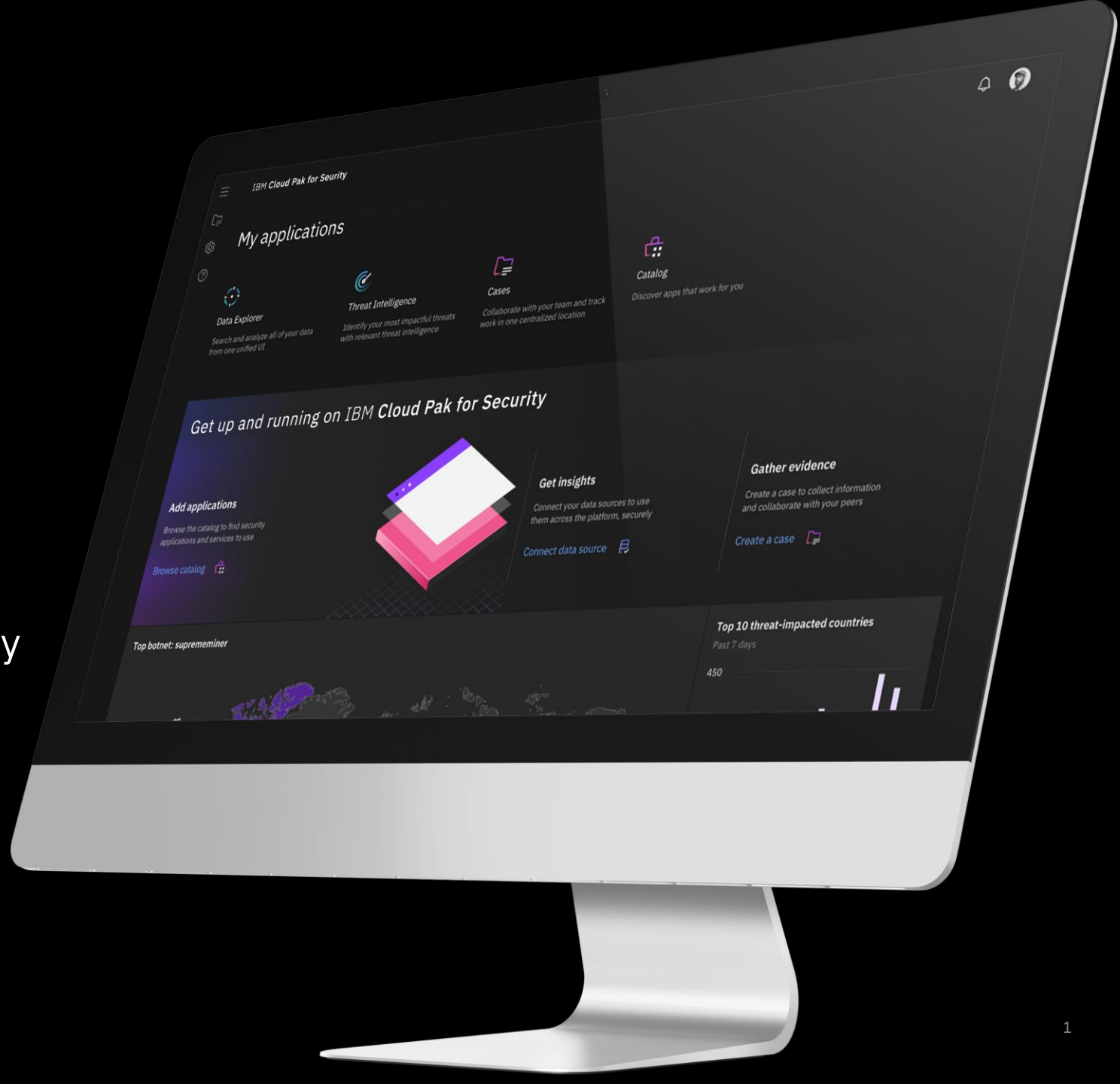
SOC
Из коробки



Дмитрий Ячевский

Руководитель направления IBM Security
в Казахстане и Средней Азии

dyachevs@kz.ibm.com

2021

OPEN SYSTEMS DEVELOPMENT | Gold Business Partner IBM

1959

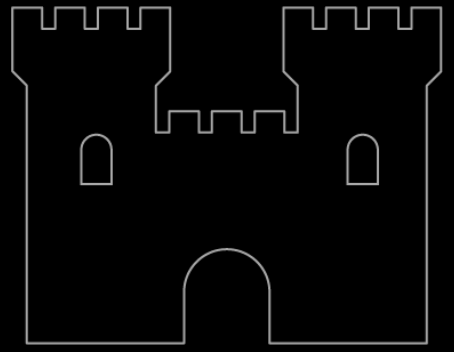
Вычислительные мощности

Сегодня

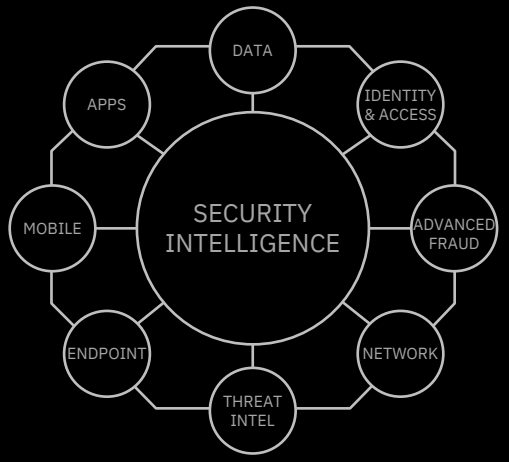
Безопасность

Будущее и настоящее.

До 2013

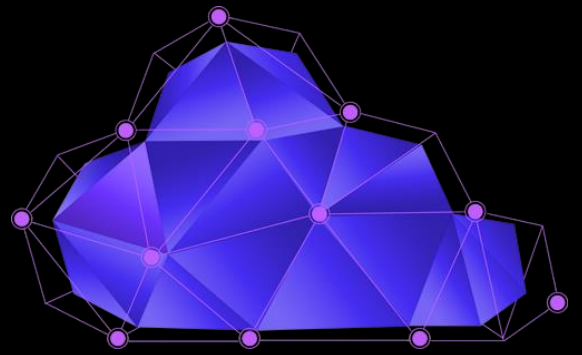


2013-2018



2019+

Connected security



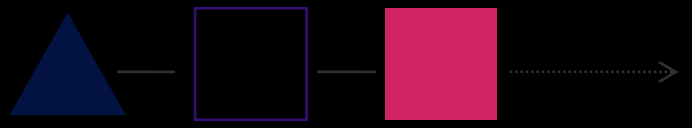
AI, ML

- 8,000+ сотрудников
- 17,500+ клиентов
- 133 страны
- 3,500+ патентов
- Самый крупный Security Стартап

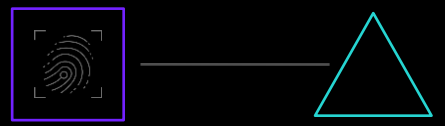
- Представительство в Казахстане
- 20+ партнеров
- Постоянные обучения

IBM Security

Безопасность очень разрознена, разделена и сложна в управлении

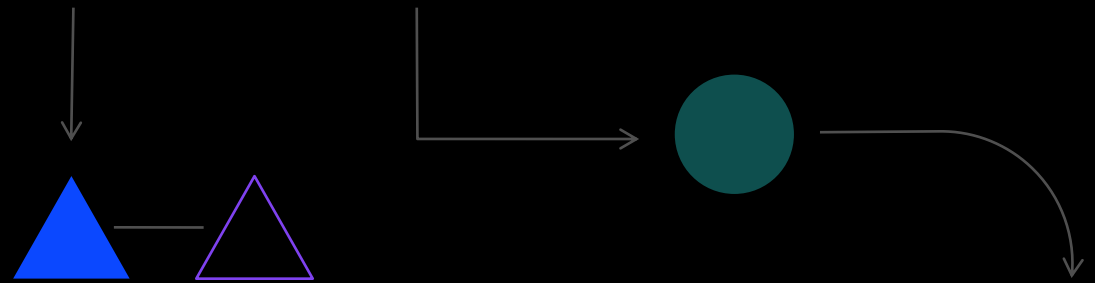


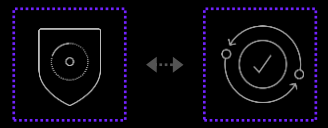
Защита данных



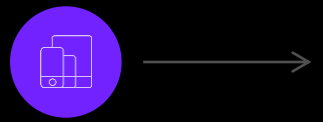
Контейнеры

Threat Hunting

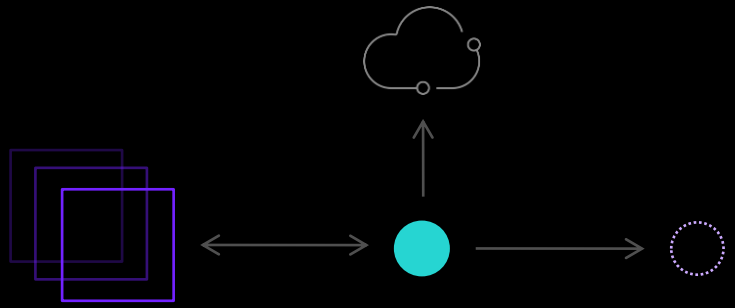




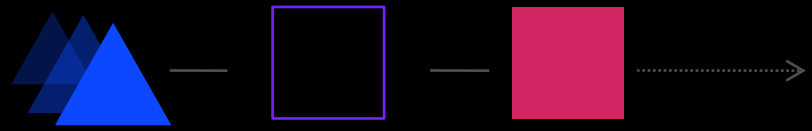
DevOps



Mobile Devices

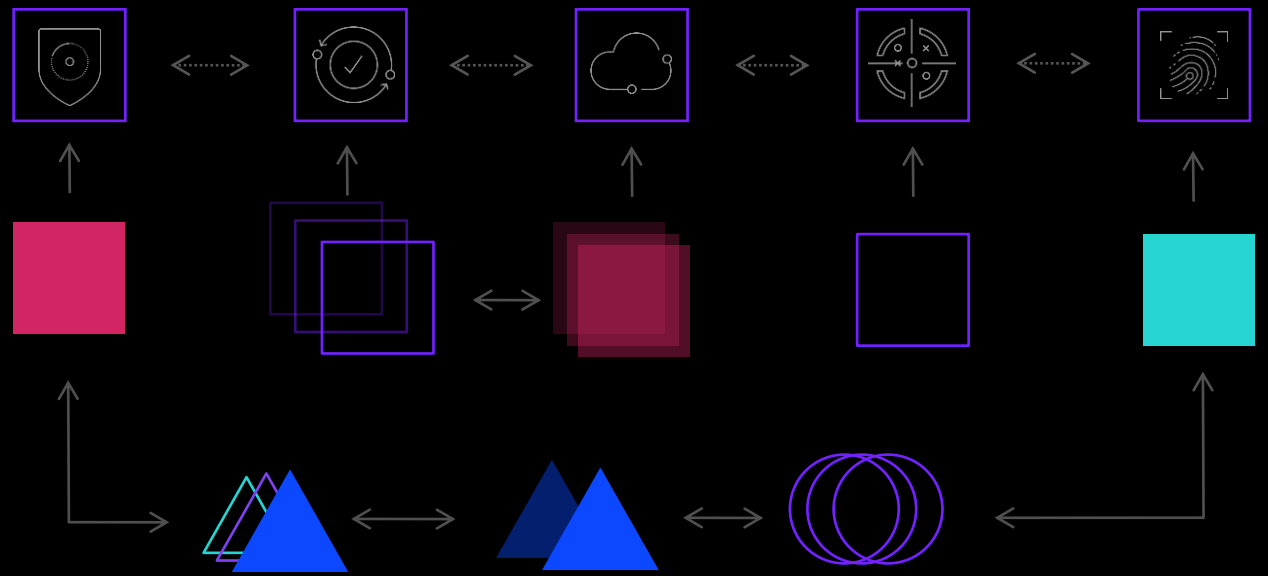


Защита облака



Анализ всех событий

А если мы начнем процесс унификации?



Запуск в любой среде

Открытая платформа

Сбор всех данных

Из любой точки

Своевременная реакция

Координация действий

Cloud Pak для безопасности!

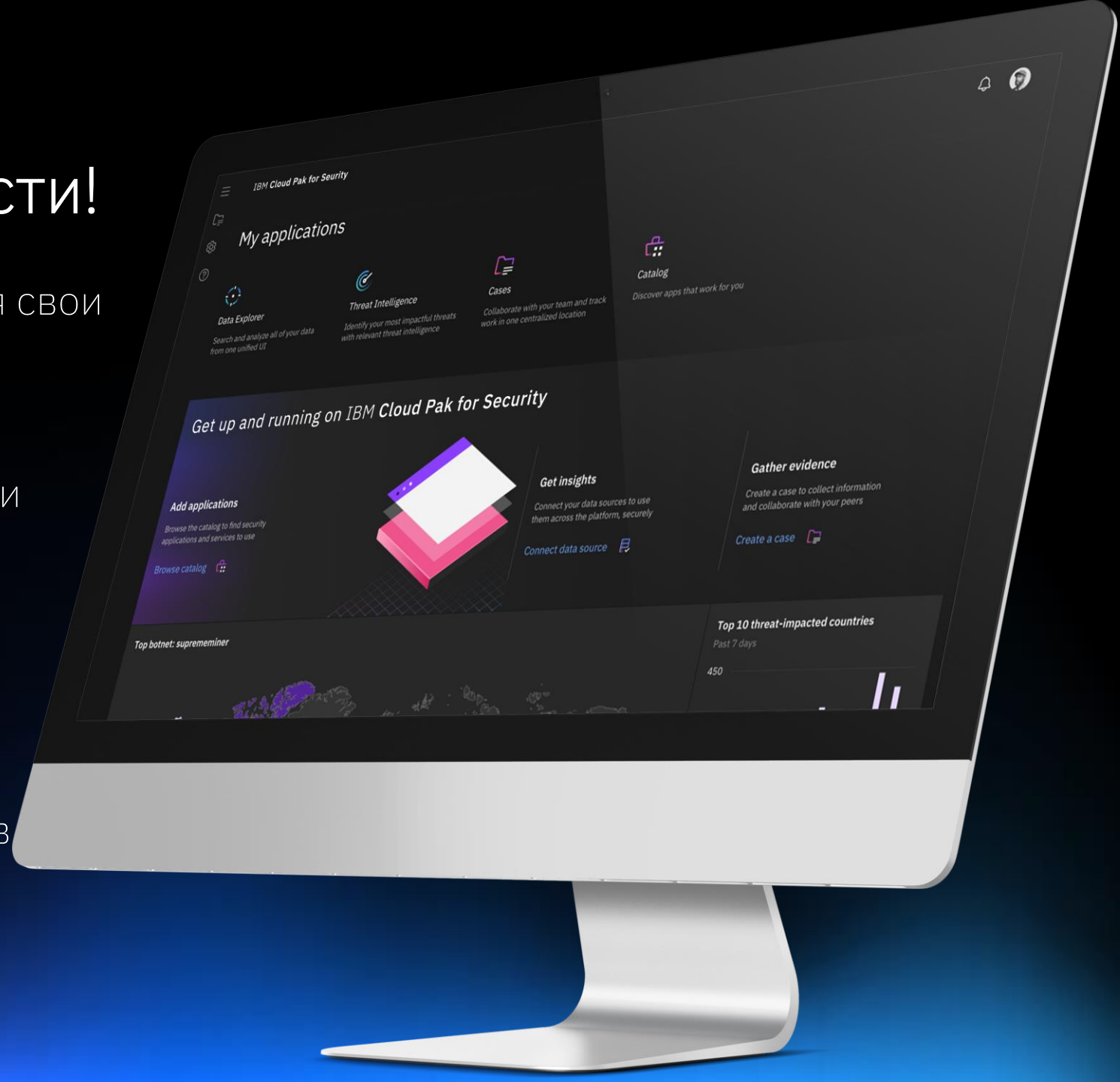
- Получайте информацию не перемещая свои данные

- Быстро реагируйте на инциденты безопасности с помощью автоматизации

- Запускайте где угодно, подключайте открыто

- SOC!

