ICORE

IBM Cloud Pak for Security

Лицензирование и преимущества

Gold
Business
Partner

Лицензия «IBM Cloud Pak for Security Domains solutions» :

Пакет QRadar XDR - содержит в себе следующие, основные on-premise продукты

- QRadar SOAR
- QRadar SIEM (Аналитика событий)
- QRadar NDR (Аналитика потоков, включает в себя QRadar Network Insights)

Пакет Guardium – Защита баз данных и файловых серверов on-premise продукты:

- QRadar SOAR
- Guardium Data Protection (Мониторинг)
- Guardium Vulnerability Assessment (Управление уязвимостями)

Пакет Verify – Безопасность удалённых работников и потребителей - только облачные решения*

Удобство лицензирования «IBM Cloud Pak for Security Domains solutions»

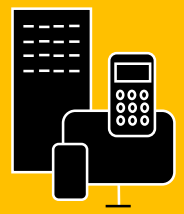
- **Единые лицензии**, которые основывается на количестве Управляемых серверов «Managed Virtual Server (MVS)», которые будут подключены к мониторингу и реагированию

- **Managed Virtual Server** – это любой Физический, Виртуальный или Облачный Сервер с Операционной системой и IP-адресом в инфраструктуре Организации

- **Пакет Verify –** рассчитывается по количеству пользователей в Организации, которые будут мониториться и обслуживаться облачными серверами

Расчёт Серверов для пакета «QRadar XDR Package»

Не считаются как MVS для мониторинга



- Network Infrastructure (Switches, Routers, Firewalls, load balancers, etc.
- SaaS Solutions
- Workstations Laptops
- IoT Infrastructure
- PoS Devices

Считаются как Managed Virtual Server

- Windows Servers
- AIX, UNIX & Linux
- AS/400
- zOS
- Kubernetes Nodes
- Cloud hosted IaaS (Windows, Linus, AIX, etc.)

Мониторинг и реагирование

Поиск, TII, SOAR, SIEM, QNI

MVS: Расчёт серверов, которые передают данные в Системы мониторинга и аналитики

Преимущества использования обновлённого лицензирования «IBM Cloud Pak for Security» для IBM Security QRadar SIEM

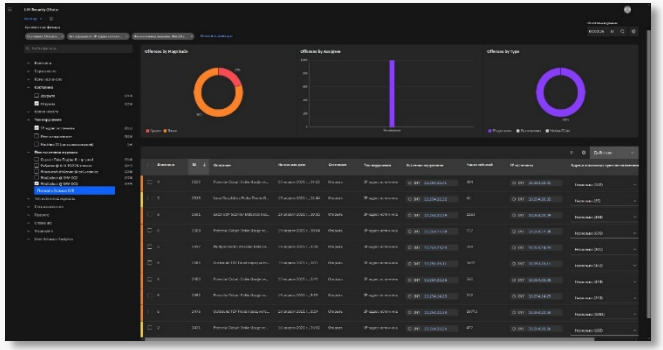
- Больше не требуется платить за дополнительные 1000 EPS – увеличение ёмкости количества событий в секунду теперь неограниченно

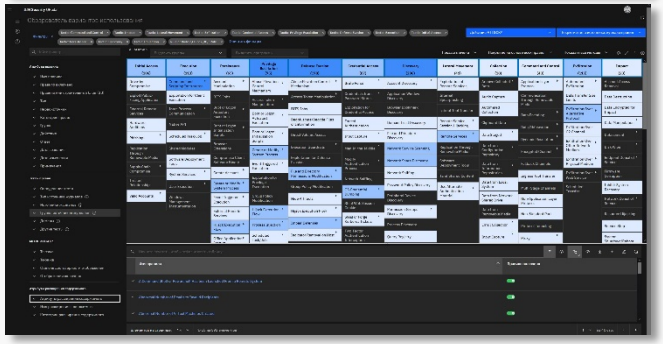
- Больше не требуется платить за дополнительные 20 000 FPM – увеличение ёмкости количества сетевых потоков в минуту теперь неограниченно

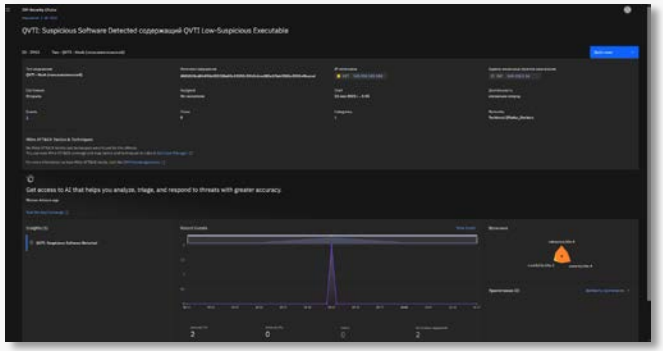
- Больше не требуется платить за **дополнительный коллектор, процессор или отказоустойчивый узел** – теперь можно устанавливать любое количество узлов в инфраструктуре (Software Node), включая узлы детальной аналитики сетевых потоков – QRadar Network Insights

Особенности IBM Security QRadar SIEM

- **IBM QRADAR SIEM** представляет собой гибкую и мощную аналитическую систему, полноценно работающую прямо из коробки и готовую решать задачи сразу после установки
- **IBM QRADAR SIEM** – решение «всё-в-одном» – не нужно устанавливать и администрировать большое количество раздельных модулей, операционных систем, баз данных
- Имеет большую Экосистему различных систем информационной безопасности и приложений легко подключаемых к системе, как от Производителя, так и от сторонних разработчиков
- Централизованно собирает, обрабатывает и хранит все события системных журналов, сетевых устройств полученных из различных систем и оборудования
- Централизованно собирает, обрабатывает и хранит сетевые потоки, полученные с ключевого сетевого оборудования
- Имеет большую базу подключаемых источников событий (начиная от сетевых устройств, IOT и заканчивая приложениями)
- Умеет анализировать сетевые потоки до уровня приложений с показом содержимого в потоке
- Встроенные возможности сетевого мониторинга и анализа, как сразу из коробки, так и с использованием большого количества приложений и наборов готовых правил от **IBM**







Расширяем IBM Security QRadar SIEM

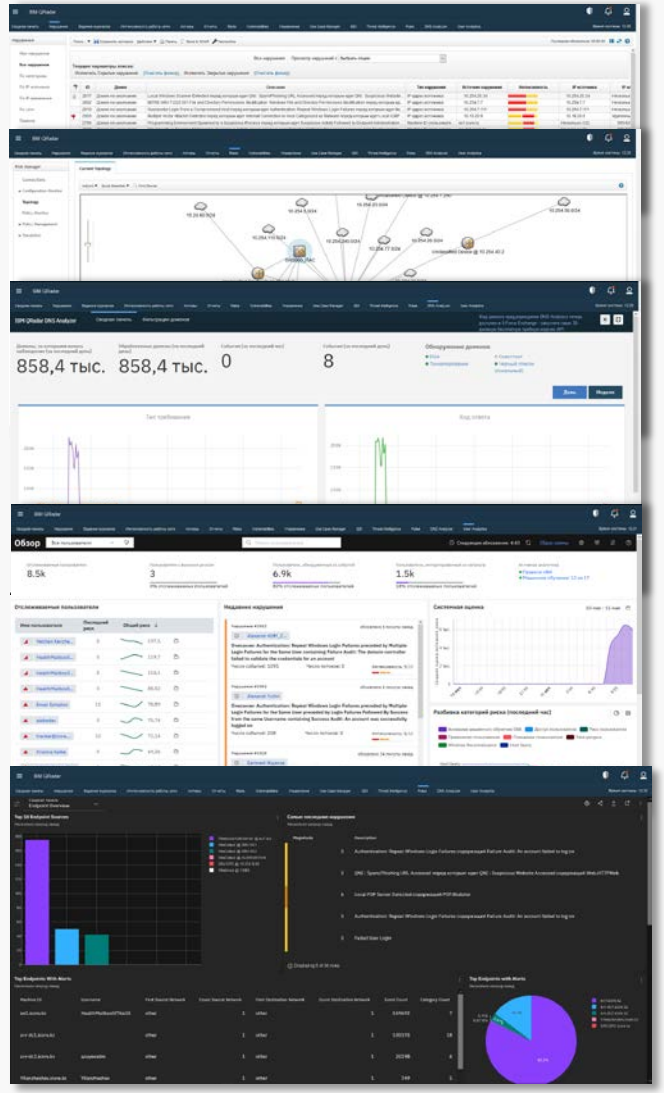
При использовании нового лицензирования и дополнительно к функционалу SIEM, Организация получает следующие преимущества:

- **Применение отказоустойчивости для любого узла** без затрат на лицензии

- **Подключение Филиалов** без затрат на лицензии – установка гибридных коллекторов/процессоров для сбора событий и сетевых потоков на любое количество Организаций и без ограничений на ёмкость EPS / FPM

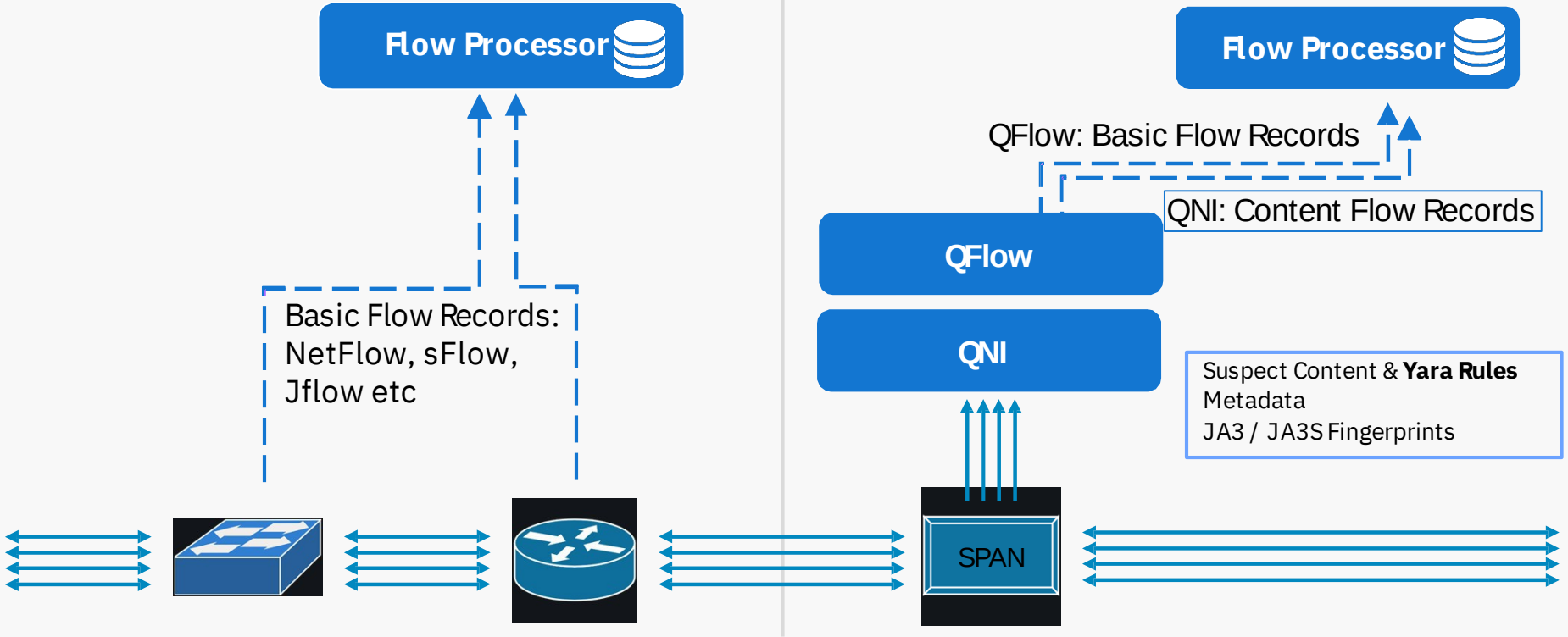
- **Построение Data Lake** без затрат на лицензии – установка узлов Data Node и Data Store при необходимости построения управляемых Хранилищ данных

