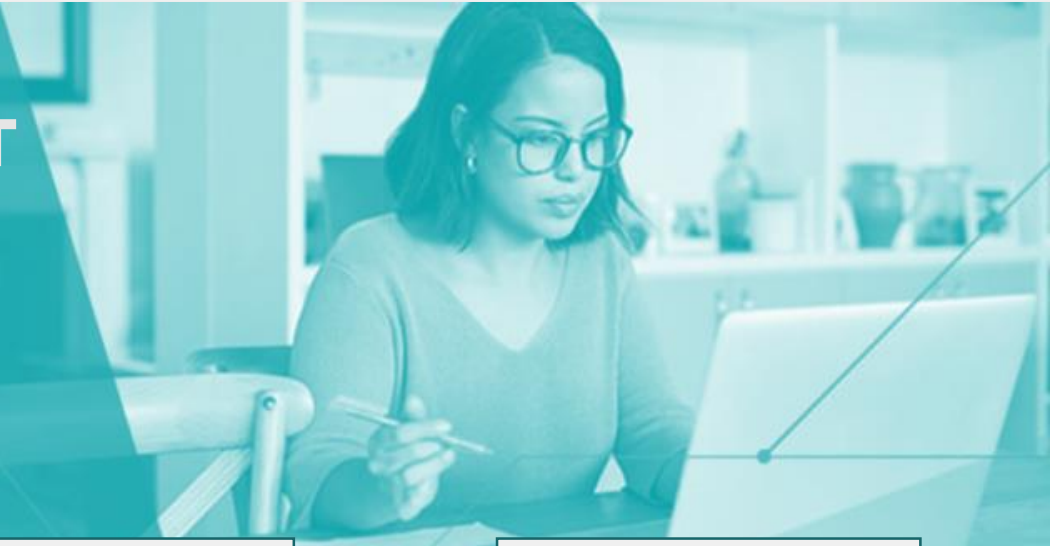
FortiSOAR – система для автоматизации реагирования на инциденты информационной безопасности

Olesya Tarabrina, SE

Сложность экосистемы замедляет реагирование и восстановление



Слишком много вендоров

Слишком много алертов

Ручной и медленный ответ

Нехватка специалистов

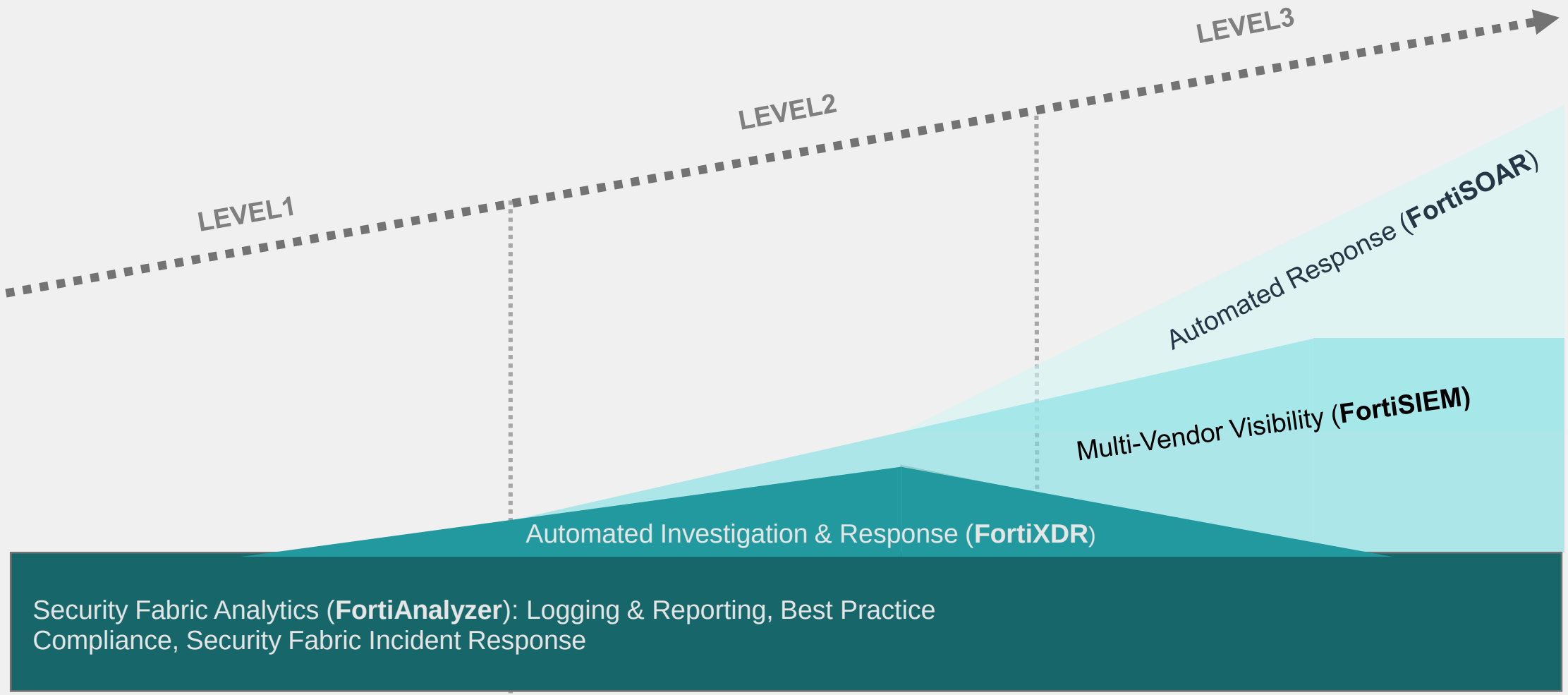
В настоящее время число SOC постоянно увеличивается, они переводят инвестиции, ресурсы и время с предотвращения угроз на обнаружение угроз и упреждающее реагирование.[1]

Организации сталкиваются с все более агрессивными угрозами ... где требуется быстрое реагирование в лучшем случае всего за несколько минут ... Это вынуждает организации сокращать время на реагирование, обычно путем делегирования большего количества задач машинам..[2]

1 Gartner. 2019 Threat Predictions. 2 Gartner. Market Guide for Security Orchestration, Automation and Response Solutions..

Упростите операции по обеспечению безопасности

Выберите предложение, соответствующее вашей зрелости SOC



Ref: 2020 CISO Benchmark Study

FortiSOAR – это независимое решение класса SOAR

- Собирает данные из нескольких источников, помогает организации интепретировать информацию и оптимизирует процессы безопасности, обеспечивая при этом автоматический ответ

Платформа управления SOC
- Управление кейсами организации
- Ролевое управление доступом
- Мультитенантность

Оркестрация и Автоматизация
- Плейбуки
- Коннекторы

Управление кейсами

- Модули «из коробки» для реагирования на инциденты, управления уязвимостями и «поиском угроз»
- Построение собственных модулей
- Контекстная визуализация

Упорядоченное реагирование

- Визуальный редактор для создания плейбуков
- 300+ коннекторов для автоматических действий
- Примеры реальных кейсов

Мультитенантность

- Распределенная/федеративная архитектура
- Контроль доступа к данным и плейбукам

FortiSOAR

4 ключевых сценария использования

Единое управление реагированием на инциденты

Автоматизация упорядочивания алертов

Оптимизация SOC

Взаимодействие в рамках SOC

Типовые сценарии применения FortiSOAR

Максимизируйте эффективность с помощью оркестрации и автоматизации

Единое управление реагированием на инциденты

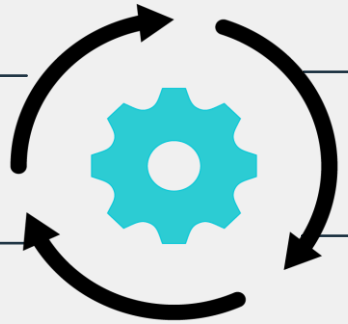
Стандартизация при централизации видимости и контроля

Повышение эффективности

Автоматизация упорядочивания алертов

Автоматическая приоритезация / назначение, корреляция, рекомендации

Приоритезация на основе рисков



Оптимизация SOC

Быстрый старт с примерами использования «из коробки», панелями мониторинга и отчетами

Сокращение ручных процессов

Взаимодействие в рамках SOC

Многофункциональный SOC с динамическими командными рабочими пространствами

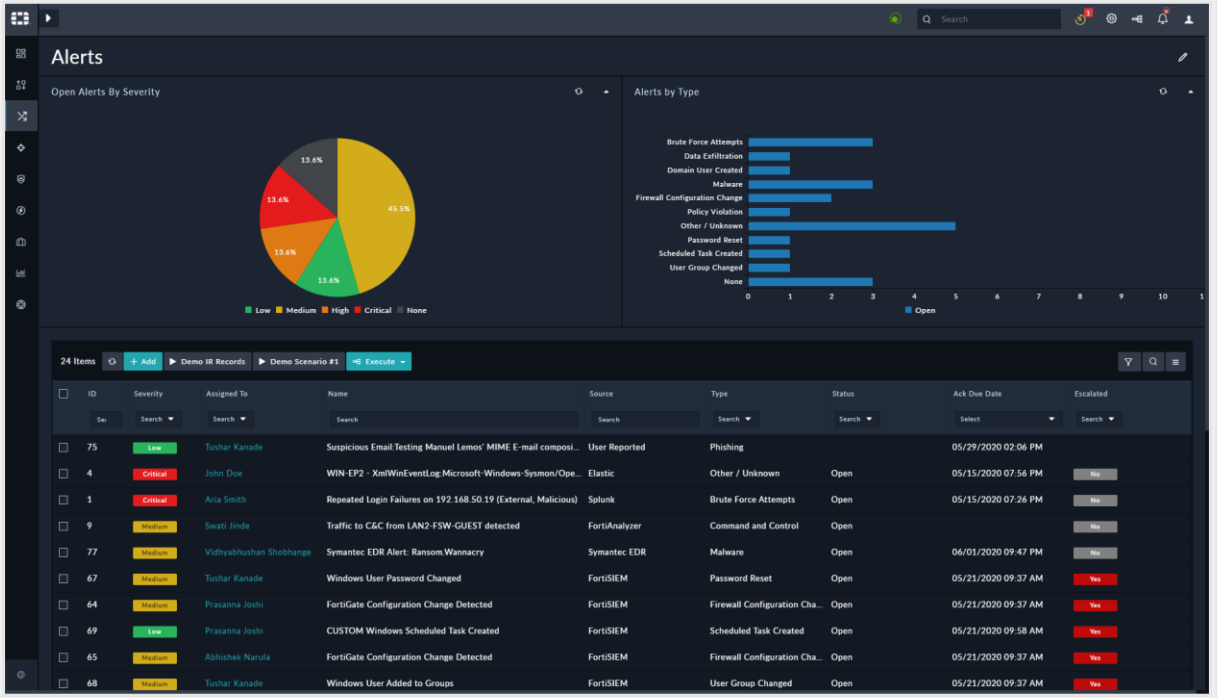
Ускорение координации реагирования

1. Единое управление реагированием на инциденты

БИЗНЕС ДРАЙВЕР

Security Operation Centers имеют возможность мгновенно управлять, автоматизировать и реагировать со всеми существующими инструментами.

