



ICORE

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



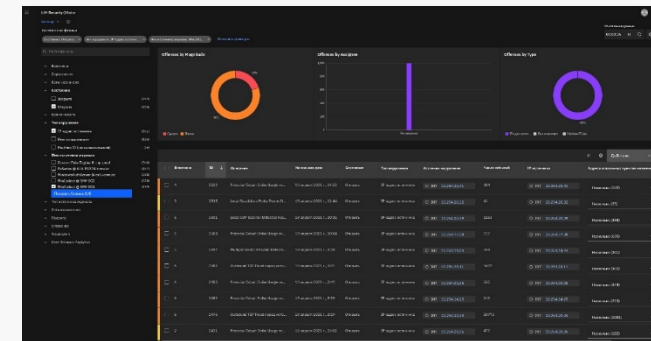
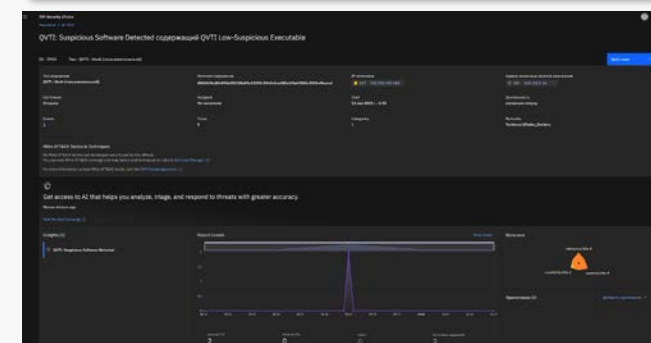
Преимущества использования обновлённого лицензирования «IBM Cloud Pak for Security» для IBM Security QRadar SIEM

- 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 отдельных 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**

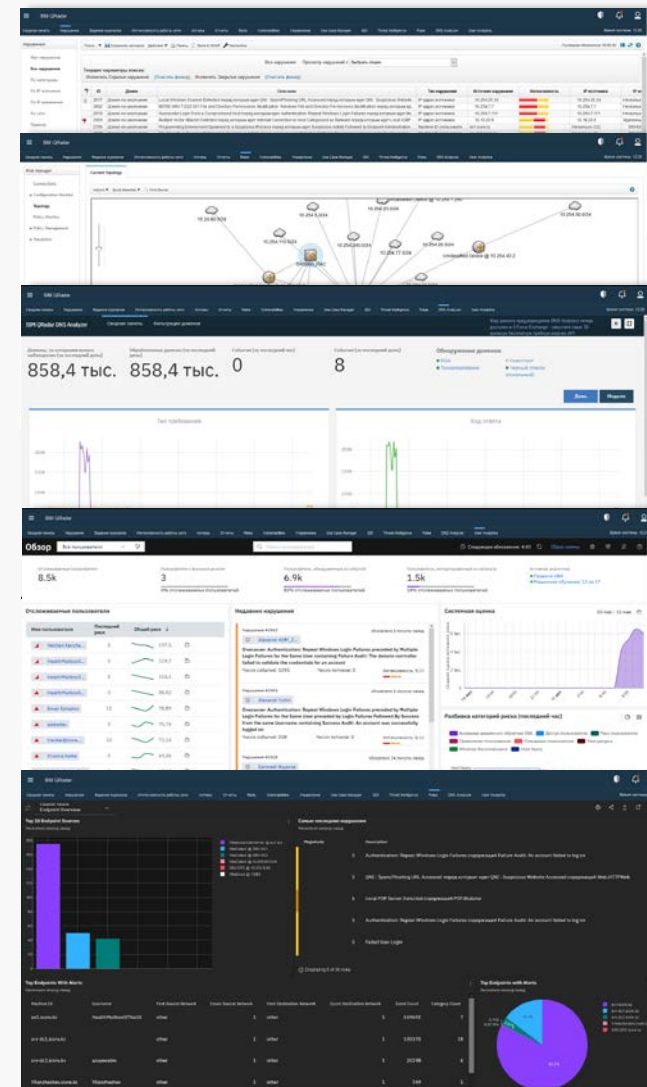
This screenshot displays a detailed view of a selected event within the IBM QRadar SIEM interface. It shows a hierarchical tree on the left and a main pane with various tabs and data fields, including logs, network flow data, and application details, all presented in a structured, tabular format.



Расширяем IBM Security QRadar SIEM

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

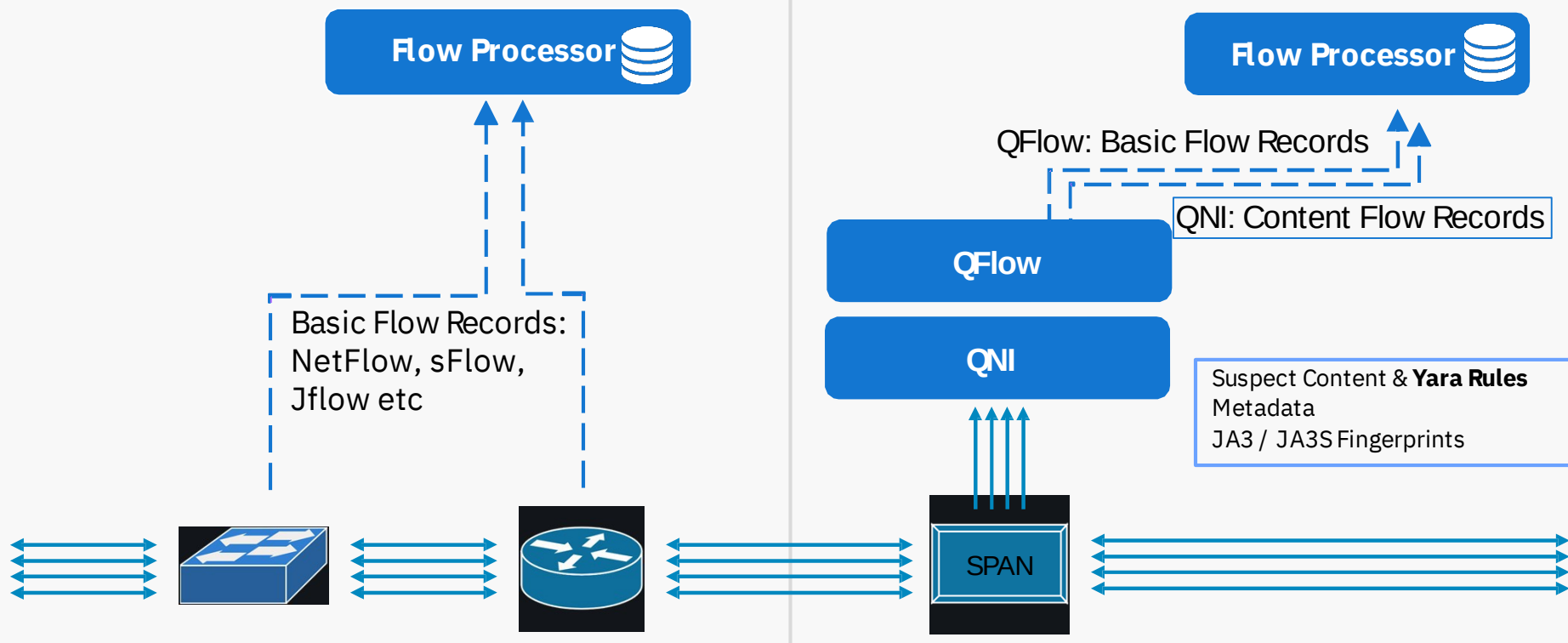
- **Применение отказоустойчивости для любого узла без затрат на лицензии**
- **Подключение Филиалов без затрат на лицензии** – установка гибридных коллекторов/процессоров для сбора событий и сетевых потоков на любое количество Организаций и без ограничений на ёмкость EPS / FPM
- **Построение Data Lake 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)

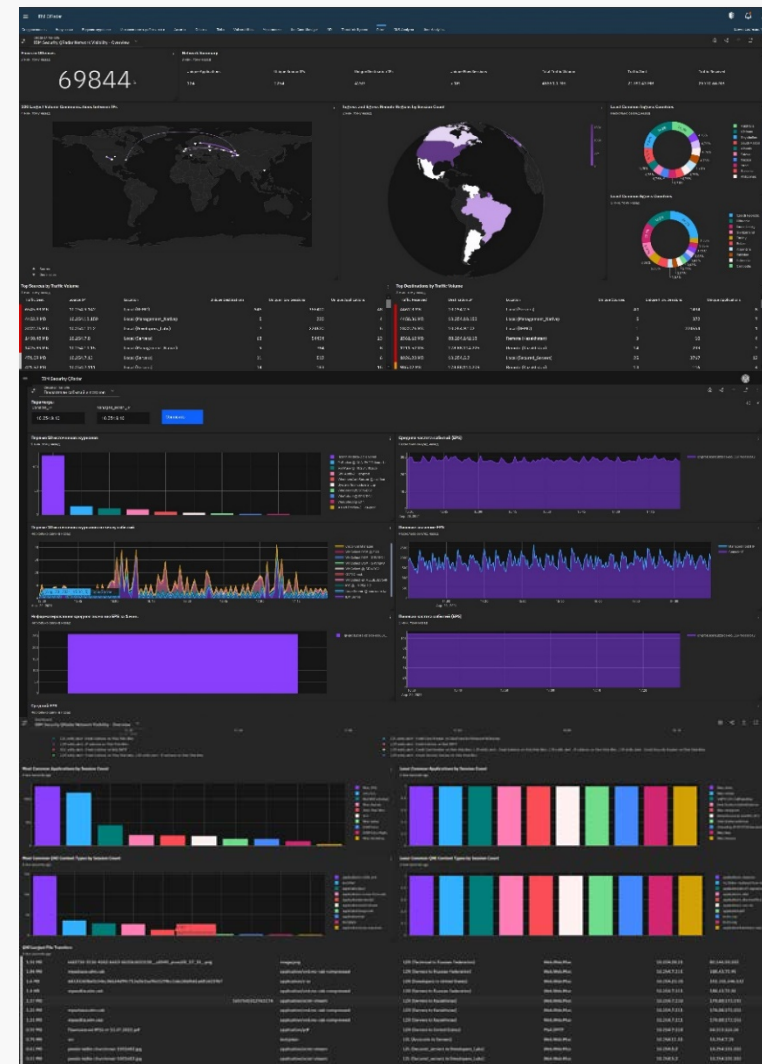
Сетевая видимость в аналитике потоков (сетевые коммуникации) и полная инспекция пакетов (**QRadar Network Insights**)





IBM Security QRadar Network Insights

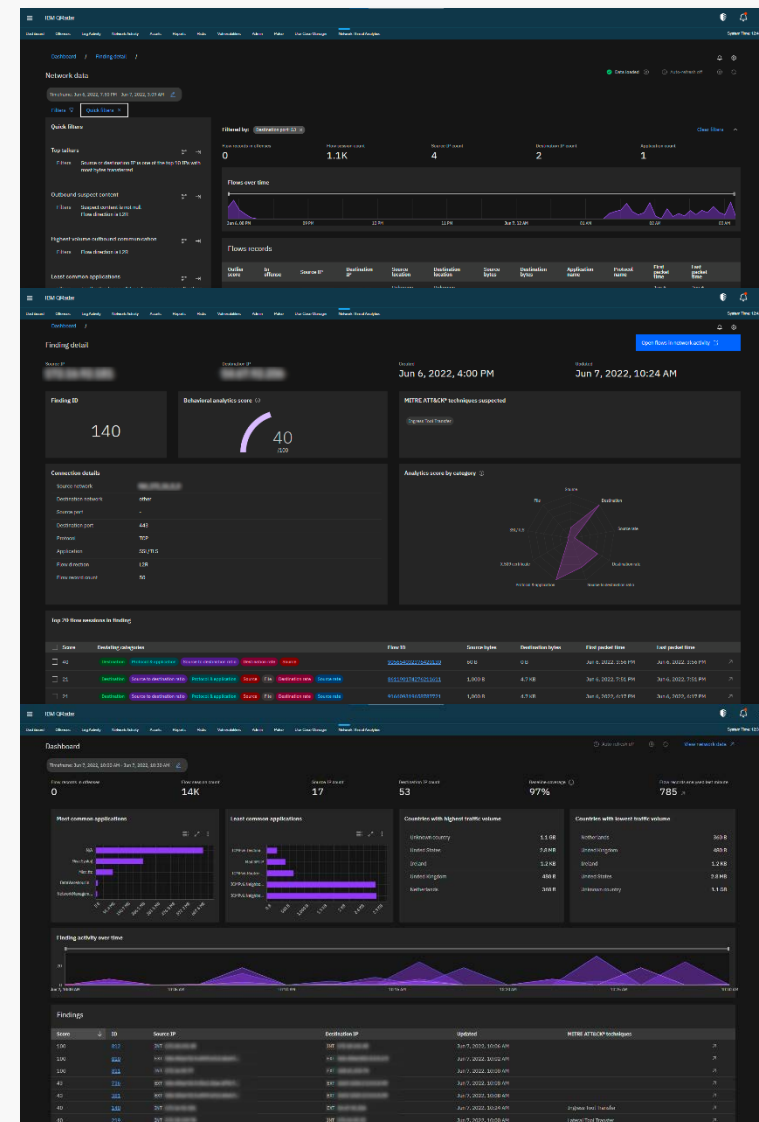
- Встроенный сетевой мониторинг и анализ сетевых потоков (**QFlow**) сразу из коробки и с использованием большого количества приложений и наборов готовых правил:
 - +64 Bytes, +Applications
- Модуль «**QRadar Network Insight**» в виде виртуального сервера для детального анализа сетевых потоков (не требует 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