- Миграции для существующих клиентов



Open Hybrid Multicloud Platform

IBM **Cloud**

AWS

Microsoft
Azure

Google
Cloud

IBM Cloud Pak for Security

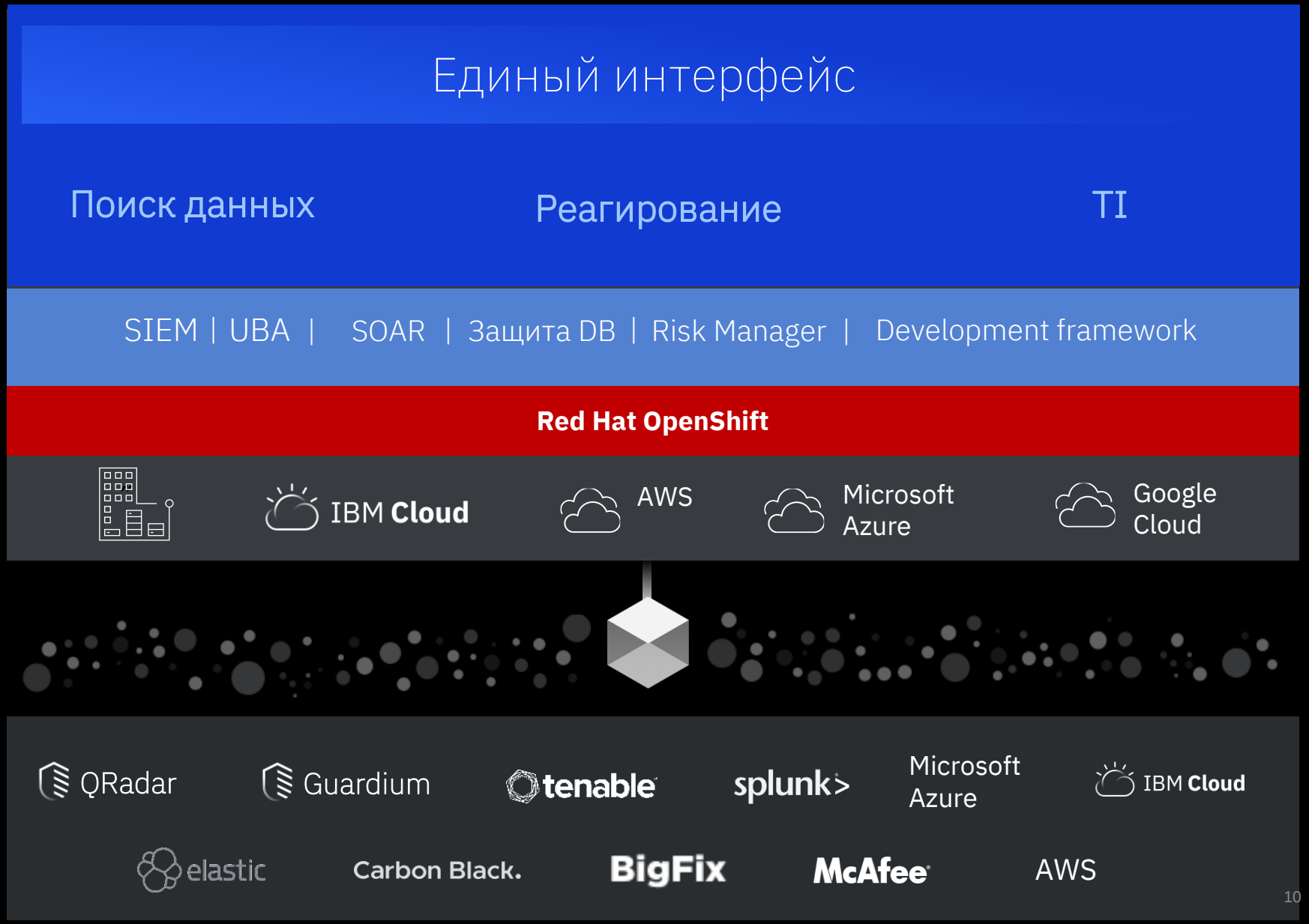
Где угодно | Любые данные | Оперативно

Интеграция с с инфраструктурой

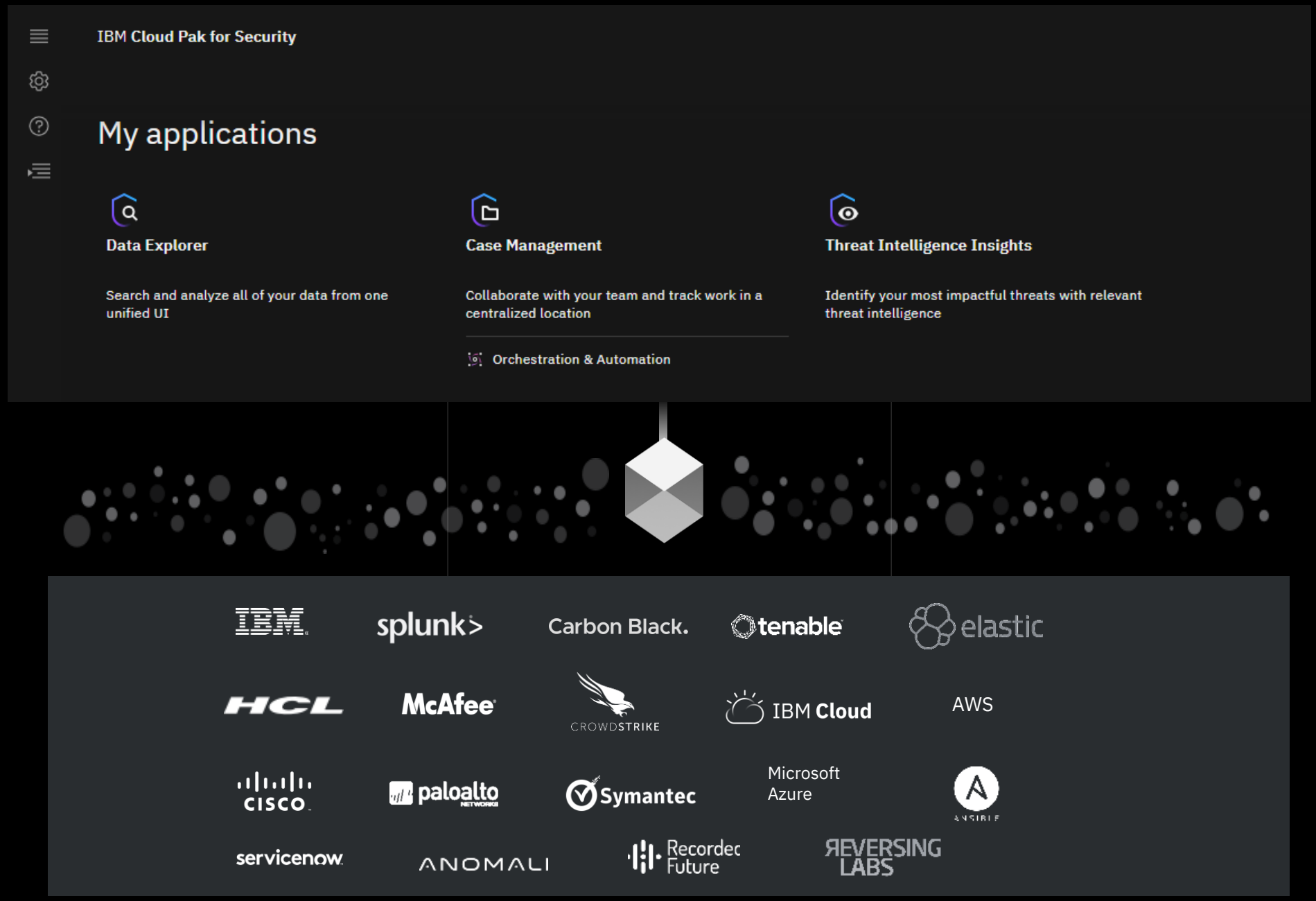
Основные сервисы

Гибридная архитектура

Существующие интеграции



Cloud Pak for Security поставляется с готовыми коннекторами ко многим из ваших существующих инструментов безопасности, поэтому вы можете оставить данные там, где они есть



IBM Cloud Pak for Security

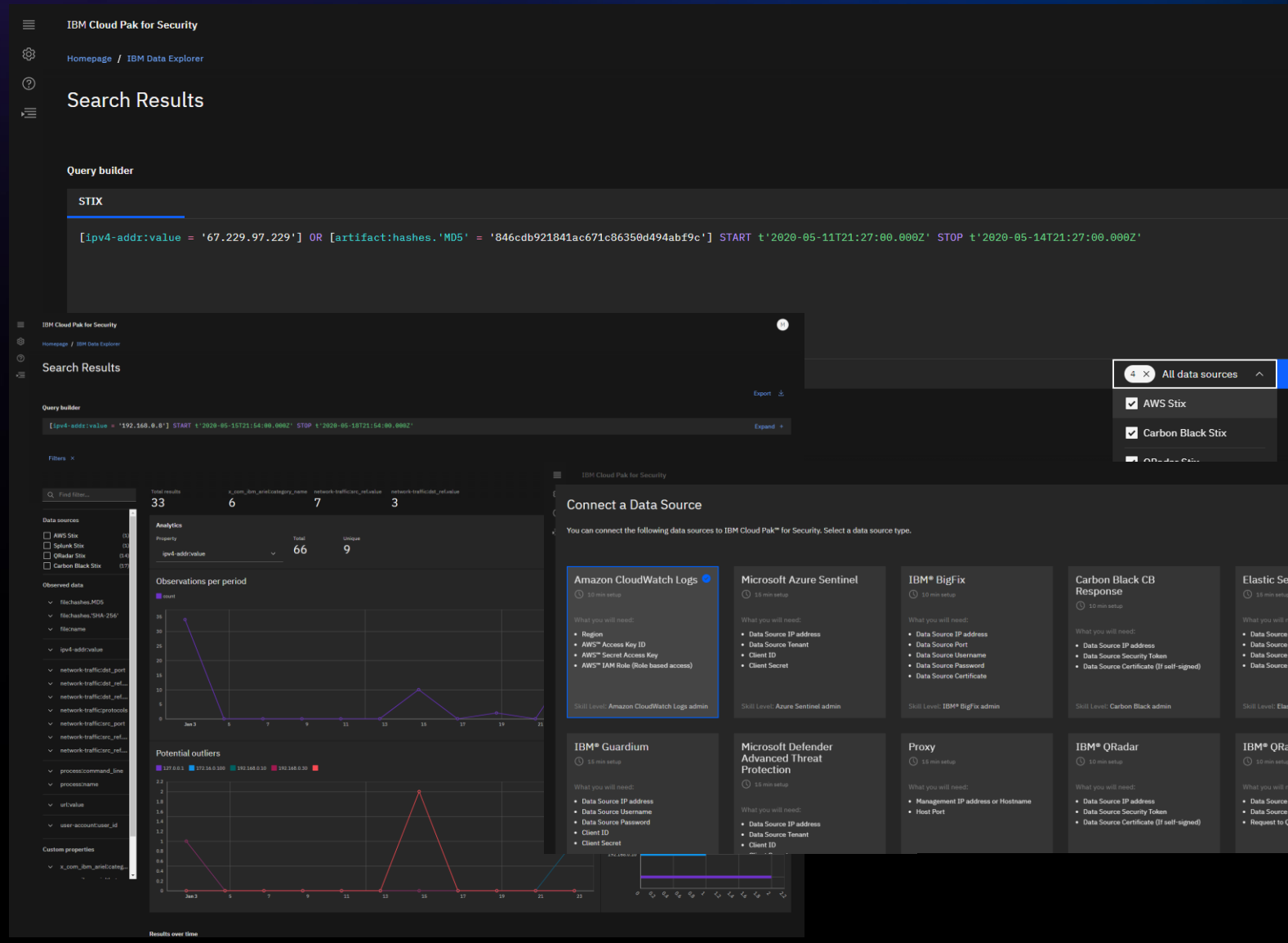
Платформа, позволяющая объединить все существующие решения и процессы для

- Развёртывание в любом облаке и локально
- Открытая платформа
- Data Explorer
- SOAR (Resilient)
- TI Feed
- Qradar Events & Flows
- Qradar Network Insights
- DataLake
- DB Protection (Guardium)
- Risk Manager

Cloud Pak for Security - Data Explorer

Федеративный поиск и расследование

- Выполняйте запросы и находите аналитические данные по нескольким источникам данных, не перемещая данные
- Проводите расследование из единого унифицированного интерфейса для поиска угроз и IOC
- Мгновенно просматривайте атрибуты в журнале и сводной таблице, чтобы обнаружить статистически значимые атрибуты



C Cloud Pak for Security нужен один язык запроса данных без их перемещения

Data source: Carbon Black Stix Last observed: Jan 15, 2020 1:29 PM

process | name | cmd.exe | pid | 1668 | file | hashes.MD5 | 00000000000000000000000000000000 | name | cmd.exe | domain-name | valu

ipv4-addr | value | 192.168.0.8 | ipv4-addr | value | 67.229.97.229 | user-account | user_id | SYSTEM