- **Доступный Network Detection and Response** - мониторинг и аналитика сетевых потоков до уровня приложений с показом содержимого в потоке (QFlow и QRadar Network Insights) – без дополнительных затрат на лицензии



IBM Security QRadar SIEM и Анализ сетевого трафика (NTA)

Сетевая видимость в аналитике потоков (сетевые коммуникации) и полная инспекция пакетов (**QRadar Network Insights**)



IBM Security QRadar Network Insights

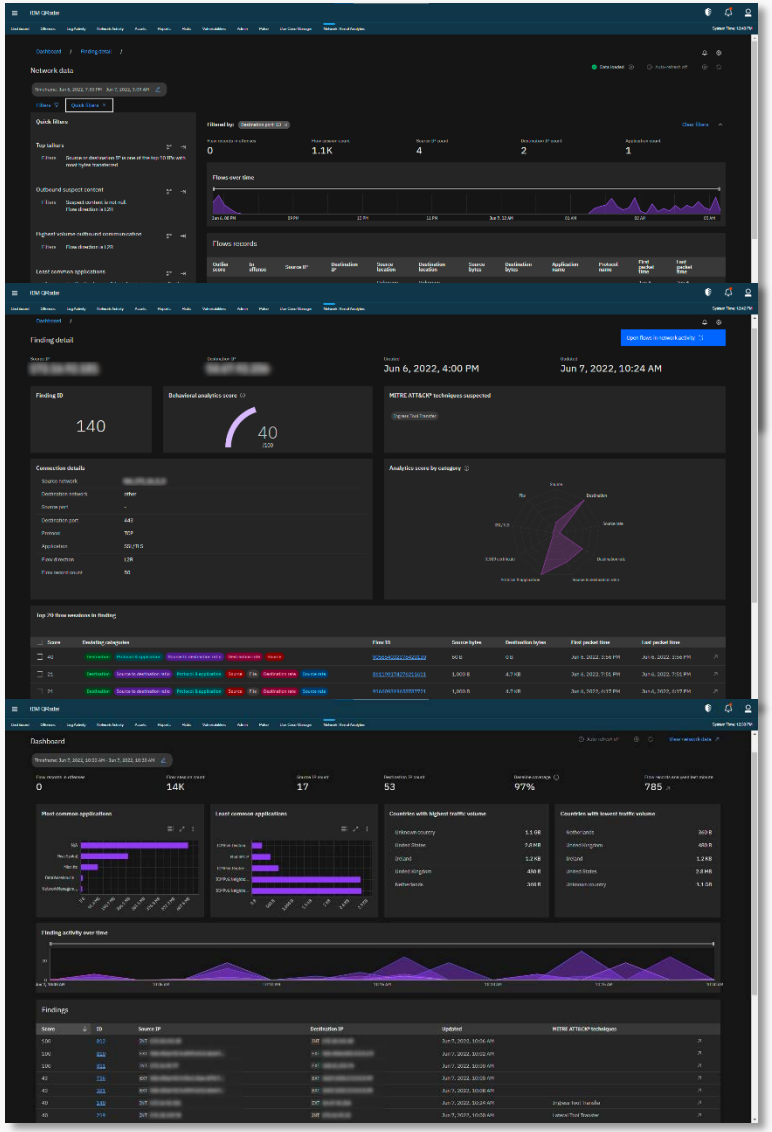
- Встроенный сетевой мониторинг и анализ сетевых потоков (**QFlow**) сразу из коробки и с использованием большого количества приложений и наборов готовых правил:
  - +64 Bytes, +Applications

- Модуль **«QRadar Network Insight»** в виде виртуального сервера для детального анализа сетевых потоков (не требует дополнительной лицензии):
  - Filename, Hashes, File Size, password, metadata, url, ftp command, action (post\share\AV Update), user agent, ssl\tls session id\version, web category
  - Зловреды, СПАМ, Фишинг, Скрипты\Макросы, Утечки, Сертификаты, DNS Атаки

- Модуль **«QRadar QFlow Virtual»** в виде виртуального сервера для анализа сетевых потоков между виртуальным сетевым оборудованием и виртуальными серверами

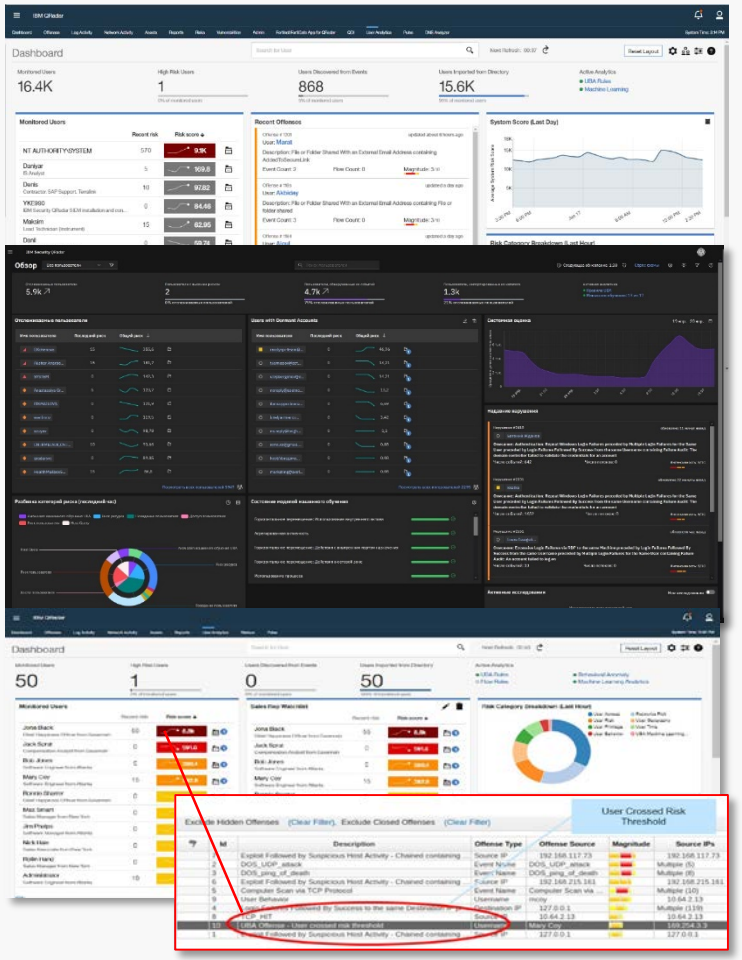
IBM Security QRadar Network Threat Analytics

- Модуль постоянно отслеживает сетевые потоки в вашей сети для выявления аномального трафика
- Подробные дашборды предоставляют визуализацию показывающую, какие записи потока больше всего отклоняются от других записей потока, обычно наблюдаемых в сети Организации
- Подробные дашборды помогают быстро определить, какие потоки указывают на подозрительное поведение в сети и определить приоритетность расследований аномалий
- Используются алгоритмы машинного обучения для построения моделей и выявления аномалий в сетевых потоках Организации



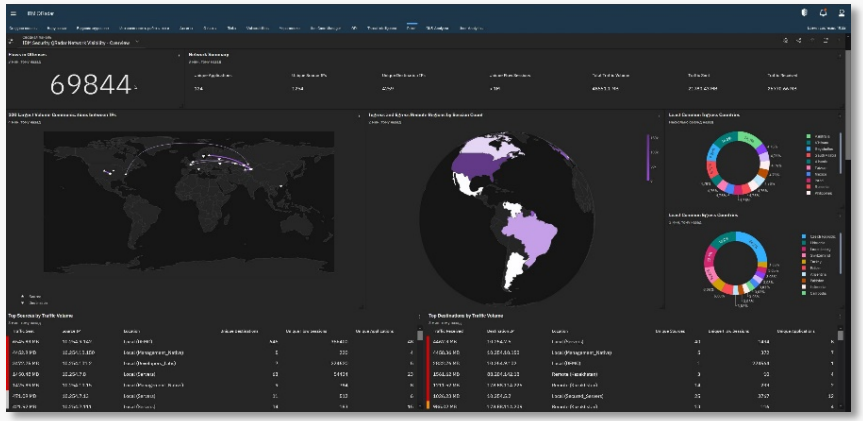
IBM Security QRadar SIEM - Аналитика поведения пользователей

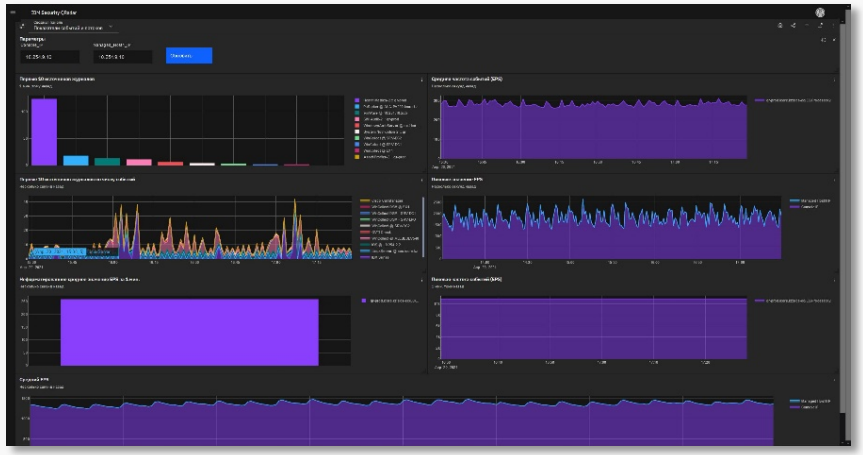
- Модуль непрерывно анализирует и запоминает поведение пользователей
- Использует алгоритмы машинного обучения
- Строит графики аномального поведения пользователей
- Оповещает офицеров безопасности о аномальном (необычном) поведении пользователя
- Позволяет создавать собственные математические модели обучения



IBM Security QRadar SIEM - PULSE

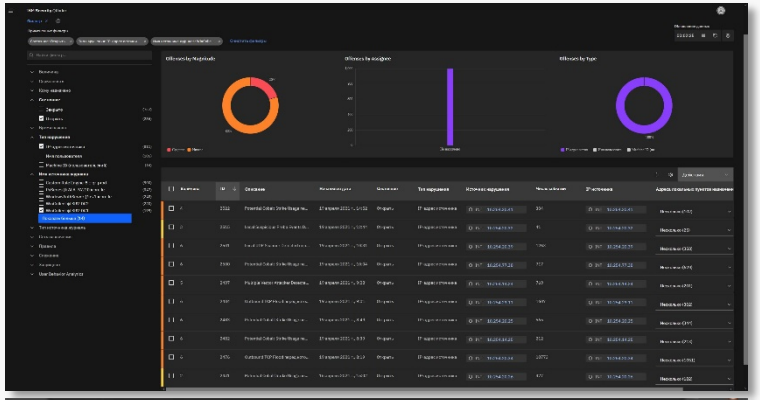
- Готовая основа для мониторинга в ОЦИБ
- Конструируемая визуализация под задачи
- Создание дашбордов на основе своих запросов
- Показ дашбордов на любом количестве экранов
- Наблюдение за ситуацией в реальном времени
- Загружаемые дашборды из IBM App Exchange