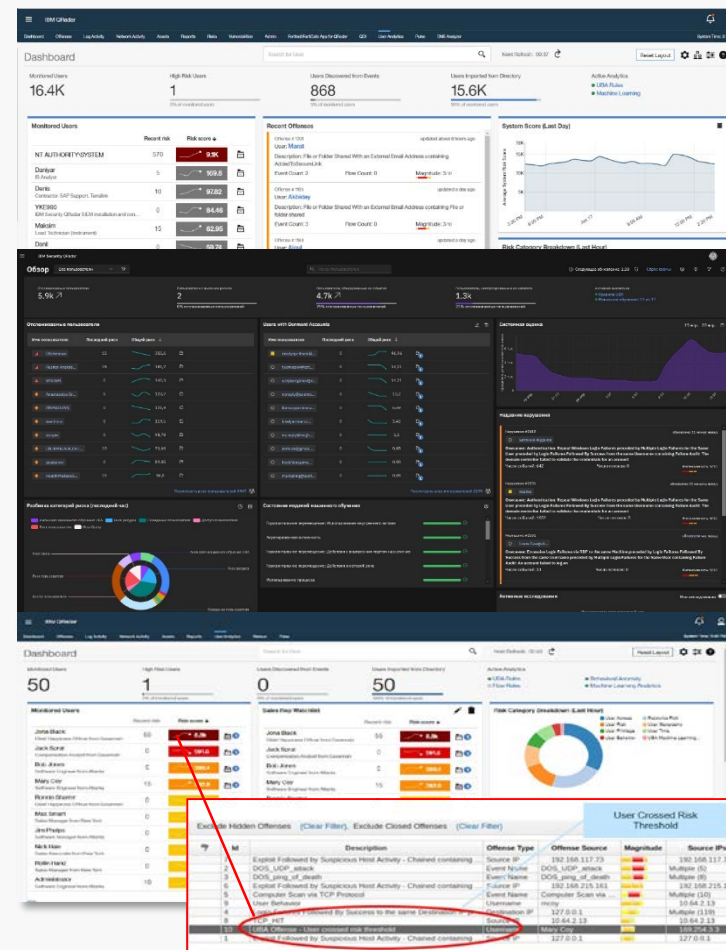
- Модуль постоянно отслеживает сетевые потоки в вашей сети для выявления аномального трафика
- Подробные дашборды предоставляют визуализацию показывающую, какие записи потока больше всего отклоняются от других записей потока, обычно наблюдаемых в сети Организации
- Подробные дашборды помогают быстро 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

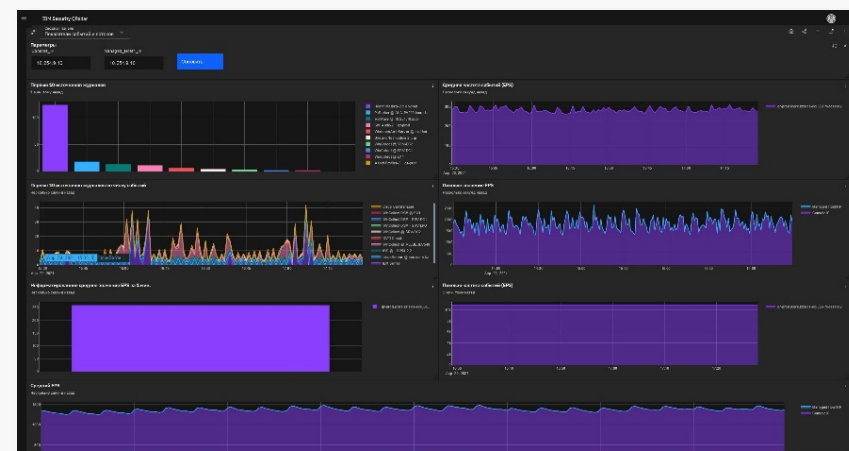
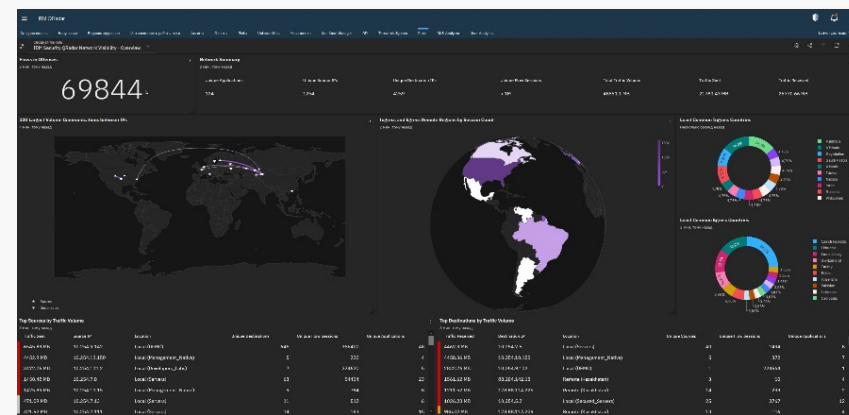
- Модуль непрерывно анализирует и запоминает поведение пользователей
- Использует алгоритмы машинного обучения
- Строит графики аномального поведения пользователей
- Оповещает офицеров безопасности о аномальном (необычном) поведении пользователя
- Позволяет создавать собственные математические модели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





IBM Security QRadar SIEM - PULSE

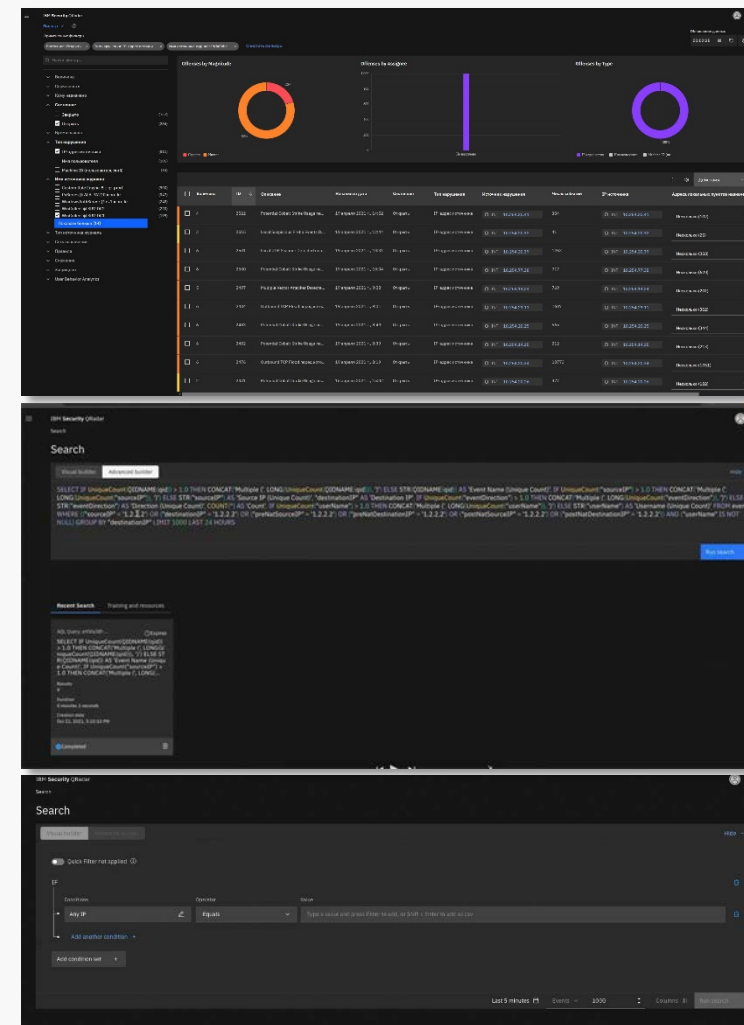
- Готовая основа для мониторинга в ОЦИБ
- Конструируемая визуализация под задачи
- Создание дашбордов на основе своих запросов
- Показ дашбордов на любом количестве экранов
- Наблюдение за ситуацией в реальном времени
- Загружаемые дашборды из IBM App Exchange





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



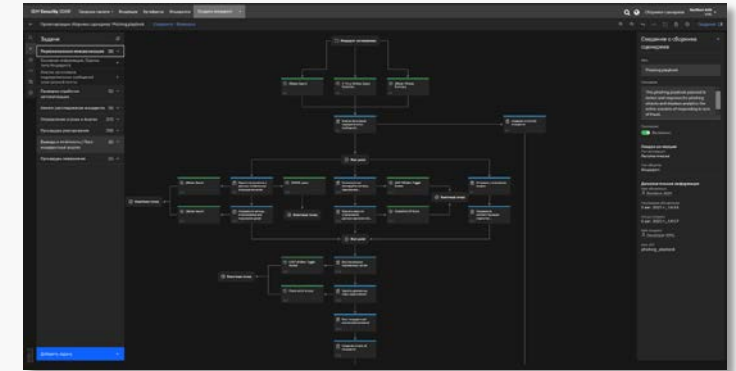


Преимущества использования обновлённого лицензирования «IBM Cloud Pak for Security» для IBM Security SOAR

- 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



Cisco ASA Network Objects									
Search Print Export									
Query Date	Cisco ASA Firewall	Network Object Group	Object Kind	Object Value	Object ID	Object Description	Status		
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Address	2001:db8:abcd::2::	—	—	Active		
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Network	10.1.1.0/24	—	—	Active		
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Address	10.2.2.4	—	—	Active		
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Address	10.2.2.78	—	—	Active		
03/24/2021 03:43:37	firewall_1	BLOCKLIST_IN	IPv4Address	7.7.7.0	—	—	Blocked		
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Network	7.7.7.0/24	IPNetwork7	—	Active		
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4FQDN	www.fdn.com	TESTFQDN	—	Active		
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Range	4.4.4.4-4.4.4.10	TESTRange4	—	Active		
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Range	7.7.7.0-7.7.7.10	Range7.0-7.10	Range7.0-7.10	Active		

[illegible]



Полностью настраиваемый интерфейс платформы - легко адаптируется под казахский язык

IBM Security SOAR

Сводные панели | Входящие | Артефакты | Инциденты | Создать инцидент

Параметры настройки

Мастеры | Правила | Сценарии | Поток операций | Функции | Целевые расположения | Этапы

Мастер Создать инц...
Вкладки инцидента
Закреть инцидент

Новый мастер

Опишите инцидент

Опишите и назовите инцидент

Тип инцидента

Описание инцидента

Имя инцидента

Источник угрозы

Кто сообщил об инциденте

Подтверждение инцидента

Дата и место

Изменить поле инцидента

Тип поля: Выберите

Метка поля: Вирус или Нет

Требование: Обязательно

Имя для доступа в API: virus_or_not

Подсказка: Описание этого поля.

Заменитель: Значения заменителя

Отслеживать время изменения

Добавить/изменить значения

Да

Нет

Неизвестно (по умолчанию)

Выберите одну из опций в качестве опции по умолчанию.

Пустая опция: Нет

Фильтр будет отображаться для списков выбора с более чем 10 опциями.

Сохранить

Поля

Адрес

Была ли вовлечена личная информация или личные данные?

Были ли данные зашифрованы

Важная информация на устройстве

Векторы атак Национального института стандартов и технологий

Вероятность воздействия

Вероятность неправильного использования закона о защите персональной информации и электронных документов

Вирус или Нет

Включены ли методы расследования

Представления

Адрес

Выбор членства

Просмотр вовлеченности сотрудников

Просмотр криминального статуса

Affected Individuals

Конструктор мастера инцидентов

Параметры настройки

Мастеры | Правила | Сценарии | Поток операций | Функции | Целевые расположения | Этапы и задачи | Типы инцидентов | Вещи | Типы артефактов

Мастер Создать инц...
Вкладки инцидента
Управление вкладками
Раздел отбора
Задачи реагирования
Детали инцидента
Вещи / Документы
Задачи / Документы
Участники процесса
Дата событий реагирования
Вложения / Упоминания
Статистика реагирования
Временная шкала
Артефакты инцидента
Электронная почта
Запланированное время
Добавить вкладку
Закреть инцидент

Инцидент: Управление вкладками

Вкладки

Детали инцидента

Вещи / Документы

Задачи / Документы

Участники процесса

Дата событий реагирования

Вложения / Упоминания

Статистика реагирования

Временная шкала

Артефакты инцидента

Электронная почта

Запланированное время

Добавить вкладку

Закреть инцидент

Этапы и задачи

Вы можете создавать инструкции и задавать задачи, а также назначать им исполнителей. Пользователи могут создавать задачи, назначать им исполнителей и задавать задачи. Для выполнения задачи необходимо выполнить следующие шаги:

Шаг 1: Проверка информации о инциденте

Шаг 2: Проверка информации о инциденте

Шаг 3: Проверка информации о инциденте

Шаг 4: Проверка информации о инциденте

Шаг 5: Проверка информации о инциденте

Шаг 6: Проверка информации о инциденте

Шаг 7: Проверка информации о инциденте

Шаг 8: Проверка информации о инциденте

Шаг 9: Проверка информации о инциденте

Шаг 10: Проверка информации о инциденте

Конструктор представления реагирования

Создание задач и инструкций

Упомянутые вами участники шаг в мастера создания нового инцидента, добавляйте компоненты (включая новые пользовательские поля) в мастер инцидента путем переноса компонентов из правого столбца в раздел мастера Создать инцидент. Новые шаги можно создать, выбрав команду "Добавить шаг" и переноса поля мышью.



