FortiSOAR – реагирование на инциденты в режиме реального времени

Olesya Tarabrina, SE

Сложность экосистемы увеличивает время реагирования и восстановления

И приводит к усложнению построения системы оркестрации, автоматизации и реагирования

Слишком много вендоров

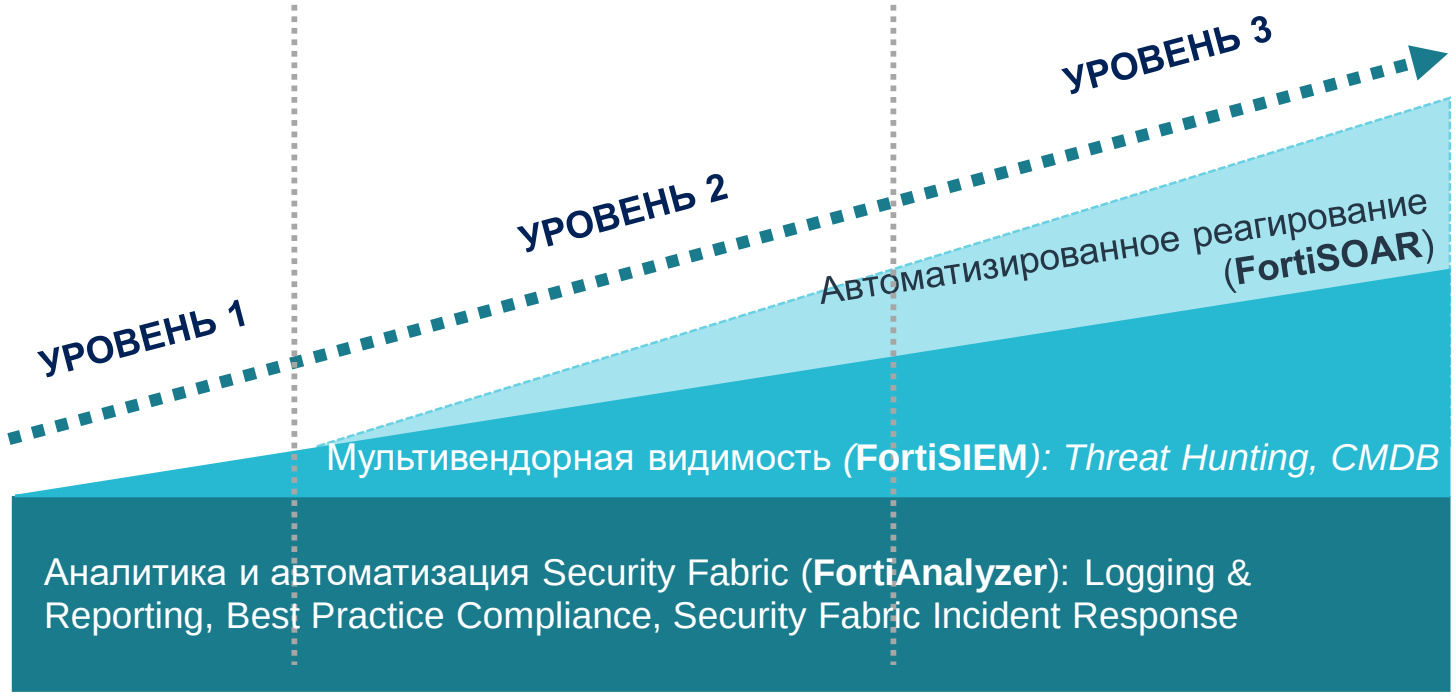
Слишком много алертов

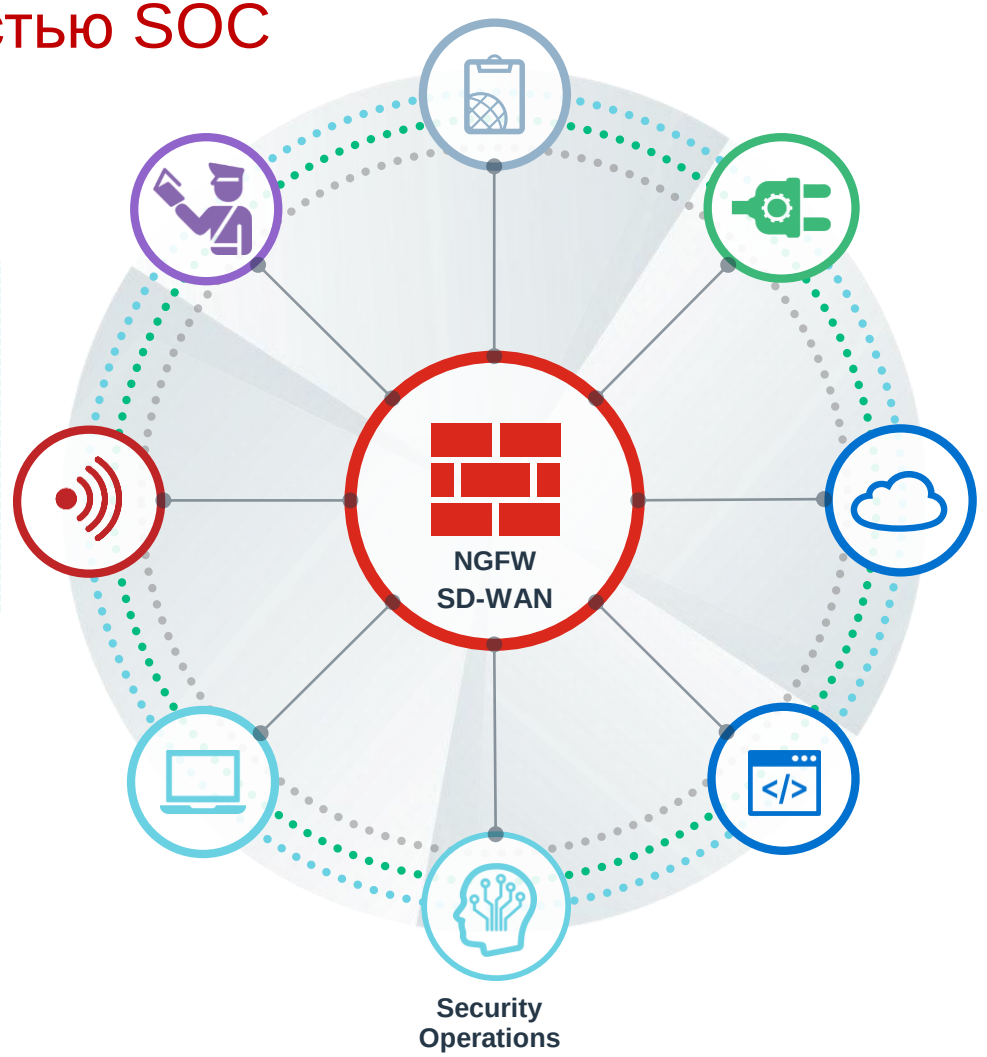
Ручной и медленный ответ

Недостаток квалифицированных специалистов

Упрощение операций безопасности

Выбор предложения в соответствии со зрелостью SOC





Уровни зрелости Security Operations Center (SOC)

	Зрелость SOC УРОВЕНЬ 1	Зрелость SOC УРОВЕНЬ 2	Зрелость SOC УРОВЕНЬ 3
Люди	Средний бизнес с одной командой - ИТ & Безопасность (<5 сотрудников IT-security)	Средне-крупный бизнес с выделенной командой безопасности (3-5 выделенных сотрудников службы безопасности)	Крупное предприятие с опытными аналитиками SOC / командой SOC (5+ выделенных сотрудников SOC)
Процессы	Реагирование на инцидент с максимальным усилием	Базовый план реагирования на инциденты	Продвинутые процессы SOC и сценарии реагирования (playbooks)
Возможности	• Logging & Reporting • Automated Detection & Response	Уровень 1 плюс: • Multi-Vendor Incident Detection	Уровень 2 плюс: • Alert Management • Unified Orchestration Automation & Response