Позволяет командам централизовывать свои процессы безопасности. Результатом является более быстрый отклик в реальном времени на машинной скорости.



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

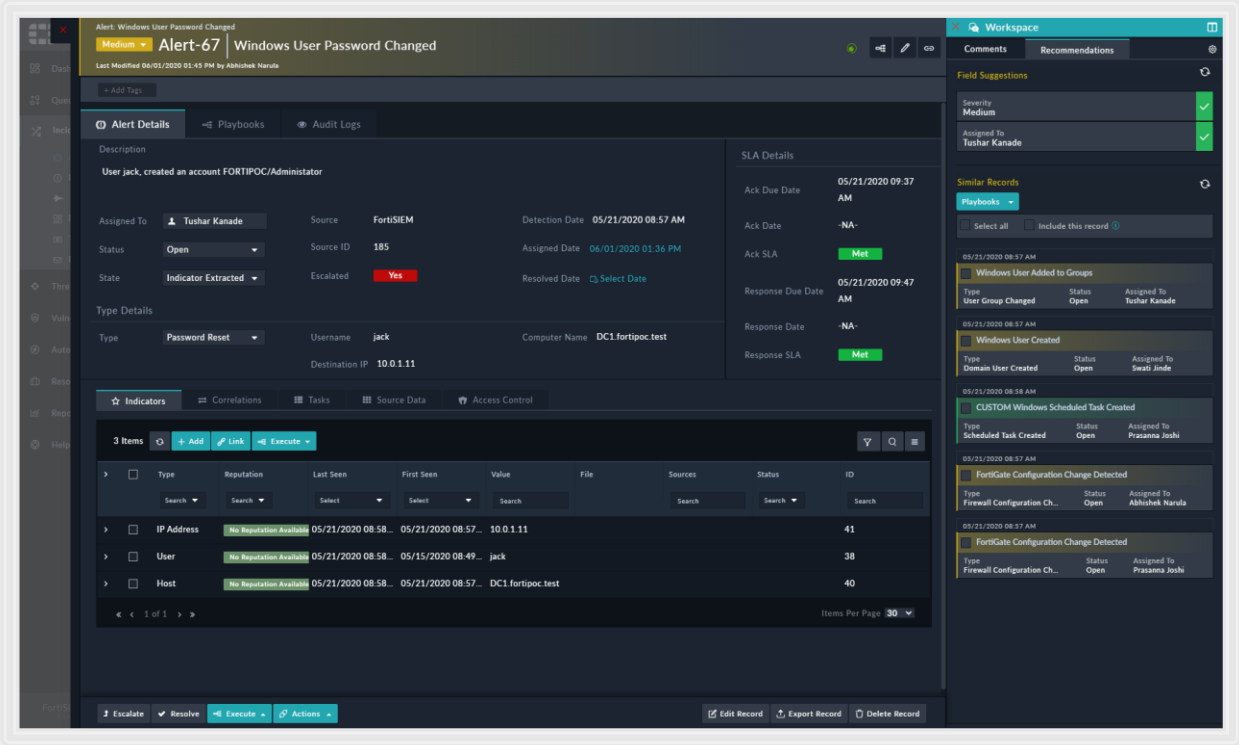
- Визуальный редактор плейбуков
- RBAC, адаптивное управление кейсами
- 300+ коннекторов, 3000+ действий

2. Автоматизация упорядочивания алертов

БИЗНЕС ДРАЙВЕР

Оптимизация процессов безопасности, автоматическое сопоставление предупреждений из всего стека безопасности в единый инцидент для расследования, сортировки и восстановления.

Сосредоточение на поиске угроз и минимизация ложных срабатываний.



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Приоритезация и распределение алертов внутри команды SOC
- Эскалация алертов, требующих расследования
- Механизм рекомендаций
- Визуализация корреляций

3. Оптимизация SOC

БИЗНЕС ДРАЙВЕР

Измерение и отслеживание своего прогресса с помощью настраиваемых панелей мониторинга FortiSOAR ™ для мониторинга ключевых показателей эффективности операций безопасности и создания автоматических отчетов на уровне предприятия для аудиторов и руководителей.

Позволяет SOC определять уязвимости и определять, где можно автоматизировать ручные процессы.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

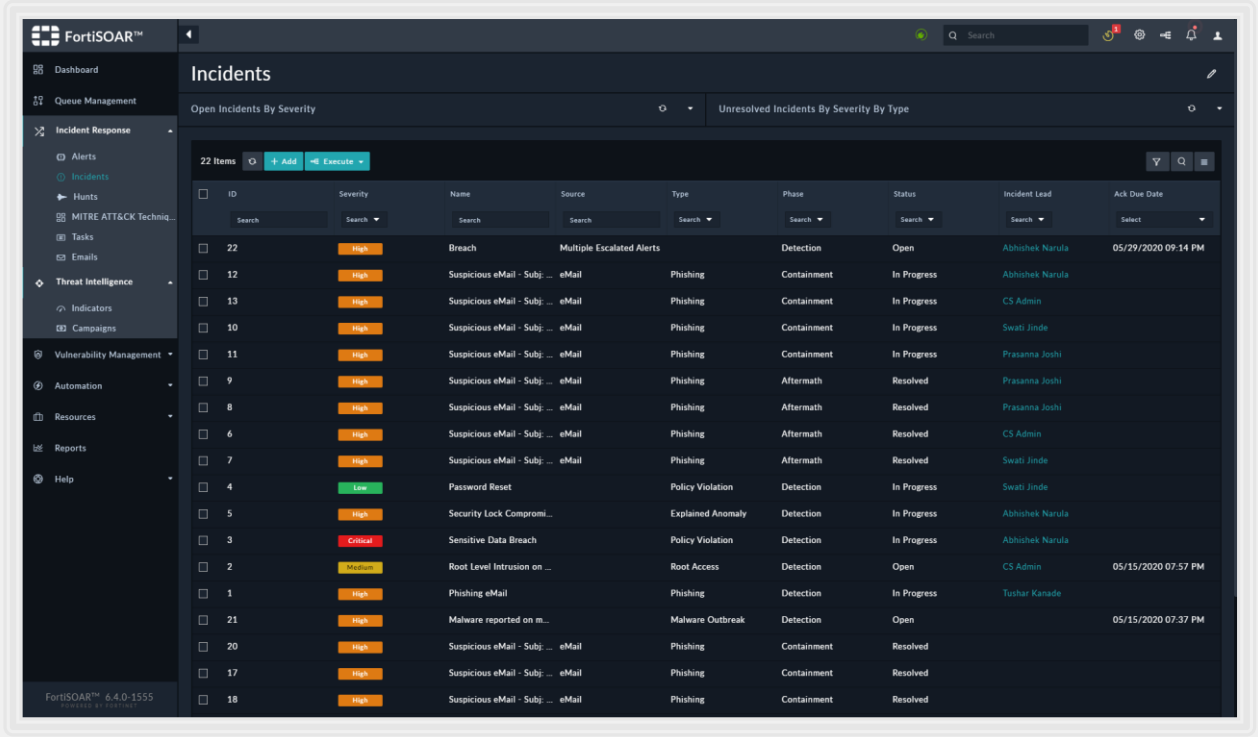
- KPI-панели для SOC (отслеживание MTTR)
- 10+ панелей мониторинга и отчетов «из коробки» (кастомизируемые)
- 20+ готовых к запуску сквозных сценариев
- 100+ сценариев использования и плейбуков

4. Взаимодействие в рамках SOC

БИЗНЕС ДРАЙВЕР

FortiSOAR устраняет проблемы, с которыми сталкиваются команды, позволяя им быстро работать вместе или обмениваться передовым опытом, обеспечивая при этом межфункциональное сотрудничество за пределами SOC организации. Подключение аналитиков к важной информации и нужным командам, таким как отдел кадров, юристы и другие ключевые заинтересованные стороны.

Ускорение процесса исправления и разрешения проблемы при обеспечении полного сквозного контроля и прозрачности за пределами команды SOC



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Рабочая область для совместной работы в команде
- Удаленный SOC
- Непрерывность рабочего пространства 24/7
- Не требуются навыки программирования

Ручное управление процессами vs Автоматизация

Экономия времени с помощью FortiSOAR

Шаги	Вручную	FortiSOAR
Обогащение данных для идентификации IOC	От 46 до 60 минут	3 минуты
Упорядочивание SIEM-событий	20 минут	1 минута
Отправка данных на дополнительную эмуляцию	От 1 часа до 6 часов	1 минута
Изоляция затронутых устройств	10 минут	1 минута
Анализ, создание и снабжение комментариями инцидента	60 минут	5 минут
Блокировка IOC на МЭ (#FortiGate)	От 45 минут до 2 часов	2 минуты
Восстановление и реагирование на инцидент	От 60 минут до 6 часов	5 минут
Подготовка и отправка отчета об инциденте	От 2 до 3 часов	2 минуты
Итого	**От 4.5 до 15 часов**	**20 минут**

Ручное управление процессами

Запросы на получение образа машины

1 час на обработку события (x20 в неделю)

Текущий процесс

email

SNOW

Шаг 1: Запрос отправлен через почту или ERP

Шаг 2: Дополнительная информация должна быть собрана через ERP/ новую заявку.