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

Элементы управления инцидентом

Описание инцидента

Summary/Сводка

Задачи реагирования

Детали Инцидента

Записи / Документирование процесса

Участники процесса реагирования

Лента событий реагирования

Вложения / Улики

Статистика реагирования

Временная шкала

Артефакты инцидента

Электронная почта

Затраченное время на реагирование

90% Выполнено

Этапы и задачи реагирования

Владелец: выбрано 0

Состояние: Активно

Выбор задачи

Добавить задачу

Имя задачи

Владелец

Срок выполнения

Флаги

Действия

Определение угрозы и анализ

Не назначено

Нет срока выполнения

Всегда можно добавить задачу и назначить ответственных

Контроль выполнения задачи – не закроется без выполнения условий

Описание задачи согласно нормативным документам

Первоначальная инициализация1

Процедуры реагирования1

Первоначальная инициализация

Подробный аудит действий

Инструкции

Для выполнения данной задачи необходимо:

- Принять решение о действительности Инцидента
- Указать наиболее подходящий Тип Инцидента.
- Указать Владеыца.
- Указать Департамент

Добавьте примечания к этой задаче, отражающие все ваши действия и первоначальные выводы. В случае возникновения вопросов по данной задаче, обращайтесь по контактам ниже:

Корпоративная почта: ASarkun@icore.kz
Сотовый номер: +77017569967

People/Люди

Кем создан инцидент

SOAR ADMINISTRATOR

Департамент

Владелец процесса реагирования

SOAR ADMINISTRATOR

Участники процесса реагирования

Нет участников.

Related Incidents/Связанные инциденты

#2110 nbk test
#2098 test4

Attachments/Вложения

Нет вложений.

Newsfeed/Новостная лента

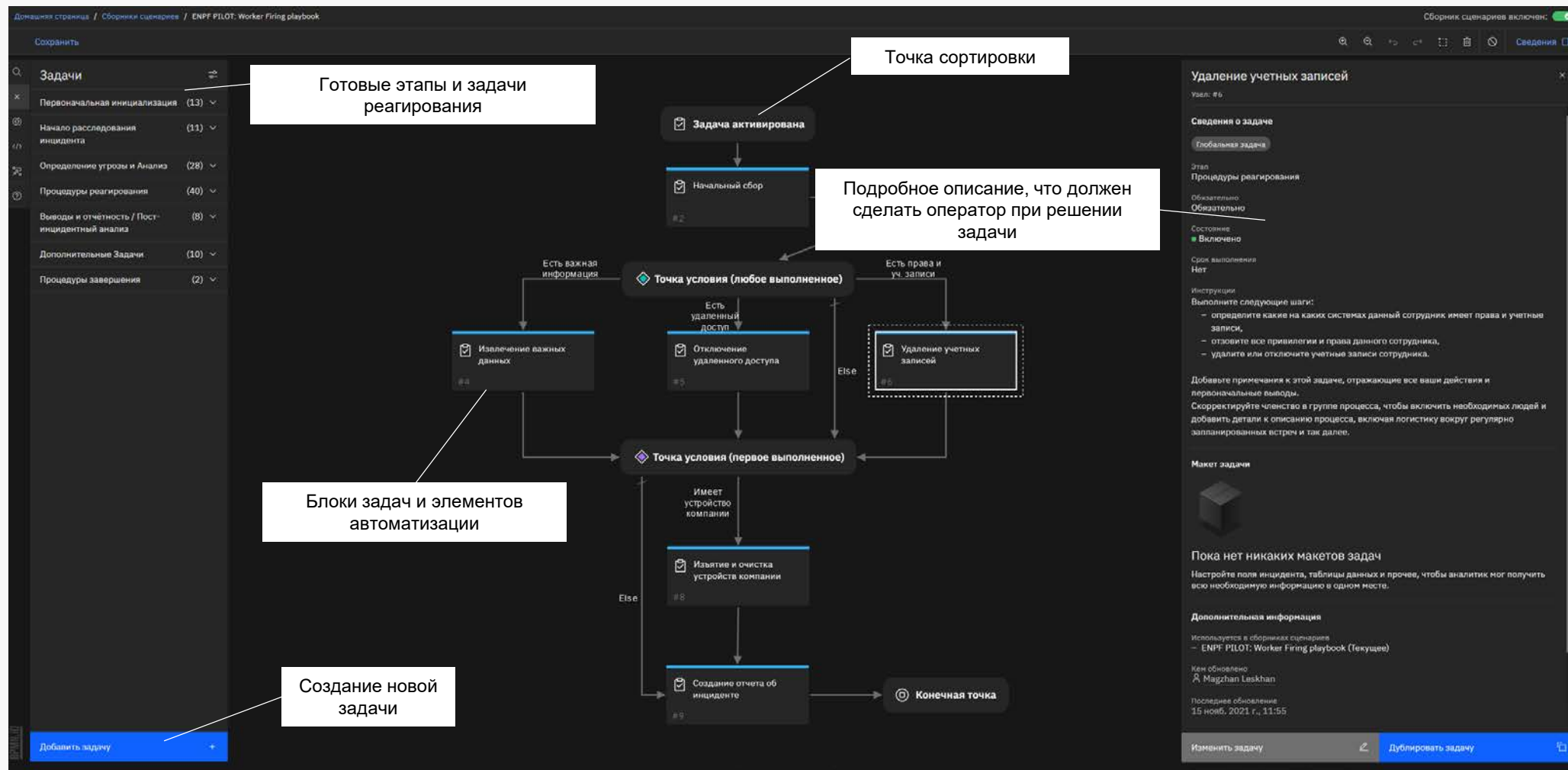
Пользователь System User изменил следующий элемент: Артефакт 118.193.42.155 01.09.2021 11:26:04

Пользователь SOAR ADMINISTRATOR обновил список задач в следующем элементе: Имитация 20.08.2021 09:38:29

Пользователь SOAR ADMINISTRATOR изменил состояние на Закрыто в следующем



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

Приложения

Требуется приложение?

Для расширения возможностей платформы SOAR доступен целый набор готовых к установке приложений и дополнений бизнес-партнеров.

IBM Безопасность App Exchange

fn_alienvault_otx
Resilient Labs
Версия: 1.0.1
A Resilient Function to integrate with the AlienVault OTX api/v1/indicators API
Состояние: Развертывание...

fn_api_void
IBM Resilient Labs
Версия: 1.0.0
Resilient Circuits Components for 'fn_api_void'
Состояние: Развертывание...

fn_checkpoint
IBM Resilient Labs
Версия: 1.0.0
Resilient Circuits Components for 'fn_checkpoint'
Состояние: Развертывание...

fn_components
Resilient Labs
Версия: 1.0.0
Resilient Circuits components for single-file integrations
Состояние: Развертывание...

fn_exchange
IBM Resilient Labs
Версия: 1.0.2
Resilient Circuits Components for 'fn_exchange'
Состояние: Развертывание...

fn_greynoise
Resilient Labs
Версия: 1.0.3
Resilient Circuits Components for 'fn_greynoise'
Состояние: Развертывание...

fn_ipinfo
Resilient Labs
Версия: 1.0.1
Resilient Circuits Components for 'fn_ipinfo'
Состояние: Развертывание...

ipstack
Resilient Labs
Версия: 1.0.0
Resilient Circuits Components for 'ipstack'
Состояние: Перезапуск...

fn_ldap_utilities
IBM Resilient Labs
Версия: 1.0.1
Resilient Circuits LDAP Utilities
Состояние: Развертывание...

fn_misp
Resilient Labs
Версия: 1.0.3
Creates Events, Attributes and Sightings in MISP from incidents and artifacts in...
Состояние: Ожидание настроек...

fn_odbc_query
IBM Resilient Labs
Версия: 1.0.3
Resilient Circuits Components for 'fn_odbc_query'
Состояние: Развертывание...

fn_outbound_email
IBM Resilient Labs
Версия: 1.0.0
Resilient Circuits Components for 'fn_outbound_email'
Состояние: Развертывание...

fn_pulsedive
Resilient Labs
Версия: 1.0.1
Resilient Circuits Components for 'fn_pulsedive'
Состояние: Развертывание...

fn_qradar_integration
IBM Resilient Labs
Версия: 2.1.1
Resilient Circuits Components for 'fn_qradar_integration'
Состояние: Готово к использованию...

fn_query_tor_network
Resilient Labs
Версия: 1.0.1
Resilient Circuits Components for 'fn_query_tor_network'
Состояние: Развертывание...

fn_scheduler
Resilient Labs
Версия: 1.0.0
Resilient Circuits Components for 'fn_scheduler'
Состояние: Развертывание...

SHODAN
Shodan
Resilient Labs
Версия: 1.0.0
Resilient Circuits Components for 'fn_shodan'
Состояние: Развертывание...

splunk>

ThreatMiner

YARA

RDAP

Cisco ASA Network Objects

Query Date Firewall Network Object Group Object Kind Object Value Object ID Object Description Status

03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv6Address	2001:db8:abcd:12::	—	—	Active
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Network	10.1.1.0/24	—	—	Active
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Address	10.2.2.4	—	—	Active
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Address	10.2.2.78	—	—	Active
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Address	7.7.7.0	—	—	Removed
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Network	7.7.7.0/24	IPNetwork7	—	Active
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4FQDN	www.qdn.com	TESTFQDN	—	Active
03/24/2021 03:41:17	firewall_1	BLOCKLIST_IN	IPv4Range	7.7.7.0-7.7.7.10	Ranges7.0-7.10	Ranges7.0-7.10	Active

Детализация от Cisco ASA

Playbook Usage

Report date Incident Type Playbook/Workflow Id Execution date Element type Element value

09/10/2021 15:50:51	Sentinel Incident 551 - Multi-stage incident involving Persistence & Credential access on one endpoint	workflow	Sentinel Get Incident Alerts	154	09/10/2021 08:43:13	incident	2663
09/10/2021 15:50:51	Sentinel Incident 551 - Multi-stage incident involving Persistence & Credential access on one endpoint	workflow	Sentinel Comment Sync	121	09/08/2021 17:58:21	note	Sentinel Incident 551 Multi-stage incident involving Persistence & Credential access on one endpoint
09/10/2021 15:50:51	Sentinel Incident 551 - Multi-stage incident involving Persistence & Credential access on one endpoint	workflow	Sentinel Get Incident Entities	120	09/08/2021 17:54:14	incident	2663
09/10/2021 15:50:51	Sentinel Incident 551 - Multi-stage incident involving Persistence & Credential access on one endpoint	workflow	Workflow Guardium Insights populate breach data types	151	09/08/2021 17:54:13	incident	2663

Индикаторы компрометации (IOC)

Детальная информация о связях между инцидентами



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

Изменить сценарий

Сведения о сценарии

Область применения сценария: Глобальный, Локальный

Имя сценария: Convert JSON to rich text v1.0

Описание (необязательно): This script converts a json object into a hierarchical display of rich text and adds the rich text to an incident's rich text (custom) field or an incident note. A workflow property is used to share the json to convert and identify parameters used on how to perform the conversion. Typically, a function will create workflow property and this script will run after that function to perform the conversion. Features: * Display the hierarchical nature of json, presenting the json keys (sorted if specified) as bold labels

Детальная страница / Сборка сценария / Publishing mail

Сохранить / Имя сценария

Функции

- fn_alertout_out
- fn_api_out
- fn_checkpoint
- fn_exchange
- Exchange Create Meeting
- Exchange Delete Emails
- Exchange Find Emails
- Exchange Get Mailbox Info
- Exchange Move Emails
- Exchange Move Folder Contents and Delete Folder
- Exchange Send Email
- fn_gynoise
- fn_ipinfo
- fn_ipstack
- fn_map_utilities
- fn_misp
- fn_odbc_query
- fn_outbound_email
- fn_pulselive
- fn_qradar_integration
- fn_query_for_network
- fn_scheduler
- fn_slack_integration
- fn_threatminer
- fn_utilities
- fn_unconnected