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

- Visual Playbook Builder
- Monitor Playbook Performance
- 290+ Connectors, 3000+ Actions

2. Автоматизация упорядочивания алертов

БИЗНЕС ДРАЙВЕР

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

Устранение усталости от алертов и способность сосредоточиться на поиске угроз.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Prioritize alerts across SOC team
- Role-based Incident Management
- Easily Create Custom Modules

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 Dashboards for SOC
- Customizable Dashboards & Reports
- Role-based User Reporting

4. Взаимодействие в рамках SOC

БИЗНЕС ДРАЙВЕР

59% организаций имеют незакрытые должности в службах беопасности. Используйте возможности FortiSOAR ™, чтобы заполнить пробелы в навыках, одновременно снижая затраты. FortiSOAR ™ обеспечивает кросс-функциональную совместную работу для ускорения процесса восстановления и работы с оповещениями безопасности.

В результате улучшается совместная работа в команде, снижается нагрузка и расширяются возможности безопасности.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Team Collaboration Workspace
- Automate Responses to Alerts, Incidents, Vulnerabilities
- 24hr Workspace Continuity

FortiSOAR 6.4

Основные возможности

FortiSOAR

Четыре столпа FortiSOAR

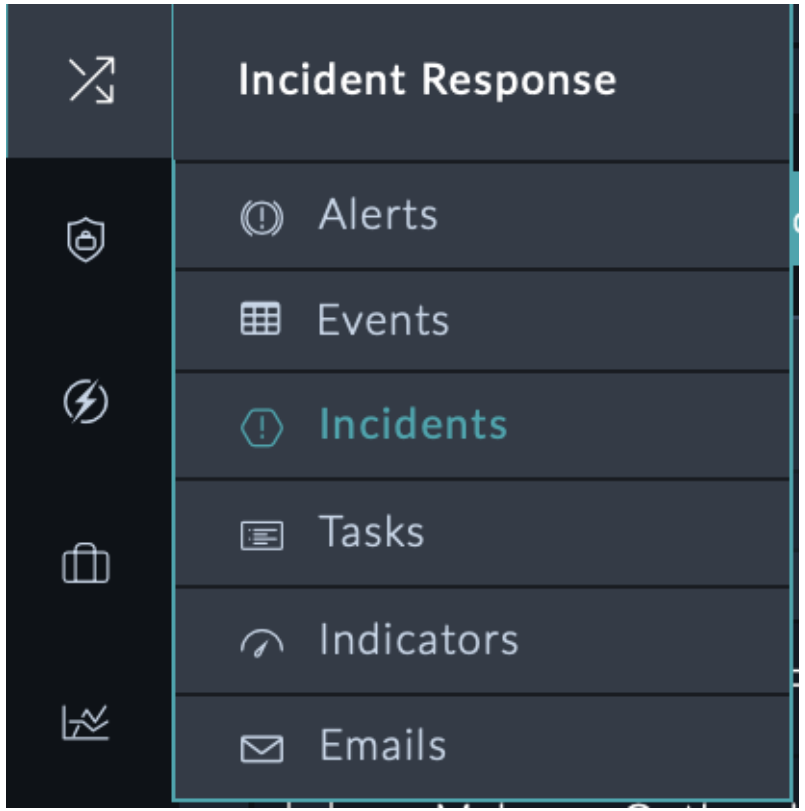
1. Incident and Case Management
2. Orchestration & Automation
3. Workflow & Collaboration
4. Threat Intelligence Management