Команда SOC остлеживает поступление новых запросов

Шаг 3: Информация о пользователе собирается из каталога AD

Шаг 4: Аналитик подключается к целевой системе для получения образа

Шаг 5: Аналитик перемещает образ в точку назначения

Шаг 6: Обновление / закрытие заявки

Шаг 7: Извещение инициатора запроса об исполнении

Автоматизация процесса с использованием FortiSOAR

Запросы на получение образа машины с использованием FortiSOAR

Пример: запрос на изменение NAT правил в конфигурации МЭ

Ручное управление процессом

Текущий процесс

Email

Запрос отправлен по почте в виде pdf-формы, содержащей перечень изменений NAT-правил

Команда SOC

Шаг 1:

Аналитик выполняет анализ запроса

Шаг 2:

Аналитик выполняет проверку текущих конфигураций

Шаг 3:

Аналитик вносит изменения в NAT-правила

Шаг 4:

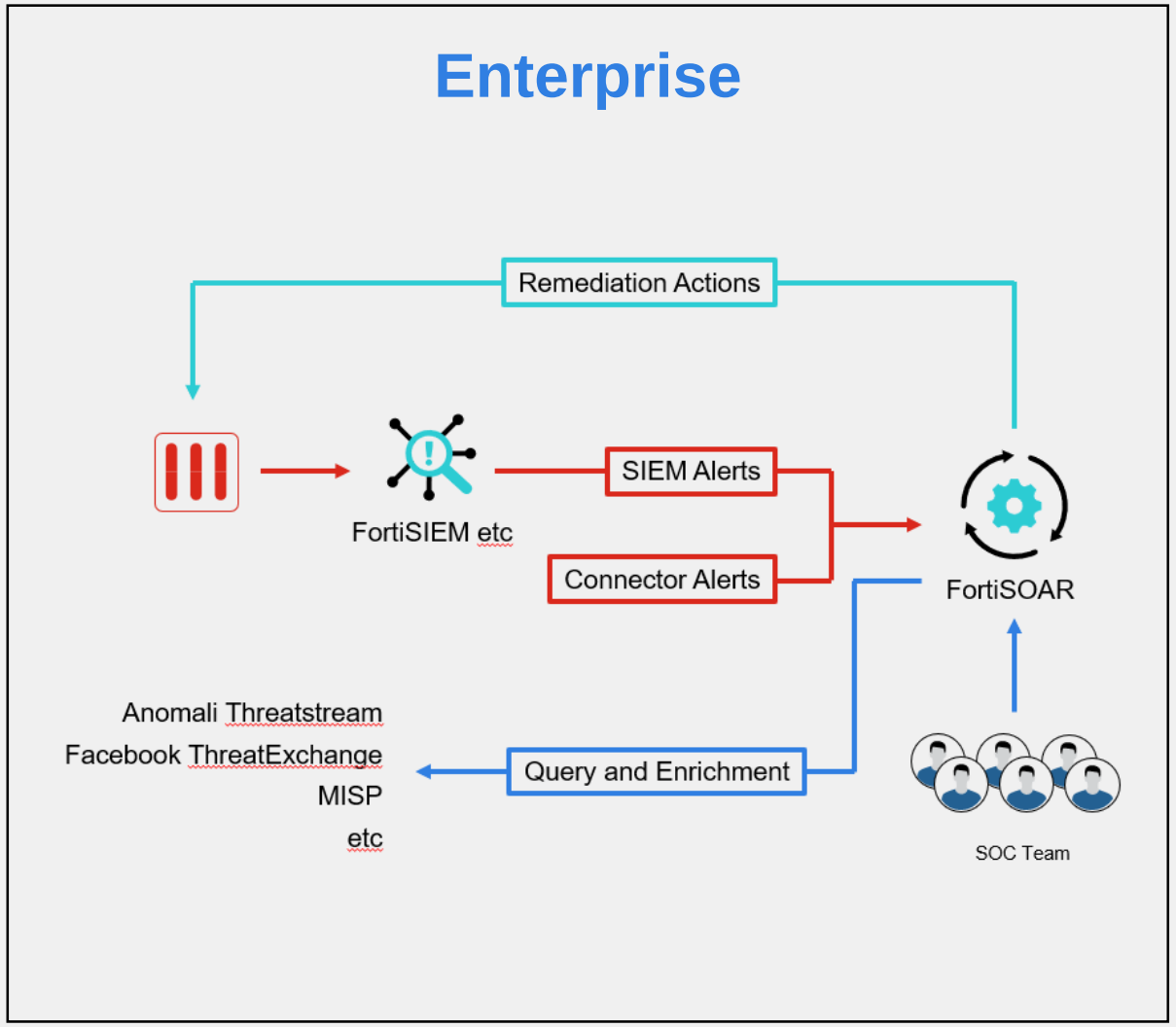
Инициатору отправляется извещение о выполнении заявки

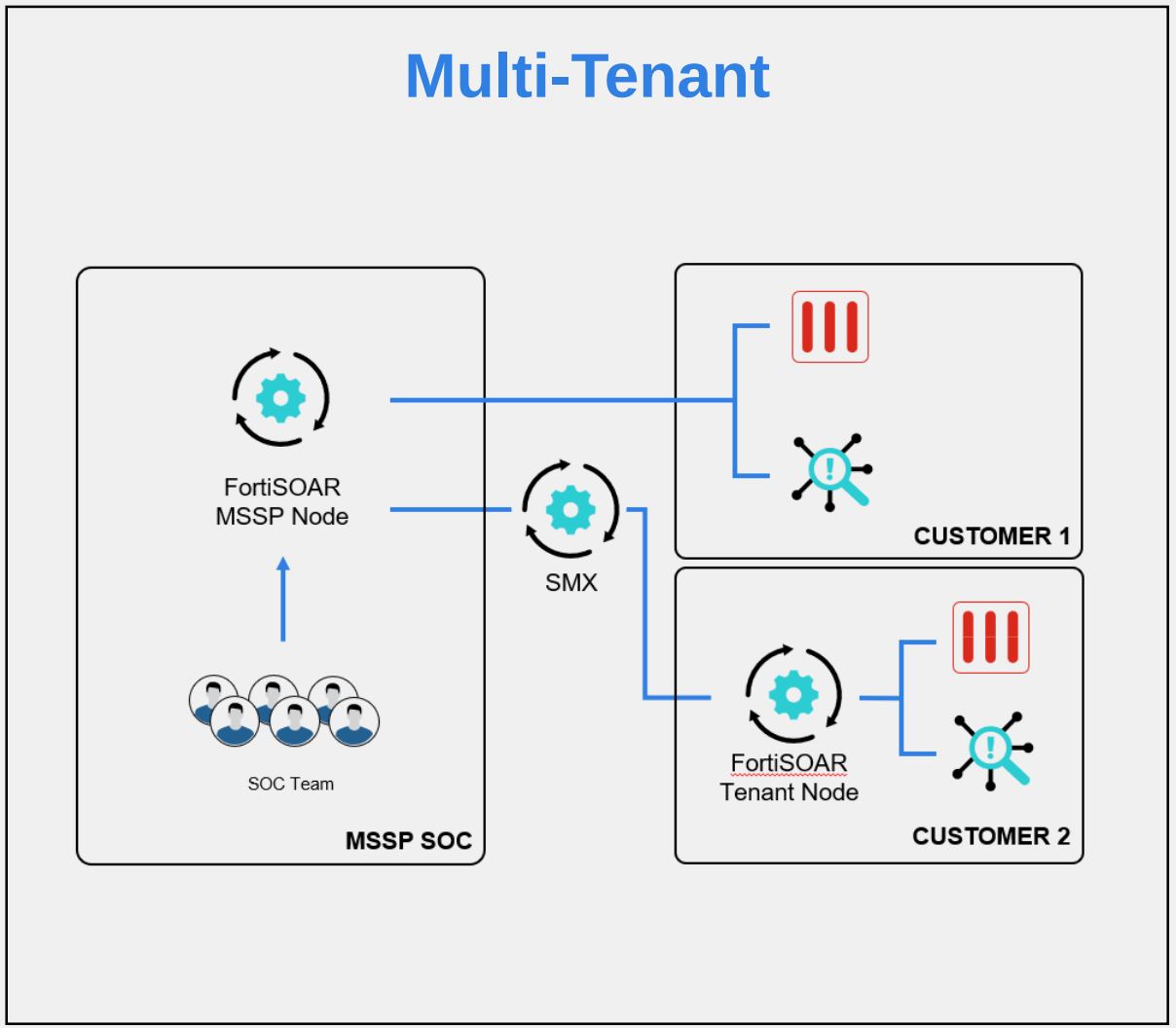
Пример: запрос на изменение NAT правил в конфигурации МЭ

Автоматизированный процесс

Архитектура

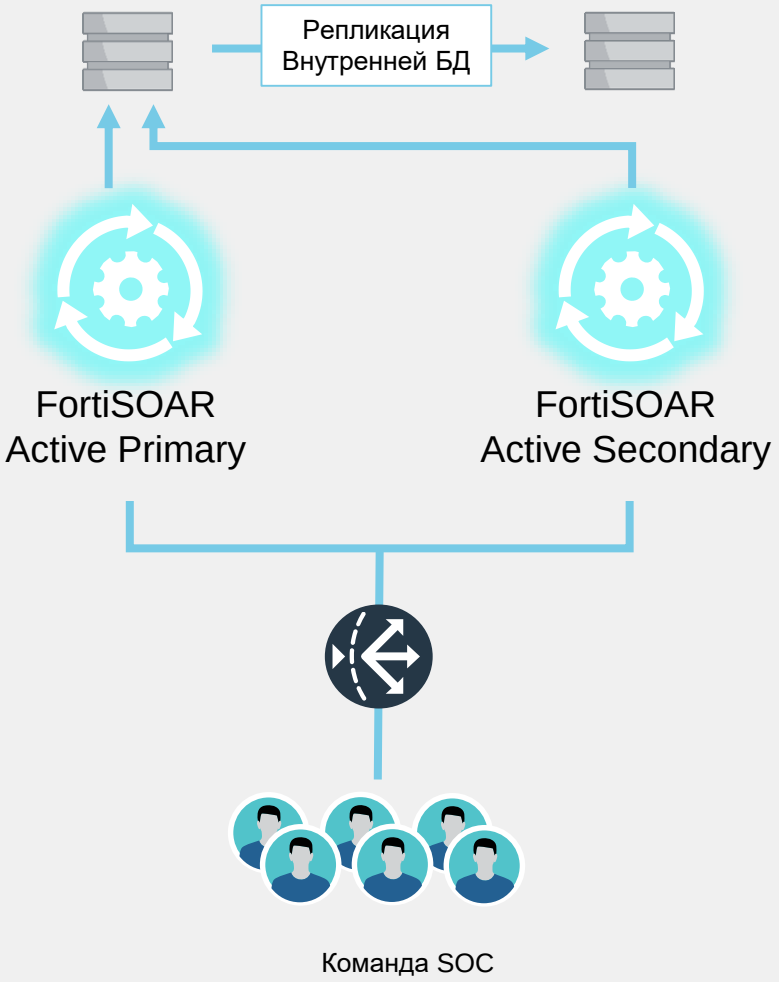
Гибкая и масштабируемая архитектура





Обеспечение высокой доступности и кластеризации

Высокая доступность и кластеризация для надежности и масштабируемости



- Active – Passive для надежности
- Active – Active для надежности и масштабируемости
  - Требуется использование балансировщика
- Поддержка внутренней и внешней базы данных
- Поддержка нескольких Secondary узлов
  - Требуется лицензия (HA license)