Запрос списка пользователей, кто мог получить письмо

АВТО: Добавление данных в таблицу пользователей

а проверки всех элементов

Запрос списка пользователей, кто открыл письмо

Создание скрипта сразу внутри Динамического сценария

Элементы автоматизации

Библиотека интеграций

Встроенный в систему интерпретатор Python

```
1 # (c) Copyright IBM Corp. 2018, 2020. All Rights Reserved.
2 VERSION = 1.0
3
4 This script converts a json object into a hierarchical display of rich text and adds the rich text to an incident's rich text (custom) field or an incident note. A workflow property is used to share the json to convert and identify parameters used on how to perform the conversion. Typically, a function will create workflow property and this script will run after that function to perform the conversion.
5 Features:
6 * Display the hierarchical nature of json, presenting the json keys (sorted if specified) as bold labels
7 * Provide links to found data
8 * Create either an incident note or add results to an incident (custom) rich text field.
9
10 In order to use this script, define a workflow property called: convert_json_to_rich_text, to define the json and workflow properties can be added using a command similar to this:
11 workflow.add_property('convert_json_to_rich_text', {
12     "json": {
13         "header": "Artifact scan results for: {format(artifact.value)}",
14         "payload": {
15             "results": [
16                 {
17                     "url": "https://www.example.com",
18                     "ip": "192.168.1.1",
19                     "domain": "example.com",
20                     "asn": "AS12345",
21                     "country": "US",
22                     "city": "New York",
23                     "state": "NY",
24                     "zip": "10001",
25                     "lat": "40.7128",
26                     "lon": "-74.0060",
27                     "org": "Example Corp",
28                     "type": "IP",
29                     "status": "Active",
30                     "last_seen": "2020-01-01",
31                     "first_seen": "2020-01-01",
32                     "last_updated": "2020-01-01",
33                     "first_updated": "2020-01-01",
34                     "last_modified": "2020-01-01",
35                     "first_modified": "2020-01-01",
36                     "last_deleted": "2020-01-01",
37                     "first_deleted": "2020-01-01",
38                     "last_created": "2020-01-01",
39                     "first_created": "2020-01-01",
40                     "last_updated_by": "Example Corp",
41                     "first_updated_by": "Example Corp",
42                     "last_modified_by": "Example Corp",
43                     "first_modified_by": "Example Corp",
44                     "last_deleted_by": "Example Corp",
45                     "first_deleted_by": "Example Corp",
46                     "last_created_by": "Example Corp",
47                     "first_created_by": "Example Corp",
48                     "last_updated_at": "2020-01-01T00:00:00Z",
49                     "first_updated_at": "2020-01-01T00:00:00Z",
50                     "last_modified_at": "2020-01-01T00:00:00Z",
51                     "first_modified_at": "2020-01-01T00:00:00Z",
52                     "last_deleted_at": "2020-01-01T00:00:00Z",
53                     "first_deleted_at": "2020-01-01T00:00:00Z",
54                     "last_created_at": "2020-01-01T00:00:00Z",
55                     "first_created_at": "2020-01-01T00:00:00Z",
56                     "last_updated_by_email": "Example Corp",
57                     "first_updated_by_email": "Example Corp",
58                     "last_modified_by_email": "Example Corp",
59                     "first_modified_by_email": "Example Corp",
60                     "last_deleted_by_email": "Example Corp",
61                     "first_deleted_by_email": "Example Corp",
62                     "last_created_by_email": "Example Corp",
63                     "first_created_by_email": "Example Corp",
64                     "last_updated_at_email": "2020-01-01T00:00:00Z",
65                     "first_updated_at_email": "2020-01-01T00:00:00Z",
66                     "last_modified_at_email": "2020-01-01T00:00:00Z",
67                     "first_modified_at_email": "2020-01-01T00:00:00Z",
68                     "last_deleted_at_email": "2020-01-01T00:00:00Z",
69                     "first_deleted_at_email": "2020-01-01T00:00:00Z",
70                     "last_created_at_email": "2020-01-01T00:00:00Z",
71                     "first_created_at_email": "2020-01-01T00:00:00Z",
72                     "last_updated_by_phone": "Example Corp",
73                     "first_updated_by_phone": "Example Corp",
74                     "last_modified_by_phone": "Example Corp",
75                     "first_modified_by_phone": "Example Corp",
76                     "last_deleted_by_phone": "Example Corp",
77                     "first_deleted_by_phone": "Example Corp",
78                     "last_created_by_phone": "Example Corp",
79                     "first_created_by_phone": "Example Corp",
80                     "last_updated_at_phone": "2020-01-01T00:00:00Z",
81                     "first_updated_at_phone": "2020-01-01T00:00:00Z",
82                     "last_modified_at_phone": "2020-01-01T00:00:00Z",
83                     "first_modified_at_phone": "2020-01-01T00:00:00Z",
84                     "last_deleted_at_phone": "2020-01-01T00:00:00Z",
85                     "first_deleted_at_phone": "2020-01-01T00:00:00Z",
86                     "last_created_at_phone": "2020-01-01T00:00:00Z",
87                     "first_created_at_phone": "2020-01-01T00:00:00Z",
88                     "last_updated_by_address": "Example Corp",
89                     "first_updated_by_address": "Example Corp",
90                     "last_modified_by_address": "Example Corp",
91                     "first_modified_by_address": "Example Corp",
92                     "last_deleted_by_address": "Example Corp",
93                     "first_deleted_by_address": "Example Corp",
94                     "last_created_by_address": "Example Corp",
95                     "first_created_by_address": "Example Corp",
96                     "last_updated_at_address": "2020-01-01T00:00:00Z",
97                     "first_updated_at_address": "2020-01-01T00:00:00Z",
98                     "last_modified_at_address": "2020-01-01T00:00:00Z",
99                     "first_modified_at_address": "2020-01-01T00:00:00Z",
100                     "last_deleted_at_address": "2020-01-01T00:00:00Z",
101                     "first_deleted_at_address": "2020-01-01T00:00:00Z",
102                     "last_created_at_address": "2020-01-01T00:00:00Z",
103                     "first_created_at_address": "2020-01-01T00:00:00Z",
104                     "last_updated_by_city": "Example Corp",
105                     "first_updated_by_city": "Example Corp",
106                     "last_modified_by_city": "Example Corp",
107                     "first_modified_by_city": "Example Corp",
108                     "last_deleted_by_city": "Example Corp",
109                     "first_deleted_by_city": "Example Corp",
110                     "last_created_by_city": "Example Corp",
111                     "first_created_by_city": "Example Corp",
112                     "last_updated_at_city": "2020-01-01T00:00:00Z",
113                     "first_updated_at_city": "2020-01-01T00:00:00Z",
114                     "last_modified_at_city": "2020-01-01T00:00:00Z",
115                     "first_modified_at_city": "2020-01-01T00:00:00Z",
116                     "last_deleted_at_city": "2020-01-01T00:00:00Z",
117                     "first_deleted_at_city": "2020-01-01T00:00:00Z",
118                     "last_created_at_city": "2020-01-01T00:00:00Z",
119                     "first_created_at_city": "2020-01-01T00:00:00Z",
120                     "last_updated_by_state": "Example Corp",
121                     "first_updated_by_state": "Example Corp",
122                     "last_modified_by_state": "Example Corp",
123                     "first_modified_by_state": "Example Corp",
124                     "last_deleted_by_state": "Example Corp",
125                     "first_deleted_by_state": "Example Corp",
126                     "last_created_by_state": "Example Corp",
127                     "first_created_by_state": "Example Corp",
128                     "last_updated_at_state": "2020-01-01T00:00:00Z",
129                     "first_updated_at_state": "2020-01-01T00:00:00Z",
130                     "last_modified_at_state": "2020-01-01T00:00:00Z",
131                     "first_modified_at_state": "2020-01-01T00:00:00Z",
132                     "last_deleted_at_state": "2020-01-01T00:00:00Z",
133                     "first_deleted_at_state": "2020-01-01T00:00:00Z",
134                     "last_created_at_state": "2020-01-01T00:00:00Z",
135                     "first_created_at_state": "2020-01-01T00:00:00Z",
136                     "last_updated_by_zip": "Example Corp",
137                     "first_updated_by_zip": "Example Corp",
138                     "last_modified_by_zip": "Example Corp",
139                     "first_modified_by_zip": "Example Corp",
140                     "last_deleted_by_zip": "Example Corp",
141                     "first_deleted_by_zip": "Example Corp",
142                     "last_created_by_zip": "Example Corp",
143                     "first_created_by_zip": "Example Corp",
144                     "last_updated_at_zip": "2020-01-01T00:00:00Z",
145                     "first_updated_at_zip": "2020-01-01T00:00:00Z",
146                     "last_modified_at_zip": "2020-01-01T00:00:00Z",
147                     "first_modified_at_zip": "2020-01-01T00:00:00Z",
148                     "last_deleted_at_zip": "2020-01-01T00:00:00Z",
149                     "first_deleted_at_zip": "2020-01-01T00:00:00Z",
150                     "last_created_at_zip": "2020-01-01T00:00:00Z",
151                     "first_created_at_zip": "2020-01-01T00:00:00Z",
152                     "last_updated_by_lat": "Example Corp",
153                     "first_updated_by_lat": "Example Corp",
154                     "last_modified_by_lat": "Example Corp",
155                     "first_modified_by_lat": "Example Corp",
156                     "last_deleted_by_lat": "Example Corp",
157                     "first_deleted_by_lat": "Example Corp",
158                     "last_created_by_lat": "Example Corp",
159                     "first_created_by_lat": "Example Corp",
160                     "last_updated_at_lat": "2020-01-01T00:00:00Z",
161                     "first_updated_at_lat": "2020-01-01T00:00:00Z",
162                     "last_modified_at_lat": "2020-01-01T00:00:00Z",
163                     "first_modified_at_lat": "2020-01-01T00:00:00Z",
164                     "last_deleted_at_lat": "2020-01-01T00:00:00Z",
165                     "first_deleted_at_lat": "2020-01-01T00:00:00Z",
166                     "last_created_at_lat": "2020-01-01T00:00:00Z",
167                     "first_created_at_lat": "2020-01-01T00:00:00Z",
168                     "last_updated_by_lon": "Example Corp",
169                     "first_updated_by_lon": "Example Corp",
170                     "last_modified_by_lon": "Example Corp",
171                     "first_modified_by_lon": "Example Corp",
172                     "last_deleted_by_lon": "Example Corp",
173                     "first_deleted_by_lon": "Example Corp",
174                     "last_created_by_lon": "Example Corp",
175                     "first_created_by_lon": "Example Corp",
176                     "last_updated_at_lon": "2020-01-01T00:00:00Z",
177                     "first_updated_at_lon": "2020-01-01T00:00:00Z",
178                     "last_modified_at_lon": "2020-01-01T00:00:00Z",
179                     "first_modified_at_lon": "2020-01-01T00:00:00Z",
180                     "last_deleted_at_lon": "2020-01-01T00:00:00Z",
181                     "first_deleted_at_lon": "2020-01-01T00:00:00Z",
182                     "last_created_at_lon": "2020-01-01T00:00:00Z",
183                     "first_created_at_lon": "2020-01-01T00:00:00Z",
184                     "last_updated_by_org": "Example Corp",
185                     "first_updated_by_org": "Example Corp",
186                     "last_modified_by_org": "Example Corp",
187                     "first_modified_by_org": "Example Corp",
188                     "last_deleted_by_org": "Example Corp",
189                     "first_deleted_by_org": "Example Corp",
190                     "last_created_by_org": "Example Corp",
191                     "first_created_by_org": "Example Corp",
192                     "last_updated_at_org": "2020-01-01T00:00:00Z",
193                     "first_updated_at_org": "2020-01-01T00:00:00Z",
194                     "last_modified_at_org": "2020-01-01T00:00:00Z",
195                     "first_modified_at_org": "2020-01-01T00:00:00Z",
196                     "last_deleted_at_org": "2020-01-01T00:00:00Z",
197                     "first_deleted_at_org": "2020-01-01T00:00:00Z",
198                     "last_created_at_org": "2020-01-01T00:00:00Z",
199                     "first_created_at_org": "2020-01-01T00:00:00Z",
200                     "last_updated_by_type": "Example Corp",
201                     "first_updated_by_type": "Example Corp",
202                     "last_modified_by_type": "Example Corp",
203                     "first_modified_by_type": "Example Corp",
204                     "last_deleted_by_type": "Example Corp",
205                     "first_deleted_by_type": "Example Corp",
206                     "last_created_by_type": "Example Corp",
207                     "first_created_by_type": "Example Corp",
208                     "last_updated_at_type": "2020-01-01T00:00:00Z",
209                     "first_updated_at_type": "2020-01-01T00:00:00Z",
210                     "last_modified_at_type": "2020-01-01T00:00:00Z",
211                     "first_modified_at_type": "2020-01-01T00:00:00Z",
212                     "last_deleted_at_type": "2020-01-01T00:00:00Z",
213                     "first_deleted_at_type": "2020-01-01T00:00:00Z",
214                     "last_created_at_type": "2020-01-01T00:00:00Z",
215                     "first_created_at_type": "2020-01-01T00:00:00Z",
216                     "last_updated_by_status": "Example Corp",
217                     "first_updated_by_status": "Example Corp",
218                     "last_modified_by_status": "Example Corp",
219                     "first_modified_by_status": "Example Corp",
220                     "last_deleted_by_status": "Example Corp",
221                     "first_deleted_by_status": "Example Corp",
222                     "last_created_by_status": "Example Corp",
223                     "first_created_by_status": "Example Corp",
224                     "last_updated_at_status": "2020-01-01T00:00:00Z",
225                     "first_updated_at_status": "2020-01-01T00:00:00Z",
226                     "last_modified_at_status": "2020-01-01T00:00:00Z",
227                     "first_modified_at_status": "2020-01-01T00:00:00Z",
228                     "last_deleted_at_status": "2020-01-01T00:00:00Z",
229                     "first_deleted_at_status": "2020-01-01T00:00:00Z",
230                     "last_created_at_status": "2020-01-01T00:00:00Z",
231                     "first_created_at_status": "2020-01-01T00:00:00Z",
232                     "last_updated_by_last_seen": "Example Corp",
233                     "first_updated_by_last_seen": "Example Corp",
234                     "last_modified_by_last_seen": "Example Corp",
235                     "first_modified_by_last_seen": "Example Corp",
236                     "last_deleted_by_last_seen": "Example Corp",
237                     "first_deleted_by_last_seen": "Example Corp",
238                     "last_created_by_last_seen": "Example Corp",
239                     "first_created_by_last_seen": "Example Corp",
240                     "last_updated_at_last_seen": "2020-01-01T00:00:00Z",
241                     "first_updated_at_last_seen": "2020-01-01T00:00:00Z",
242                     "last_modified_at_last_seen": "2020-01-01T00:00:00Z",
243                     "first_modified_at_last_seen": "2020-01-01T00:00:00Z",
244                     "last_deleted_at_last_seen": "2020-01-01T00:00:00Z",
245                     "first_deleted_at_last_seen": "2020-01-01T00:00:00Z",
246                     "last_created_at_last_seen": "2020-01-01T00:00:00Z",
247                     "first_created_at_last_seen": "2020-01-01T00:00:00Z",
248                     "last_updated_by_first_seen": "Example Corp",
249                     "first_updated_by_first_seen": "Example Corp",
250                     "last_modified_by_first_seen": "Example Corp",
251                     "first_modified_by_first_seen": "Example Corp",
252                     "last_deleted_by_first_seen": "Example Corp",
253                     "first_deleted_by_first_seen": "Example Corp",
254                     "last_created_by_first_seen": "Example Corp",
255                     "first_created_by_first_seen": "Example Corp",
256                     "last_updated_at_first_seen": "2020-01-01T00:00:00Z",
257                     "first_updated_at_first_seen": "2020-01-01T00:00:00Z",
258                     "last_modified_at_first_seen": "2020-01-01T00:00:00Z",
259                     "first_modified_at_first_seen": "2020-01-01T00:00:00Z",
260                     "last_deleted_at_first_seen": "2020-01-01T00:00:00Z",
261                     "first_deleted_at_first_seen": "2020-01-01T00:00:00Z",
262                     "last_created_at_first_seen": "2020-01-01T00:00:00Z",