Data source: AWS Stix Last observed: Jan 20, 2020 10:42 AM

network-traffic | src_port | 0 | dst_port | 0 | protocols[0] | reserved | ipv4-addr | value | 192.168.0.8 | mac-addr | value | 00:00:00:00:00:0

mac-addr | value | 00:00:00:00:00:00 | user-account | user_id | DanielJones | file | name | CustomerDataOctober | domain | path | s3.amazonav

artifact

payload_bin | localhost:accountId:911534260404,accessKeyId:ASIA5IO5NAC2O...

x_com_ibm_ariel | qid_name | Object Downloaded | category_name | AWS CloudTrail Message | log_source_name | AWS CloudTrail

Data source: QRadar Stix Last observed: Jan 3, 2020 10:42 AM

network-traffic | src_port | 0 | dst_port | 0 | protocols[0] | reserved | ipv4-addr | value | 67.229.97.229 | mac-addr | value | 00:00:00:00:00:0

mac-addr | value | 00:00:00:00:00:00 | user-account | user_id | DanielJones | domain | path | s3.amazonaws.com

artifact

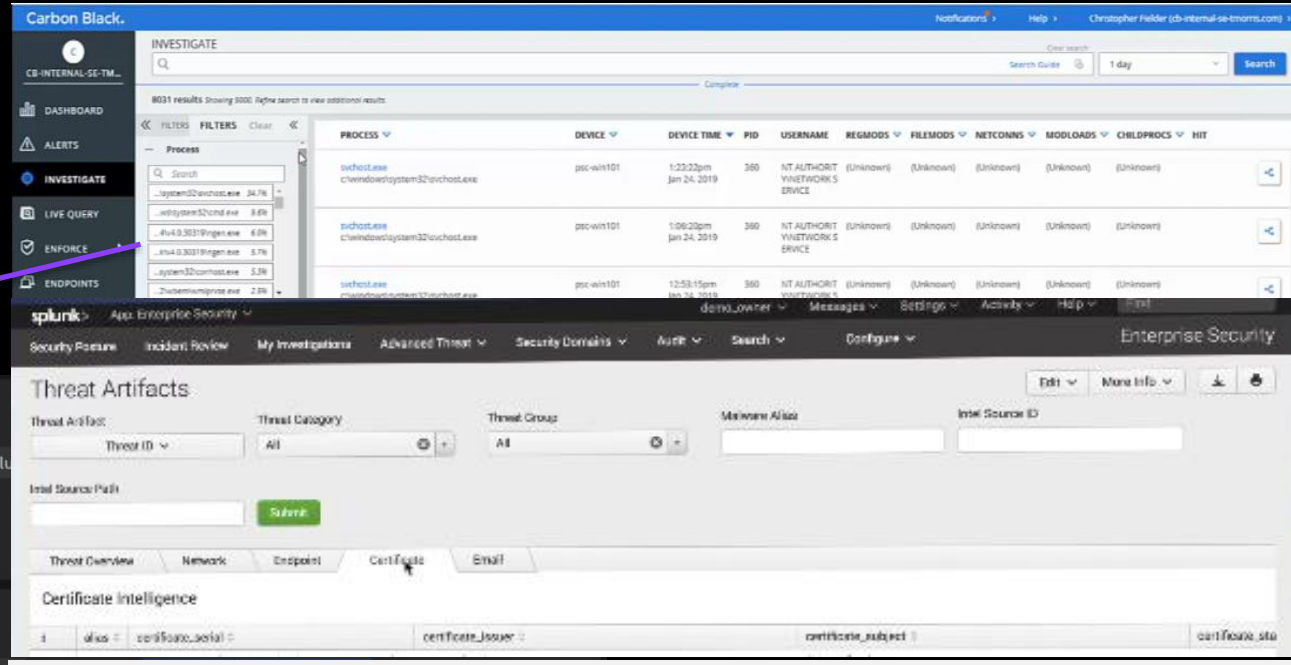
payload_bin | localhost:accountId:911534260404,accessKeyId:ASIA5IO5NAC2O...

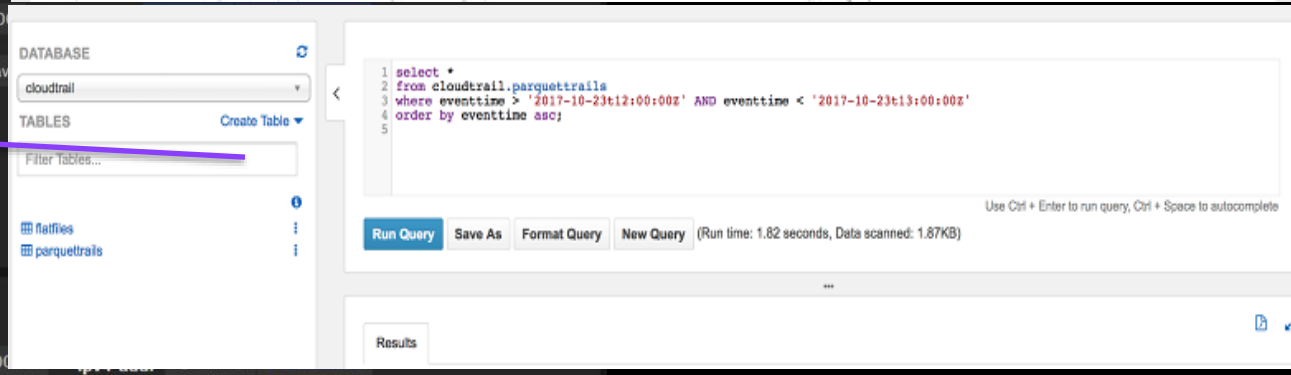
x_com_ibm_ariel | devicetype | 18 | qid_name | Object Downloaded | qid | 67500346 | category_name | AWS CloudTrail Message | category_id | 70

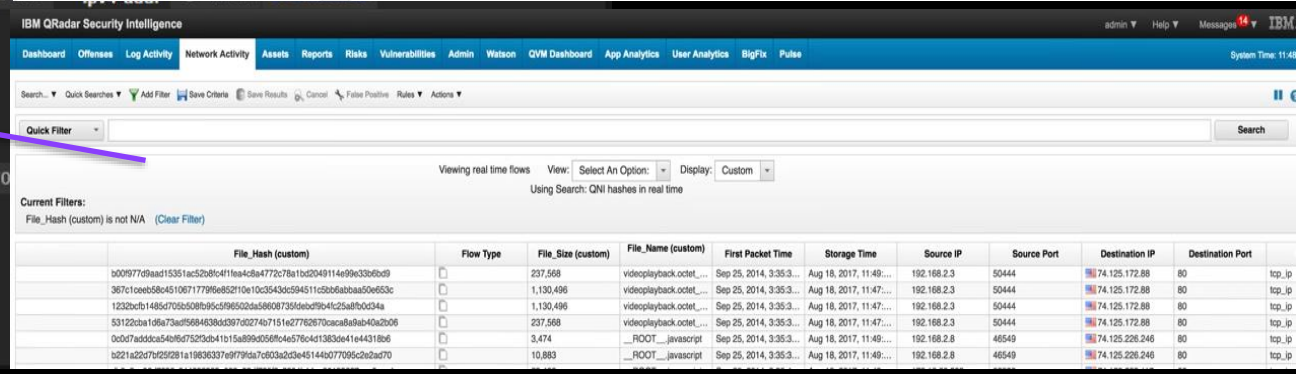
identity_ip | 0.0.0.0

utf8_payload | localhost:accountId:911534260404,accessKeyId:ASIA5IO5NAC2...

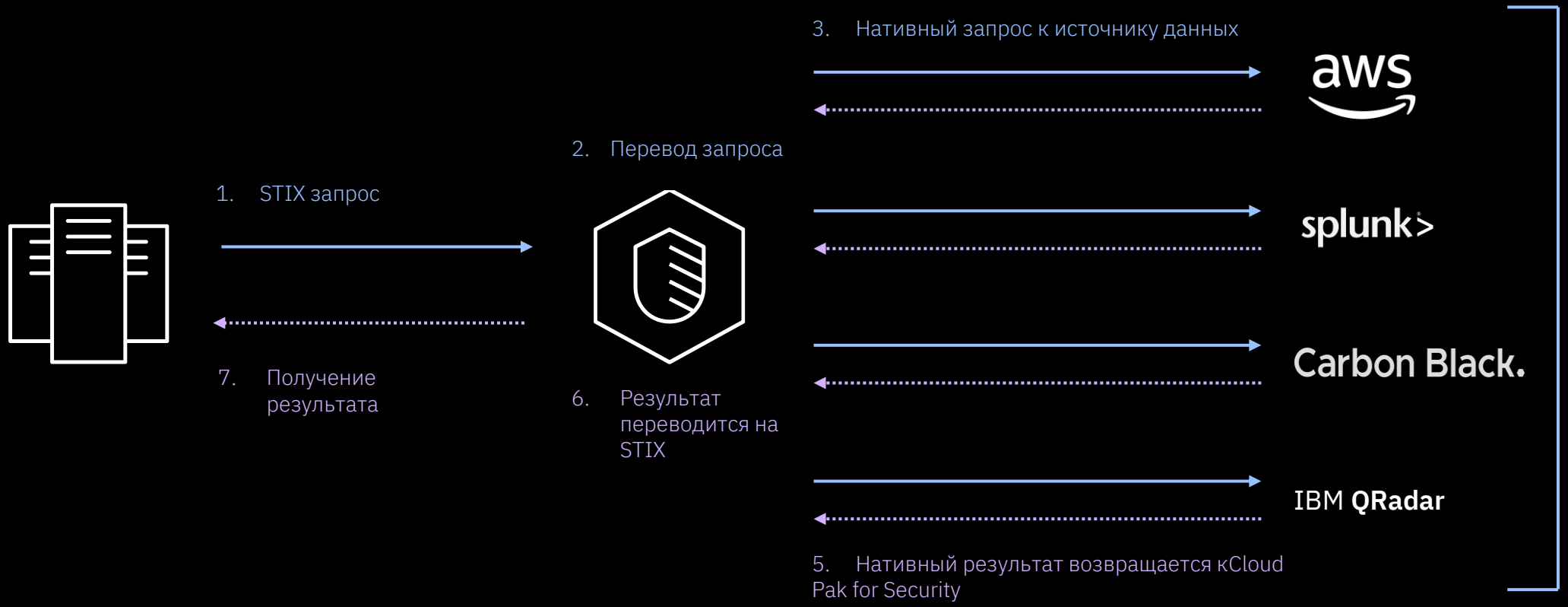
magnitude | 5







STIX Shifter – как это работает:



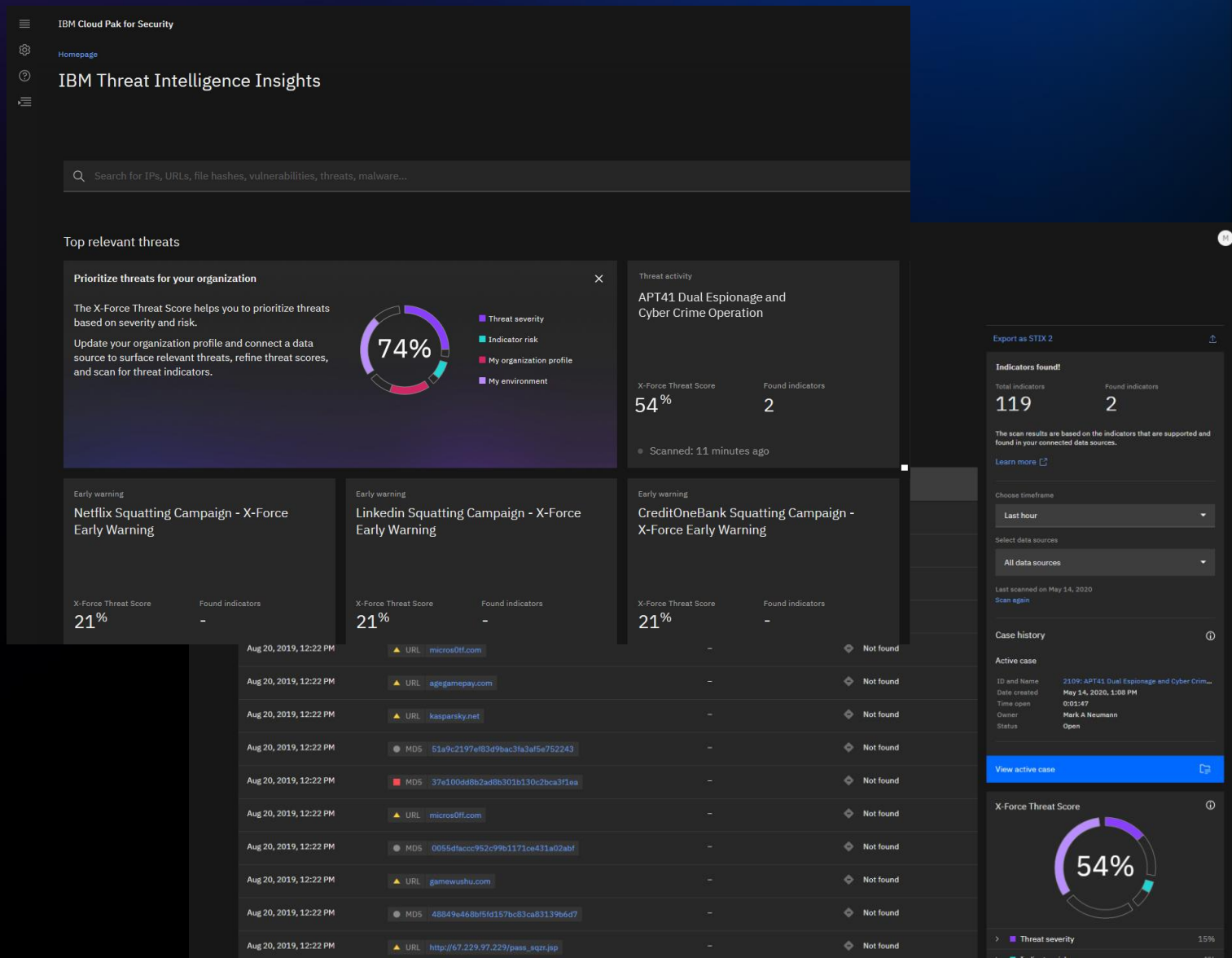
1. Федеративный запрос с использованием шаблона STIX
2. Запрос переводится на собственный язык запросов каждого из источников данных
3. Затем преобразованный запрос отправляется (передается) во все источники данных
4. Каждый источник данных выполняет собственный собственный запрос
5. Затем из источника данных возвращаются собственные результаты запроса
6. Возвращенные результаты переведены в объекты STIX (в основном структура JSON)
7. Затем объекты STIX хранятся в облаке, где они используются другими службами