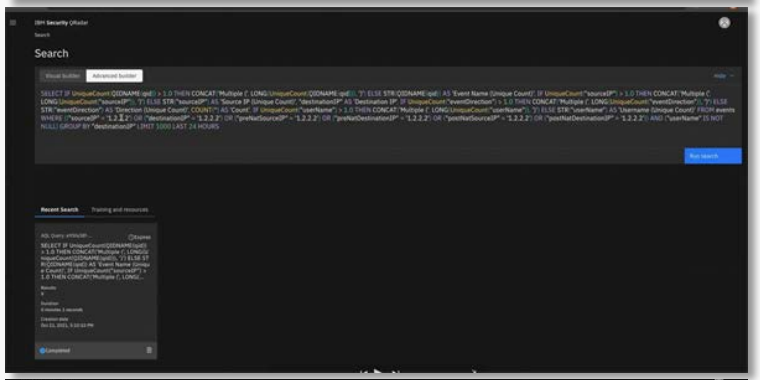


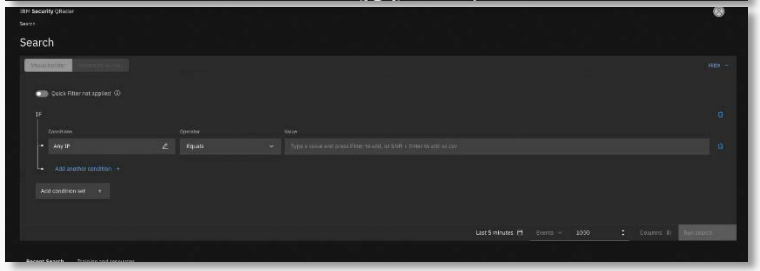


IBM Security QRadar SIEM - Рабочее место Аналитика 2.0

- Новый интерфейс для анализа Нарушений
- Быстрый доступ к критической информации, активам, тестам правил, содержимому событий, проверке TI
- Глобальный поиск по всем полученным данным (событиям и потокам)
- Визуальный конструктор запросов
- Прямая интеграция с матрицей MITRE ATT&CK tactics and techniques с отображением тактик в Нарушении
- Большое количество фильтров для отображения Нарушений







Преимущества использования обновлённого лицензирования «IBM Cloud Pak for Security» для IBM Security SOAR

- Больше не требуется платить за каждого пользователя и на количество пользователей в Системе теперь нет ограничений

- Больше не требуется платить за модули расширения (Team Management, Disaster recovery, MSSP, Non-production)

- Нет ограничений по количеству «Действий (Actions)» для управления системами информационной безопасности и сервисами участвующими в процессах реагирования – теперь и 1001 действие заблокирует угрозу

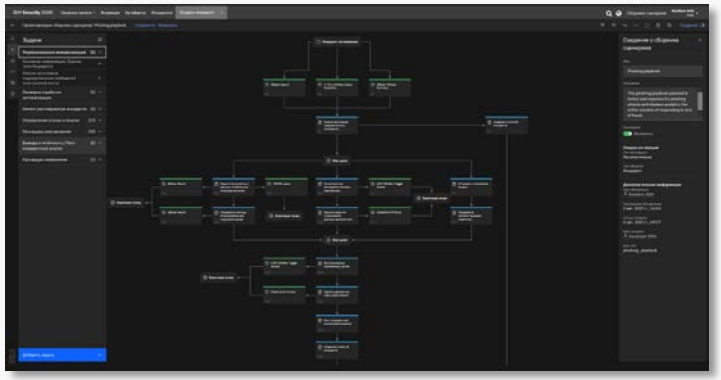
IBM Security SOAR

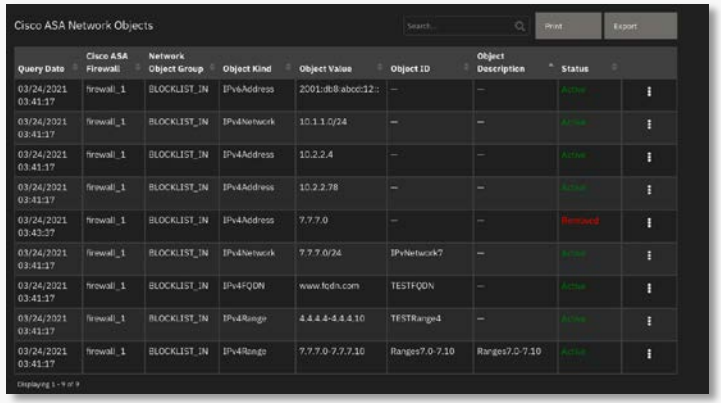
- Лидер аналитики Gartner среди решений по координации и автоматизации процессов реагирования на инциденты информационной безопасности

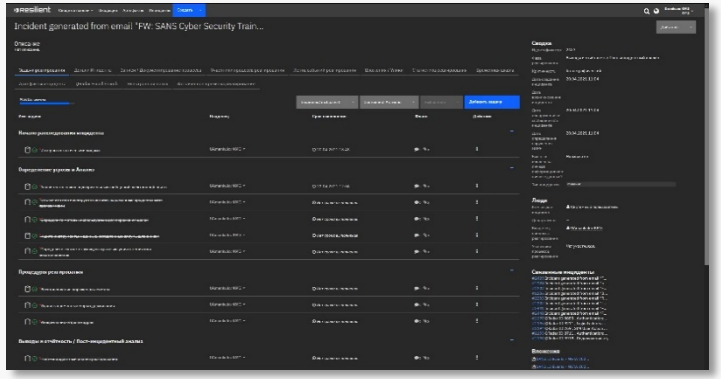
- Интегрируется с 99% средств мониторинга событий информационной безопасности (SIEM) других производителей, системами защиты информации, ИТ-службами и сервисами

- Адаптивное реагирование силами оператора на сложные кибератаки – изменение «Динамического сценария» в процессе реагирования

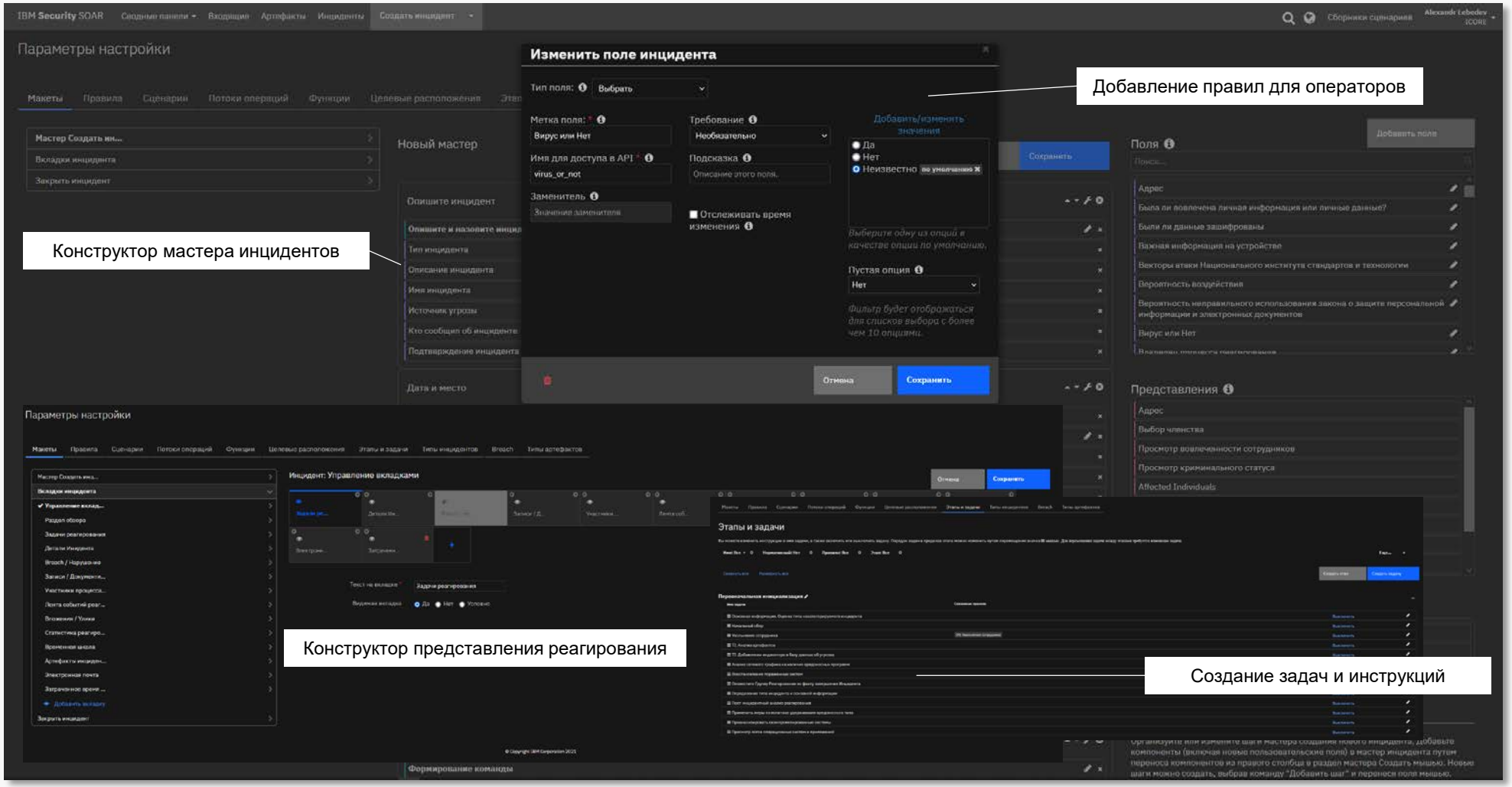
- Реагирование и завершение инцидента в автоматическом режиме без участия оператора - создание «Динамического сценария» и автоматического реагирования до включения в работу команды ОЦИБ