263                     "first_created_at_first_seen": "2020-01-01T00:00:00Z",
264                     "last_updated_by_last_updated": "Example Corp",
265                     "first_updated_by_last_updated": "Example Corp",
266                     "last_modified_by_last_updated": "Example Corp",
267                     "first_modified_by_last_updated": "Example Corp",
268                     "last_deleted_by_last_updated": "Example Corp",
269                     "first_deleted_by_last_updated": "Example Corp",
270                     "last_created_by_last_updated": "Example Corp",
271                     "first_created_by_last_updated": "Example Corp",
272                     "last_updated_at_last_updated": "2020-01-01T00:00:00Z",
273                     "first_updated_at_last_updated": "2020-01-01T00:00:00Z",
274                     "last_modified_at_last_updated": "2020-01-01T00:00:00Z",
275                     "first_modified_at_last_updated": "2020-01-01T00:00:00Z",
276                     "last_deleted_at_last_updated": "2020-01-01T00:00:00Z",
277                     "first_deleted_at_last_updated": "2020-01-01T00:00:00Z",
278                     "last_created_at_last_updated": "2020-01-01T00:00:00Z",
279                     "first_created_at_last_updated": "2020-01-01T00:00:00Z",
280                     "last_updated_by_first_updated": "Example Corp",
281                     "first_updated_by_first_updated": "Example Corp",
282                     "last_modified_by_first_updated": "Example Corp",
283                     "first_modified_by_first_updated": "Example Corp",
284                     "last_deleted_by_first_updated": "Example Corp",
285                     "first_deleted_by_first_updated": "Example Corp",
286                     "last_created_by_first_updated": "Example Corp",
287                     "first_created_by_first_updated": "Example Corp",
288                     "last_updated_at_first_updated": "2020-01-01T00:00:00Z",
289                     "first_updated_at_first_updated": "2020-01-01T00:00:00Z",
290                     "last_modified_at_first_updated": "2020-01-01T00:00:00Z",
291                     "first_modified_at_first_updated": "2020-01-01T00:00:00Z",
292                     "last_deleted_at_first_updated": "2020-01-01T00:00:00Z",
293                     "first_deleted_at_first_updated": "2020-01-01T00:00:00Z",
294                     "last_created_at_first_updated": "2020-01-01T00:00:00Z",
295                     "first_created_at_first_updated": "2020-01-01T00:00:00Z",
296                     "last_updated_by_last_modified": "Example Corp",
297                     "first_updated_by_last_modified": "Example Corp",
298                     "last_modified_by_last_modified": "Example Corp",
299                     "first_modified_by_last_modified": "Example Corp",
300                     "last_deleted_by_last_modified": "Example Corp",
301                     "first_deleted_by_last_modified": "Example Corp",
302                     "last_created_by_last_modified": "Example Corp",
303                     "first_created_by_last_modified": "Example Corp",
304                     "last_updated_at_last_modified": "2020-01-01T00:00:00Z",
305                     "first_updated_at_last_modified": "2020-01-01T00:00:00Z",
306                     "last_modified_at_last_modified": "2020-01-01T00:00:00Z",
307                     "first_modified_at_last_modified": "2020-01-01T00:00:00Z",
308                     "last_deleted_at_last_modified": "2020-01-01T00:00:00Z",
309                     "first_deleted_at_last_modified": "2020-01-01T00:00:00Z",
310                     "last_created_at_last_modified": "2020-01-01T00:00:00Z",
311                     "first_created_at_last_modified": "2020-01-01T00:00:00Z",
312                     "last_updated_by_first_modified": "Example Corp",
313                     "first_updated_by_first_modified": "Example Corp",
314                     "last_modified_by_first_modified": "Example Corp",
315                     "first_modified_by_first_modified": "Example Corp",
316                     "last_deleted_by_first_modified": "Example Corp",
317                     "first_deleted_by_first_modified": "Example Corp",
318                     "last_created_by_first_modified": "Example Corp",
319                     "first_created_by_first_modified": "Example Corp",
320                     "last_updated_at_first_modified": "2020-01-01T00:00:00Z",
321                     "first_updated_at_first_modified": "2020-01-01T00:00:00Z",
322                     "last_modified_at_first_modified": "2020-01-01T00:00:00Z",
323                     "first_modified_at_first_modified": "2020-01-01T00:00:00Z",
324                     "last_deleted_at_first_modified": "2020-01-01T00:00:00Z",
325                     "first_deleted_at_first_modified": "2020-01-01T00:00:00Z",
326                     "last_created_at_first_modified": "2020-01-01T00:00:00Z",
327                     "first_created_at_first_modified": "2020-01-01T00:00:00Z",
328                     "last_updated_by_last_deleted": "Example Corp",
329                     "first_updated_by_last_deleted": "Example Corp",
330                     "last_modified_by_last_deleted": "Example Corp",
331                     "first_modified_by_last_deleted": "Example Corp",
332                     "last_deleted_by_last_deleted": "Example Corp",
333                     "first_deleted_by_last_deleted": "Example Corp",
334                     "last_created_by_last_deleted": "Example Corp",
335                     "first_created_by_last_deleted": "Example Corp",
336                     "last_updated_at_last_deleted": "2020-01-01T00:00:00Z",
337                     "first_updated_at_last_deleted": "2020-01-01T00:00:00Z",
338                     "last_modified_at_last_deleted": "2020-01-01T00:00:00Z",
339                     "first_modified_at_last_deleted": "2020-01-01T00:00:00Z",
340                     "last_deleted_at_last_deleted": "2020-01-01T00:00:00Z",
341                     "first_deleted_at_last_deleted": "2020-01-01T00:00:00Z",
342                     "last_created_at_last_deleted": "2020-01-01T00:00:00Z",
343                     "first_created_at_last_deleted": "2020-01-01T00:00:00Z",
344                     "last_updated_by_first_deleted": "Example Corp",
345                     "first_updated_by_first_deleted": "Example Corp",
346                     "last_modified_by_first_deleted": "Example Corp",
347                     "first_modified_by_first_deleted": "Example Corp",
348                     "last_deleted_by_first_deleted": "Example Corp",
349                     "first_deleted_by_first_deleted": "Example Corp",
350                     "last_created_by_first_deleted": "Example Corp",
351                     "first_created_by_first_deleted": "Example Corp",
352                     "last_updated_at_first_deleted": "2020-01-01T00:00:00Z",
353                     "first_updated_at_first_deleted": "2020-01-01T00:00:00Z",
354                     "last_modified_at_first_deleted": "2020-01-01T00:00:00Z",
355                     "first_modified_at_first_deleted": "2020-01-01T00:00:00Z",
356                     "last_deleted_at_first_deleted": "2020-01-01T00:00:00Z",
357                     "first_deleted_at_first_deleted": "2020-01-01T00:00:00Z",
358                     "last_created_at_first_deleted": "2020-01-01T00:00:00Z",
359                     "first_created_at_first_deleted": "2020-01-01T00:00:00Z",
360                     "last_updated_by_last_created": "Example Corp",
361                     "first_updated_by_last_created": "Example Corp",
362                     "last_modified_by_last_created": "Example Corp",
363                     "first_modified_by_last_created": "Example Corp",
364                     "last_deleted_by_last_created": "Example Corp",
365                     "first_deleted_by_last_created": "Example Corp",
366                     "last_created_by_last_created": "Example Corp",
367                     "first_created_by_last_created": "Example Corp",
368                     "last_updated_at_last_created": "2020-01-01T00:00:00Z",
369                     "first_updated_at_last_created": "2020-01-01T00:00:00Z",
370                     "last_modified_at_last_created": "2020-01-01T00:00:00Z",
371                     "first_modified_at_last_created": "2020-01-01T00:00:00Z",
372                     "last_deleted_at_last_created": "2020-01-01T00:00:00Z",
373                     "first_deleted_at_last_created": "2020-01-01T00:00:00Z",
374                     "last_created_at_last_created": "2020-01-01T00:00:00Z",
375                     "first_created_at_last_created": "2020-01-01T00:00:00Z",
376                     "last_updated_by_first_created": "Example Corp",
377                     "first_updated_by_first_created": "Example Corp",
378                     "last_modified_by_first_created": "Example Corp",
379                     "first_modified_by_first_created": "Example Corp",
380                     "last_deleted_by_first_created": "Example Corp",
381                     "first_deleted_by_first_created": "Example Corp",
382                     "last_created_by_first_created": "Example Corp",
383                     "first_created_by_first_created": "Example Corp",
384                     "last_updated_at_first_created": "2020-01-01T00:00:00Z",
385                     "first_updated_at_first_created": "2020-01-01T00:00:00Z",
386                     "last_modified_at_first_created": "2020-01-01T00:00:00Z",
387                     "first_modified_at_first_created": "2020-01-01T00:00:00Z",
388                     "last_deleted_at_first_created": "2020-01-01T00:00:00Z",
389                     "first_deleted_at_first_created": "2020-01-01T00:00:00Z",
390                     "last_created_at_first_created": "2020-01-01T00:00:00Z",
391                     "first_created_at_first_created": "2020-01-01T00:00:00Z",
392                     "last_updated_by_last_updated_by": "Example Corp",
393                     "first_updated_by_last_updated_by": "Example Corp",
394                     "last_modified_by_last_updated_by": "Example Corp",
395                     "first_modified_by_last_updated_by": "Example Corp",
396                     "last_deleted_by_last_updated_by": "Example Corp",
397                     "first_deleted_by_last_updated_by": "Example Corp",
398                     "last_created_by_last_updated_by": "Example Corp",
399                     "first_created_by_last_updated_by": "Example Corp",
400                     "last_updated_at_last_updated_by": "2020-01-01T00:00:00Z",
401                     "first_updated_at_last_updated_by": "2020-01-01T00:00:00Z",
402                     "last_modified_at_last_updated_by": "2020-01-01T00:00:00Z",
403                     "first_modified_at_last_updated_by": "2020-01-01T00:00:00Z",
404                     "last_deleted_at_last_updated_by": "2020-01-01T00:00:00Z",
405                     "first_deleted_at_last_updated_by": "2020-01-01T00:00:00Z",
406                     "last_created_at_last_updated_by": "2020-01-01T00:00:00Z",
407                     "first_created_at_last_updated_by": "2020-01-01T00:00:00Z",
408                     "last_updated_by_first_updated_by": "Example Corp",
409                     "first_updated_by_first_updated_by": "Example Corp",
410                     "last_modified_by_first_updated_by": "Example Corp",
411                     "first_modified_by_first_updated_by": "Example Corp",
412                     "last_deleted_by_first_updated_by": "Example Corp",
413                     "first_deleted_by_first_updated_by": "Example Corp",
414                     "last_created_by_first_updated_by": "Example Corp",
415                     "first_created_by_first_updated_by": "Example Corp",
416                     "last_updated_at_first_updated_by": "2020-01-01T00:00:00Z",
417                     "first_updated_at_first_updated_by": "2020-01-01T00:00:00Z",
418                     "last_modified_at_first_updated_by": "2020-01-01T00:00:00Z",
419                     "first_modified_at_first_updated_by": "2020-01-01T00:00:00Z",
420                     "last_deleted_at_first_updated_by": "2020-01-01T00:00:00Z",
421                     "first_deleted_at_first_updated_by": "2020-01-01T00:00:00Z",
422                     "last_created_at_first_updated_by": "2020-01-01T00:00:00Z",
423                     "first_created_at_first_updated_by": "2020-01-01T00:00:00Z",
424                     "last_updated_by_last_modified_by": "Example Corp",
425                     "first_updated_by_last_modified_by": "Example Corp",
426                     "last_modified_by_last_modified_by": "Example Corp",
427                     "first_modified_by_last_modified_by": "Example Corp",
428                     "last_deleted_by_last_modified_by": "Example Corp",
429                     "first_deleted_by_last_modified_by": "Example Corp",
430                     "last_created_by_last_modified_by": "Example Corp",
431                     "first_created_by_last_modified_by": "Example Corp",
432                     "last_updated_at_last_modified_by": "2020-01-01T00:00:00Z",
433                     "first_updated_at_last_modified_by": "2020-01-01T00:00:00Z",
434                     "last_modified_at_last_modified_by": "2020-01-01T00:00:00Z",
435                     "first_modified_at_last_modified_by": "2020-01-01T00:00:00Z",
436                     "last_deleted_at_last_modified_by": "2020-01-01T00:00:00Z",
437                     "first_deleted_at_last_modified_by": "2020-01-01T00:00:00Z",
438                     "last_created_at_last_modified_by": "2020-01-01T00:00:00Z",
439                     "first_created_at_last_modified_by": "2020-01-01T00:00:00Z",
440                     "last_updated_by_first_modified_by": "Example Corp",
441                     "first_updated_by_first_modified_by": "Example Corp",
442                     "last_modified_by_first_modified_by": "Example Corp",
443                     "first_modified_by_first_modified_by": "Example Corp",
444                     "last_deleted_by_first_modified_by": "Example Corp",
445                     "first_deleted_by_first_modified_by": "Example Corp",
446                     "last_created_by_first_modified_by": "Example Corp",
447                     "first_created_by_first_modified_by": "Example Corp",
448                     "last_updated_at_first_modified_by": "2020-01-01T00:00:00Z",
449                     "first_updated_at_first_modified_by": "2020-01-01T00:00:00Z",
450                     "last_modified_at_first_modified_by": "2020-01-01T00:00:00Z",
451                     "first_modified_at_first_modified_by": "2020-01-01T00:00:00Z",
452                     "last_deleted_at_first_modified_by": "2020-01-01T00:00:00Z",
453                     "first_deleted_at_first_modified_by": "2020-01-01T00:00:00Z",
454                     "last_created_at_first_modified_by": "2020-01-01T00:00:00Z",
455                     "first_created_at_first_modified_by": "2020-01-01T00:00:00Z",
456                     "last_updated_by_last_deleted_by": "Example Corp",
457                     "first_updated_by_last_deleted_by": "Example Corp",
458                     "last_modified_by_last_deleted_by": "Example Corp",
459                     "first_modified_by_last_deleted_by": "Example Corp",
460                     "last_deleted_by_last_deleted_by": "Example Corp",
461                     "first_deleted_by_last_deleted_by": "Example Corp",
462                     "last_created_by_last_deleted_by": "Example Corp",
463                     "first_created_by_last_deleted_by": "Example Corp",
464                     "last_updated_at_last_deleted_by": "2020-01-01T00:00:00Z",
465                     "first_updated_at_last_deleted_by": "2020-01-01T00:00:00Z",
466                     "last_modified_at_last_deleted_by": "2020-01-01T00:00:00Z",
467                     "first_modified_at_last_deleted_by": "2020-01-01T00:00:00Z",
468                     "last_deleted_at_last_deleted_by": "2020-01-01T00:00:00Z",
469                     "first_deleted_at_last_deleted_by": "2020-01-01T00:00:00Z",
470                     "last_created_at_last_deleted_by": "2020-01-01T00:00:00Z",
471                     "first_created_at_last_deleted_by": "2020-01-01T00:00:00Z",
472                     "last_updated_by_first_deleted_by": "Example Corp",
473                     "first_updated_by_first_deleted_by": "Example Corp",
474                     "last_modified_by_first_deleted_by": "Example Corp",
475                     "first_modified_by_first_deleted_by": "Example Corp",
476                     "last_deleted_by_first_deleted_by": "Example Corp",
477                     "first_deleted_by_first_deleted_by": "Example Corp",
478                     "last_created_by_first_deleted_by": "Example Corp",
479                     "first_created_by_first_deleted_by": "Example Corp",
480                     "last_updated_at_first_deleted_by": "2020-01-01T00:00:00Z",
481                     "first_updated_at_first_deleted_by": "2020-01-01T00:00:00Z",
482                     "last_modified_at_first_deleted_by": "2020-01-01T00:00:00Z",
483                     "first_modified_at_first_deleted_by": "2020-01-01T00:00:00Z",
484                     "last_deleted_at_first_deleted_by": "2020-01-01T00:00:00Z",
485                     "first_deleted_at_first_deleted_by": "2020-01-01T00:00:00Z",
486                     "last_created_at_first_deleted_by": "2020-01-01T00:00:00Z",
487                     "first_created_at_first_deleted_by": "2020-01-01T00:00:00Z",
488                     "last_updated_by_last_created_by": "Example Corp",
489                     "first_updated_by_last_created_by": "Example Corp",
490                     "last_modified_by_last_created
```