Cloud Pak for Security - Threat Intelligence Insights

Приоритетная, действенная аналитика угроз

- Приоритетная аналитика угроз с помощью адаптивной оценки X-Force Threat Score, рассчитываемой на основе релевантности, серьезности, степени проникновения, воздействия и фактических наблюдений за окружающей средой

- Выявление угроз, действующих в вашей среде, с помощью Am I Affected, которая выполняет непрерывный и автоматический поиск в подключенных источниках данных



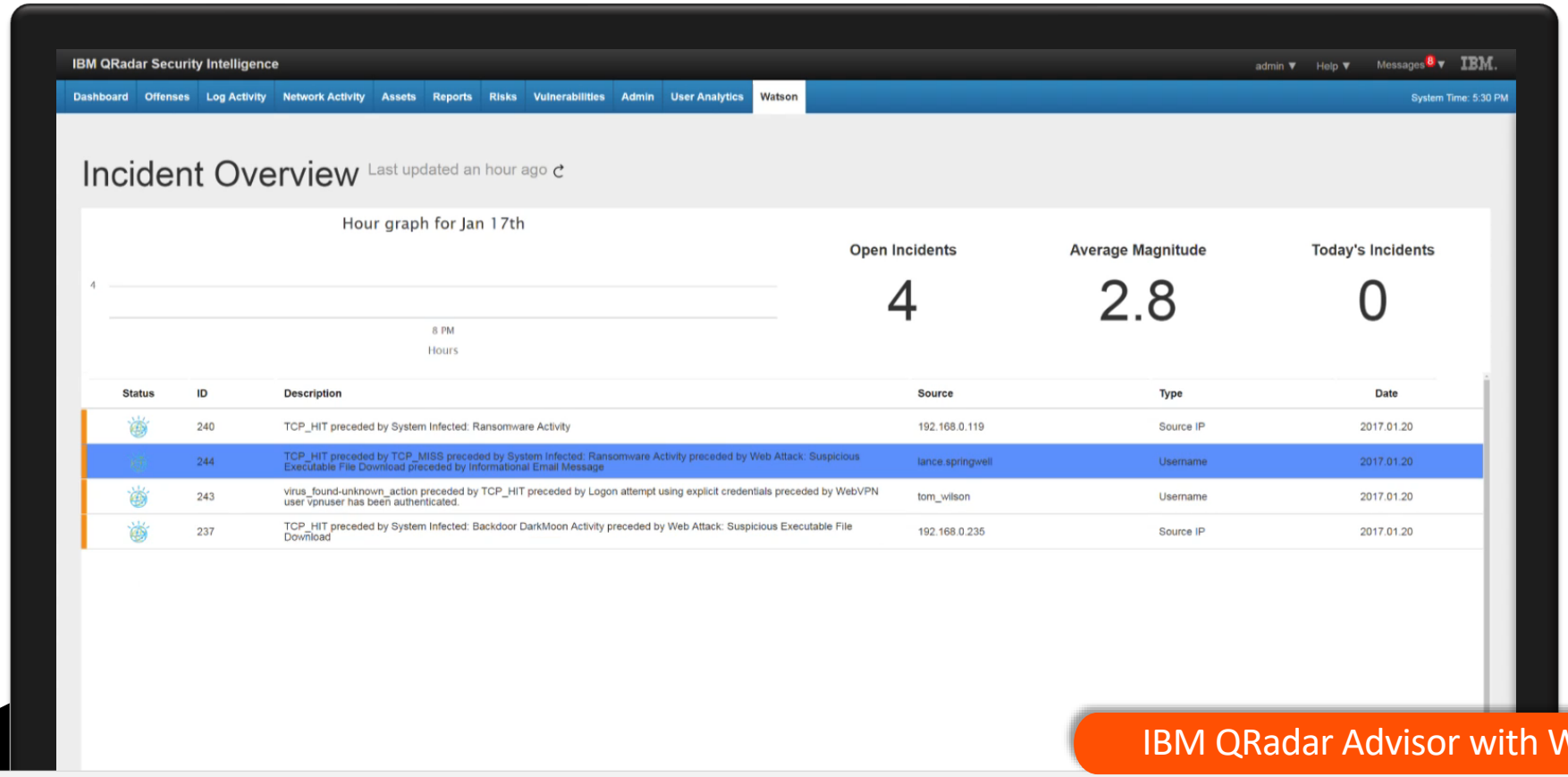
QRadar @ Cloud Pak 4 Security

- Qradar Events
- Qradar Flows
- Data Lake
- UBA
- QNI software
- Risk manager

Интегрированная, унифицированная архитектура в одной web-консоли

- **Log Management**
- **Security Intelligence and Sense Analytics**
- **Network Activity Monitoring**
- **Risk Management**
- **Network Forensics**
- **Incident Response**

Революционное изменение в работе аналитиков ИБ



IBM QRadar Advisor with Watson

Автоматически раскрывает новый контекст ИБ и полную картину инцидента

- **2.3 Млн+** документов ИБ
- **10 Млрд+** элементов данных ИБ
- **80 тыс+** новых документов читается каждый день
- **250 тыс+** расследований проведено за последние 6 месяцев

QRadar Advisor with Watson в действии

QRadar SIEM
Аналитика и
Корреляция данн

1. Инциденты

6. Применение собранных знаний для расследования и квалификации инцидента

5. Результаты анализа

4. Исследование угроз
экспертный анализ

Watson for Cyber Security
ПОНИМАНИЕ | ПРИЧИНЫ | ОБУЧЕНИЕ

Активность устройств

Граф знаний

Связи эквивалентов

Контекст инцидента

2. Сбор локального контекста и формирование стратегии расследования угроз

3. Индикаторы

QRadar Advisor with Watson
СБОР ДАННЫХ | КЛЮЧЕВЫЕ ВВОДНЫЕ

CNEWS FORUM 10 НОЯБРЯ скоро
CNEWS AWARDS 10 НОЯБРЯ скоро
ЧТО ХОЧЕТ БИЗНЕС?
ЭЛЕКТРОННОЕ ПРАВОСУДИЕ new
ЭКСПЕРТИЗА REDSYS new
ИННОВАЦИИ В СХД new
DELL ДЛЯ БИЗНЕСА new
СЕТИ BROCADE new
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ
ОБЛАЧНЫЕ ТЕХНОЛОГИИ
ИТ В ГОССЕКТОРЕ
ИТ В БАНКАХ
БЕЗОПАСНОСТЬ
ТЕЛЕКОМ
ИНФОРМАТИЗАЦИЯ
ИНТЕРНЕТ

Сбербанк обезопасит себя с помощью искусственного интеллекта

Безопасность Бизнес **ИТ в банках** ИТ в госсекторе мобильная версия

10.06.2016, ПТ, 19:10, Мск , Текст: Павел Лебедев

В Сбербанке по окончании второго этапа строительства центра безопасности ИТ-системы станут рассматривать миллионы подозрительных финансовых «событий» в день, для анализа которых будут внедрены средства искусственного интеллекта.

Центр безопасности 2.0

Сбербанк приступил ко второму этапу строительства центра информационной безопасности (Security Operational Center, SoC), который будет завершен до конца 2016 г. В ходе данных работ планируется внедрить решения с использованием искусственного интеллекта, а также инструменты для работы с большими данными (bigdata), рассказал зампредседателя правления Сбербанка **Станислав Кузнецов**.

В результате количество рассмотренных в день подозрительных «событий» в работе систем организации увеличится до нескольких миллионов (сейчас этот показатель составляет 1 млн в сутки, а до создания SoC банку удавалось изучить лишь 100-200 инцидентов в день).

Первый этап по созданию SoC, который включал в себя внедрение SIEM-системы, ориентированной на сбор и корреляцию событий безопасности, был завершен в апреле 2016 г. Консультантом по реализации проекта выступила компания IBM, заключившая в декабре 2015 г. контракт со «Сбербанком» на ₽ 56,9 млн. Правда, по словам Кузнецова, в целом в проекте задействован ряд других компаний, названия которых он не сообщил.

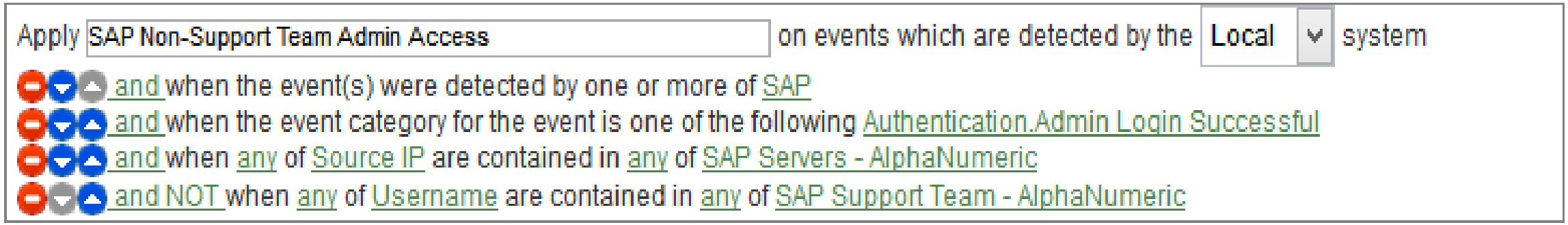
В общей сложности работу центра безопасности обеспечивают более сотни сотрудников. Точное количество специалистов и местоположение SoC в Сбербанке не уточняют. Совокупный ИБ-бюджет банка в 2015 г. (включая строительство SoC) составил ₽ 1,5 млрд.

Станислав Кузнецов,

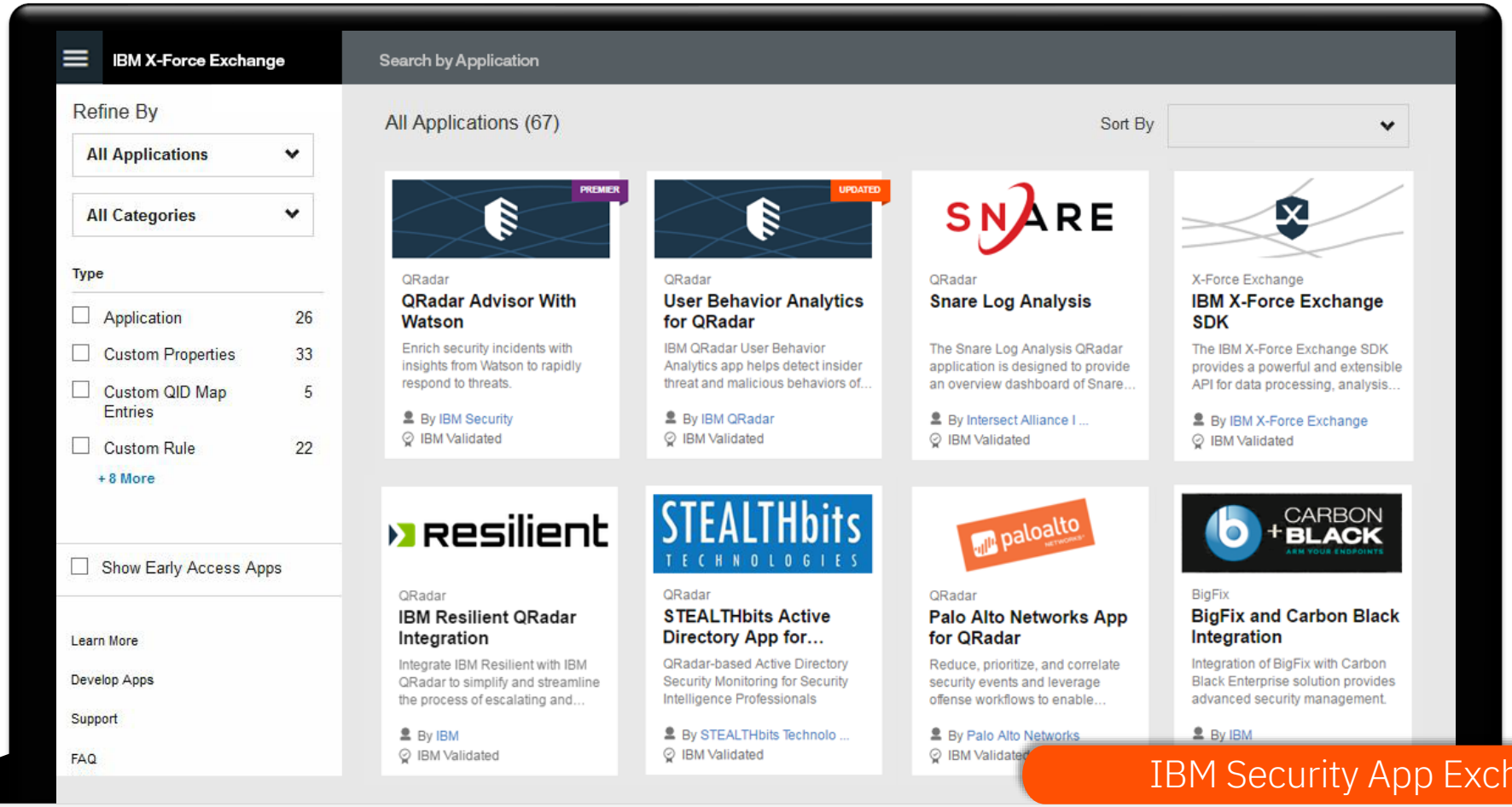
Заместитель председателя правления ПАО Сбербанк.