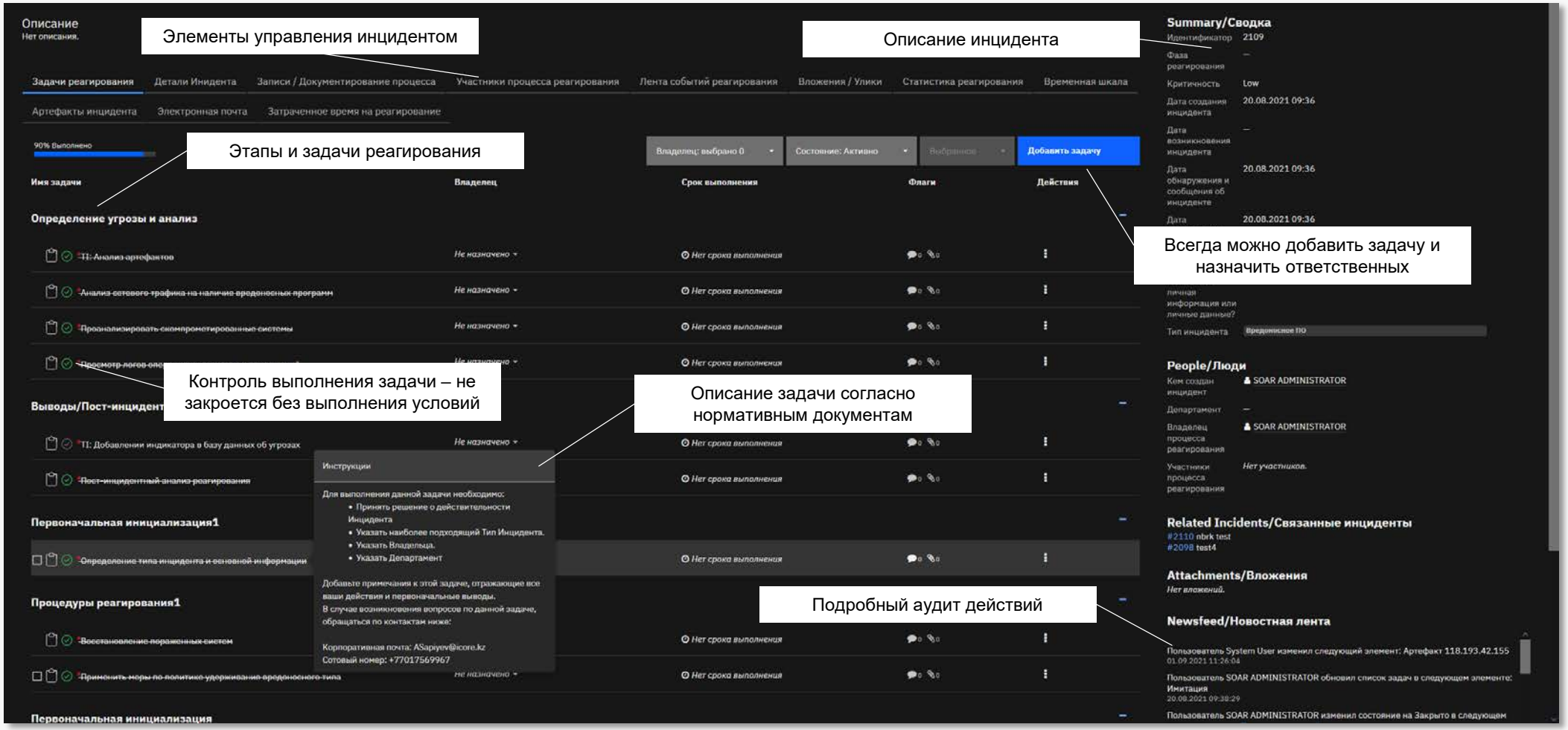




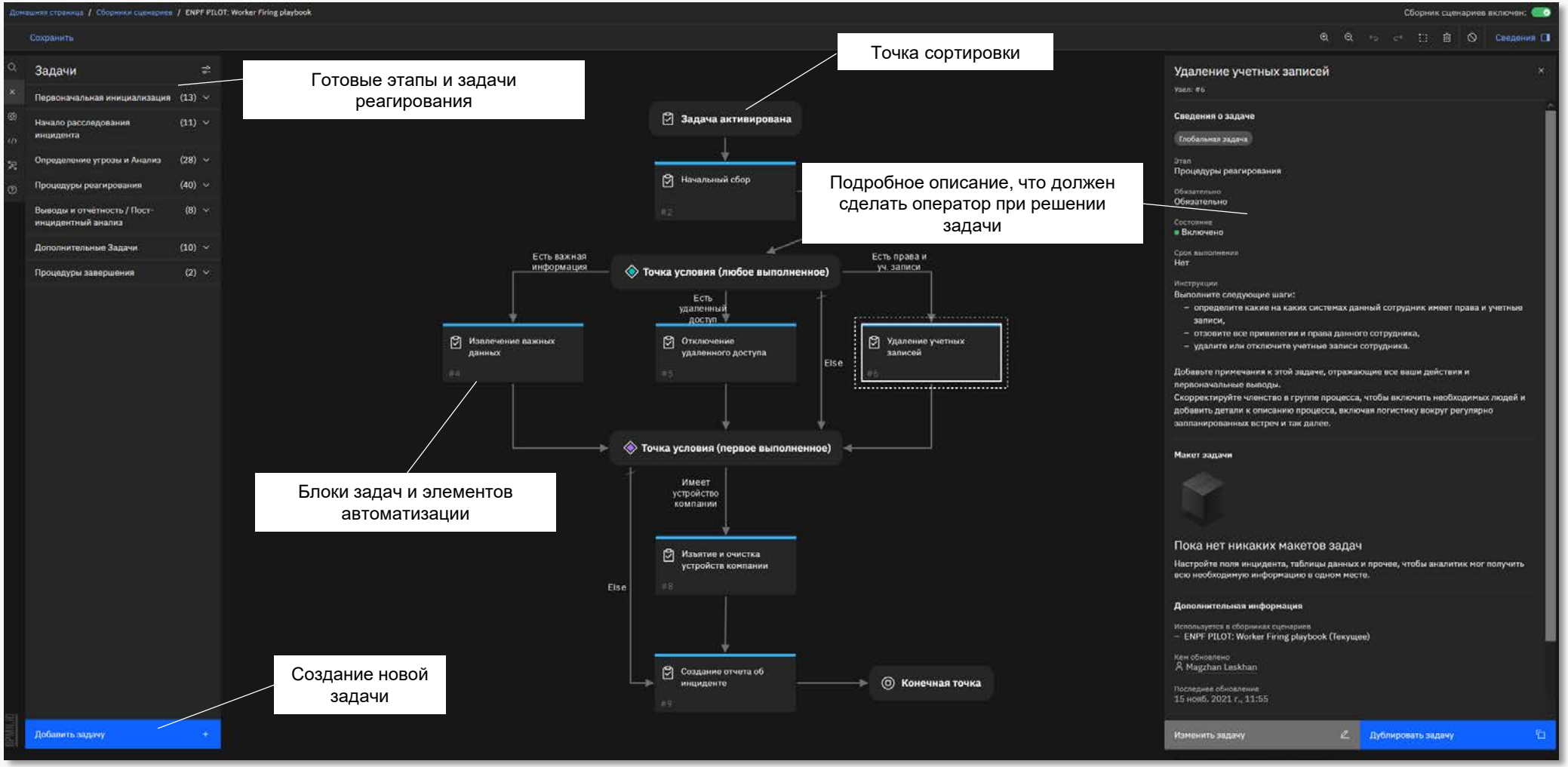
Полностью настраиваемый интерфейс платформы - легко адаптируется под казахский язык



«Динамические сценарии» - подробные задачи для аналитиков и операторов команды реагирования ОЦИБ

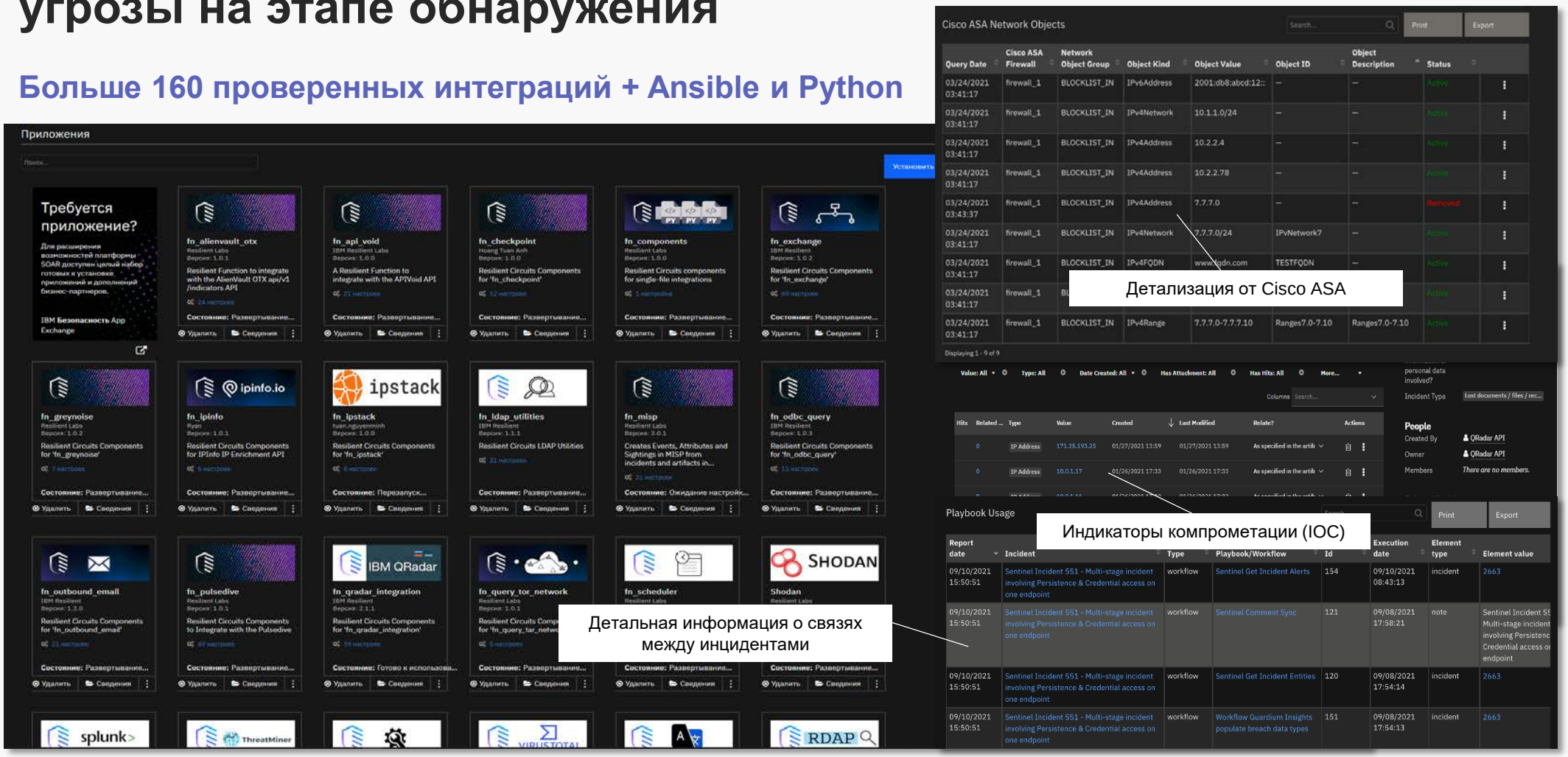


Конструктор «Динамических сценариев» - весть процесс реагирования на инцидент строится в одном окне