FortiSOAR 6.4

Основные возможности

FortiSOAR

Четыре столпа FortiSOAR:

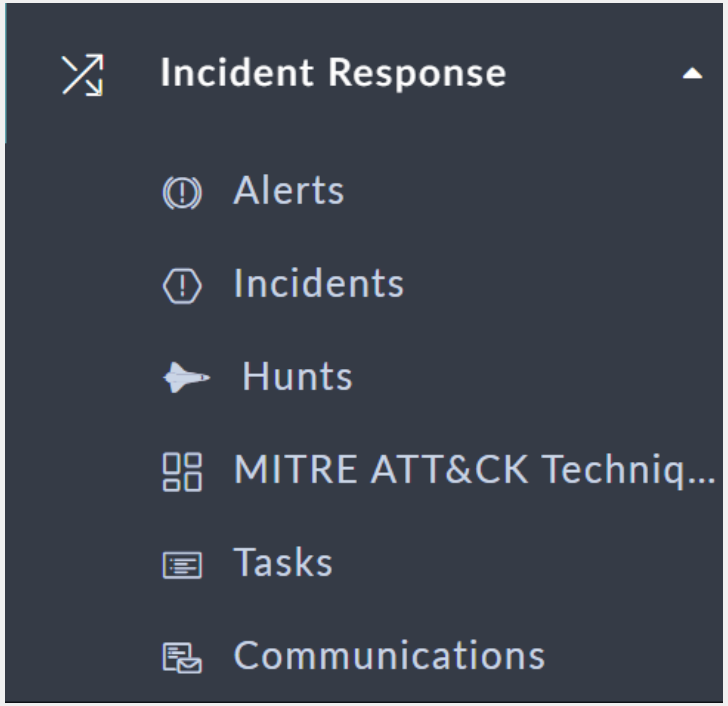
1. Incident and Case Management
2. Orchestration & Automation
3. Workflow & Collaboration
4. Threat Intelligence Management

Incident & Case Management

Компонент реагирования на инциденты

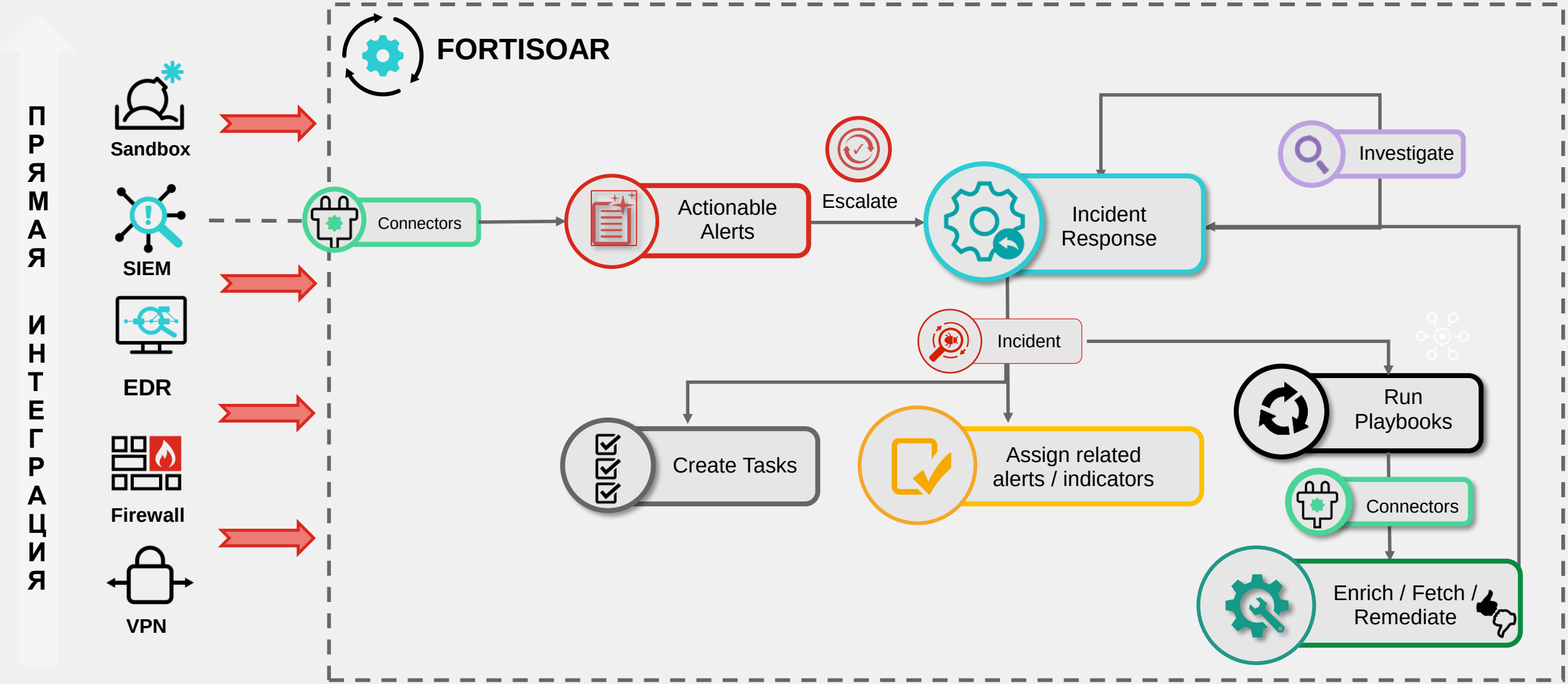
Компонент реагирования на инциденты содержит коллекцию модулей, связанных с инцидентами безопасности:

- Alerts: записи о подозрительной активности
- Incidents: записи фактического нарушения безопасности
- Hunts: записи о проводимых «поисках угроз»
- MITRE ATT&CK Techniques
- Tasks: действие, предпринимаемое индивидуальным или автоматическим ответом
- Communications: взаимодействия, выполняемые в рамках расследования запроса



Incident & Case Management

Реагирование на инциденты – Пример типового процесса

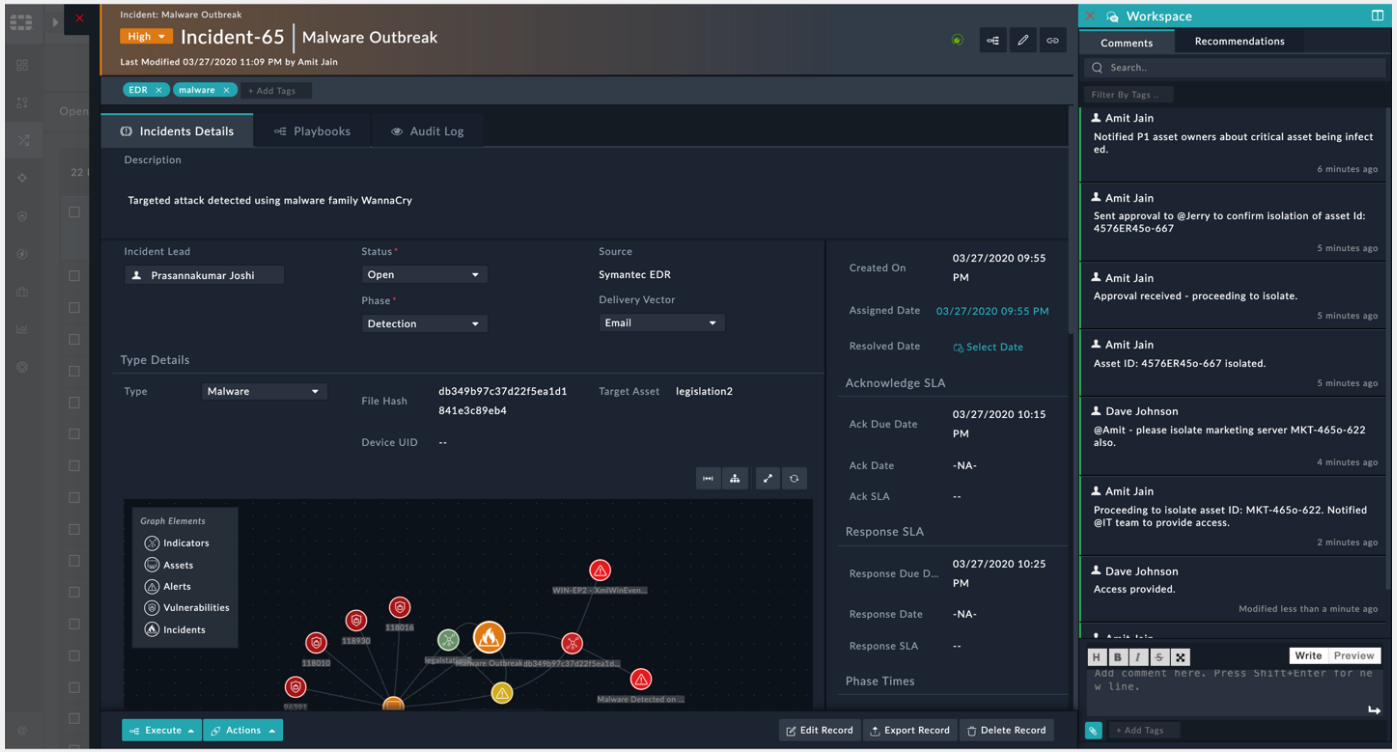


Incident & Case Management

Реагирование на инциденты – Alerts & Incidents

Единое место для просмотра и организации данных безопасности, которое позволяет уменьшить ручную работу с разрозненными инструментами безопасности.