Executive спонсор проекта создания SOC в Сбербанке

Написание правил



Экосистема защиты через сотрудничество



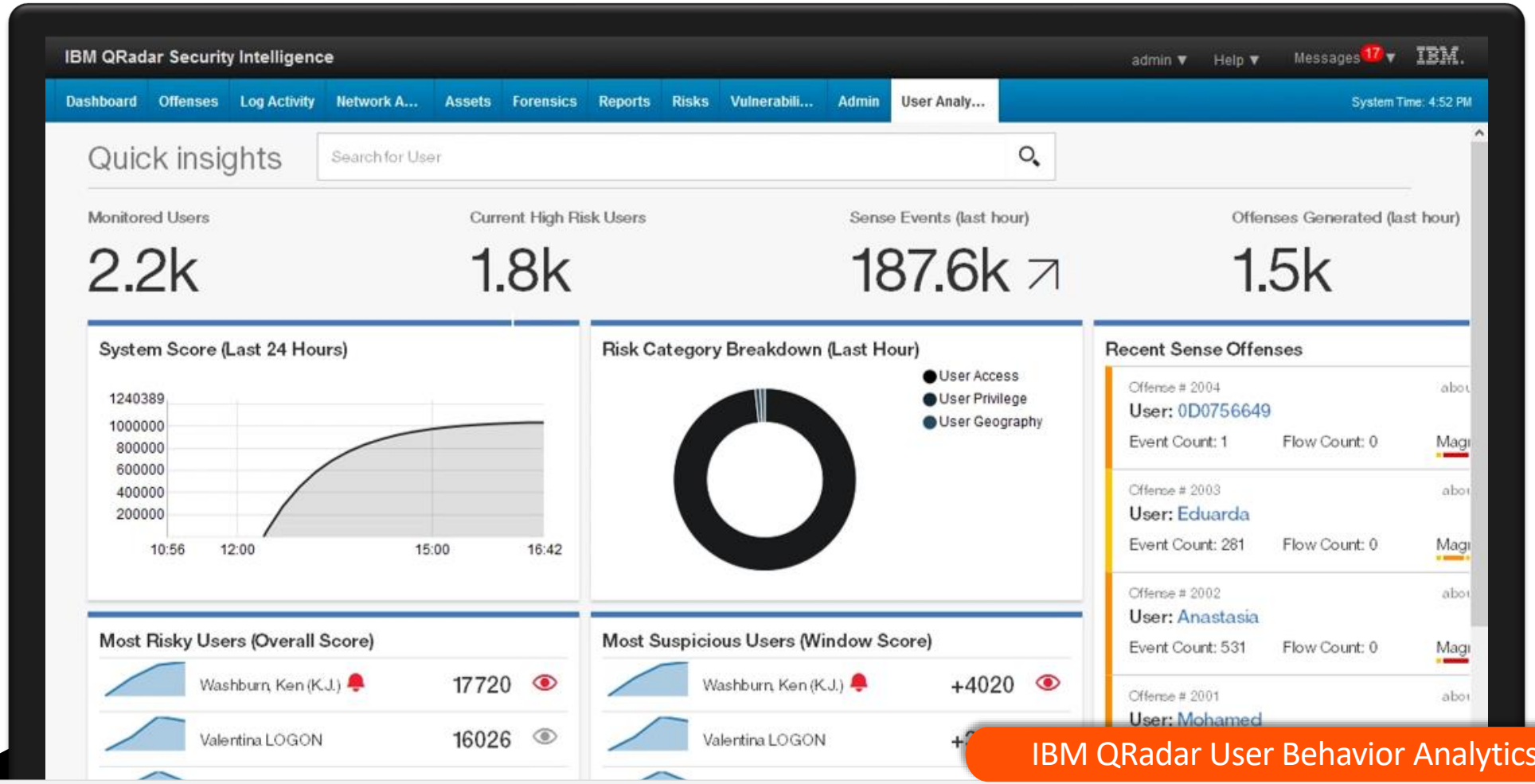
IBM Security App Exchange

Создавайте и используйте приложения на основе технологий IBM security

- 100+ приложений созданных IBM и партнерами
- 49K+ посещений 28K+ скачиваний приложений

с момента начала работы в Декабре 2015

Обнаружить аномальное поведение одним кликом

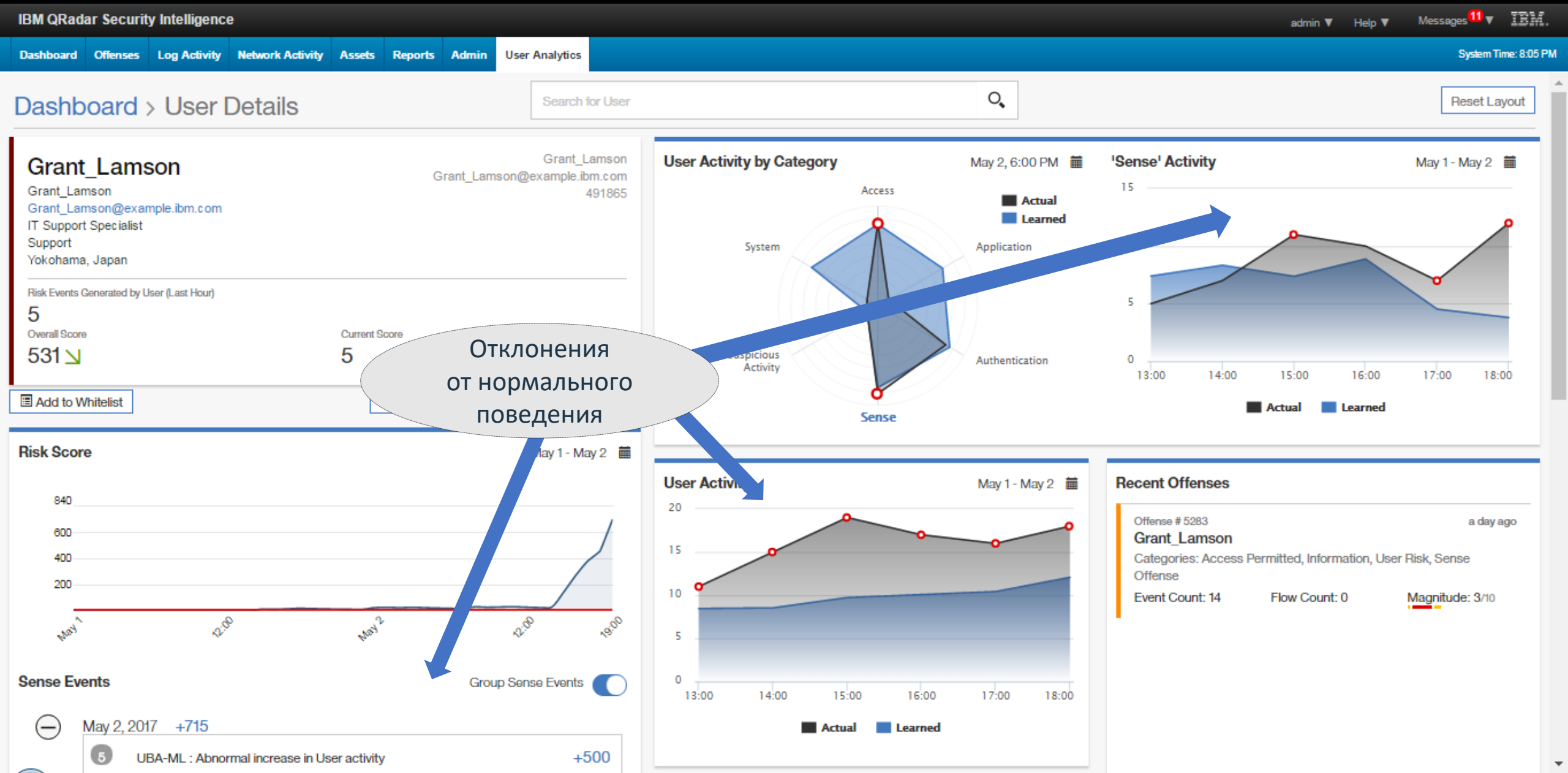


IBM QRadar User Behavior Analytics

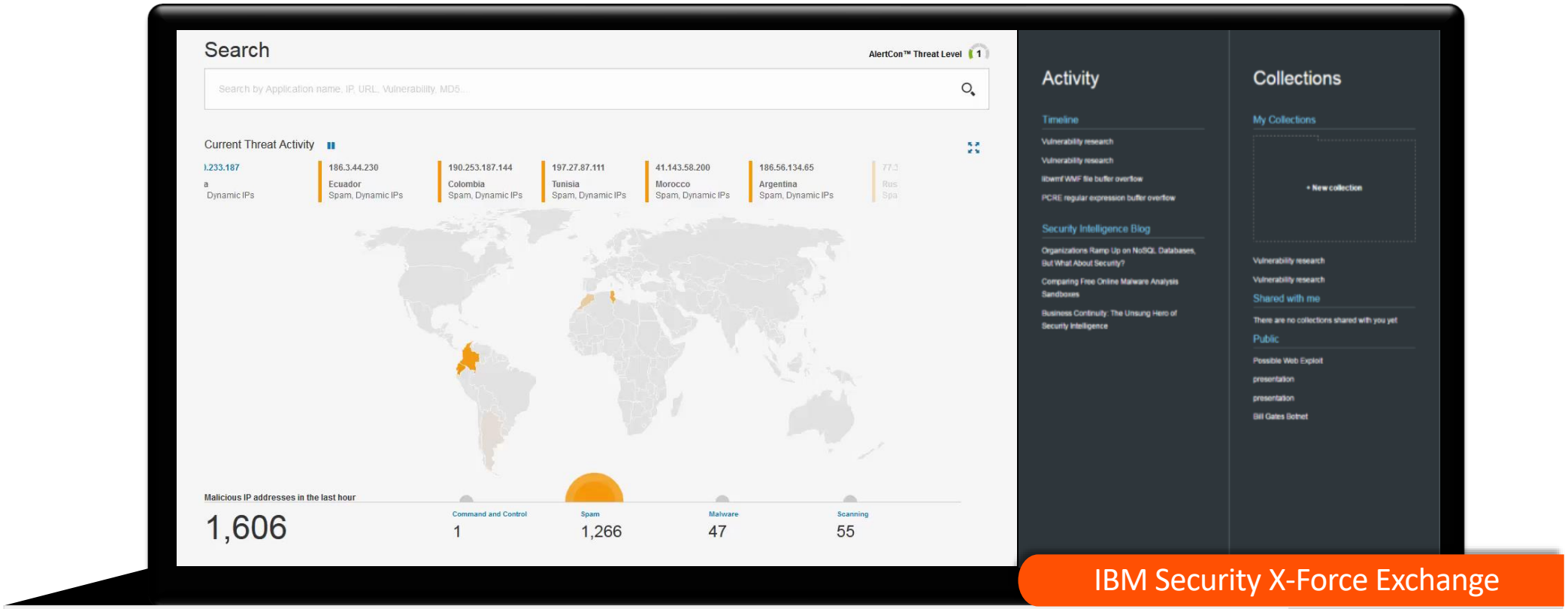
Приложение для визуализации действий каждого пользователя и выявления его аномального поведения

Консоль User Behavior Analytics является интегрированной частью консоли QRadar

UBA: Алгоритмы машинного обучения



Совместное использование базы 800ТВ+ данных об угрозах



IBM Security X-Force Exchange

Доступ к интегрированной базе угроз в режиме реального времени

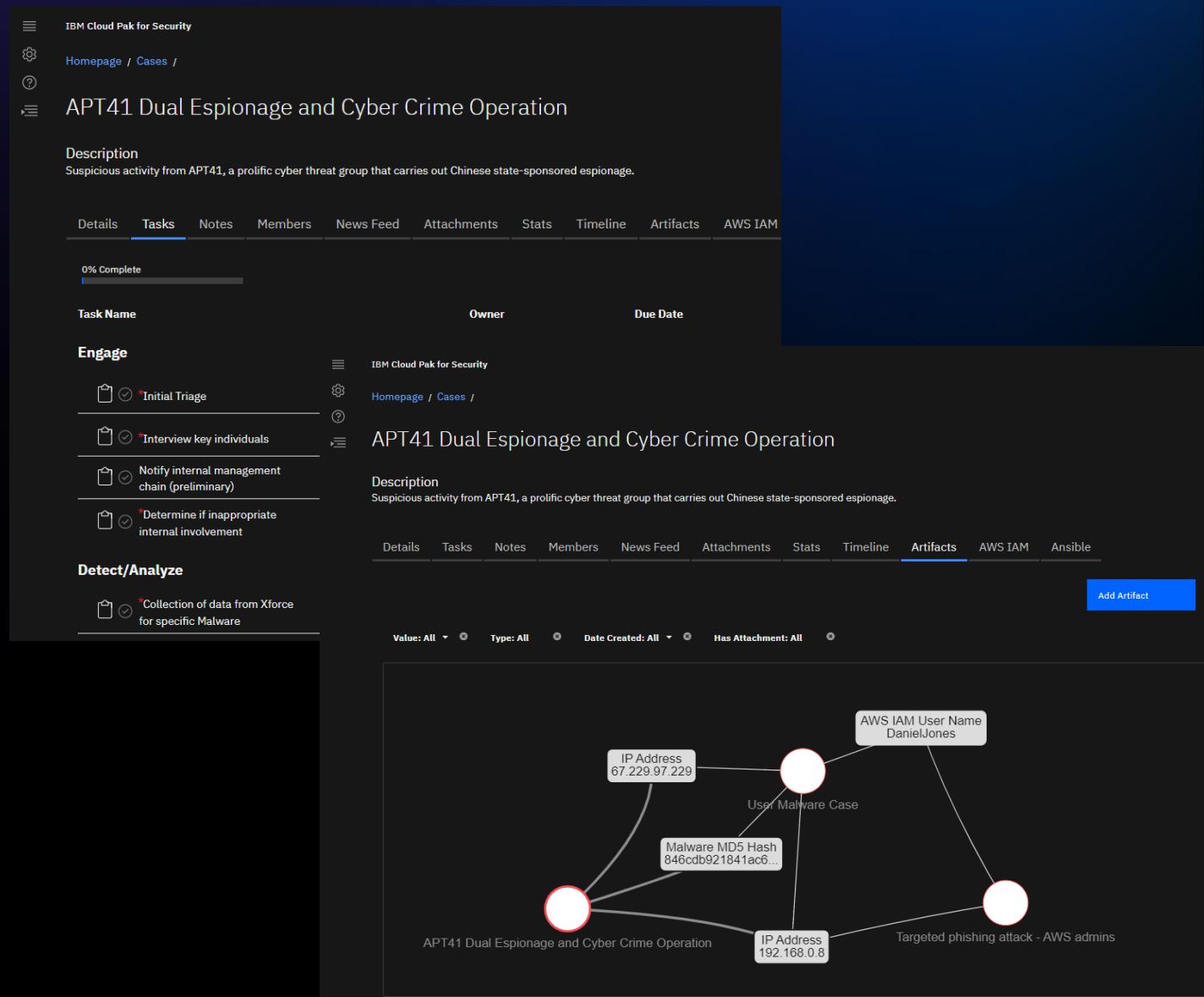
- 15Млрд+ мониторинг событий ИБ в день
- Данные о вредоносных угрозах с 270Млн+ конечных точек
- 1Млн+ вредоносных IP-адресов
- 1000+ сэмплов финансовых вредоносов в день