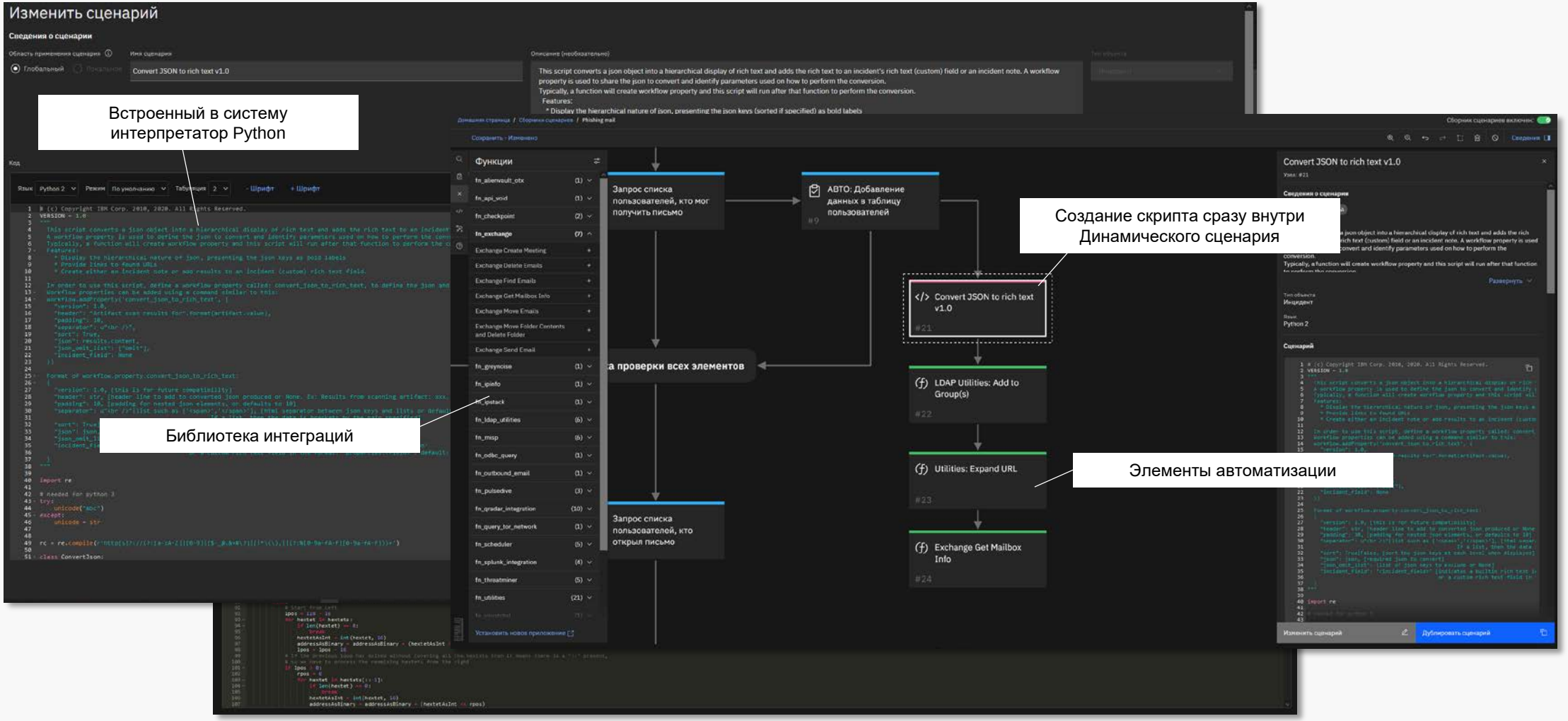


Интеграции предоставляют ценную аналитическую информацию об участниках и проактивно предотвращают угрозы на этапе обнаружения

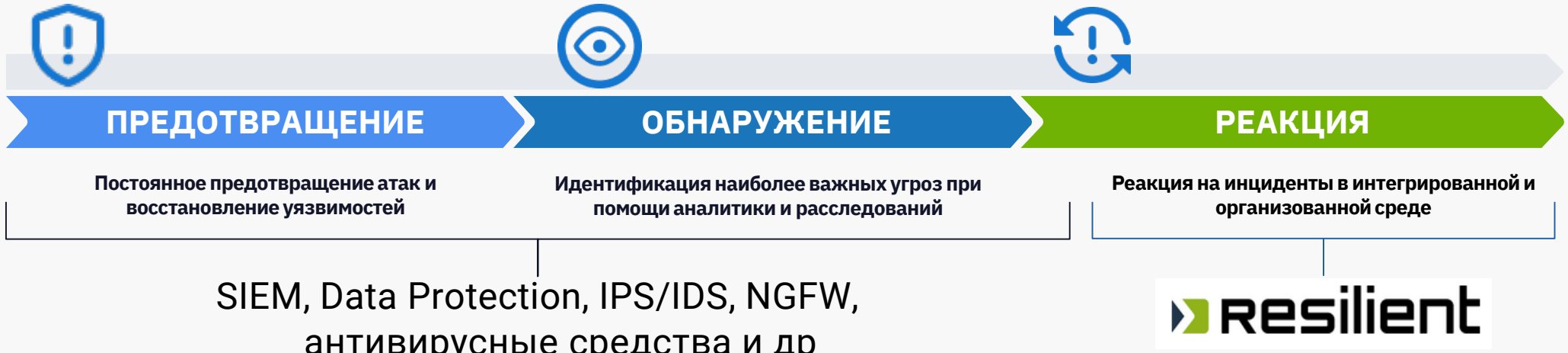
Больше 160 проверенных интеграций + Ansible и Python



Python: применение скриптов, создание своих компонентов и приложений внутри IBM Security SOAR



IBM Security SOAR - самодостаточный продукт решающий все задачи ОЦИБ



Объединить ответственных для реагирования на инцидент

IBM Security QRadar SOAR расширяет возможности аналитиков ОЦИБ по командному предотвращению, обнаружению и реакции на угрозы

Единый Центр Управления Реагированием

IBM Security QRadar SOAR позволяет аналитикам ОЦИБ управлять процессами реагирования и разбирать инциденты умнее, быстрее и эффективнее

Бесшовная интеграция с SIEM Qradar, Splunk и другими

IBM Security QRadar SOAR интегрируется с SIEM в обе стороны и позволяет передавать инциденты в SOAR, производить поиск, передавать описание инцидентов в SIEM

Преимущества использования обновлённого лицензирования «IBM Cloud Pak for Security» для IBM Security Guardium Data and File protection

- Больше не требуется платить за отдельные агрегаторы обработки и аналитики - теперь можно устанавливать неограниченное количество
- Больше не требуется платить за отдельные коллекторы сбора данных - теперь можно устанавливать неограниченное количество узлов сбора

- Включена лицензия на мониторинг и аналитику данных в кластерах Big Data
- Включена лицензия на мониторинг и аналитику данных сервисов и конфигураций ОС БД
- Включена лицензия на мониторинг и аналитику данных в распределённых хранилищах
- Включена лицензия на мониторинг и аналитику данных в мейнфреймах z/OS
- Включена лицензия на мониторинг и аналитику данных для SAP HANA
- Включена лицензия на мониторинг и аналитику файловых хранилищ Организации

Расчёт Серверов для «Guardium Packages»

Не считаются как MVS для защиты БД

- Windows Servers
- Kubernetes Nodes
- Cloud hosted IaaS (windows, etc)
- Workstation Laptops
- IOT Infrastructure
- PoS Devices

Считаются как Managed Virtual Server
(Databases, for Data Warehouses, and for Big Data)

- DB2
- Oracle
- Snowflake
- AWS PostgreSQL
- ...

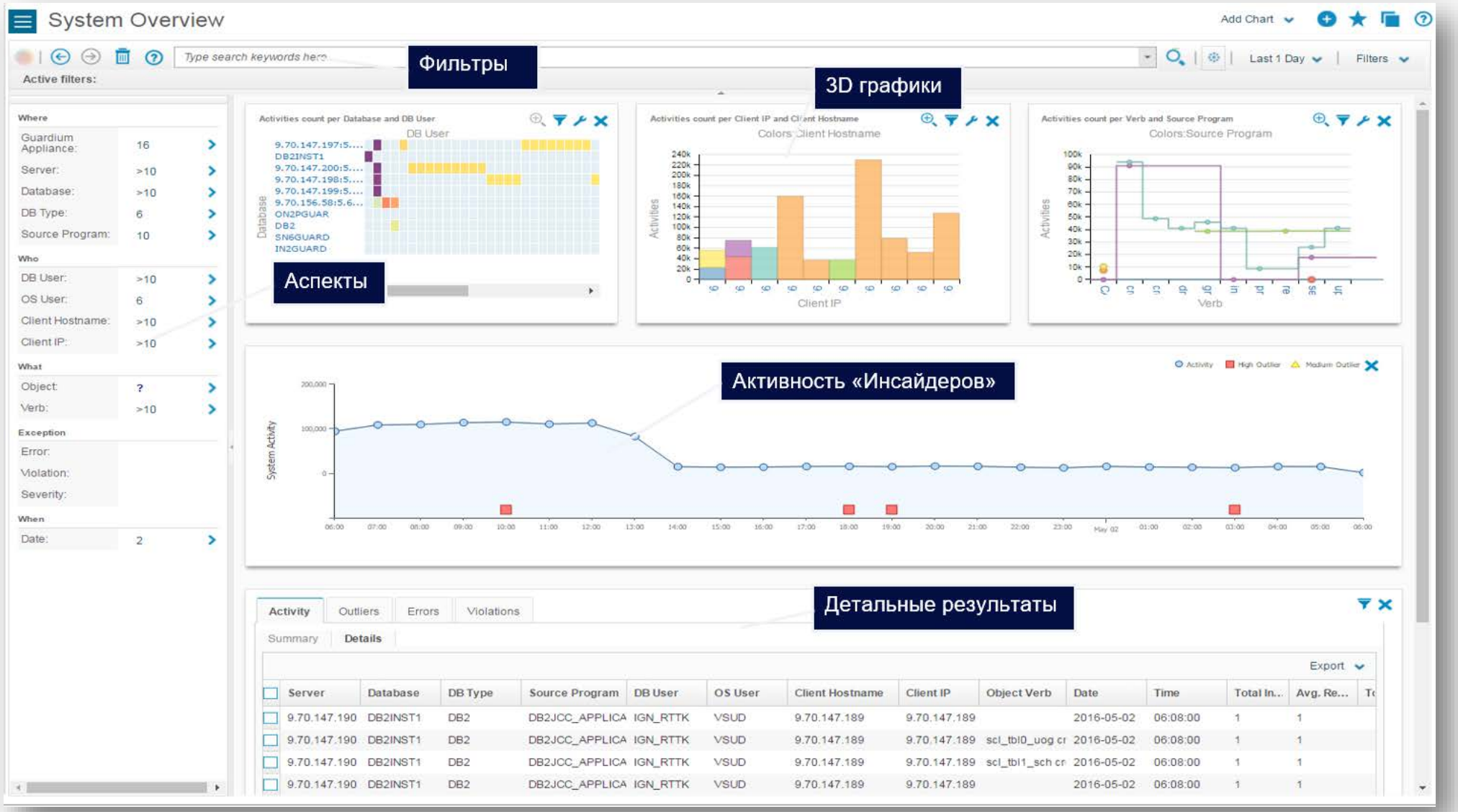
Защита данных

Guardium Data Protection, Guardium Vulnerability Assessment, Guardium Insights
MVS: Расчёт серверов, которые содержат критические данные, мониторятся и анализируются