Incident & Case Management

Компонент реагирования на инциденты

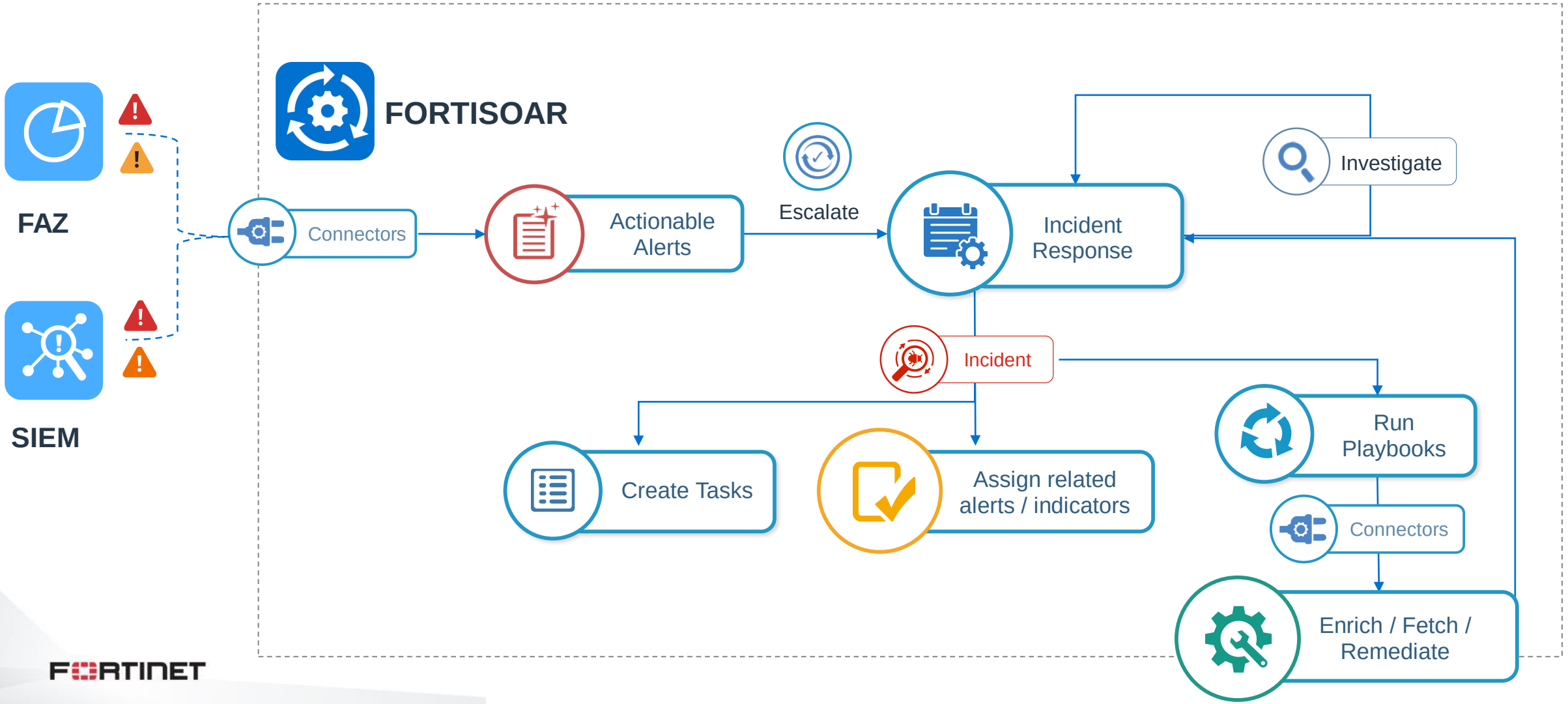
Компонент реагирования на инциденты содержит коллекцию всех модулей, связанных с инцидентами безопасности.