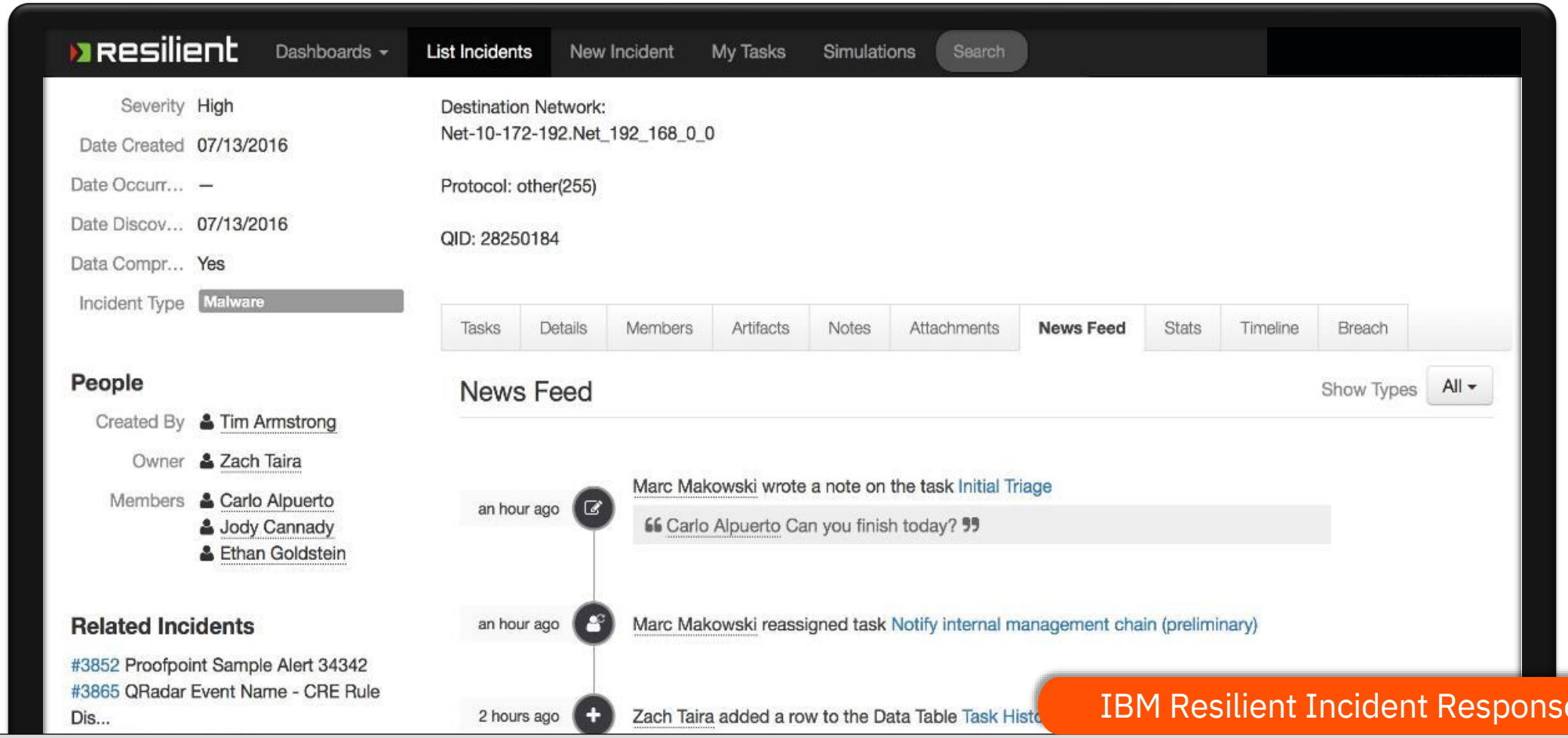
Данные от более 2000 организаций среди 16 индустрий

Cloud Pak for Security - Case Management

Оркестровка, автоматизация и ответ

- Сокращение времени на реагирование и устранение сложных киберугроз за счет автоматизации процессов реагирования на инциденты с надежным управлением делами и задачами
- Оптимизируйте и автоматизируйте ручные и повторяющиеся задачи, такие как обогащение IOC
- Расставьте приоритеты в рабочей нагрузке аналитика по важным расследованиям и действиям по реагированию, направляя ответы аналитиков





IBM Resilient Incident Response

Организовать реагирование на инциденты из единой консоли объединяя людей, процессы и технологии

- Организовать и автоматизировать реагирование на инциденты
- Сбор индикаторов компрометации с использованием глубокого расследования
- Внедрение процедур реагирования и экспертизы

QRadar + IBM SOAR = SIEM + Incident Response

QRadar
Приоритезация информации из Logs, Flows, Vulns, User, Config Data и т.п.

Процесс реагирования SOC на инцидент ИБ для ответа на угрозы, дыры, уязвимости

Создание инцидента
- Присвоение типа (напр. уязвимость)
- Присвоение бизнес характеристики в зависимости от типа (напр. Риск)

Сбор контекста и назначение задач
- Сбор дополнительных доказательств
- Применение требований регуляторов
- Назначение задач ответственным

Восстановление и Закрытие
- Постановка задач восстановления команде
- Подтверждение восстановления
- Закрытие инцидента
- Отчет/Уведомление

База всех инцидентов ИБ

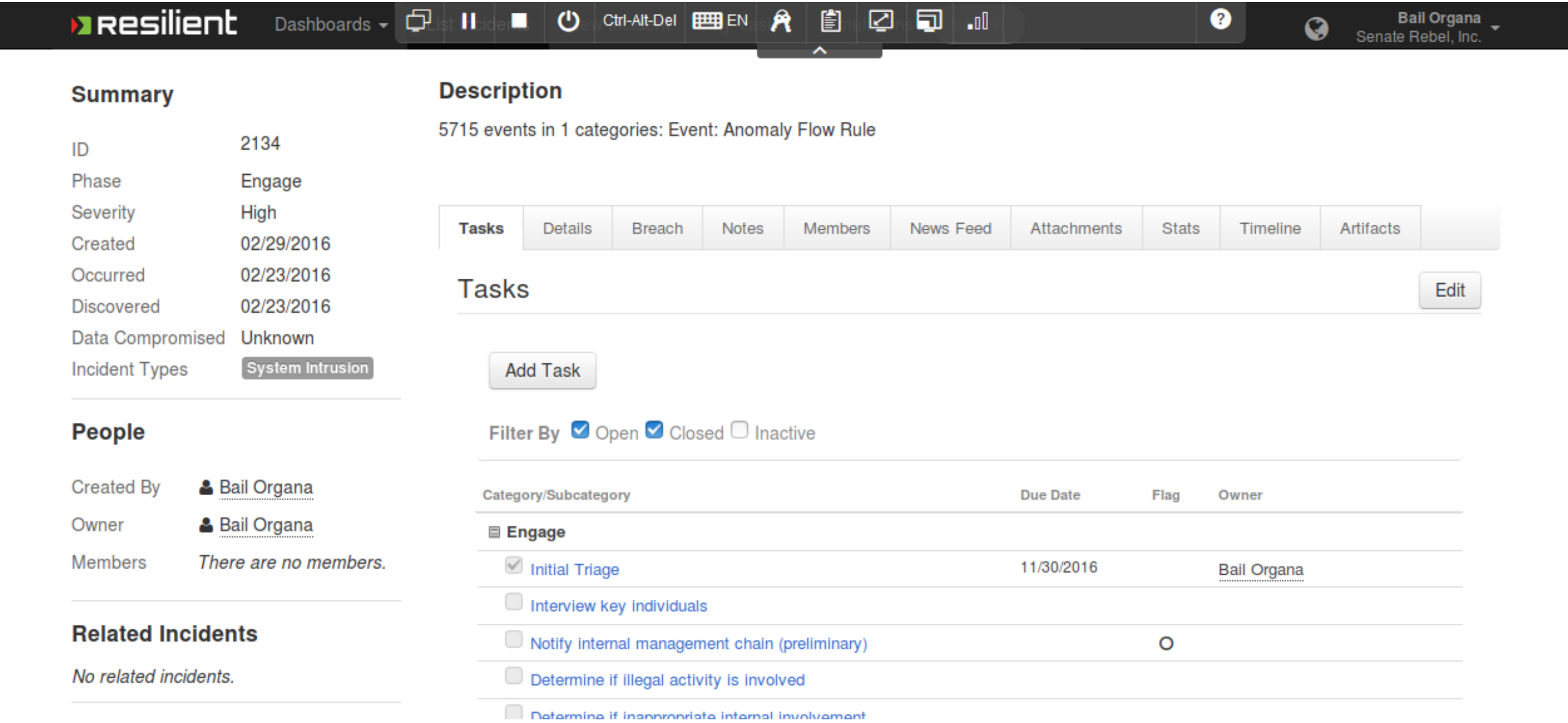
Отчет по инциденту и уведомление

Постоянная аналитика ИБ

Три этапа инцидента ИБ

Улучшение процесса выявления инцидентов

Модуль управления инцидентами



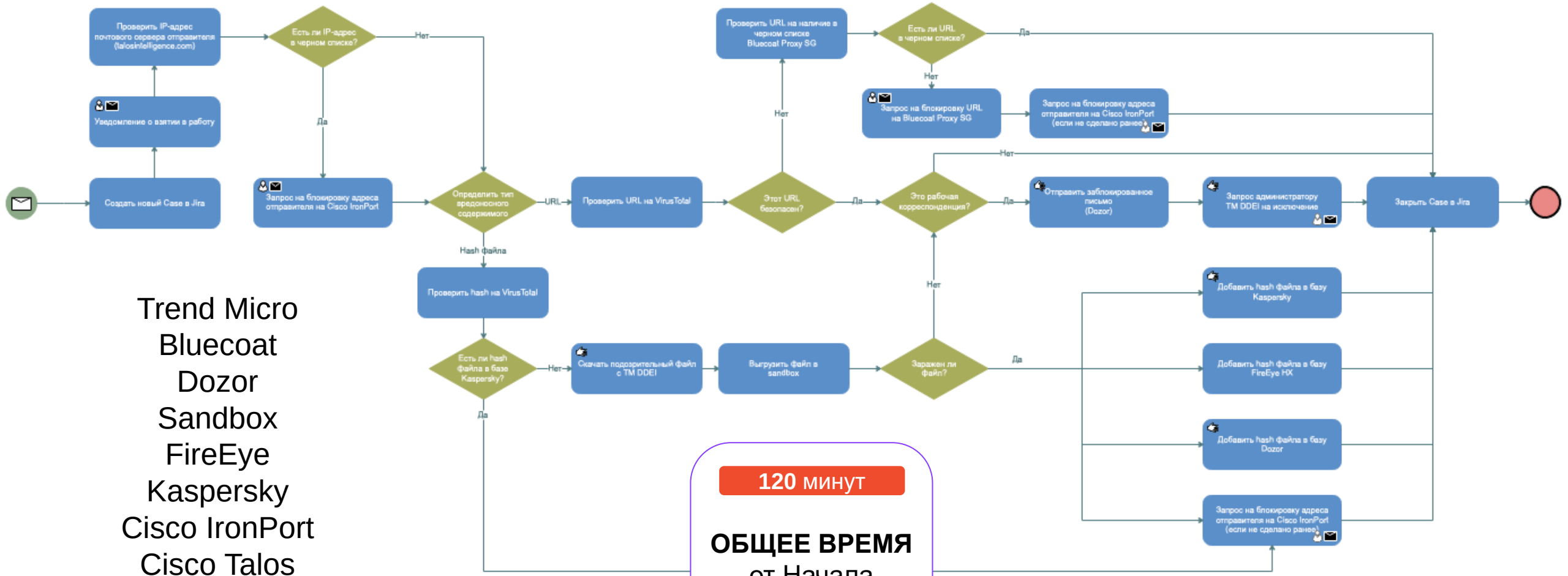
Многообразие процессов SOC – как упростить?

Существует около 30 процессов SOC, часть из которых может быть автоматизирована;

Примеры процессов, требующих автоматизации:

- Процесс пост-анализа инцидентов ИБ;
- Процесс управления изменениями;
- Процесс реагирования на инцидент ИБ;

Сценарий инцидента: phishing - РЕАЛЬНОСТЬ



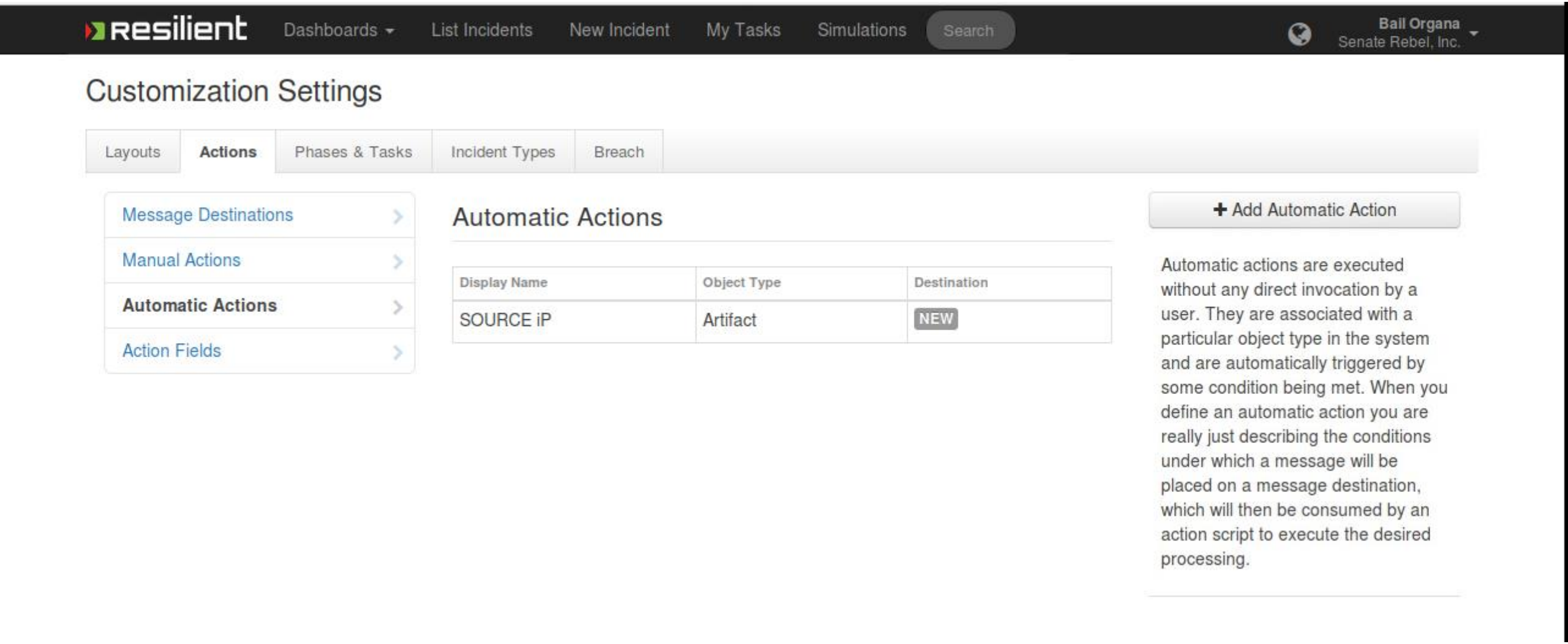
Trend Micro
Bluecoat
Dozor
Sandbox
FireEye
Kaspersky
Cisco IronPort
Cisco Talos
Virus Total
JIRA