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

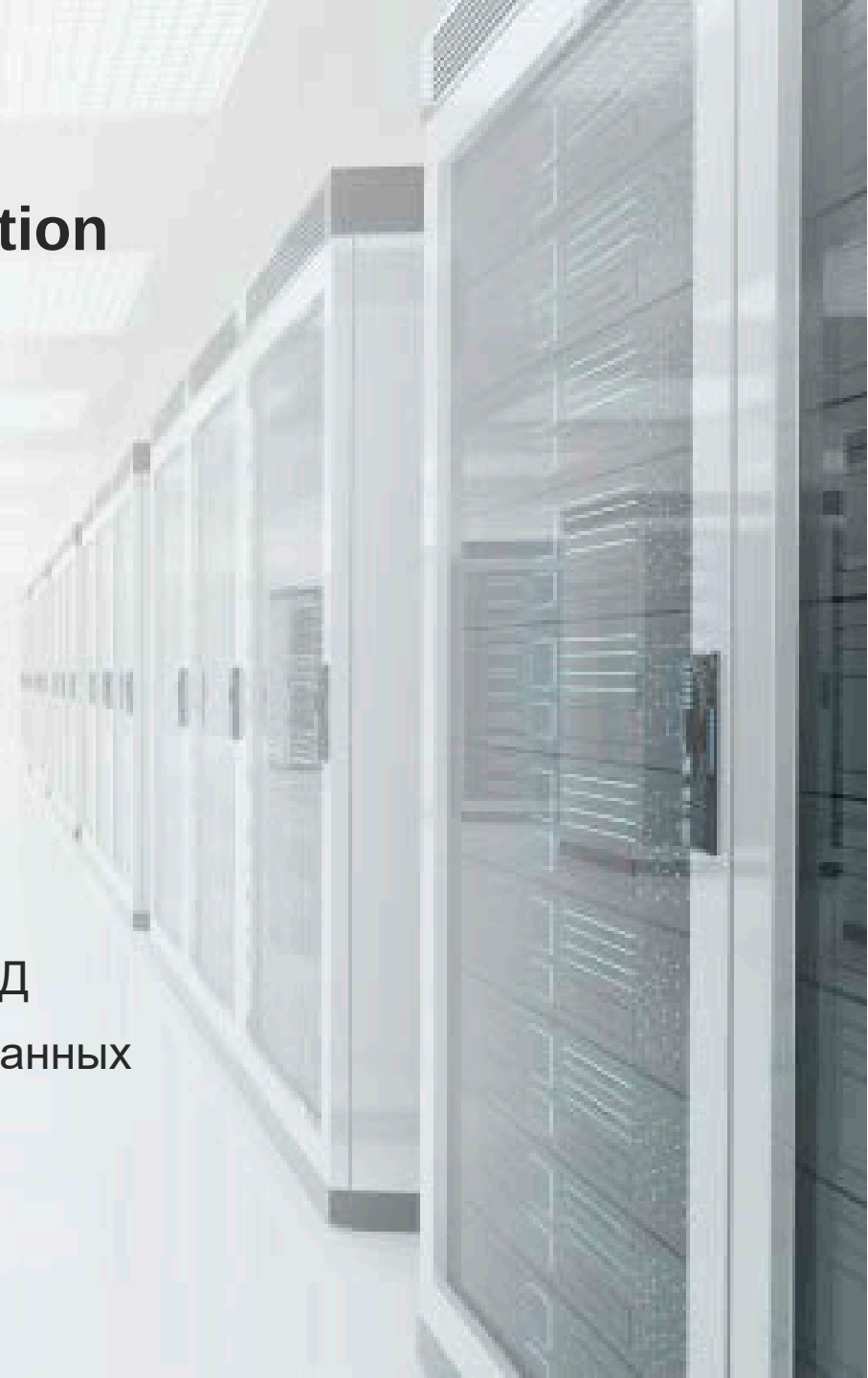
Guardium Data Protection, Guardium Vulnerability Assessment, Guardium Insights

MVS: Расчёт серверов, которые содержат критические данные, мониторятся и анализируются



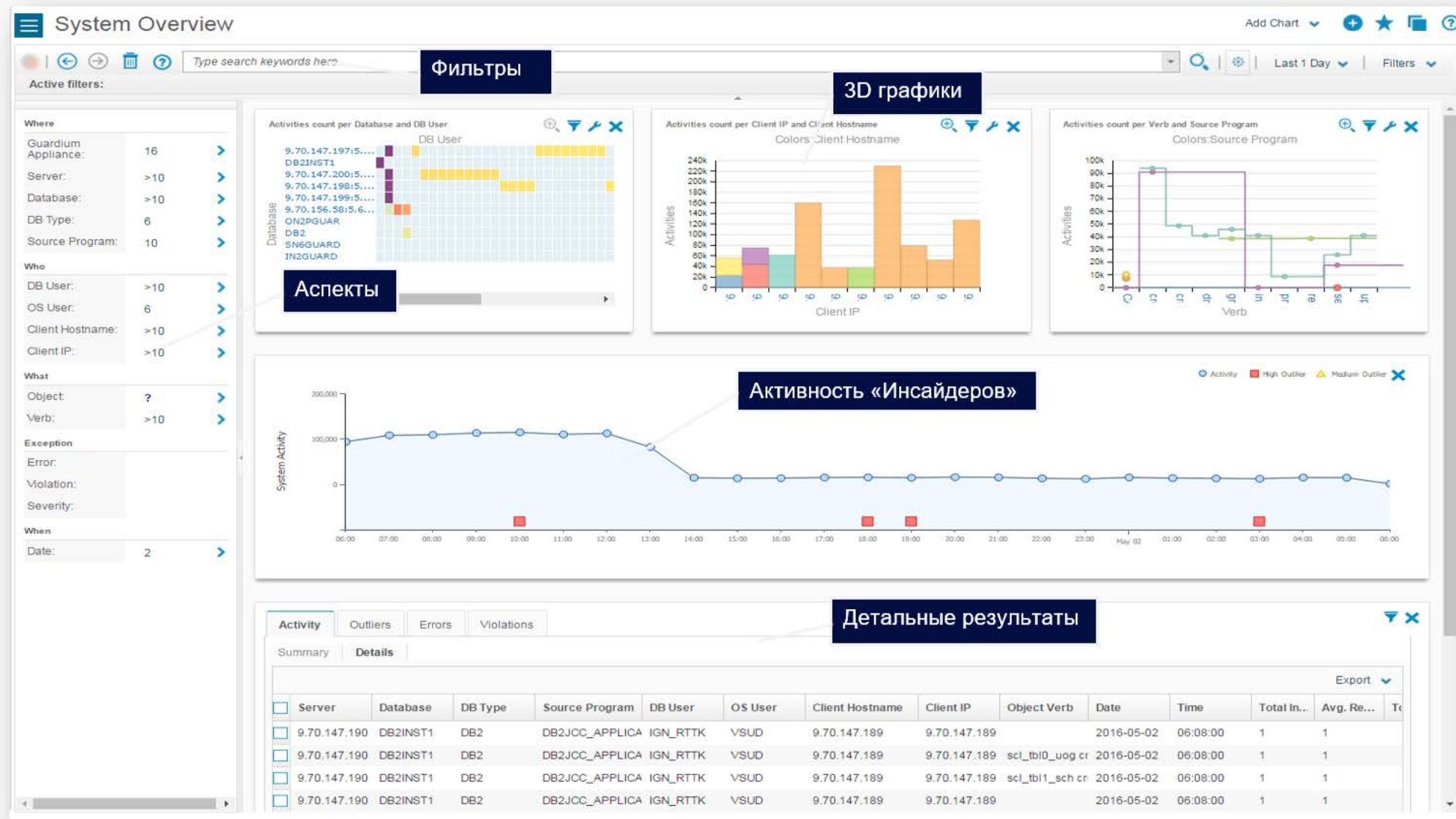
IBM Security Guardium Data and File Protection