- Отслеживание всего жизненного цикла инцидента
  - данные, статус, назначенный аналитк, дата и время последнего обновления
- Связывание записей
  - связывание активов, пользователей, индикаторов и уязвимостей
- Интуитивно понятный и настраиваемый вид
  - просмотр списка / сетки, фильтрация и поиск
- Интеграция с системами заявок

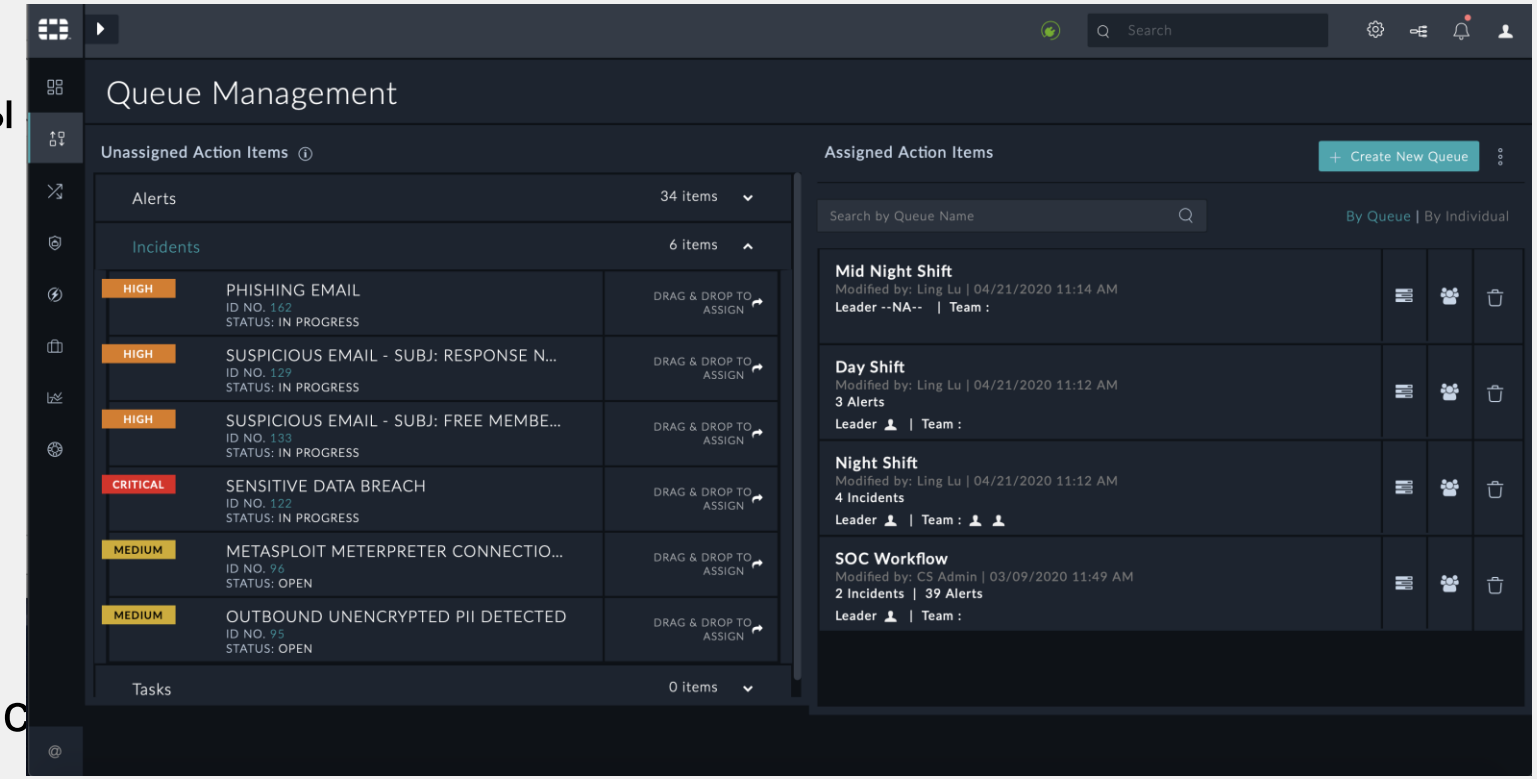


Incident & Case Management

Реагирование на инциденты – Queue Management

Предоставление обзора работы для менеджера SOC. Позволяет назначать ожидающие задачи командам или отдельным лицам.

- Создание очередей и добавление членов команды
- Назначать оповещения, инциденты и задачи в очередь
  - Вручную (drag and drop)
  - Автоматически через playbook
- Просмотр назначений по очередям или по отдельным людям
- Очереди могут управляться с помощью playbook’ов



Orchestration & Automation

Разве оркестрация и автоматизация не одно и то же?

Orchestration: возможность управлять или контролировать внешние системы через определенные коннекторы

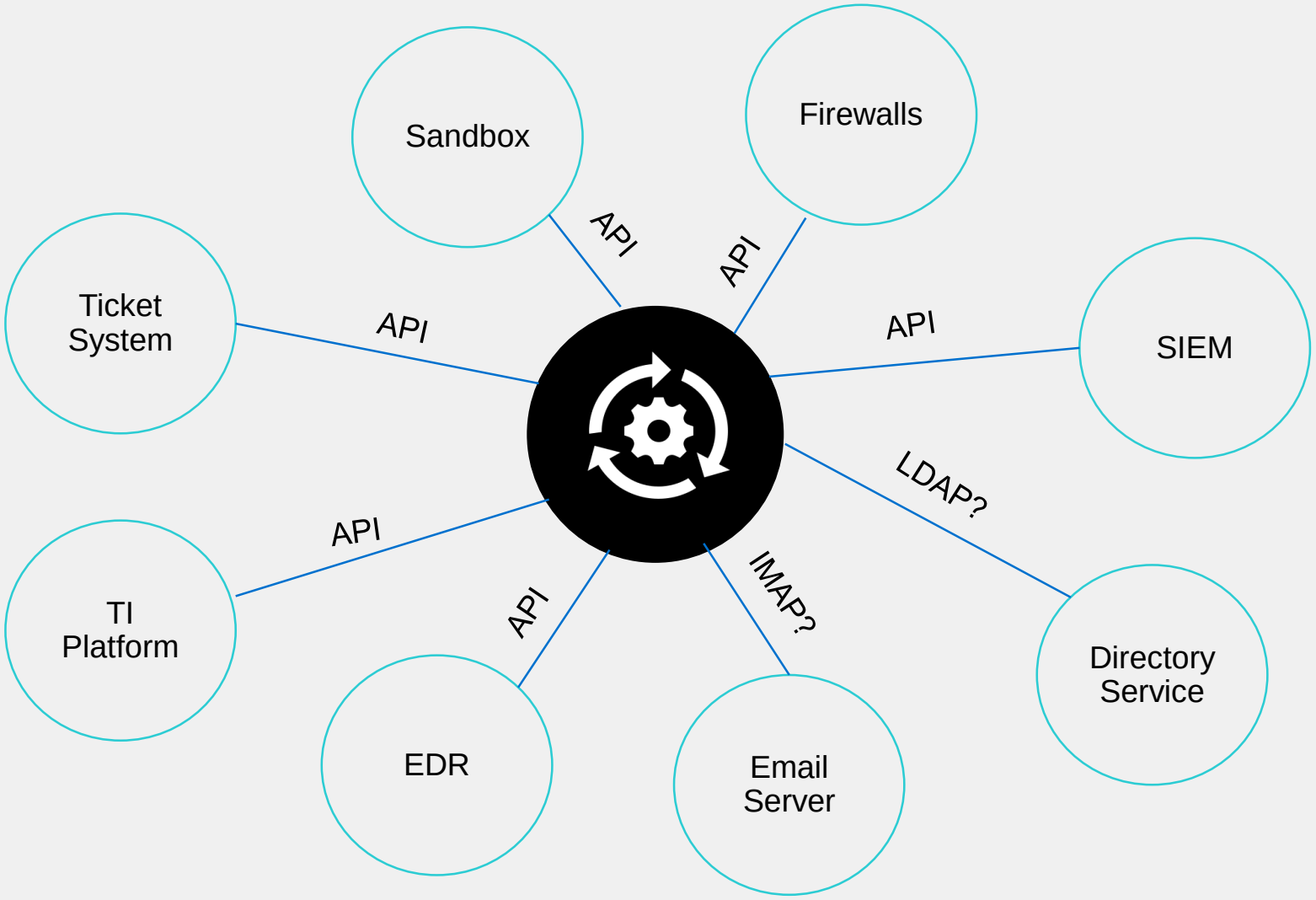
Automation: выполнение сценария реагирования (playbook) при выполнении определенных условий

Playbooks: коллекция действий на основании скриптов

Например, может быть создан playbook, который срабатываем при получении определенного предупреждения от SIEM и автоматически собирает дополнительные контекстные данные, прежде чем привлекать оператора-аналитика.

