автокредитовании, а также МСБ в цифровом формате, на системном обслуживании компаний транспортно-логистической отрасли, на комплексных решениях в private banking.[1]

1 absolutbank.ru/about/today/stages/

Руслан Ложкин
Руководитель
службы информационной
безопасности
АКБ «Абсолют Банк»

«MaxPatrol SIEM наиболее полно удовлетворил нашей концепции по своим возможностям. **Продукт уже из коробки более чем на 80% соответствует требованиям Банка России**, а компания Positive Technologies самостоятельно взаимодействовала с Банком России и **помогла нашим экспертам реализовать все необходимые требования регулятора**, описанные в ГОСТ Р 57580.1-2017. Кроме того, отмечу техническое сопровождение. В банках, как правило, нет узких компетенций, которые предполагают администрирование и глубокую настройку SIEM. При внедрении и дальнейшей поддержке MaxPatrol SIEM этими вопросами занимаются эксперты Positive Technologies»

MAXPATROL SIEM

- Система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры
- Лидирующее отечественное SIEM-решение .
- Регулярно получает экспертизу для обнаружения угроз .
- Знает наиболее актуальные для России угрозы.
- Быстро развивается
- Выполняет требования по защите информации

Результаты

К настоящему времени MaxPatrol SIEM мониторит около 5 тысяч узлов, что охватывает 95% инфраструктуры банка. Были успешно категоризированы все активы и подключены все источники событий: антивирусы, песочницы, сетевые устройства, рабочие станции, серверы.

MaxPatrol SIEM – один из важнейших инструментов центра операционного реагирования «Абсолют Банка». Система дает полную видимость IT-инфраструктуры, учитывает изменения в ней и в режиме реального времени предоставляет информацию об инцидентах кибербезопасности. Благодаря этому банк может своевременно реагировать на возникающие угрозы и предотвращать реализацию рисков.

Закажите бесплатный пилот:

ptsecurity.com/ru-ru/products/mpsiem/#free-demo

ptsecurity.com
pt@ptsecurity.com

PT-MS_Absolut Bank_SS_A4.RUS.0003.004.MAR.13.2023