- 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



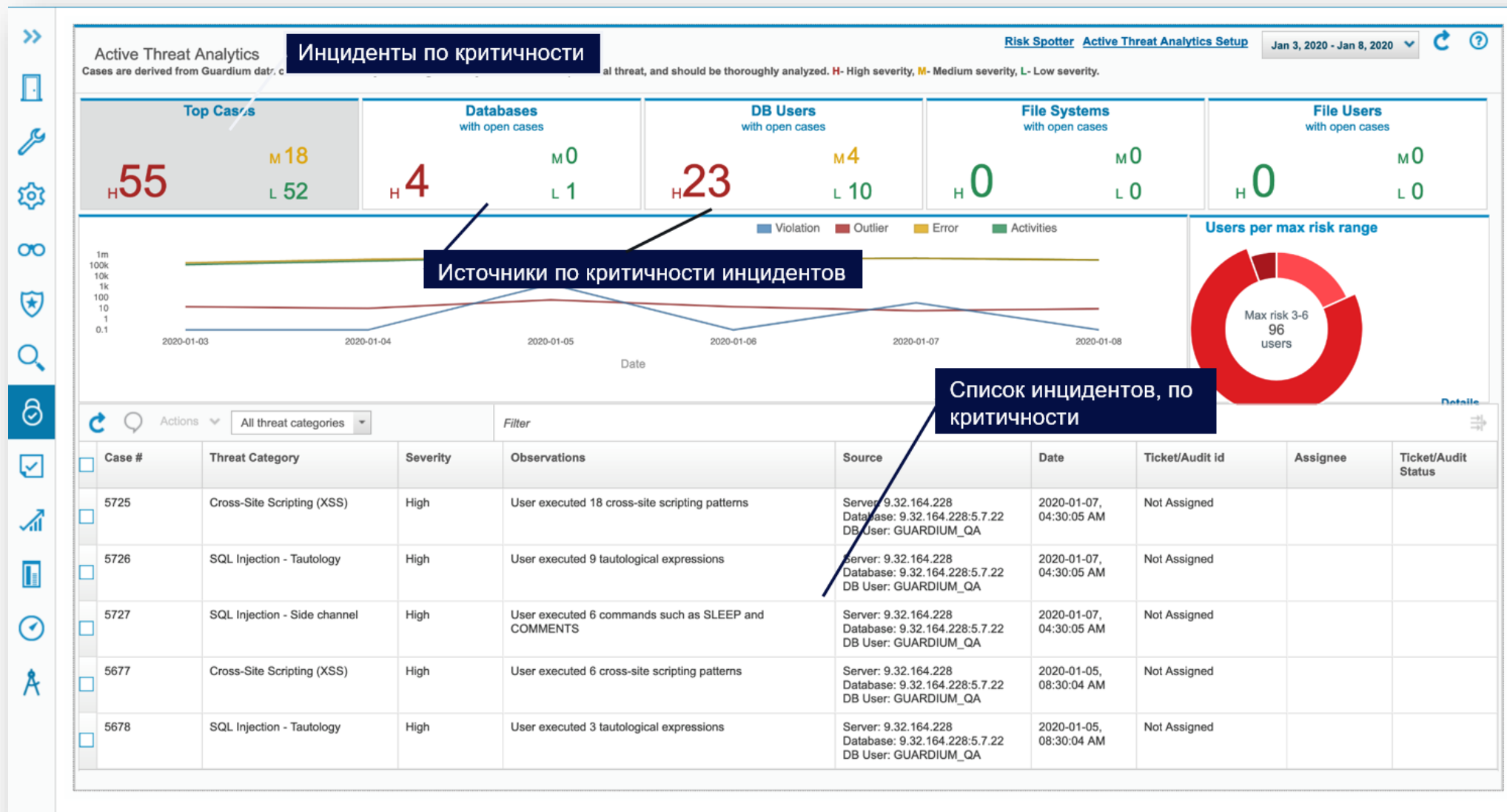


Мониторинг всех действий с СУБД и Базами данных



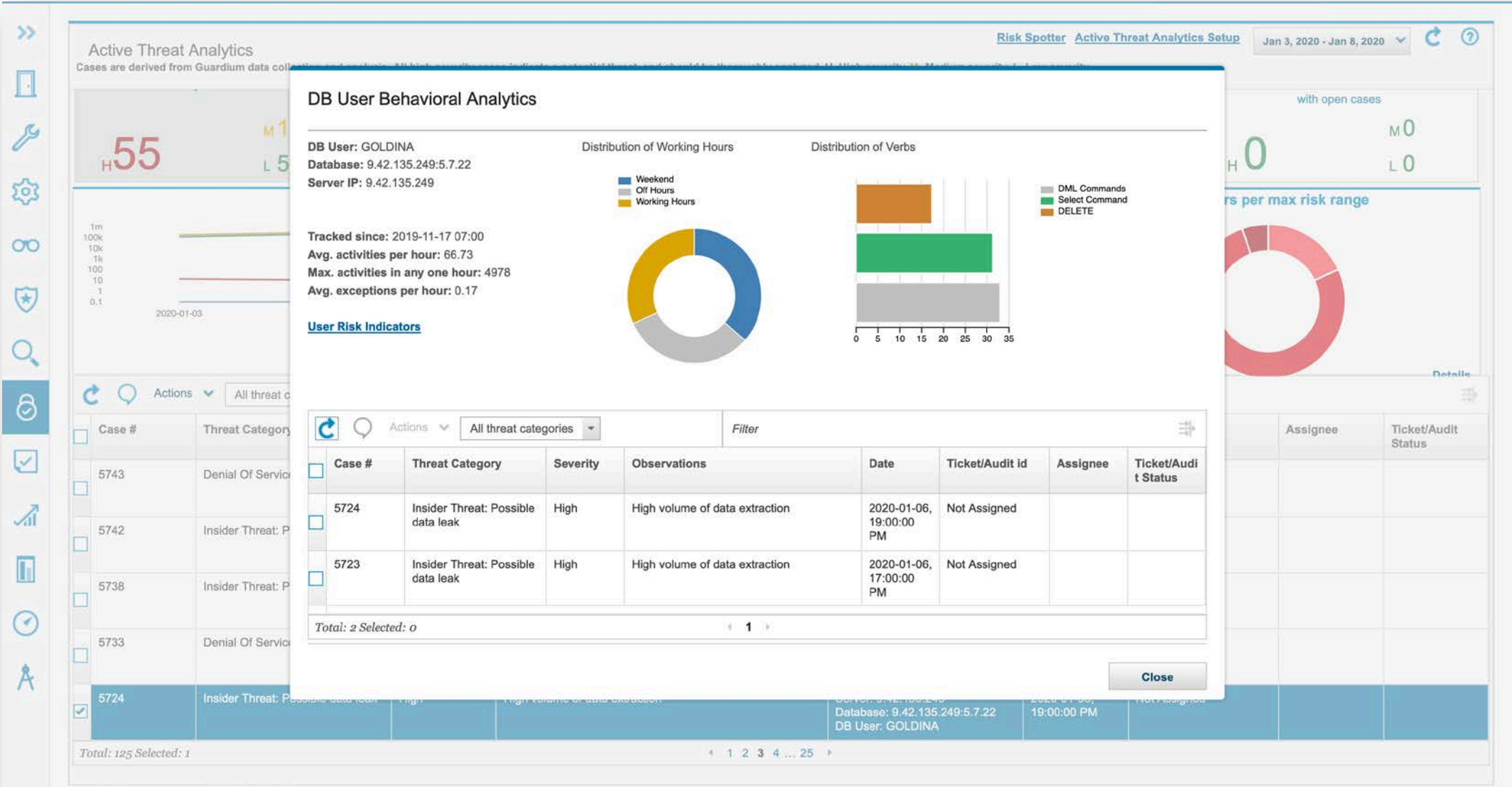


Обнаружение атак на СУБД и Базы данных





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

Assessment Test Selections

Tests for Security Assessment Monitoring

Select All Unselect All Delete Selected

Type	Test Name	Tuning
☐	MS SQL SERVER Access to server level permissions granted to non-Database Administrators	PRIV Major (n/a)
☐	MS SQL SERVER Allow Updates To System Tables Is Off	CONF Major (n/a)
☐	MS SQL SERVER Change Data Capture	PRIV Major (n/a)
☐	MS SQL SERVER Critical accounts locked - MS-SQL	AUTH Critical (n/a)
☐	MS SQL SERVER CVE-2001-0509	CONF Major (n/a)
☐	MS SQL SERVER CVE-2001-0879	CONF Major (n/a)
☐	MS SQL SERVER CVE-2002-0056	CONF Major (n/a)

Tests available for addition

Filter By

Test Type ☐ Predefined ☐ Query based ☐ CVE ☐ APAR ☒ All

Severity ☐ Critical ☐ Major ☐ Minor ☐ Caution ☐ Info ☒ All

Other ☒ Include CAS

IBM Guardium®

Results for Security Assessment: **dbst212**

Assessment executed: 2019-10-28 14:57:07

[Download PDF](#)

Warning: This execution did not fully complete - it was either canceled or halted.

Tests passing: **58%**

CIS Tests passing: 32/46

STIG Tests passing: 27/44

CVE Tests passing: 0/10

*The above tests passing statistics do not take into account any filtering that may currently be applied, and do not include tests in any status other than passed or failed.

Based on the tests performed under this assessment, data access of the defined database environments is nearing best practice. Refer to the recommendations of the individual tests to learn how you can achieve best practice status. You should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

[View log](#)

[Jump to Datasource list \(5\)](#)

[Add Selected](#)

[Groups](#)

Result Summary Showing 152 of 152 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	1p	20p	0f	13e	1f
Authentication	3p	1f	3p	2e	1f
Configuration	2e	20p	21f	43e	1f
Version	1p	1f	1f	1f	1f
Other	1p	1f	1f	1f	1f

Current filtering applied:

Test Severities: Show All

Datasource Severities: Show All

Scores: Show All

Types: Show All

[Reset Filtering](#) [Filter / Sort Controls](#)

Assessment Test Results

Test / Datasource

Fixed Server Role Members

Test category: Priv. Severity: Critical

This test checks for members in the fixed server roles. Fixed server roles provide a mechanism to grant groups of privileges to grantees. These privilege groupings are defined by the installation or upgrade of the SQL Server software at the discretion of Microsoft. Memberships in these roles granted to grantees should be strictly monitored and monitored. Default system grantees like "NT SERVICE\SQLSERVER" and "SA" that same with the installation are excluded from the test.

Ext. Reference: CIS SQL2005 v2.0.0 Item # 1.14.7

STIG Reference: DM2030, SQL2-00-009500, SQL2-00-009400, SQL2-00-009500

STIG Severity: CAT I

STIG Scorecard: SQLP

STIG Srg: SRG-APP-000062-00-000034, SRG-APP-000062-00-000016, SRG-APP-000063-00-000019

Result

fail Fixed Server roles have unauthorized users or groups assigned as members. Including 0 items present in exception group.