Orchestration & Automation

Оркестрация – Методы интеграции

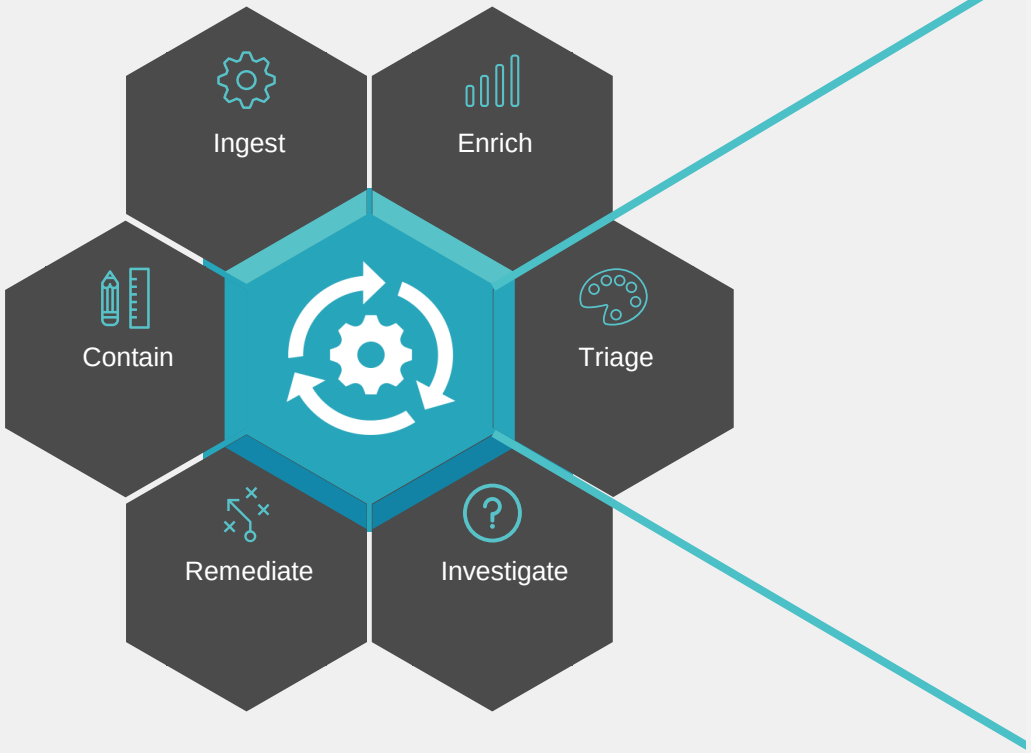


Connectors

- Сбор
- Обогащение
- Содержание
- Восстановление
- Сортировка
- Расследование

Orchestration & Automation

Оркестрация – Connectors



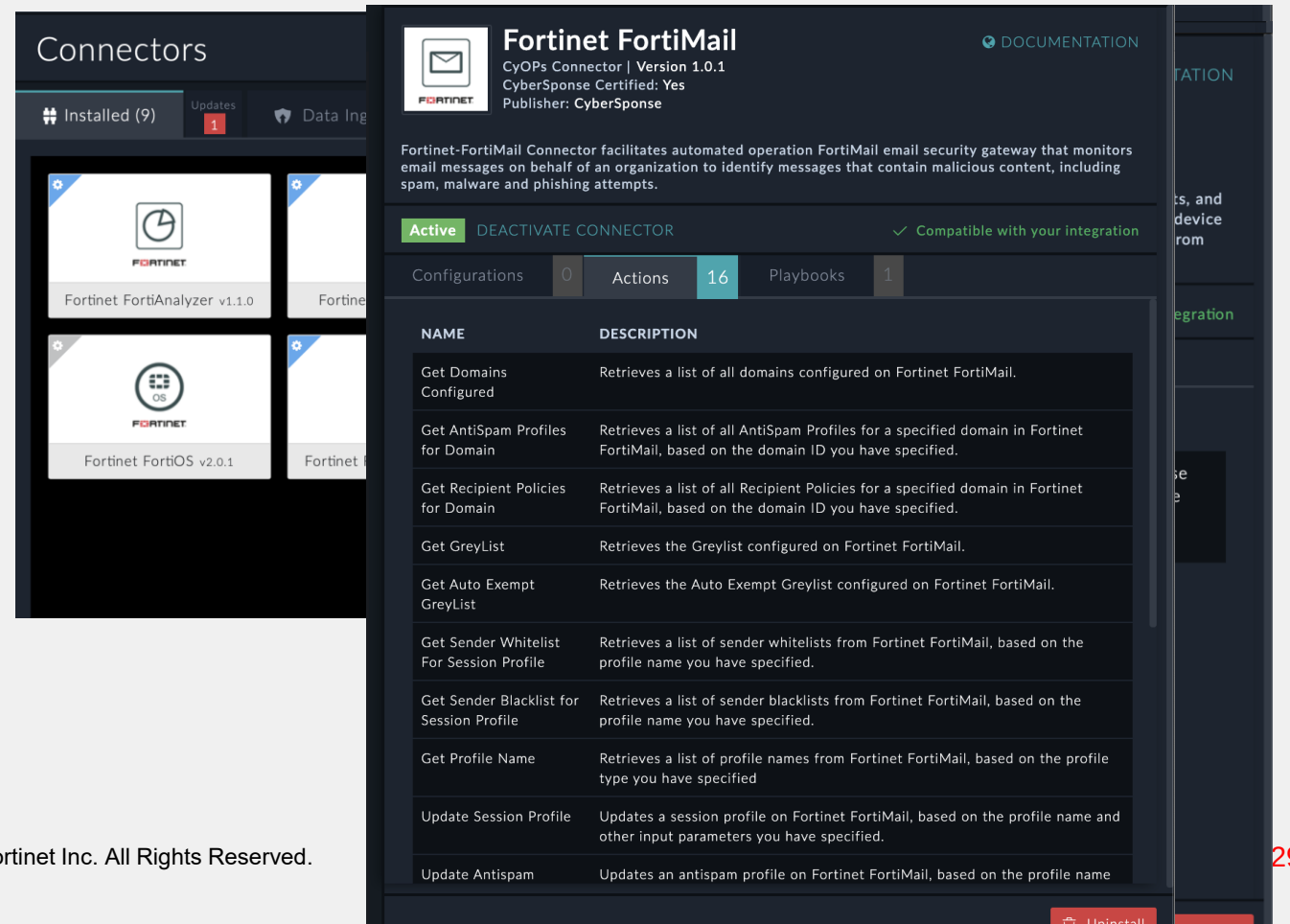
- 300+ коннекторов, 3000+ действий
- Дополнительные интеграции разрабатываются каждые 3 недели

Orchestration & Automation

Оркестрация – Connectors

Используя коннекторы, вы можете подключаться к внешним инструментам кибербезопасности для выполнения различных автоматических взаимодействий с использованием playbook’ов.

- Connectors Store
  - Просмотр, поиск, установка, обновление и удаление
  - Для установки необходимы права на чтение (Read) и создание (Create) на Connectors module
- Built-in Connectors
- Custom Connectors
  - Создание собственных коннекторов с помощью SDK



Orchestration & Automation

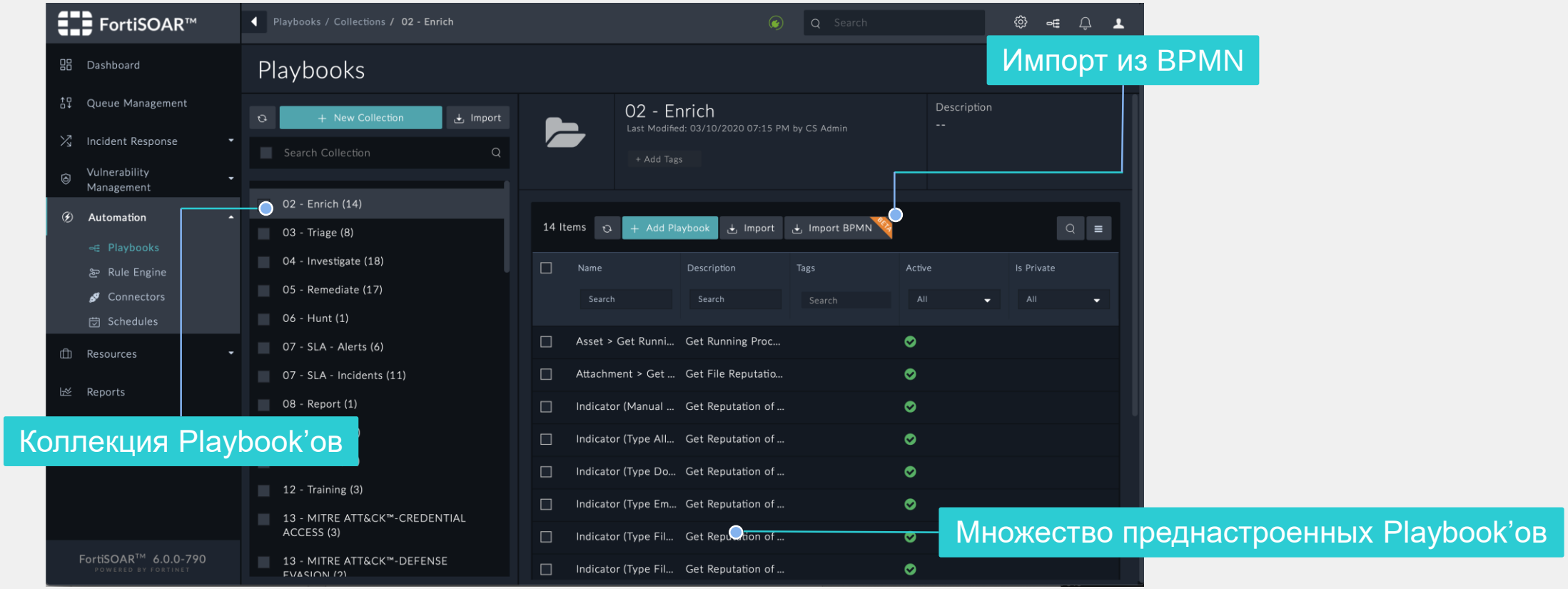
Оркестрация – Data Ingestion

Коннекторы FortiSOAR предоставляются с примерами playbook’ов для сбора данных из разных источников.

- Источники данных
  - SIEM, Threat Intelligence Platforms, Vulnerability Management Tools
- Прием данных при помощи коннекторов
  - Ingestion wizard
  - Ingestion playbook
- Режим приема данных
  - На базе оповещений
  - На базе расписания
  - App Push