- Alerts: записи о подозрительной активности
- Incidents: записи фактического нарушения безопасности
- Tasks: действие, предпринимаемое индивидуальным или автоматическим ответом
- Indicators: записи, идентифицирующие угрозу
- Emails & MITRE ATT&CK Techniques



Incident & Case Management

Реагирование на инциденты – Пример типового процесса

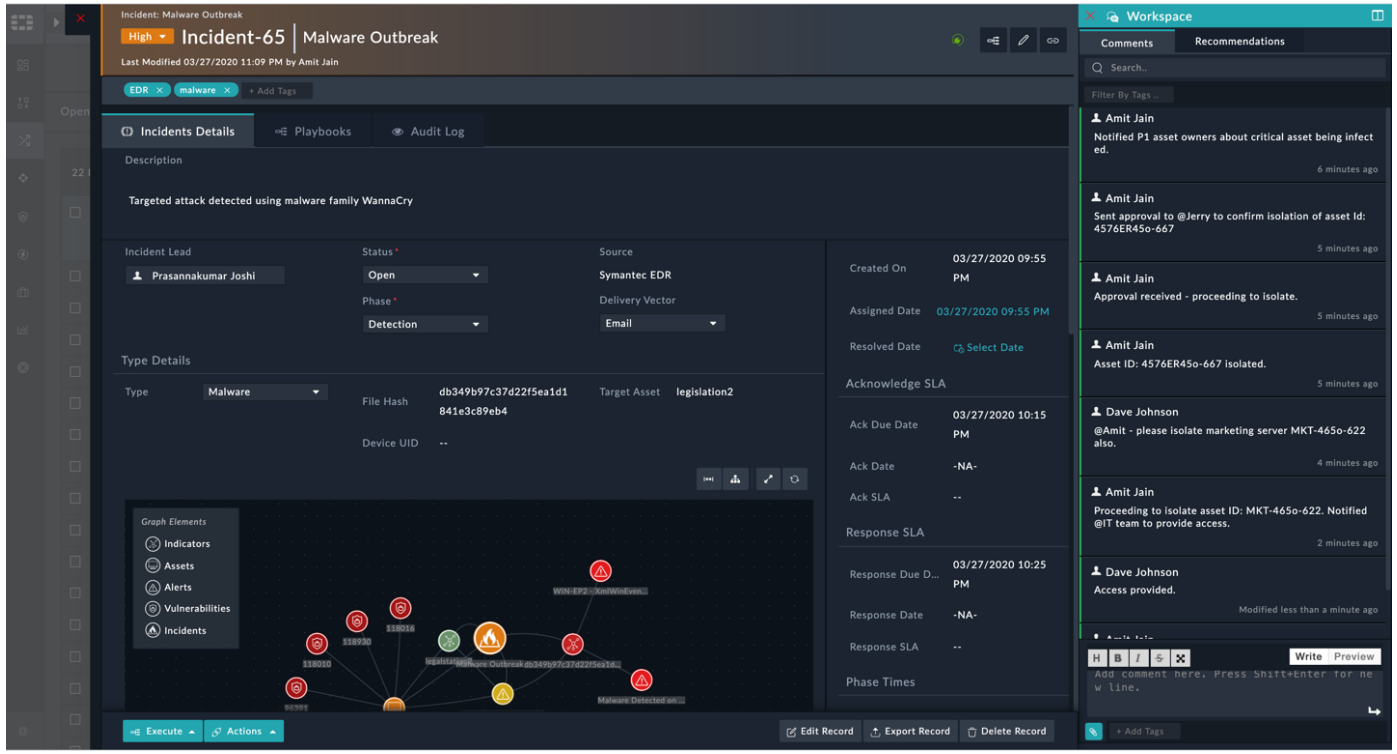


Incident & Case Management

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

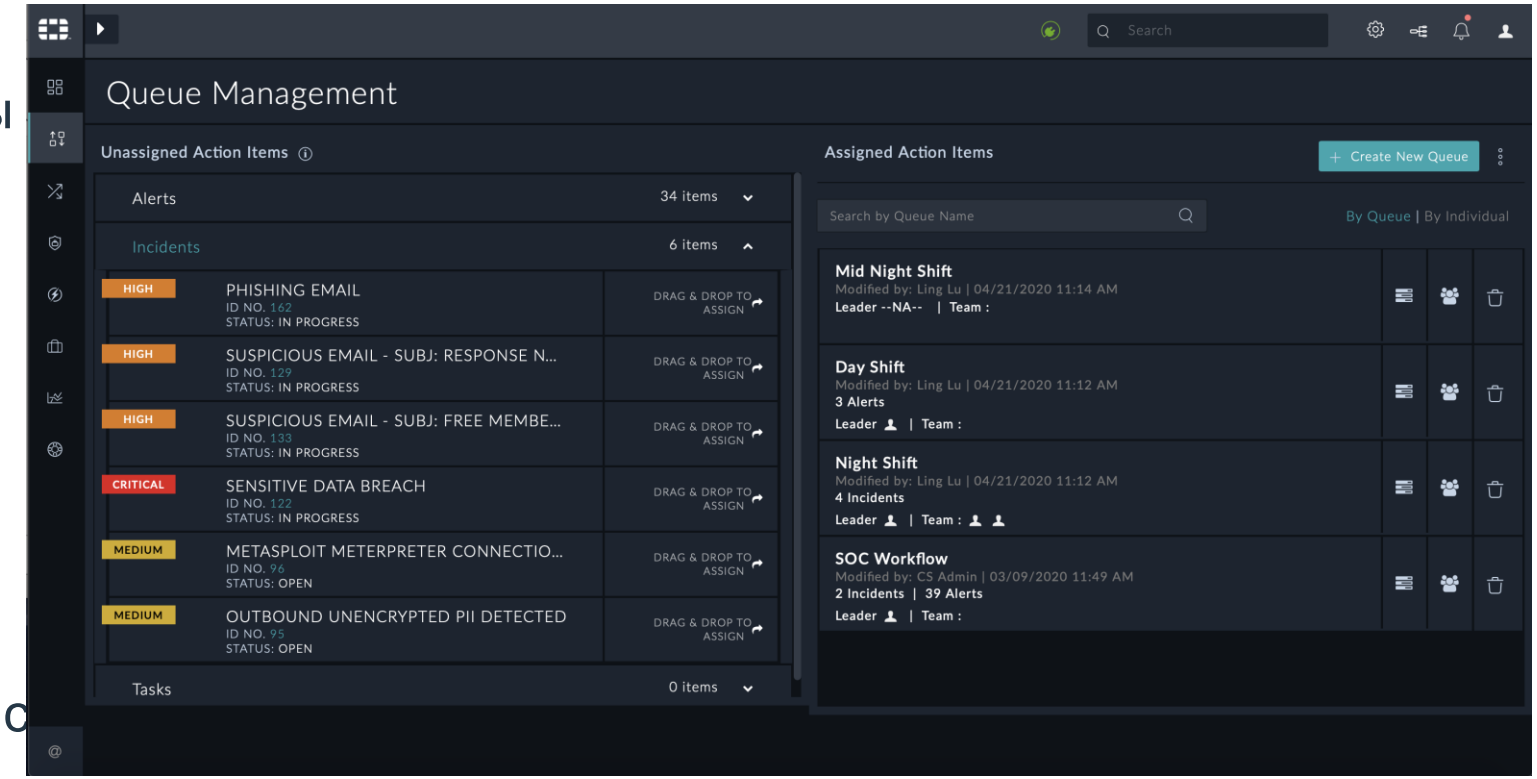


Incident & Case Management