[Add test exception](#)

Recommendations: Please review the list of members that are assigned to the fixed server roles. We recommend you to resolve fixed server role assignments from unauthorized users. Grant fixed server roles only to database administrators or authorized grantees, including grantees who execute Guardium vulnerability assessment. If you need to exclude a certain grantee from a fixed server role, you can create an exception group and populate it with the authorized grantee name and the granted fixed server role name, then link your exception group to this test. To resolve an unauthorized grantee from assigned roles: EXEC sp_dropserverrole (grantee);

Assessment Result History

Download XML

Download PDF

Assessment Result History

100% 80% 60% 40% 20% 0%

12:00 PM 6:00 PM 10:00 PM 6:00 PM 12:00 PM 6:00 PM



«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, Sylon, 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 мобильных приложений
- ❑ Помощь ИТ-архитекторам в Zero-trust
- ❑ Ответы на почтовые запросы, касающиеся ИБ
- ❑ Редактирование отчётности для Управляющих
- ❑ Участие в найме персонала
- ❑ Написание планов тестирования
- ❑ Контроль и улучшение ИБ инфраструктуры

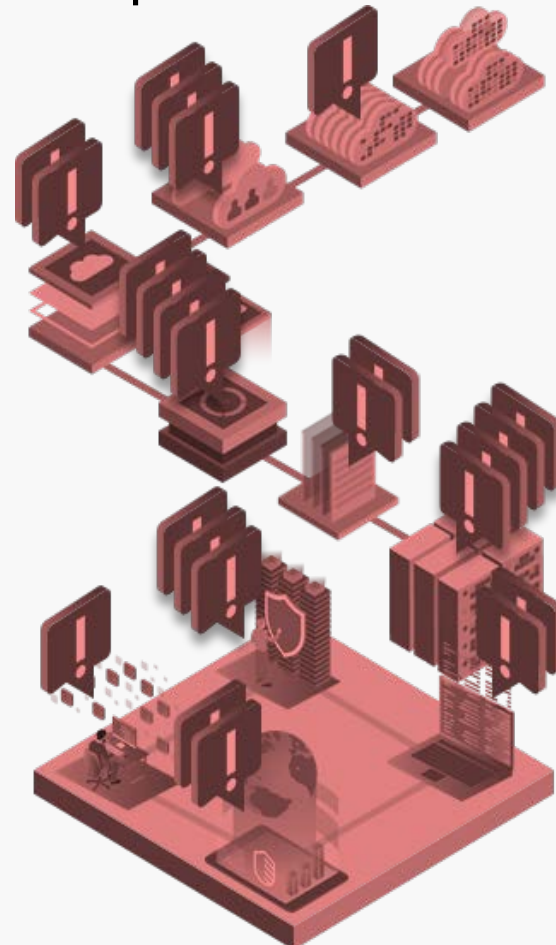
Слишком много Вендоров



Слишком много сложности



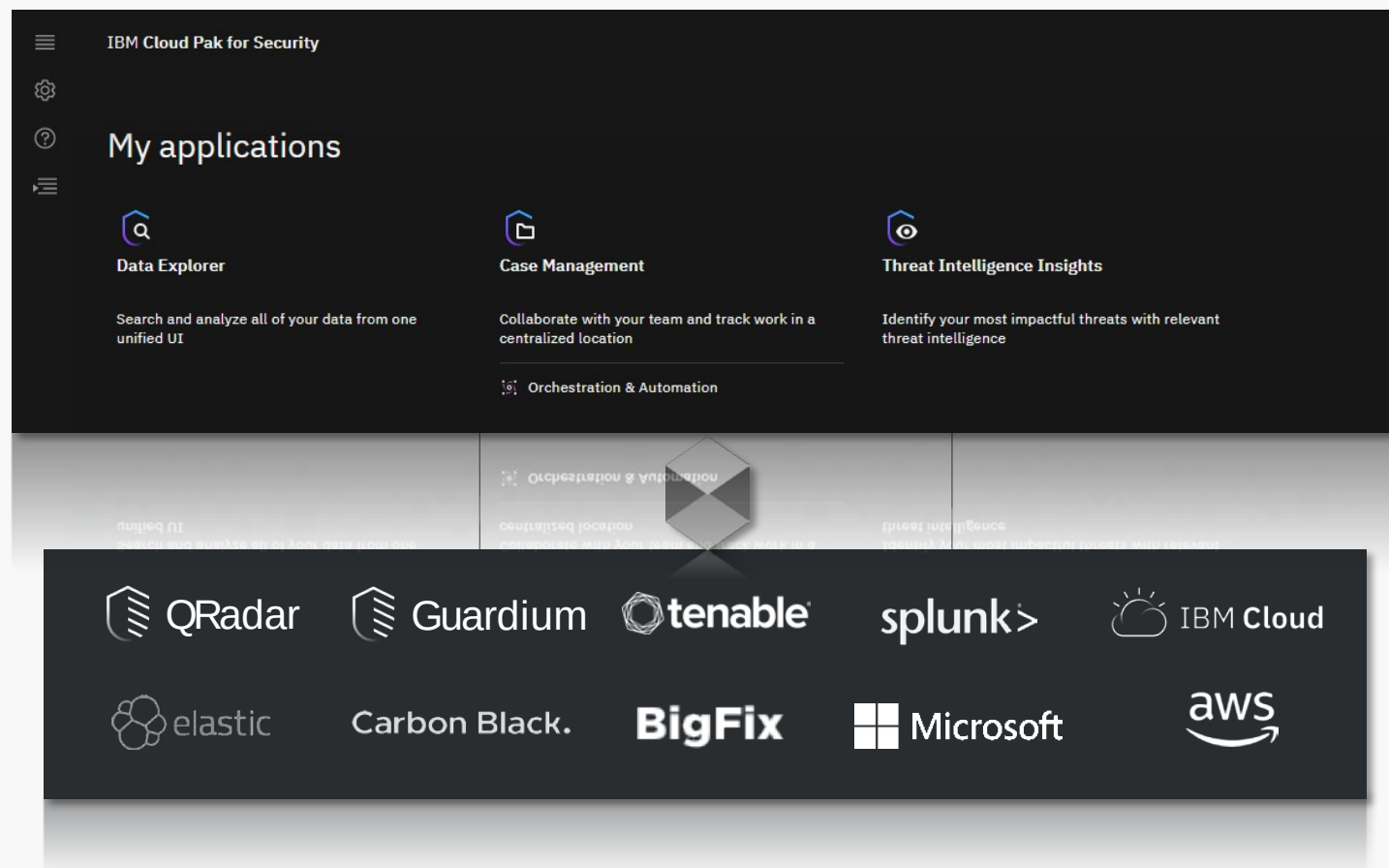
Слишком много алертов





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

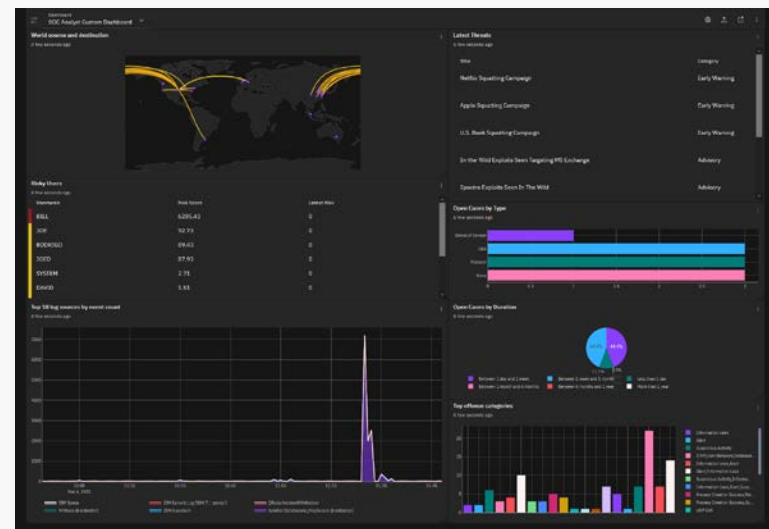
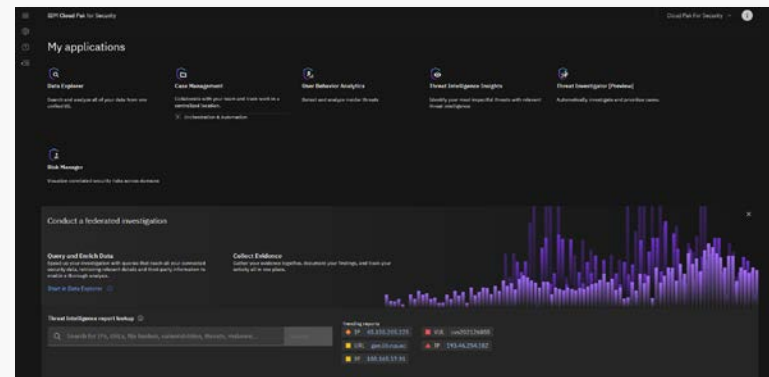




Что делает платформа «IBM Cloud Pak for Security»?

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

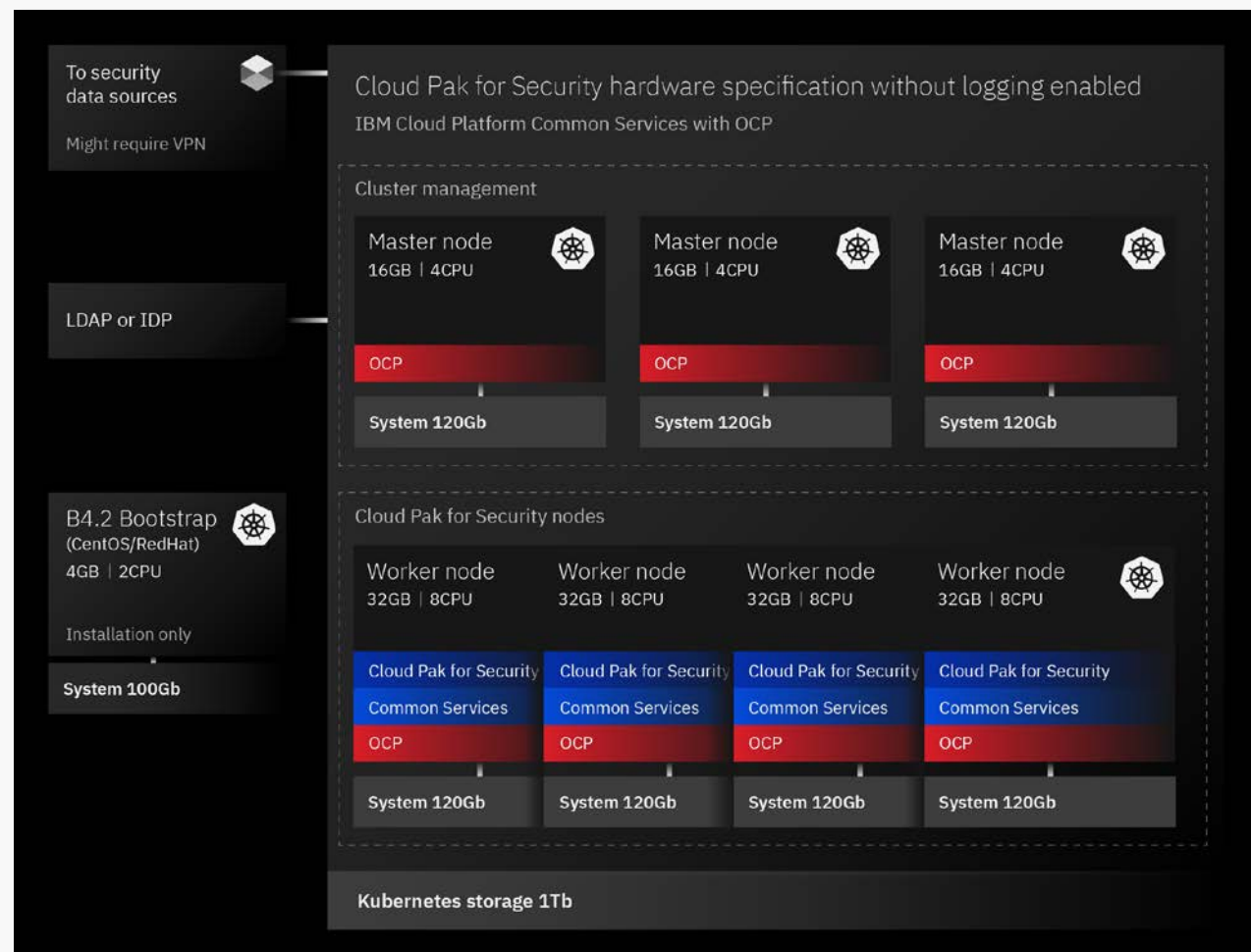
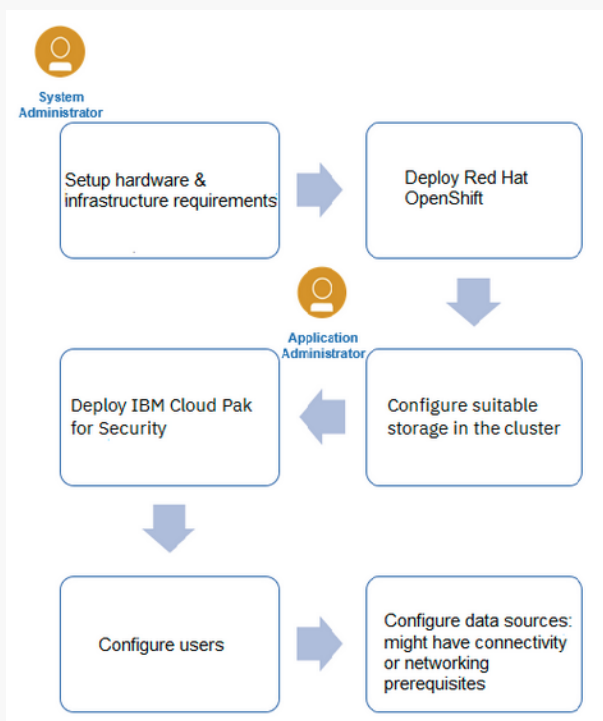
- Автоматическое исследование и расследование инцидентов
- Понимание источника и последствий атаки для эффективного реагирования
- Сопоставление расследований с матрицей MITRE ATT&CK tactics and techniques
- Представление временной шкалы инцидента



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