120 минут

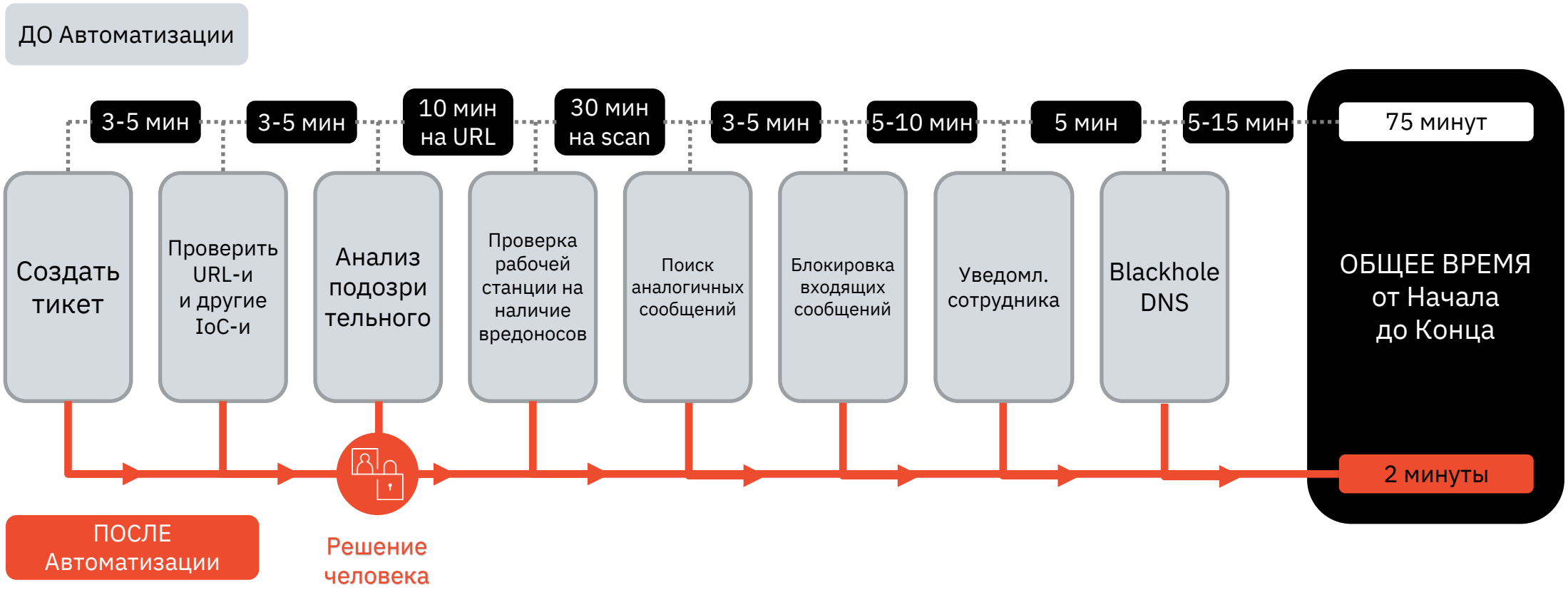
ОБЩЕЕ ВРЕМЯ
от Начала
до Конца

10-15 минут

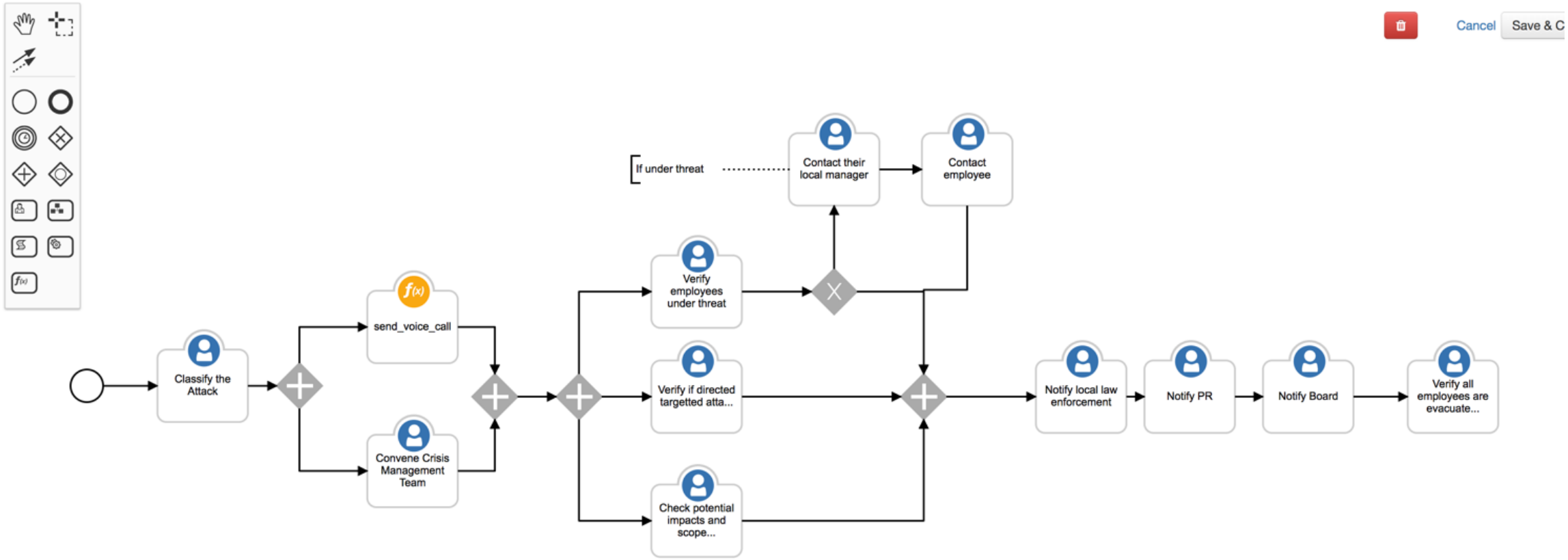
Модуль автоматизации

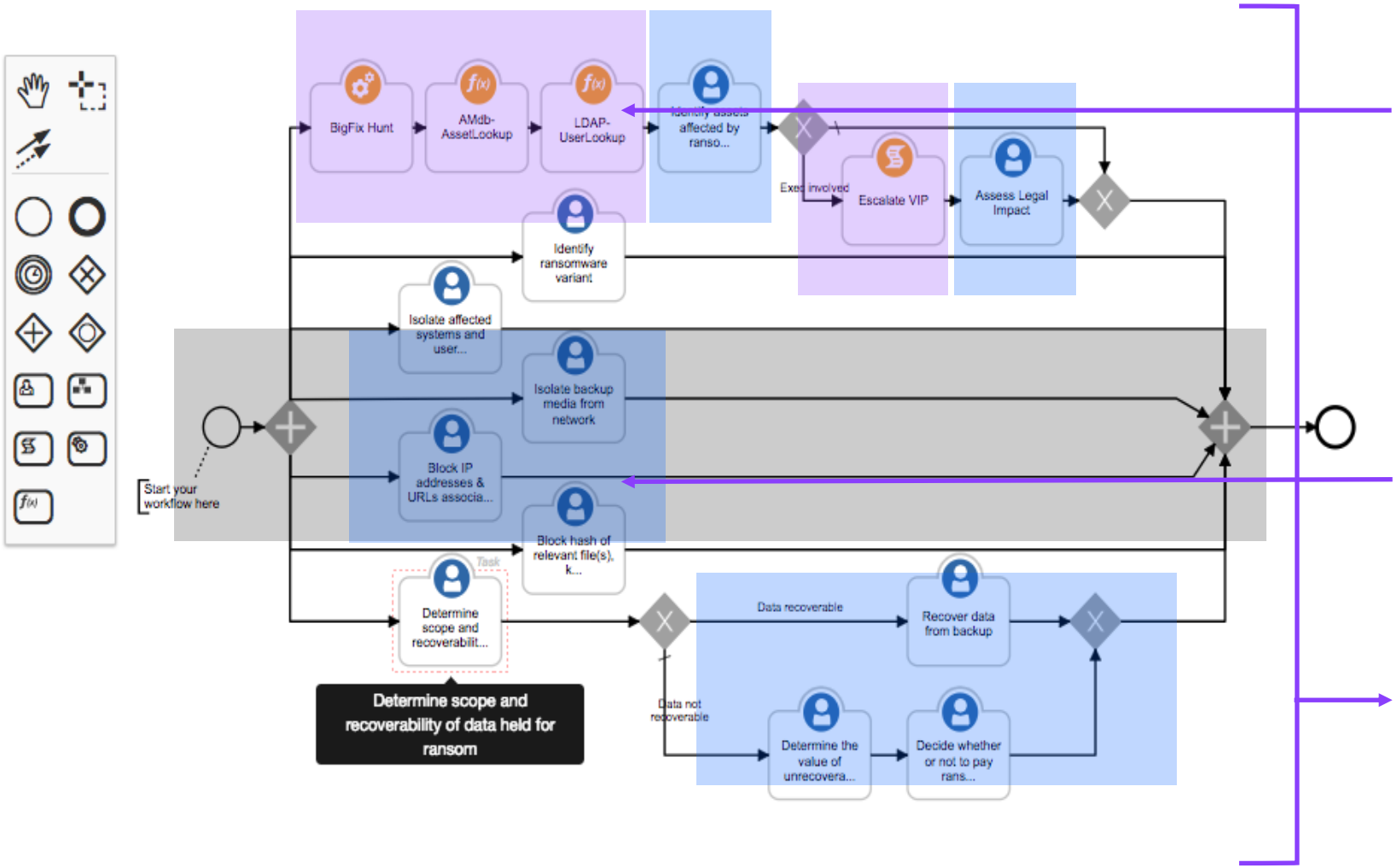


Модуль автоматизации



Разработка динамических плейбуков





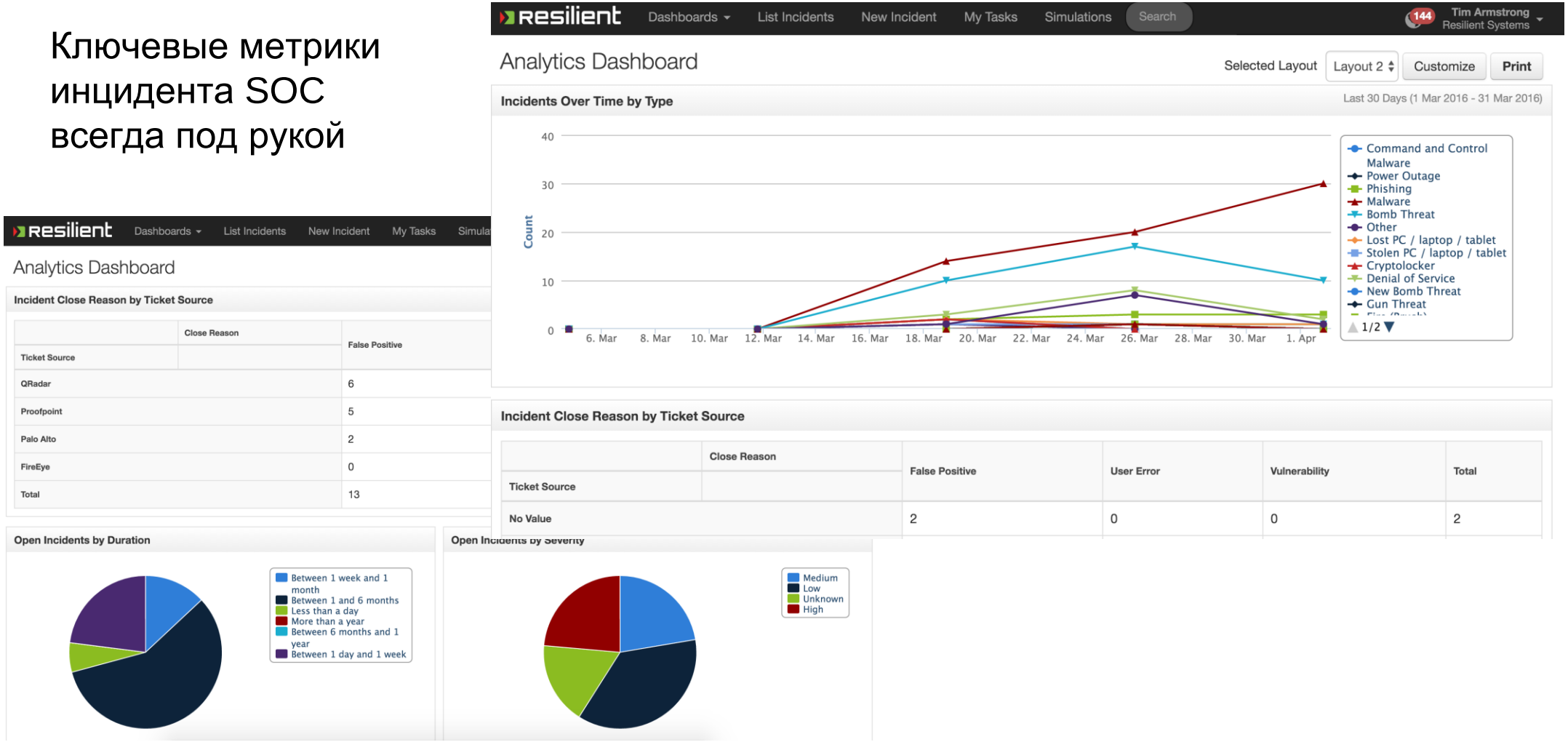
Автоматизация рутинных задач для ускорения процесса