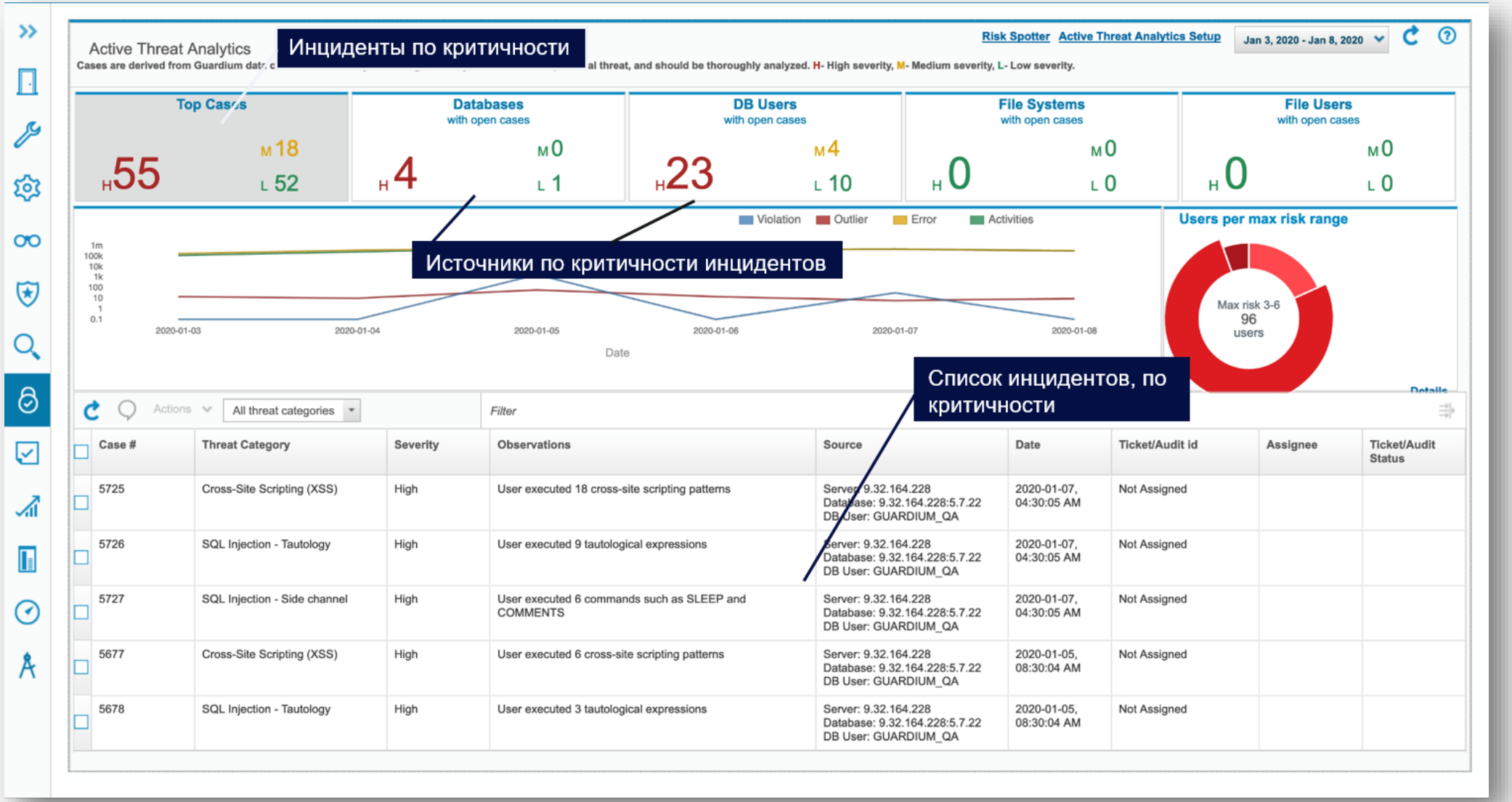
IBM Security Guardium Data and File Protection

- Контроль неавторизованных изменений данных
- Контроль изменения операционной системы СУБД
- Использование ИИ в аналитике всех событий и действий
- Повышение оперативности реагирования на инциденты
- Определение различных атак злоумышленников
- Предотвращение утечек данных в реальном времени
- Упрощение процессов отчётности и аудита
- Контроль уязвимостей СУБД
- Замена нативного аудита и уменьшение нагрузки на СУБД
- Сокращение затрат на обслуживание Систем хранения данных

Мониторинг всех действий с СУБД и Базами данных

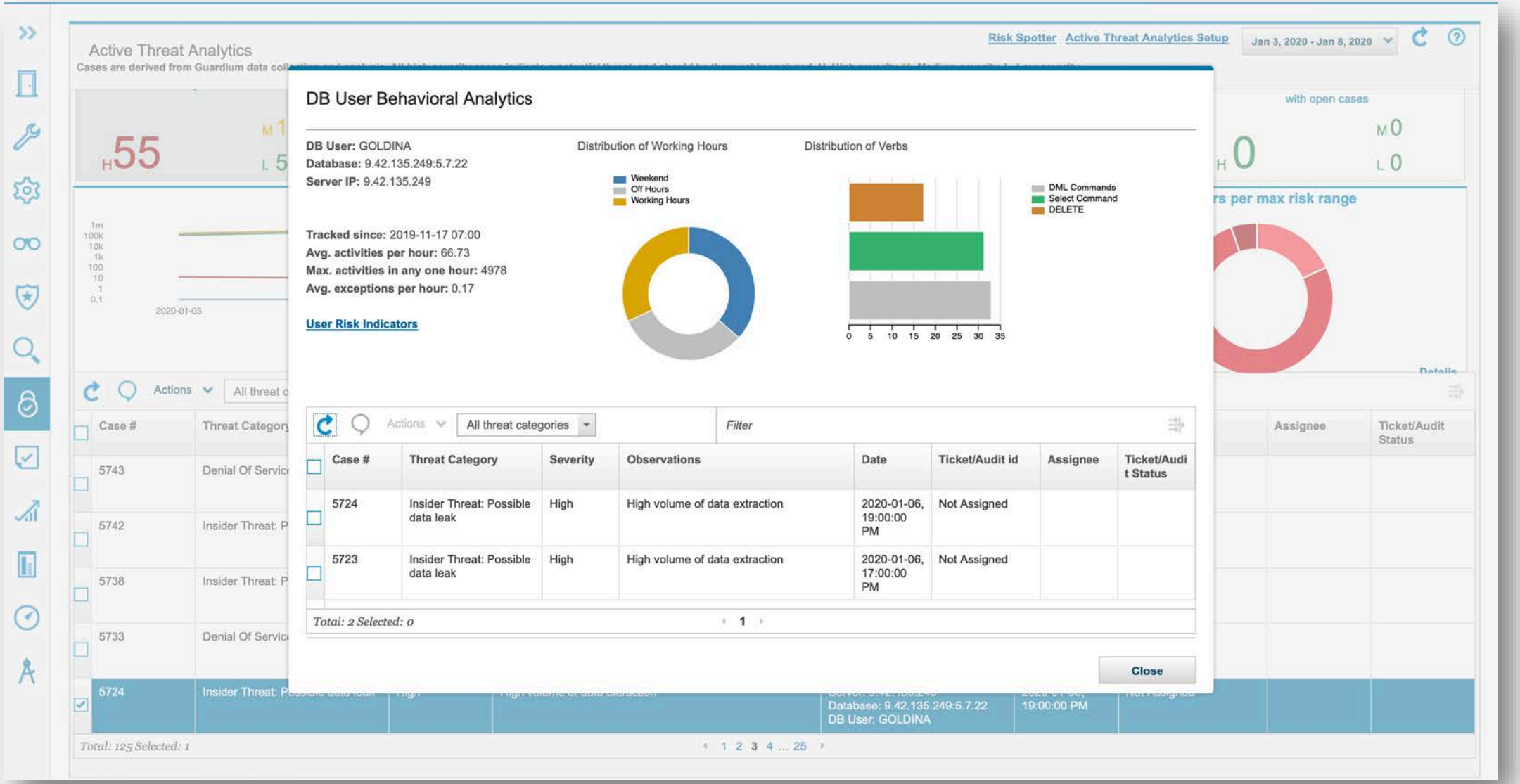


Обнаружение атак на СУБД и Базы данных



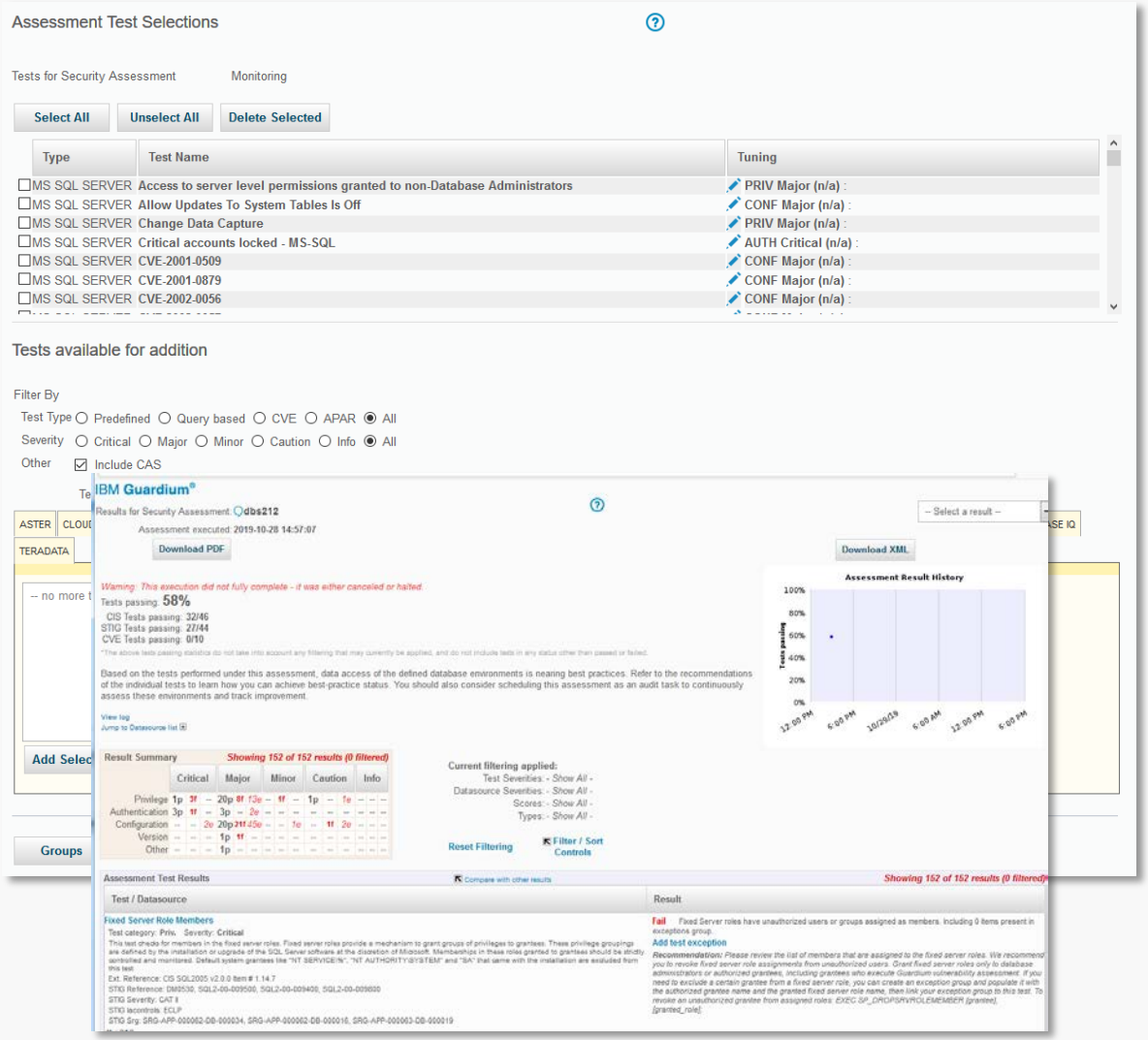
Case #	Threat Category	Severity	Observations	Source	Date	Ticket/Audit id	Assignee	Ticket/Audit Status
5725	Cross-Site Scripting (XSS)	High	User executed 18 cross-site scripting patterns	Server: 9.32.164.228 Database: 9.32.164.228:5.7.22 DB User: GUARDIUM_QA	2020-01-07, 04:30:05 AM	Not Assigned		
5726	SQL Injection - Tautology	High	User executed 9 tautological expressions	Server: 9.32.164.228 Database: 9.32.164.228:5.7.22 DB User: GUARDIUM_QA	2020-01-07, 04:30:05 AM	Not Assigned		
5727	SQL Injection - Side channel	High	User executed 6 commands such as SLEEP and COMMENTS	Server: 9.32.164.228 Database: 9.32.164.228:5.7.22 DB User: GUARDIUM_QA	2020-01-07, 04:30:05 AM	Not Assigned		
5677	Cross-Site Scripting (XSS)	High	User executed 6 cross-site scripting patterns	Server: 9.32.164.228 Database: 9.32.164.228:5.7.22 DB User: GUARDIUM_QA	2020-01-05, 08:30:04 AM	Not Assigned		
5678	SQL Injection - Tautology	High	User executed 3 tautological expressions	Server: 9.32.164.228 Database: 9.32.164.228:5.7.22 DB User: GUARDIUM_QA	2020-01-05, 08:30:04 AM	Not Assigned		