Orchestration & Automation

Автоматизация – Репозиторий сценариев реагирования

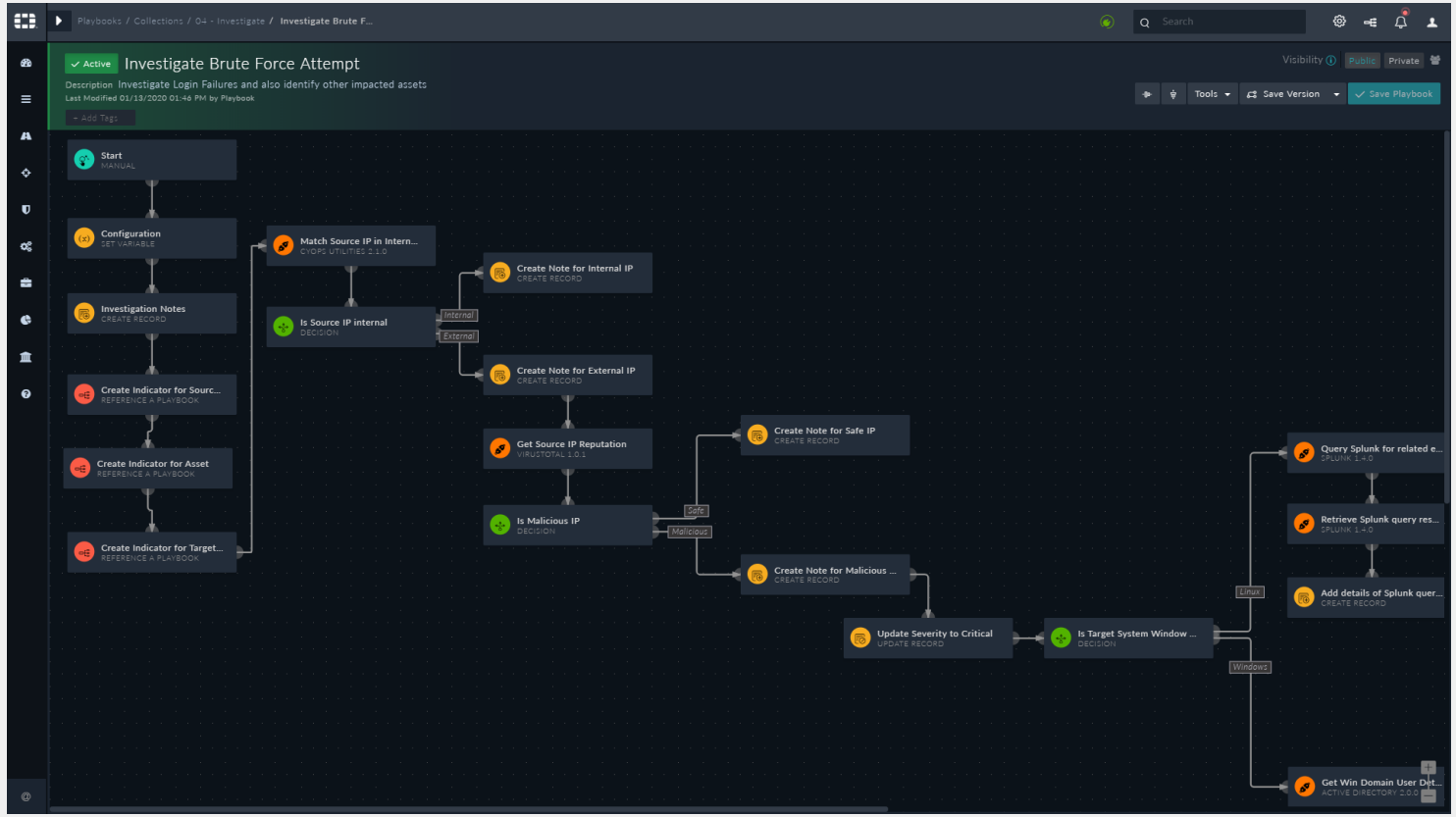


Orchestration & Automation

Автоматизация – Visual Playbook Editor для создания кастомного playbook’а

Внедряйте свои лучшие практики и весь рабочий процесс в playbook’и для последовательной обработки инцидентов и реагирования.

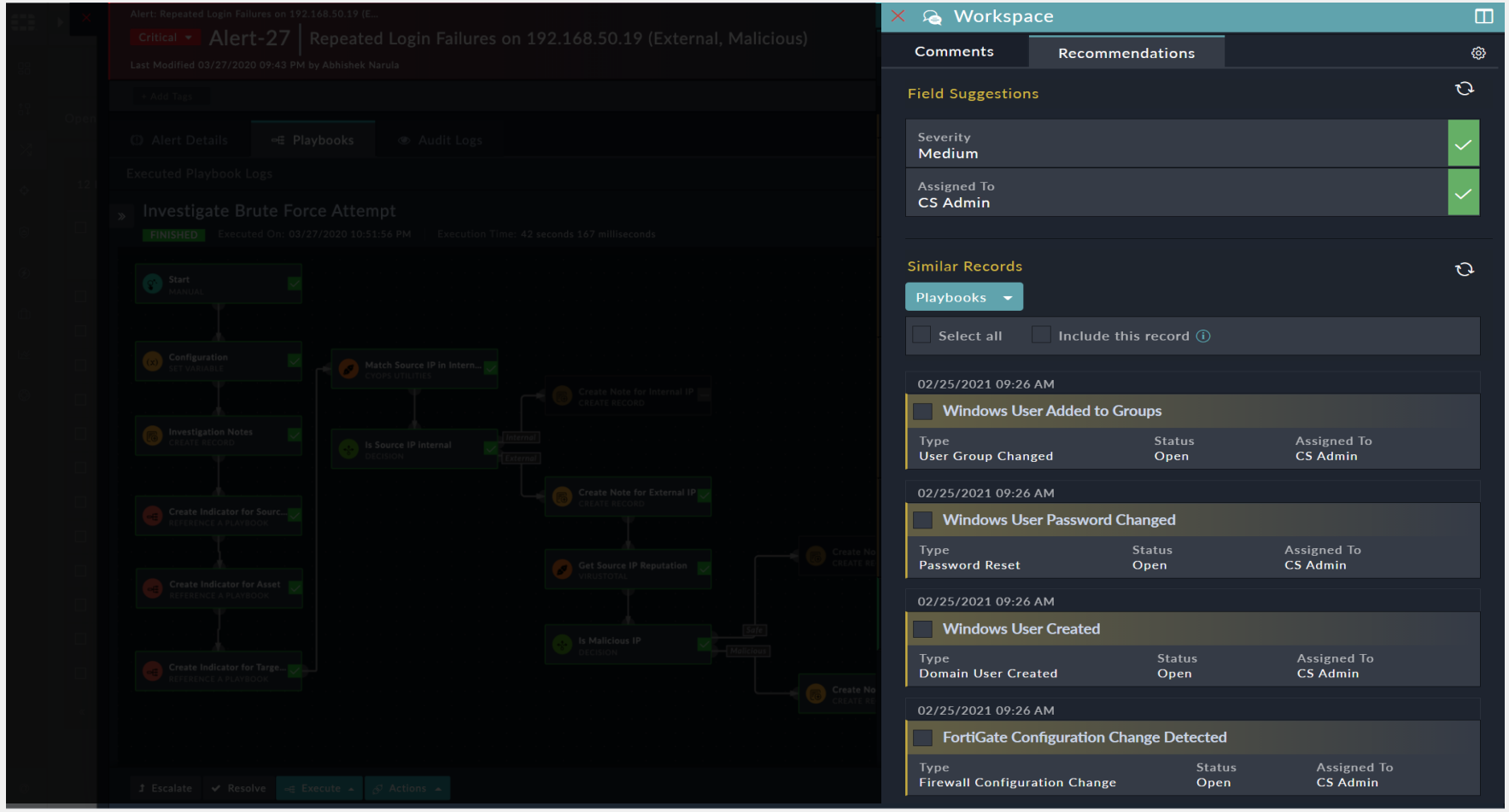
- Перетащите блок в режиме drag and drop для модификации и добавления шага в playbook’е
- Разнообразие выбора из графических меню
  - Создать/Обновить/Найти запись
  - Логические решения, согласования и задачи
  - Коннекторы и утилиты
  - Вложенные playbook’и



Workflow & Collaboration

Рабочая область для совместной работы & SOC FAQs

- Рабочая область Workspace
- Comments для обмена вспомогательными документами и взаимодействия
- Recommendations для поиска схожих записей
- Раздел FAQs для фиксации ответов на наиболее частые вопросы

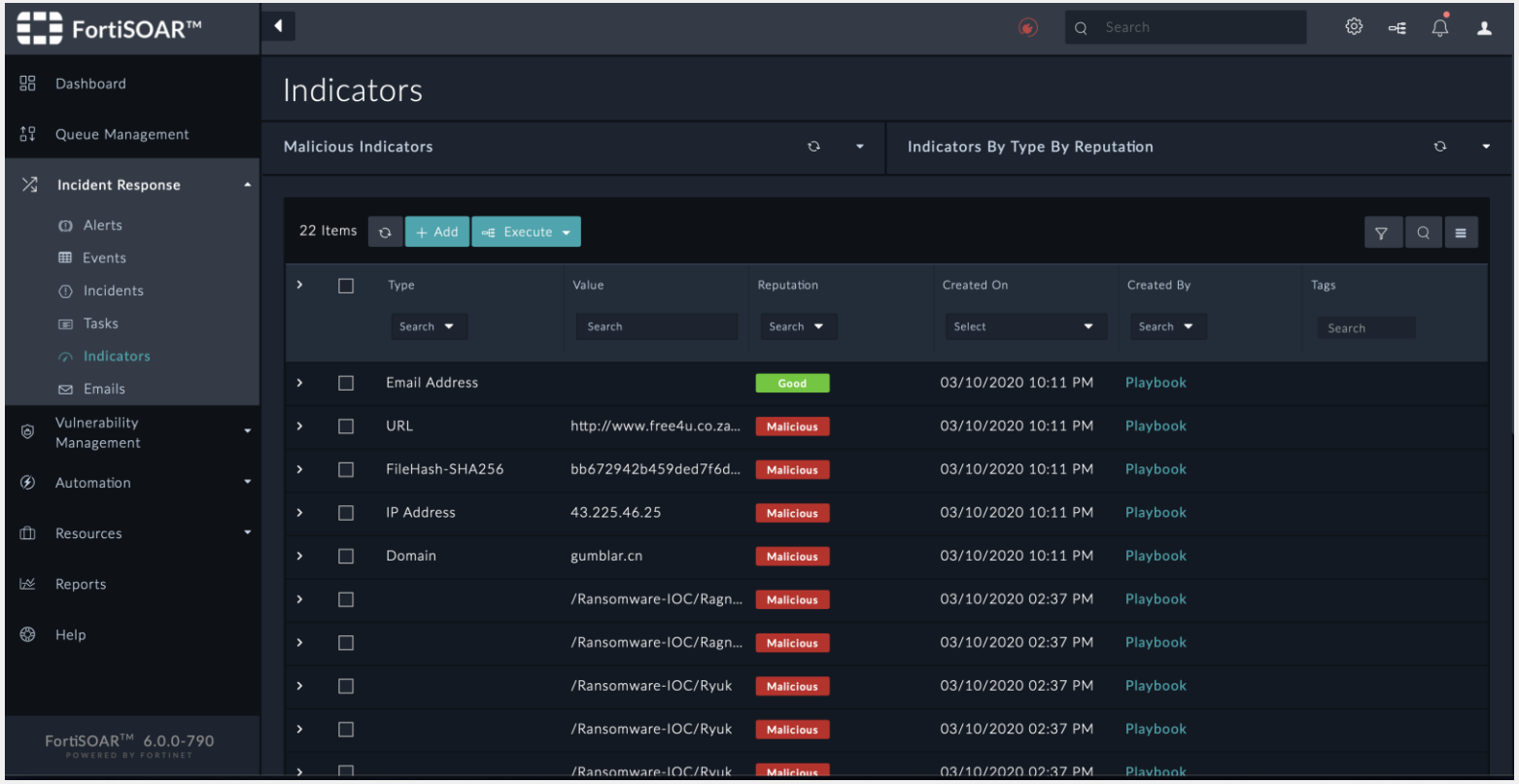


Threat Intelligence Management

Модуль Indicators

Управление несколькими форматами и источниками TI из центральной системы и связывание данных об угрозах с оповещениями и инцидентами.

