открытие

Автоматизация реагирования на инциденты ИБ:

опыт банка «ФК Открытие»

- Системно значимый банк, акционером которого является Банк России со **100%** долей владения
- **7** место по размеру активов среди банков РФ(1)
- **5** место по балансовому капиталу среди банков РФ(1)

Финансовые показатели

2,7 ТРЛН ₽
АКТИВЫ

350 МЛРД ₽
РЕГУЛЯТОРНЫЙ КАПИТАЛ

13,7 %
ОБЩИЙ НОРМАТИВ ДОСТАТОЧНОСТИ КАПИТАЛА (Н1.0)

1,8 ТРЛН ₽
КРЕДИТЫ ДО РЕЗЕРВОВ

2,0 ТРЛН ₽
СРЕДСТВА КЛИЕНТОВ

25,9 МРЛД ₽
ЧИСТАЯ ПРИБЫЛЬ

По предварительным данным отчетности банка «Открытие» на 01.04.2021 по РСБУ на неконсолидированной основе; клиенты банка на 01.04.2021

Клиенты банка

3,1 млн
Розничных клиентов

506 тыс.
Клиентов в сегменте МСБ*
* с учетом АО «Точка»

10,4 тыс.
Корпоративных клиентов

Кредитные рейтинги

Ba2
Moody's
Прогноз – стабильный

AA+.RU
НКР
Прогноз – стабильный

AA(RU)
АКРА
Прогноз – стабильный

ruAA–
Эксперт РА
Прогноз – позитивный

(1) По данным неконсолидированной отчетности банков РСБУ на 01.04.2021 по методике Банка России, без учета НКЦ