Аналитика поведения пользователей СУБД



Оценка защищённости СУБД (Vulnerability Assessment)

- CVE, STIG, CIS, тесты по производителям
- Анализ базового состояния
- Настраиваемые тесты – скрипты ОС, SQL-запросы к СУБД, файловые запросы
- Проверки конфигурации СУБД, неизменность файлов ОС, активность в СУБД



«IBM Cloud Pak for Security Domains solutions» Пакет Verify :

- **QRadar SOAR** – Платформа реагирования на инциденты информационной безопасности

- **Verify** – аутентификатор на основе двухфакторной аутентификации (2FA), который обеспечивает внеполосную 2FA по отдельному защищенному каналу с использованием мобильного устройства пользователя

- **Trusteer** - предотвращает кражу банковских аккаунтов, перехват учетных данных и утечку конфиденциальной информации посредством банковских троянов, таких как ZeuS, SpyEye, Silon, Torpig и других финансовых вредоносных программ

- **MaaS360** - комплексное решение по управлению мобильными устройствами для мониторинга и управления смартфонами, планшетами и другими мобильными устройствами

Лицензия «IBM Cloud Pak for Security» позволяет установить и использовать платформу «Единый центр аналитики и реагирования» и операционные системы Red Hat

- Платформа «IBM Cloud Pak for Security», как «Единый центр аналитики и реагирования» on-premise, в собственном кластере Red Hat OpenShift

- Red Hat OpenShift Container Platform
- Red Hat Enterprise Linux CoreOS (RHCOS)
- Red Hat Enterprise Linux (RHEL)

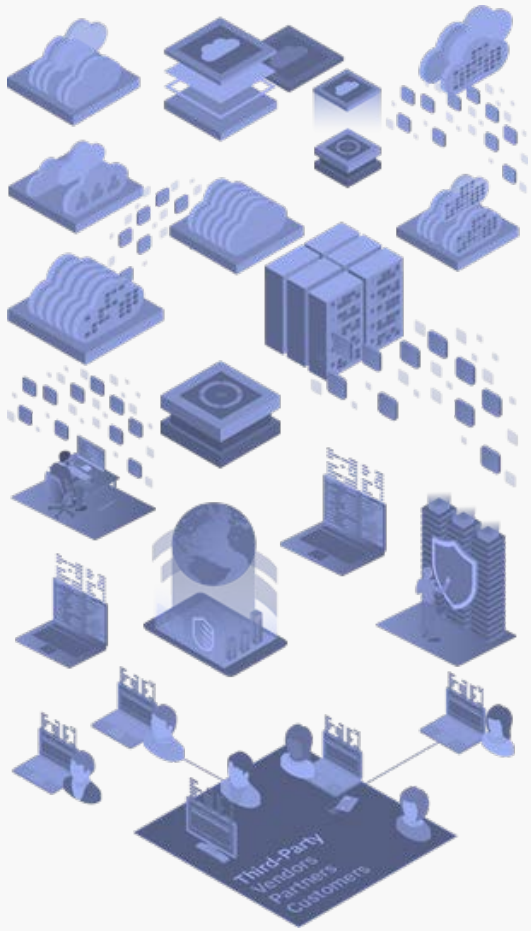
Зачем нужна платформа «IBM Cloud Pak for Security»?

Слишком много нужно делать

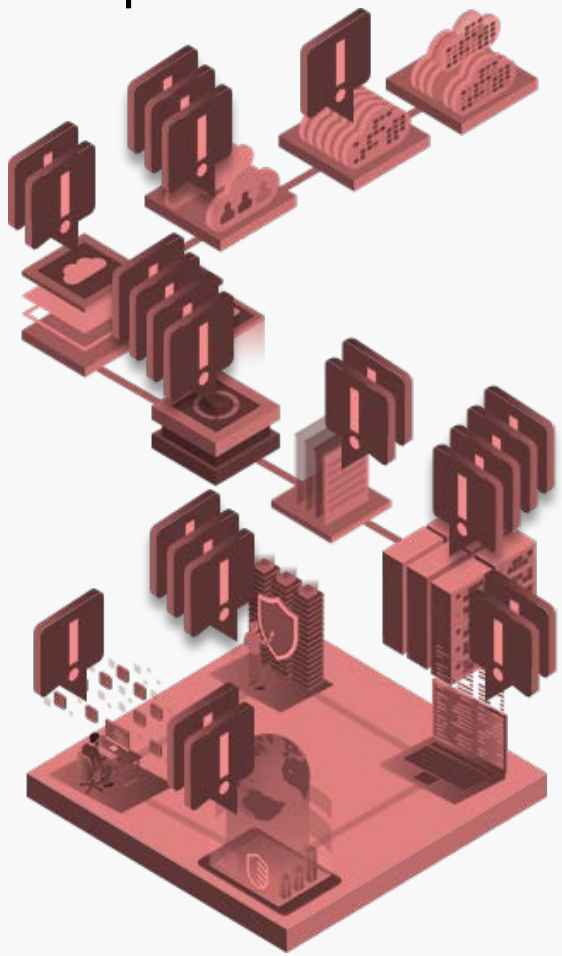
- Встречи с CIO и Владельцами ИС
- Контролировать риски третьих лиц
- Управлять Персональными данными
- Отвечать на вопросы Регулятор
- Подготавливать отчёты для CEO
- Обновлять бюджеты
- Описывать нормативные акты в контрактах
- Продвигать «бесконечные» проекты
- Анализировать и обновлять проекты
- Редактировать календарь мероприятий
- Обновлять риски в планировании ИБ
- Политика использования внешних носителей
- Тестировать инструменты шифрования
- Обеспечение защиты данных
- Планирование новых закупок
- Встречи с проектными менеджерами
- Информирование разработчиков об угрозах
- Аналитика данных на мошеннические действия
- Помощь в расследовании инсайдерских угроз
- Определение критичных данных в Хранилищах
- Расследование заражений систем
- Pen testing новых мобильный приложений
- Помощь ИТ-архитекторам в Zero-trust
- Ответы на почтовые запросы, касающиеся ИБ
- Редактирование отёчности для Управляющих
- Участие в найме персонала
- Написание планов тестирования
- Контроль и улучшение ИБ инфраструктуры

Слишком много Вендоров

Слишком много сложности

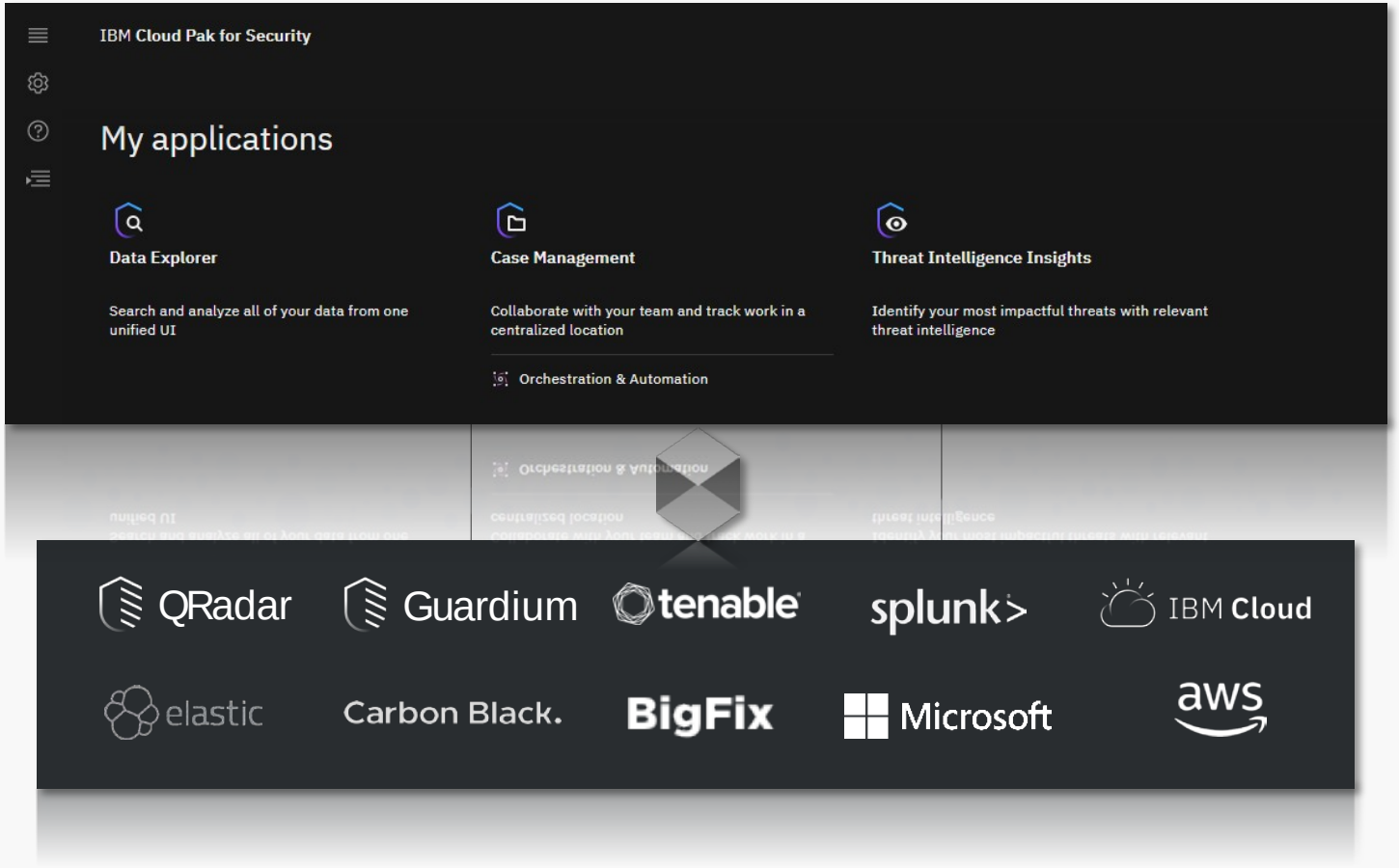


Слишком много алертов



Что такое платформа «IBM Cloud Pak for Security»?