- Извлечение информации об угрозах из оповещений, загруженных файлов, электронных писем и внешних источников анализа угроз (TI)
- Сохранение информации об угрозе в БД для использования другими модулями

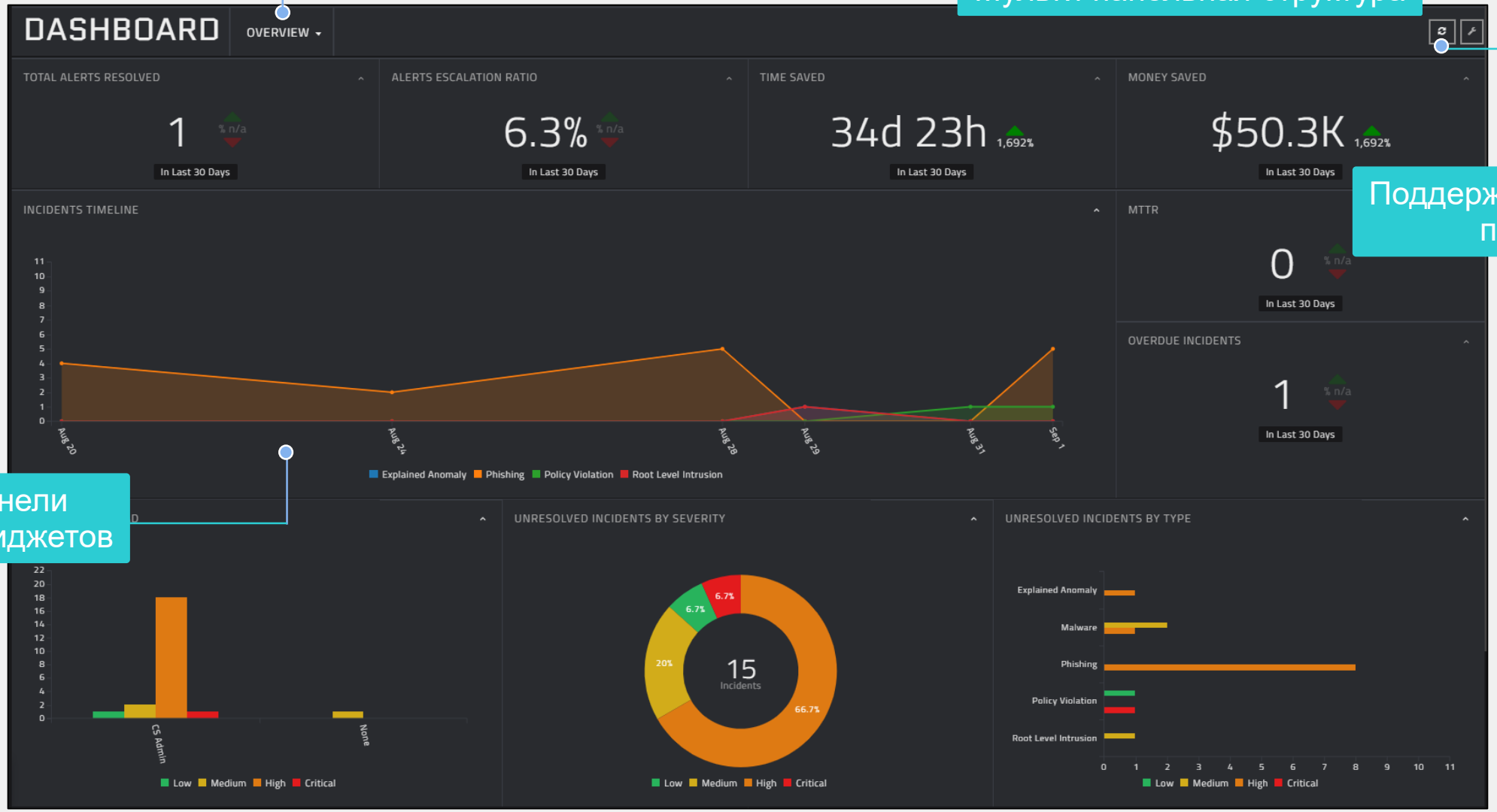


Панели управления (Dashboards)

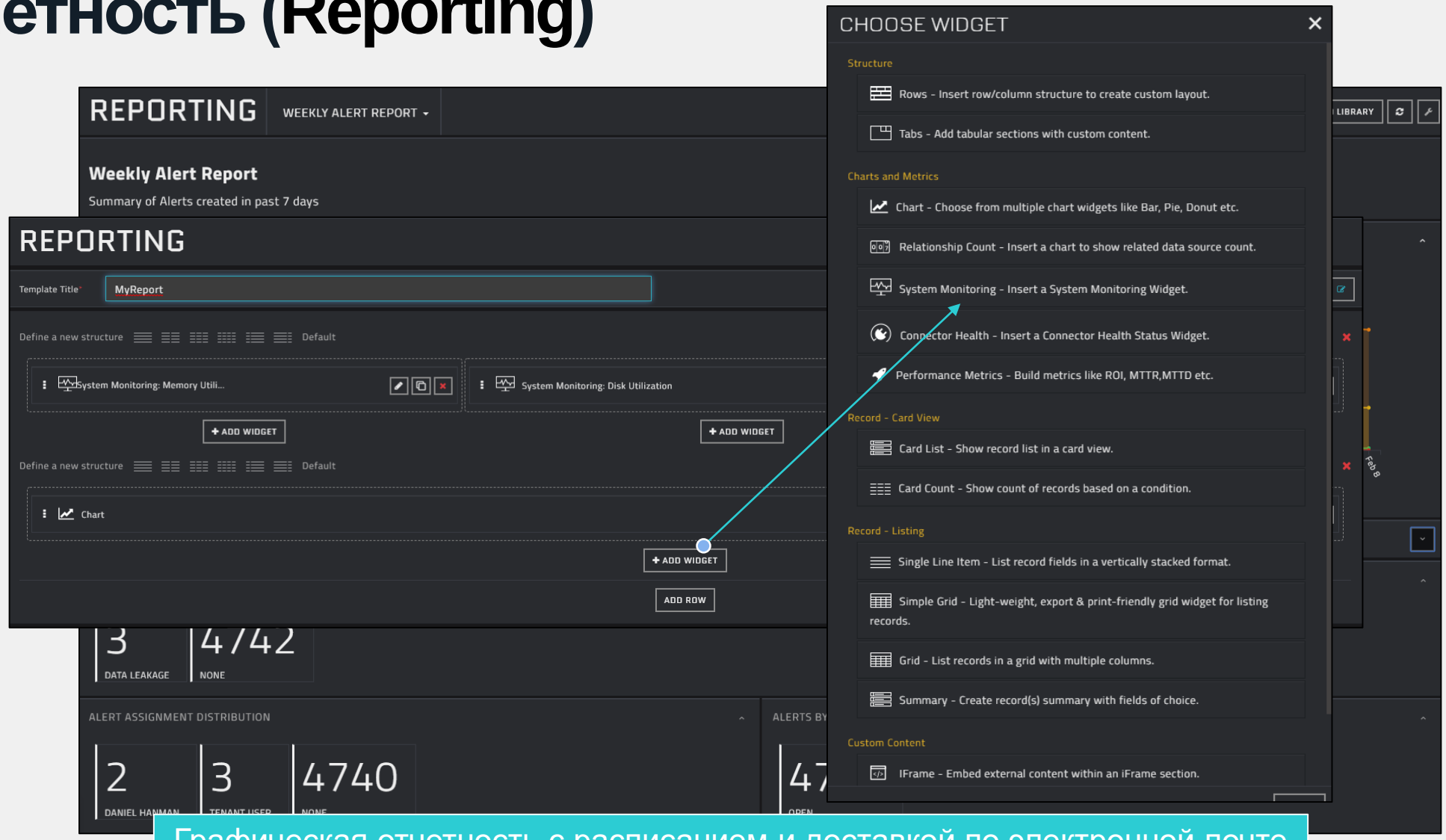
Мульти-панельная структура

Поддержка кастомных панелей

Гибкие панели на основе виджетов



Отчетность (Reporting)

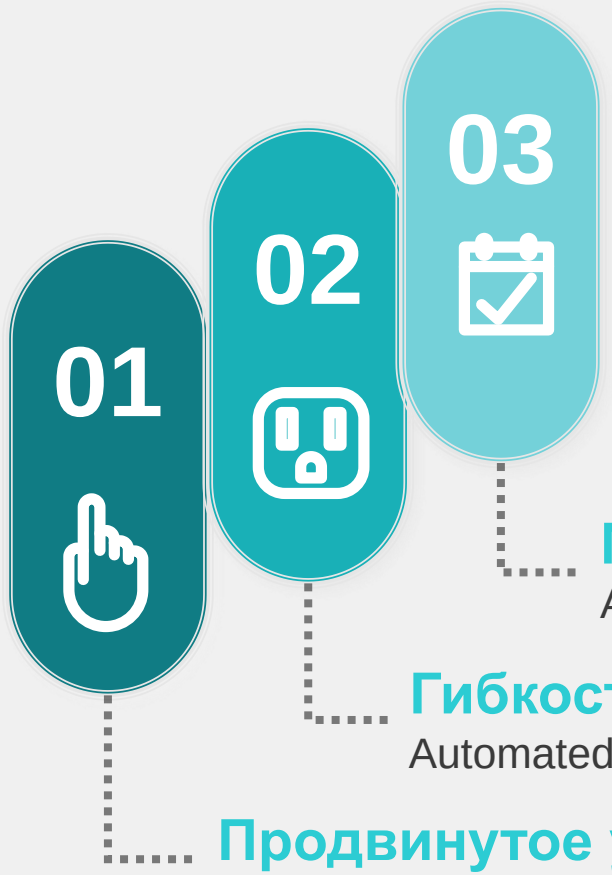


Графическая отчетность с расписанием и доставкой по электронной почте

Построение пользовательских отчетов с помощью редактора отчетов на основе виджетов

Особенности

Ключевые особенности FortiSOAR



Комплексная автоматизация и оркестрация

- Повышение безопасности
- Перекрестное сотрудничество
- Разделение команд и обязанностей

Масштабируемая архитектура

Active/Active HA, Distributed Multi-Tenancy, Light weight agent, dedicated tenant

Гибкость продукта

Automated beyond the investigation, Modify existing modules, Customize Modules

Продвинутое управление кейсами

SOAR + IR + VM + Legal + Dashboards, Reporting, Role Based Access Control

Демонстрация


FORTINET