8
Федеральных округов

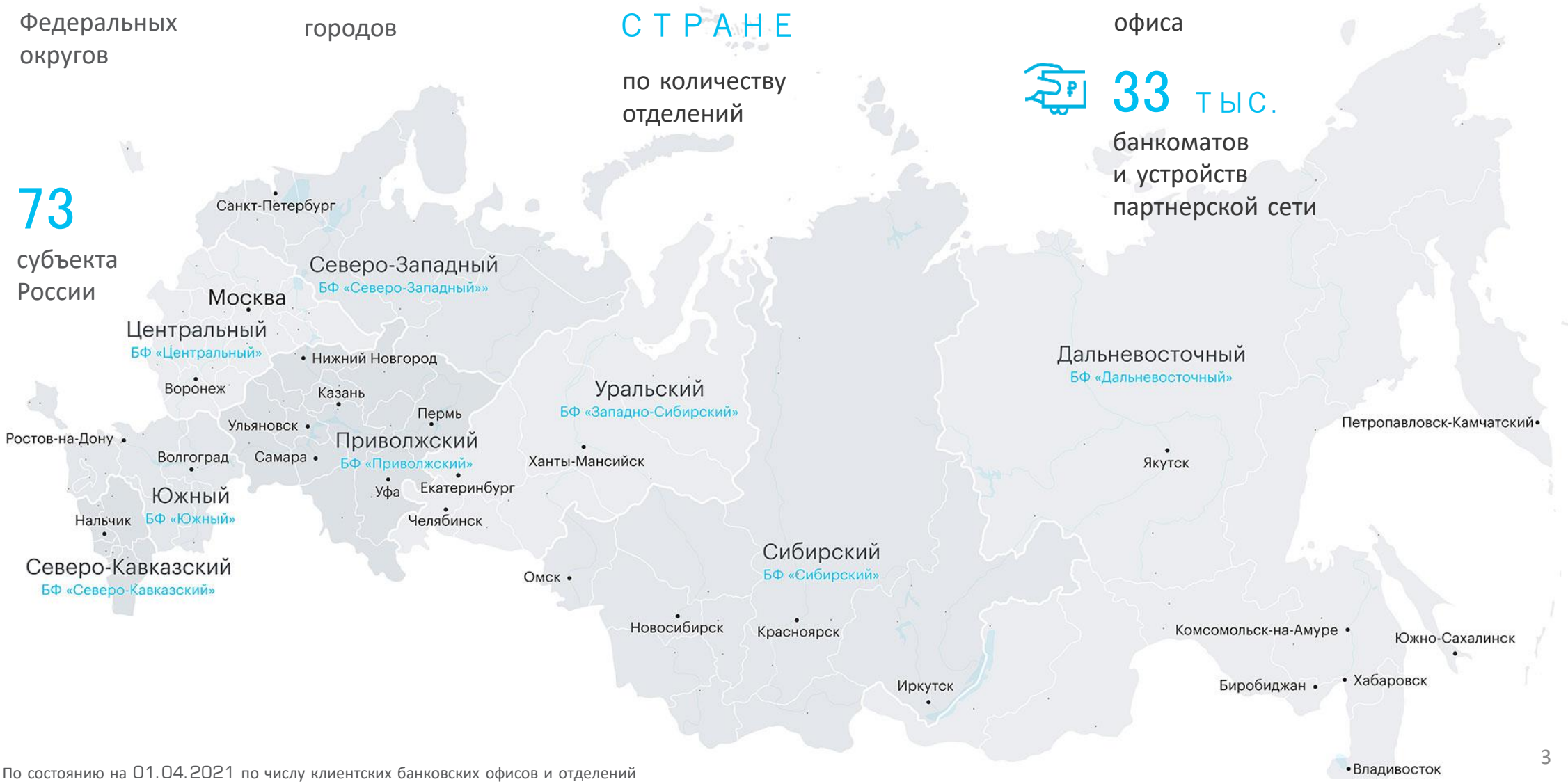
227
городов

№5 в СТРАНЕ
по количеству отделений

524
офиса

33 тыс.
банкоматов и устройств партнерской сети

73
субъекта России



По состоянию на 01.04.2021 по числу клиентских банковских офисов и отделений

2019 г. - внедрение Security Vision Incident Response Platform (IRP/SOAR)
Решены следующие задачи:

- Автоматический сбор и формирование базы активов с регулярным обновлением и использованием в процессах реагирования
- Автоматизировано более **30** сценариев реагирования на инциденты ИБ
- Проведено более **50** интеграций с СЗИ банка
- Раньше специалисту банка нужно было не менее двух часов для проверки **1-2** сложных параметров, а сейчас система осуществляет по **200+** проверок за несколько секунд
- Повысились не только **ширина** охвата, но и **глубина** автоматических проверок параметров
- Небольшой штат сотрудников службы мониторинга и реагирования на инциденты информационной безопасности обеспечивает контроль защищенности более **30 000** серверов и рабочих станций без потери качества
- На базе Security Vision реализована **подготовка оперативной и тактической отчетности**, которая теперь используется как операторами SOC, так и руководителями департамента ИБ
- Платформа является центром накопления **знаний по киберинцидентам** внутри банка