Принятие решений на ключевых этапах

Люди, процессы и технологии

Аналитика по всем инцидентам в организации

Ключевые метрики инцидента SOC всегда под рукой



SOAR + Ansible Automation

Red Hat Ansible - Open Source Automation

1000+ новых интеграций

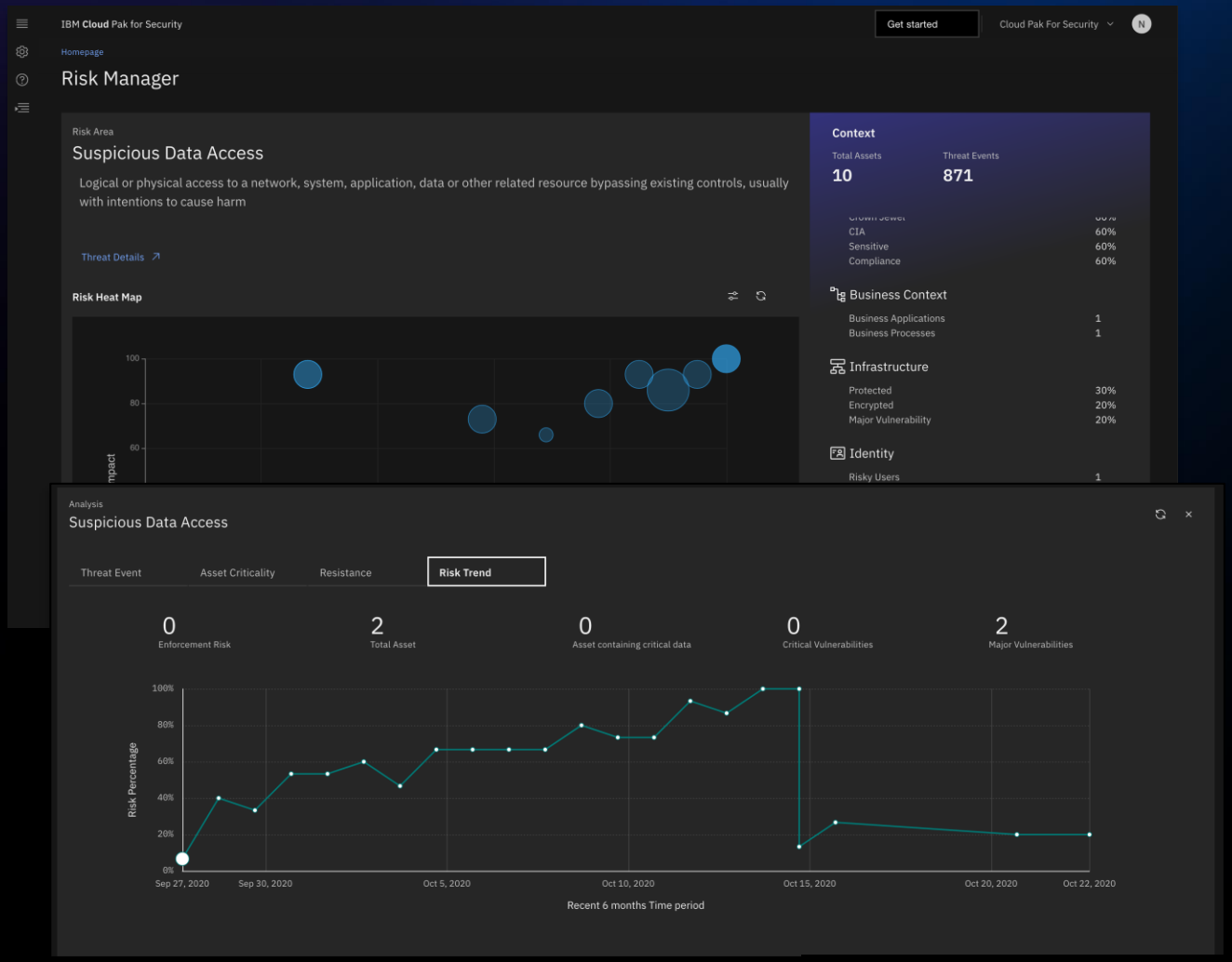
Risk Manager

Информация о потенциальных рисках ИБ, путем сопоставления аналитических данных по векторам рисков и критичности активов

- **Единое представление разрозненных метрик риска**
  Визуализируйте индикаторы консолидированного риска с помощью инструментов безопасности. Изучите индикаторы воздействия, такие как критичность актива для бизнеса или вероятность возникновения события угрозы.

- **Общее определение риска**
  Получите ясность в отношении значимости и срочности ваших областей риска. Механизм оценки риска решения использует единое определение риска по источникам уязвимостей и угроз для контекстуализации данных о рисках.

- **Приоритезация управления исправлений**
  Понимание факторов, способствующих общему риску безопасности, расстановка приоритетов и принятие корректирующих мер для смягчения или снижения выявленного риска



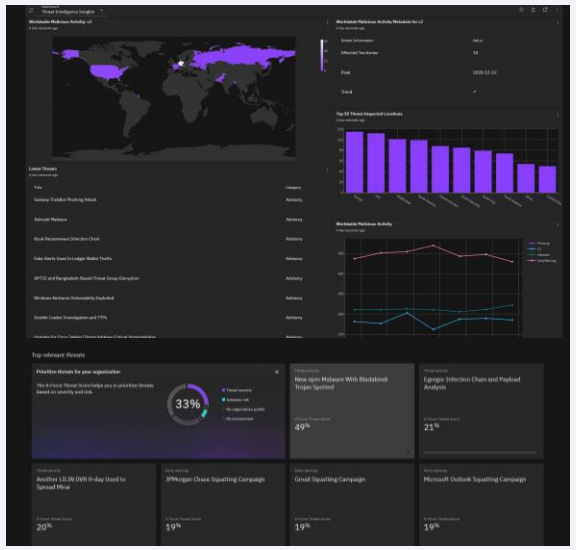
Guardium - Мониторинг БД

- Продуманная архитектура
- Универсальное решение для разных СУБД
- 100% контроля, включая локальный доступ DBA

- Не полагается на логи в БД, которые могут быть стерты
- Детальные политики и аудит
- Автоматическая отчетность (SOX, PCI, NIST, и т.д.)

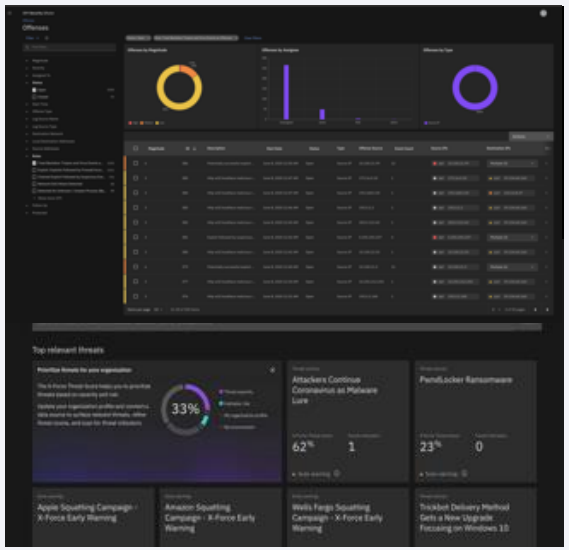
Объединенное управление угрозами с IBM Security

Видимость



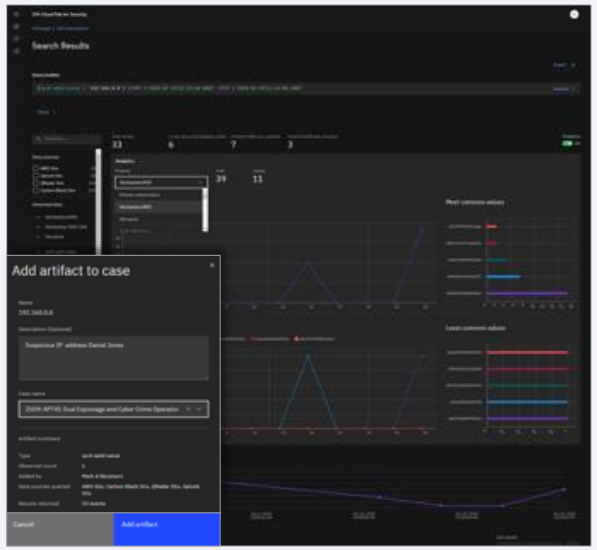
Подключение к источникам данных в любых местах, настройка дэшбордов для полной видимости

Реагирование



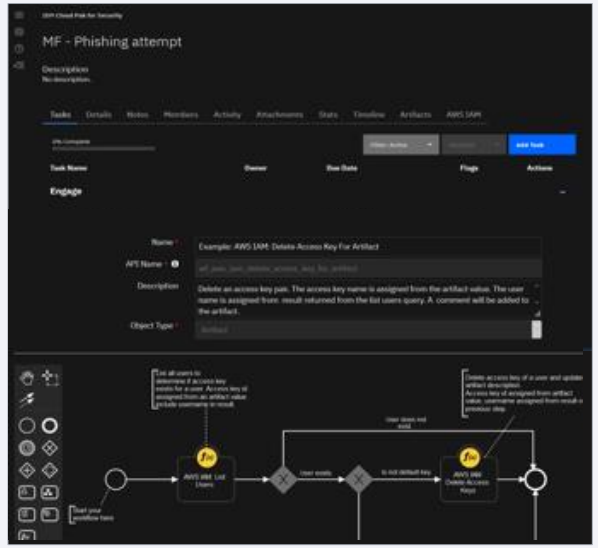
Отслеживание и изоляция угроз, снижение false positives

Расследование



Поиск данных, где бы они не находились с федеративным поиском, автоматизация угроз и расследования с Case Management

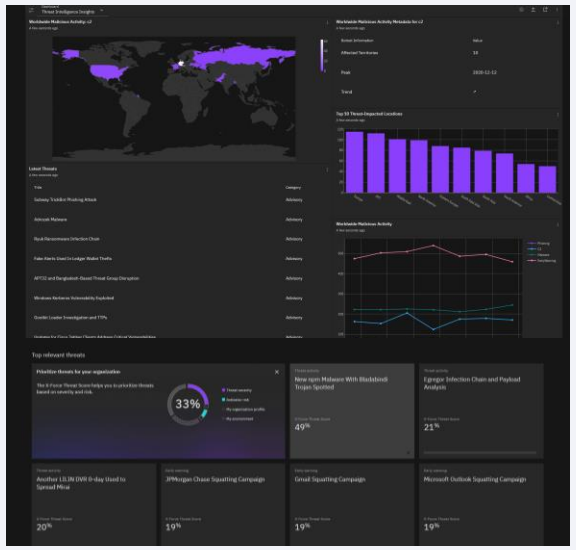
Ответ



Сценарии реагирования из коробки, встроенная оркестрация и автоматизация с Ansible

Результат

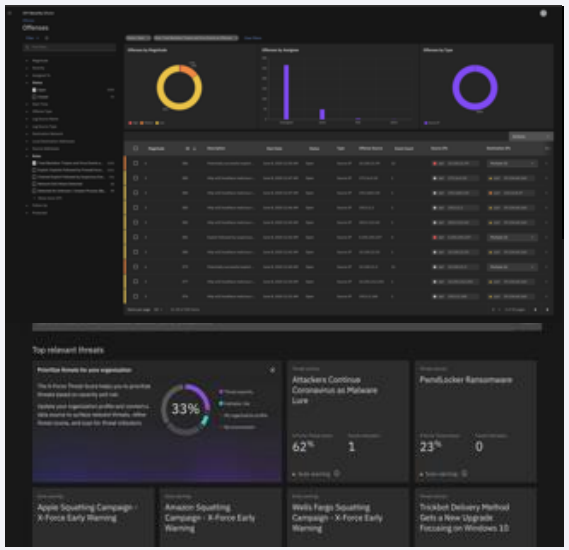
Видимость



600+

валидированных интеграций чтобы снизить риск и время реагирования

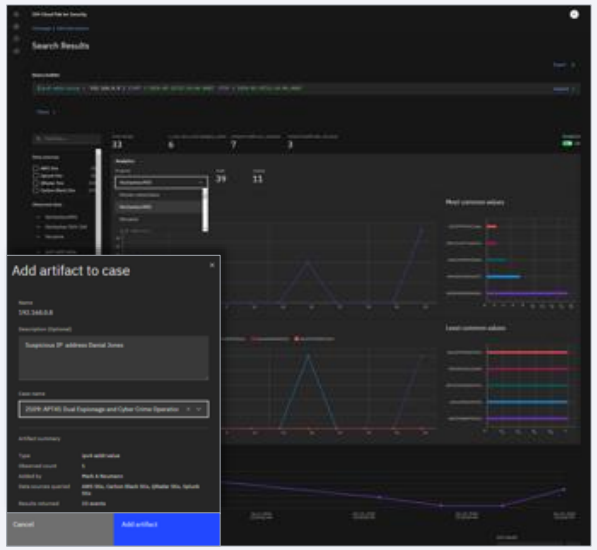
Реагирование



51%

увеличение вероятности определить атаку

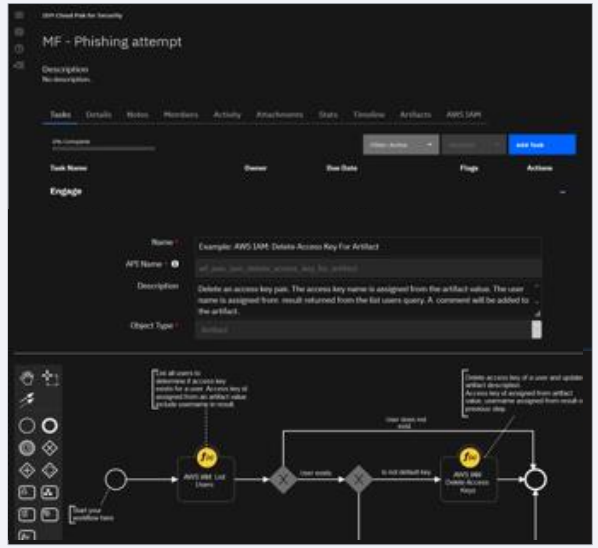
Расследование



60x

ускорение по времени расследования

Ответ



8x

ускорения реагирования на инцидент

Ценность для клиента

1. Ускорение расследования инцидентов с помощью федеративного поиска по нескольким источникам данных, без перемещения данных
2. Упрощение работы с помощью единого инструмента расследования и поиска в мультиоблачной среде
3. Легко отслеживайте ход расследования с помощью Case management
4. Отвечайте быстрее и тщательнее с помощью надежных возможностей оркестрации и автоматизации
5. Развертывание в любом месте с помощью гибридной мультиоблачной архитектуры - локально, в частном облаке, в публичном облаке
6. Расширяйте источники данных и возможности с помощью SDK или партнерских служб для создания новых соединителей