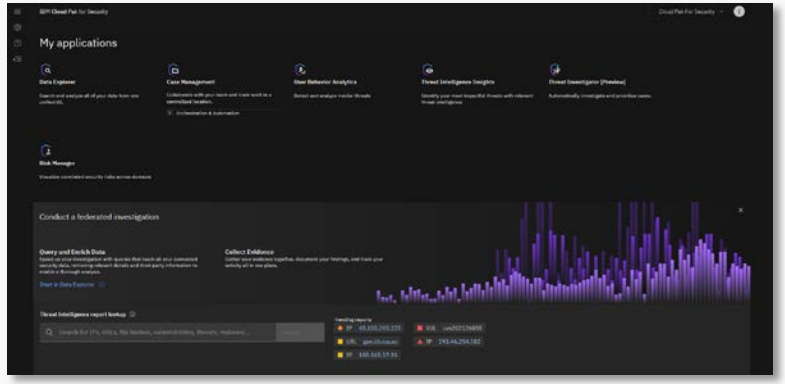
- Единый центр аналитики и реагирования
- Имеет готовые коннекторы ко многим из существующих инструментов безопасности
- Новые коннекторы создаются непрерывно
- Данные остаются там, где они есть

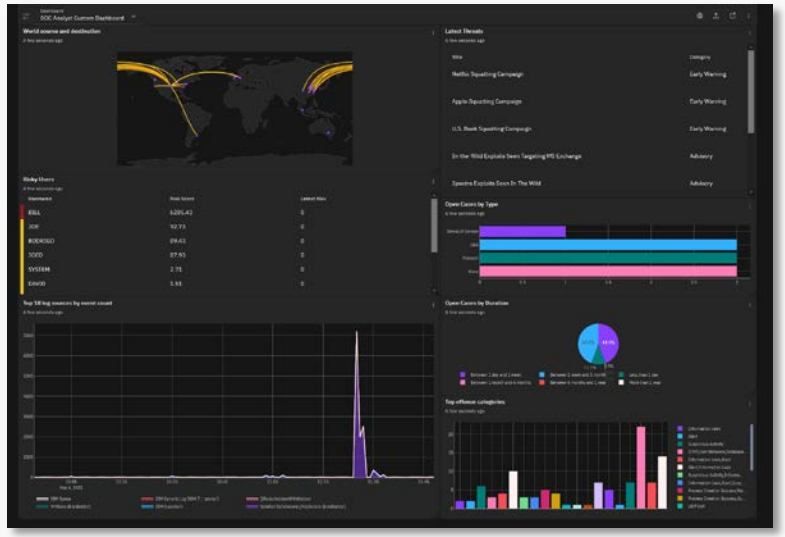


Что делает платформа «IBM Cloud Pak for Security»?

Объединяет системы защиты информации, СУБД, процессы реагирования для:

- Общего, глобального поиска в данных подключенных систем
- Исследования актуальных уязвимостей и угроз
- Расследования нарушений ИБ
- Реагирования на инциденты ИБ
- Наблюдения и анализа возможных рисков для Организации
- Глобальной аналитики поведения пользователей из всех источников данных





Какие инструменты встроены в платформу «IBM Cloud Pak for Security»?

Глобальный Поиск

- Видимость всех данных без перемещения
- Язык описания для обмена данными TI (STIX)
- Автоматическое обогащение данных и атрибутов
- Статистическая фокусировка без запросов
- Прямая интеграция с инцидентами в SOAR

SOAR

- Короткий промежуток между обнаружением и реагированием
- Поток и автоматизация
- Управляемый и быстрый запуск расследований с последовательным реагированием
- Настраиваемые и изменяемые динамические сценарии
- Соответствие требованиям

Аналитика Поведения Пользователей

- Быстрая идентификация рискованных пользователей, связанных с внутренними угрозами в рамках сквозного рабочего процесса
- Обогащение процесса унифицированного управления инсайдерскими угрозами
- Прямая интеграция с SOAR и Глобальным поиском

Исследование Угроз

- Глобальная информация об угрозах
- Определение приоритетности угроз для вашей организации с помощью X-Force Threat Score
- Идентифицируйте и действуйте в отношении угроз, активных в вашей среде, с помощью функции Am I Affected
- Использование сторонних каналов данных об угрозах

Менеджер Рисков Организации

- Интегрированный обзор состояния рисков в удобной для бизнеса приборной панели
- Ранняя информация о потенциальных рисках по сфере деятельности
- Визуализация потенциала воздействия
- Количественная оценка и передача информации о рисках безопасности на понятном языке

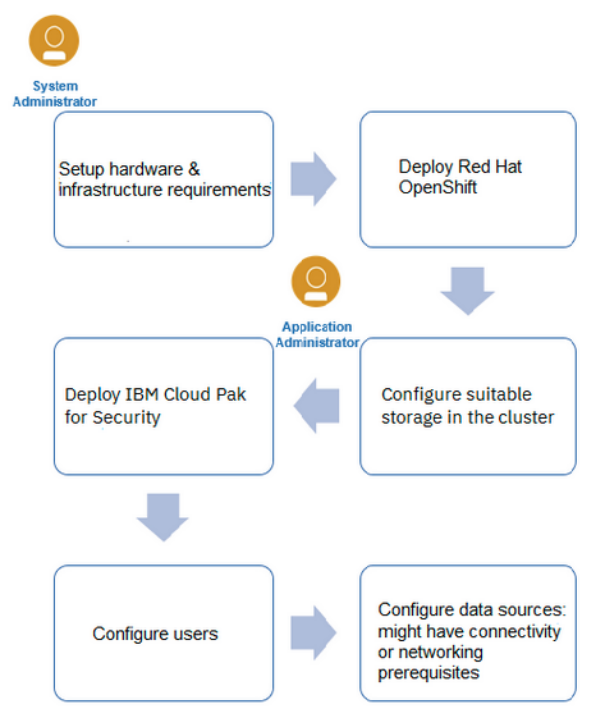
Расследование Угроз

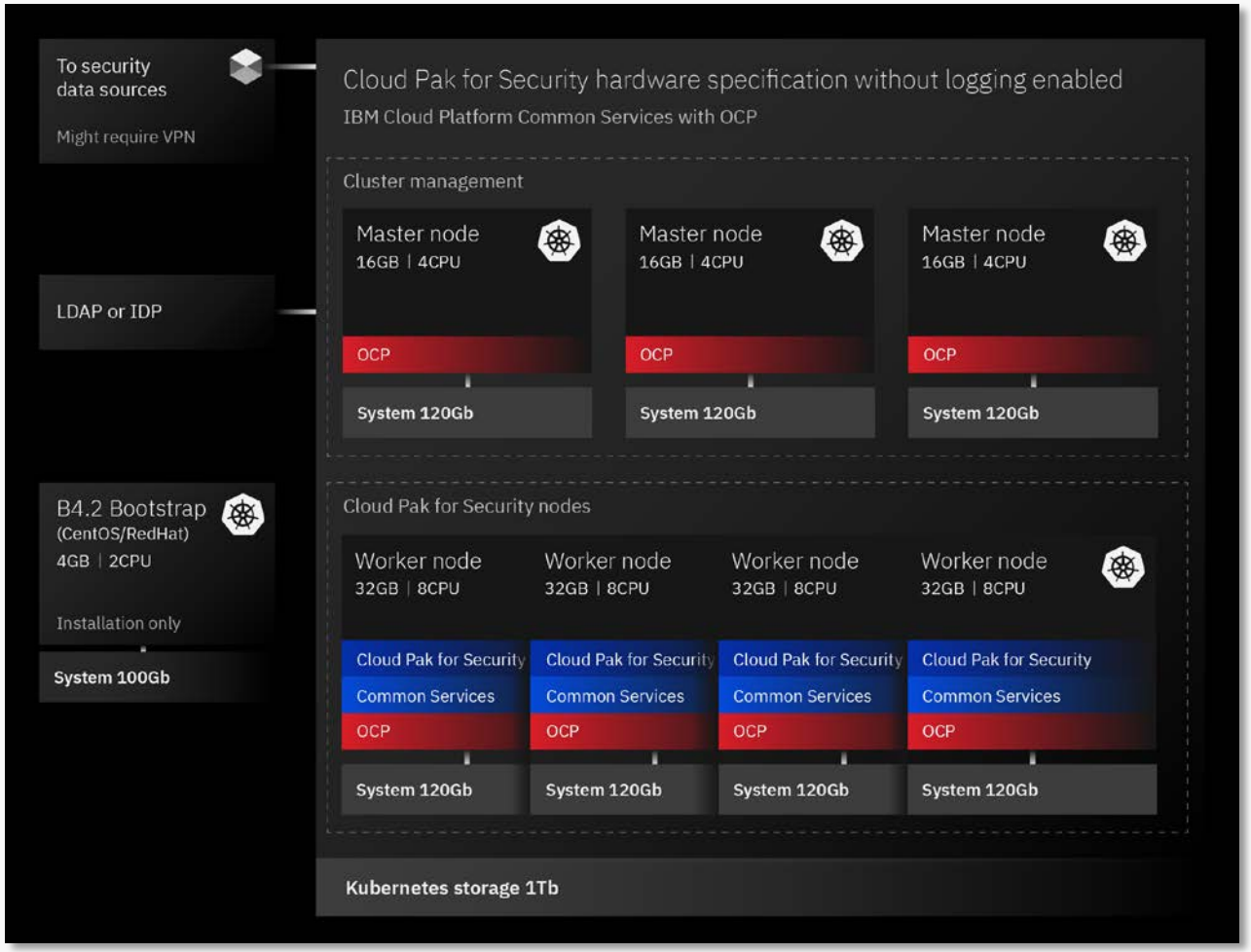
- Автоматическое исследование и расследование инцидентов
- Понимание источника и последствий атаки для эффективного реагирования
- Сопоставление расследований с матрицей MITRE ATT&CK tactics and techniques
- Представление временной шкалы инцидента

Аппаратные требования для установки платформы «IBM Cloud Pak for Security»

Устанавливается:

- В удобном вам Облаке
- На собственных серверах:





«IBM Cloud Pak for Security»

- **IBM Cloud Pak for Security** — платформа, построенная на контейнеризации, предварительно интегрированная с Red Hat OpenShift

- **IBM Cloud Pak for Security** — интегрирует существующие инструменты информационной безопасности без перемещения данных

- **IBM Cloud Pak for Security** — упрощение и ускорение расследований: Глобальный поиск позволяет расследовать угрозы и признаки взлома, используя все данные инструментов информационной безопасности и информацией из источников аналитических данных об угрозах

- **IBM Cloud Pak for Security** — комплексное реагирование на угрозы с помощью интегрированных приложений, средств автоматизации, приоритезации задач и обеспечения совместной работы аналитиков ОЦИБ

Преимущество лицензирования «IBM Cloud Pak for Security Domains solutions»

- Вы можете выбрать Пакет, который вам необходим в зависимости от решаемых задач
- Вы можете выбрать любую из Систем входящую в Пакет
- Вы неограниченны в типах и объёме обрабатываемых данных
- Вы неограниченны в применении точек сбора, мониторинга и контроля
- Вы неограниченны в команде реагирования
- Вы неограниченны в интеграциях и автоматизации

Вывод

Построение и использование новой политики лицензирования, экосистемы «IBM Security» и платформы «IBM Cloud pak for Security», даёт широкие возможности и инструменты для выявления и реагирования на критичные и современные угрозы и уязвимости для всех информационных инфраструктур в Организациях