ЭТАПНОСТЬ ЦУМ

SCALE

- Масштабирование процессов и контролей в группе компаний

ADVANCED

- Расширенные ИТ и ИБ процессы
- Отраслевые процессы

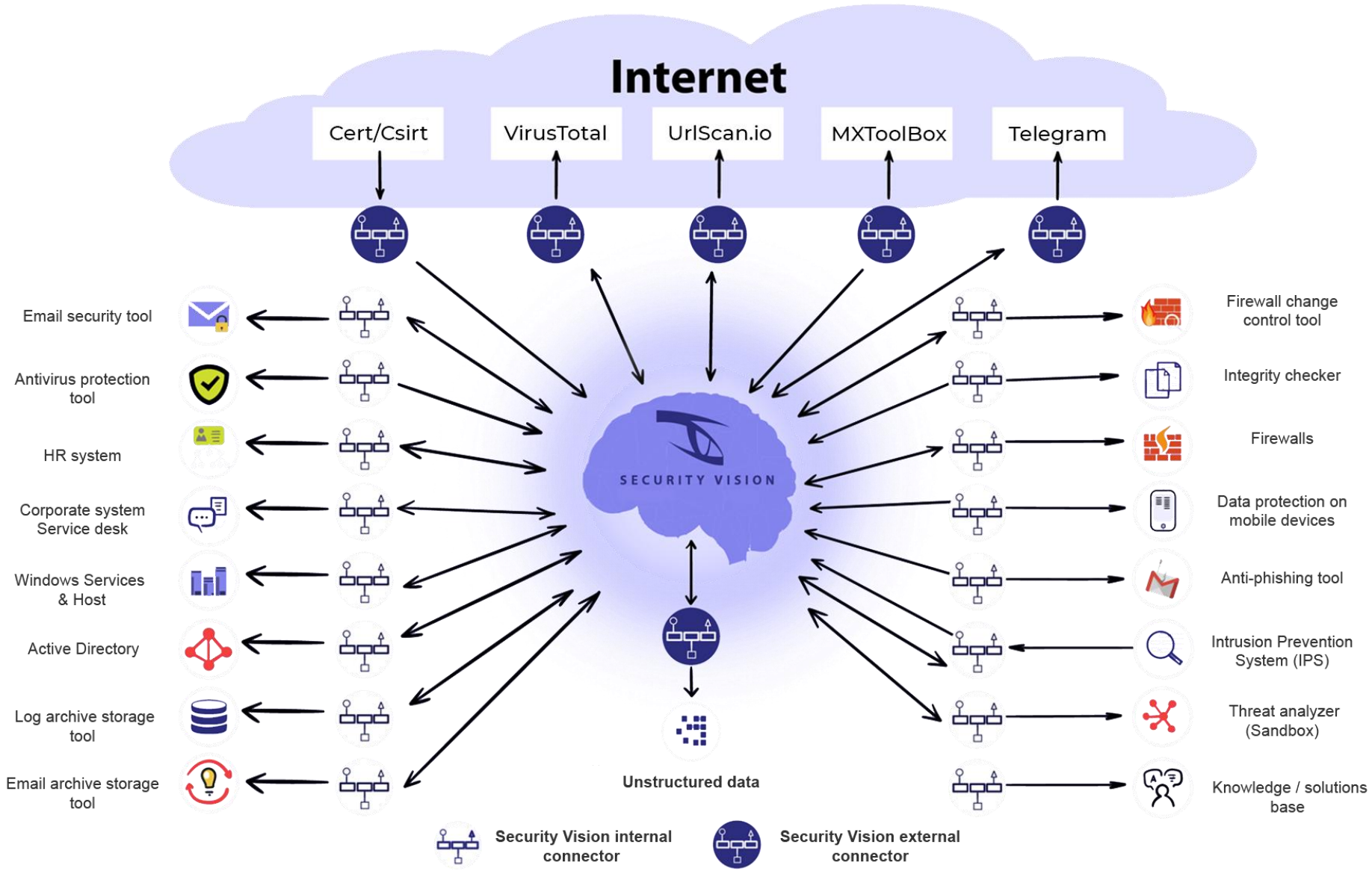
BASE

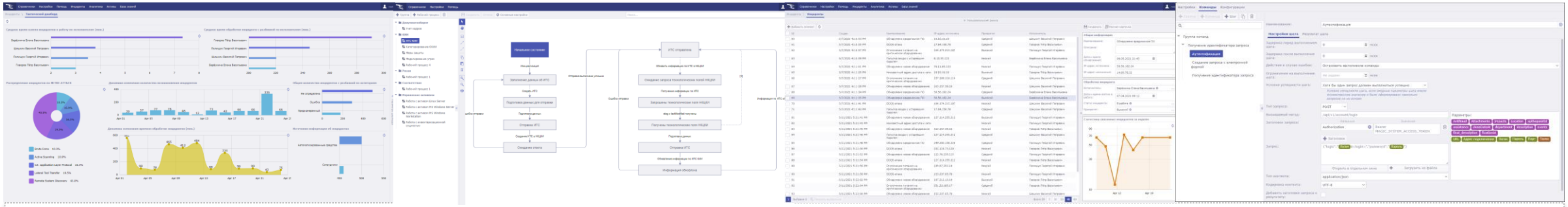
- Базовые ИТ и ИБ процессы
- Визуализация и отчетность

SCOPE

- Первичный аудит
- Инвентаризация ИТ активов, ландшафт

ПРИМЕР СТРУКТУРЫ





БИЗНЕС СЕРВИСЫ

Auto-Compliance, GDPR, ISO 2700x, ISO 22301,…	Audit	Risk Management	Incident management	Awareness	…

РАБОЧИЕ ПРОЦЕССЫ

ФАБРИКА ДАННЫХ

КОННЕКТОРЫ

CMDB	EMAIL	WIKI	SIEM	PAM	MDM	AV	TI	CRM	ARM	SRV	DNS	CCTV	DLP	ERP	FW	VPN	WiFi	НСД

ITSM	IPS	NETW	ACMS	ABS	DAM	ABS	VM	IDM	DB	IC	SANDBOX	SCADA	LDAP	BYOD	IoT	WAF	…

За счет интеграций и разработанных сценариев реагирования область действия SOC теперь покрывает следующие основные области обеспечения ИБ:

- Антивирусная защита
- Сетевая защита
- Защита электронной почты
- Защита веб-траффика
- Контроль внешних публикаций
- Контроль целостности критичных серверов
- Контроль изменений
- Контроль доступа

В результате первого этапа проекта были автоматизированы **ключевые процессы** реагирования на инциденты кибербезопасности, позволяющие специалистам SOC Банка обеспечить необходимый уровень кибербезопасности. Созданная система процессов позволяет легко масштабировать зону мониторинга, в том числе на другие компании группы «Открытие», подключать новые источники событий информационной безопасности, не меняя архитектуру системы и процессы реагирования

2020 г. - расширение области мониторинга и усовершенствование процессов Центра информационной безопасности на базе системы Security Vision IRP/SOAR

Решены следующие задачи:

- Интеграция в Security Vision IRP/SOAR **10** новых систем и средств защиты информации
- Разработка и внедрение **20** новых процедур реагирования на инциденты ИБ
- Автоматизация ряда процессов **смежных подразделений** Центра информационной безопасности, относящихся к ежедневной деятельности их сотрудников
- Автоматизация процесса отправки данных о выявленных угрозах и инцидентах ИБ в **ФинЦЕРТ**

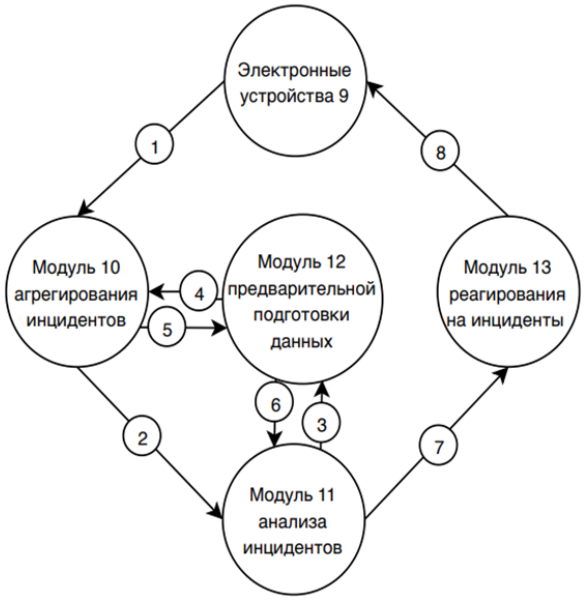
Решены следующие задачи (продолжение):

- Реализация взаимодействия с новым компонентом ИБ-инфраструктуры банка, представляющим собой **аналитический блок больших данных**
- Реализация **новых сценариев реагирования**, связанных с контролем привилегированных пользователей, утечками информации, защитой бренда, защитой от DDoS-атак
- Реализация и автоматизация процессов, связанных с регулярной деятельностью **SOC** банка:
  - контроль подключения источников к системе мониторинга
  - управление сетевыми средствами защиты
  - внутренний Service desk
- Добавлены **новые источники** инцидентов — подключены системы защиты компаний группы
- По мере реализации проекта сотрудники банка самостоятельно разрабатывали **новые сценарии** реагирования

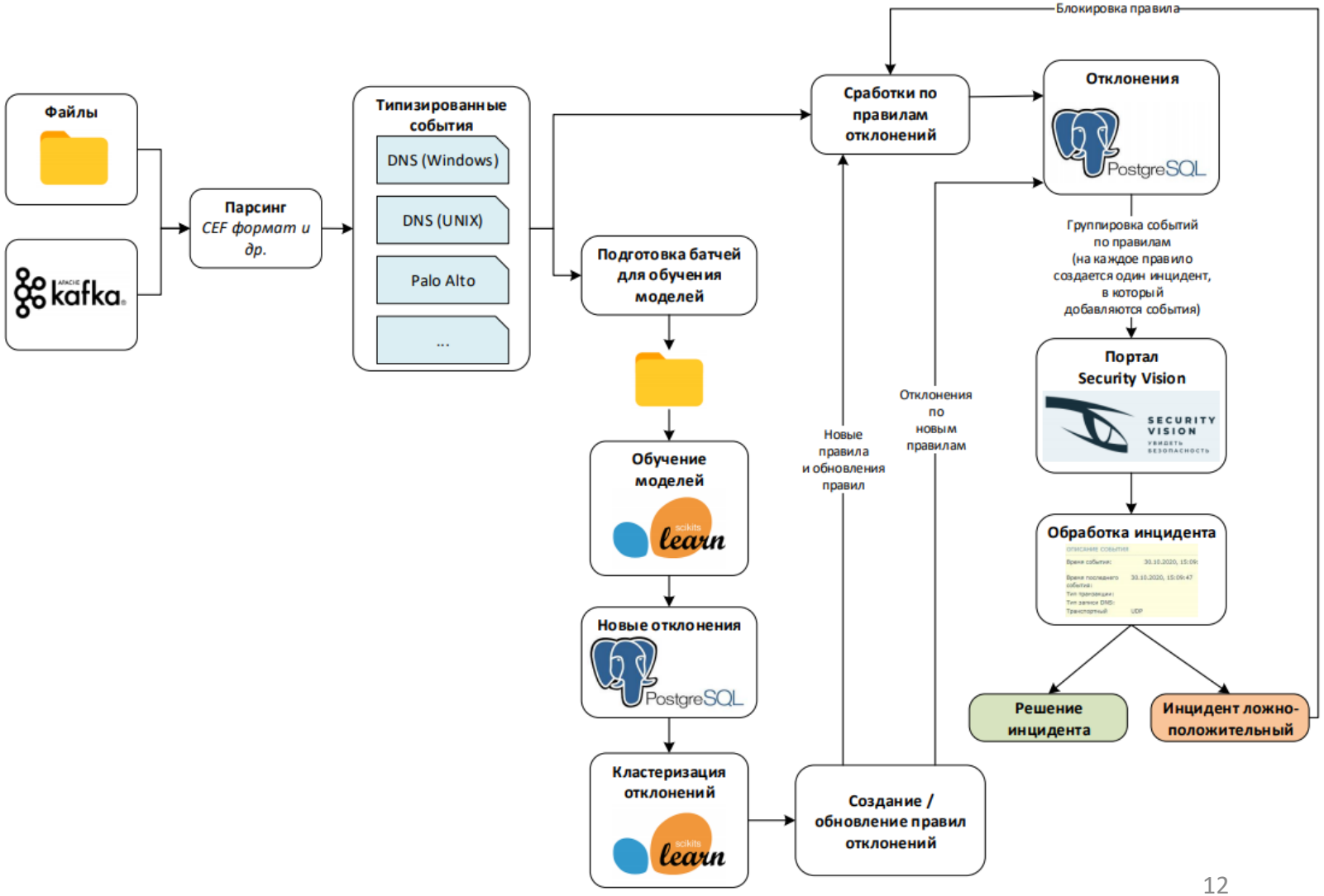
Big data & ML

- Реализован проект с использованием больших данных на базе технологии **Hadoop**. Решение используется для надежных, масштабируемых и распределенных вычислений, а также применяется как хранилище файлов общего назначения, способное вместить петабайты данных
- На платформе Security Vision есть аналитический модуль, также позволяющий работать с большими данными. Это **модуль семантического анализа инцидентов**, содержащий модель машинного обучения и выполненный с возможностью автоматического определения и выполнения команд реагирования на инциденты кибербезопасности. Таким образом, использование алгоритмов ML для выявления аномалий обеспечивает автоматическое «взведение» инцидентов с возможностью автоматического определения команд реагирования на инцидент, обеспечивая автоматизацию на всем жизненном цикле инцидента

Краткий алгоритм работы модуля платформы можно представить в следующим виде:



Выявление отклонений в событиях ИБ средствами Machine learning и обработка их на платформе Security Vision



Работа с данными

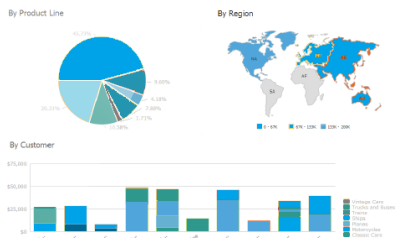
Аналитика данных

Предиктивная аналитика

Deep Machine Learning

DATA

ACTION



открытие | Банк

Спасибо за внимание