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

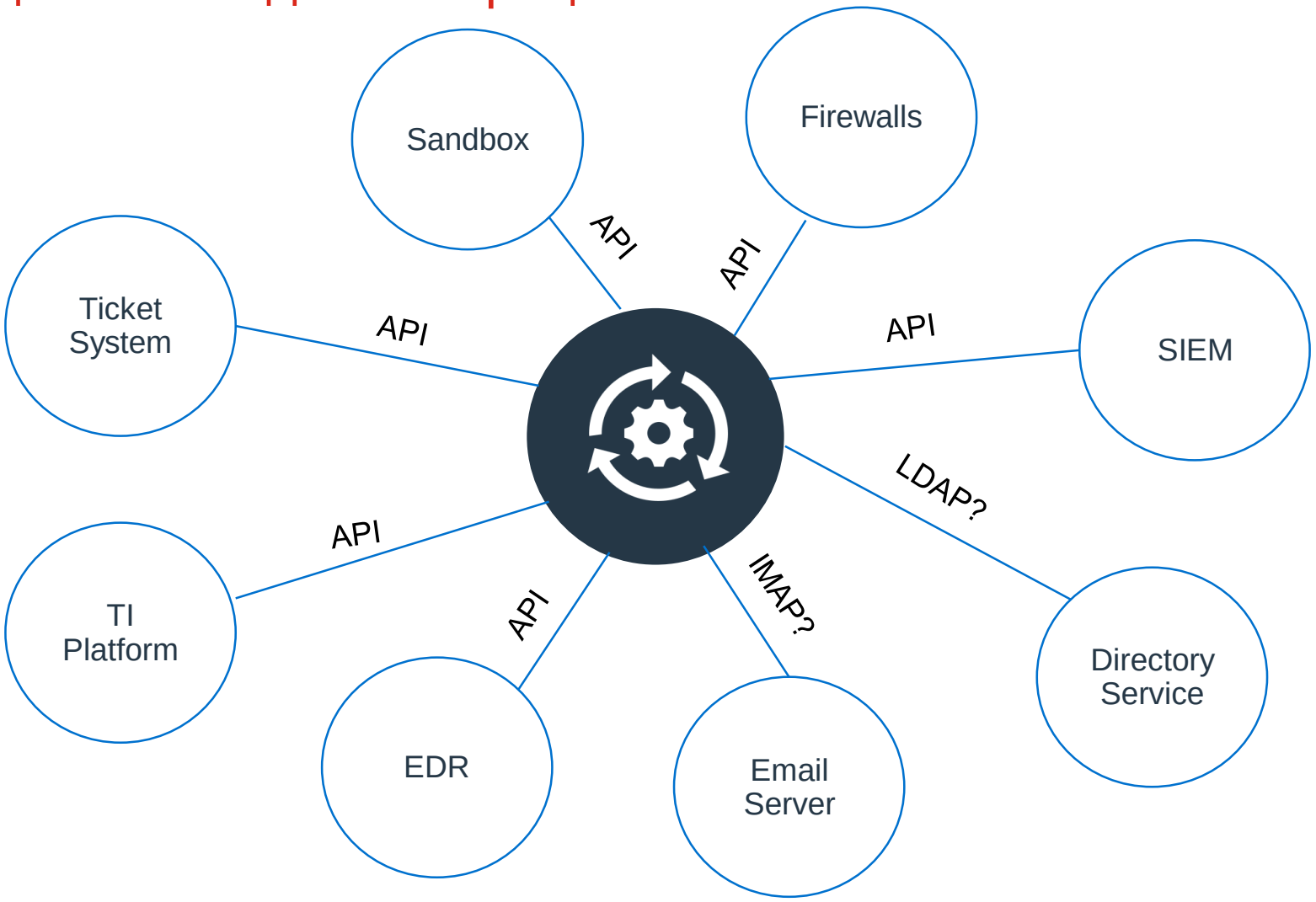
Automation: выполнение сценария реагирования (playbook) при выполнении определенных условий

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

280+ коннекторов, 3000+ действий

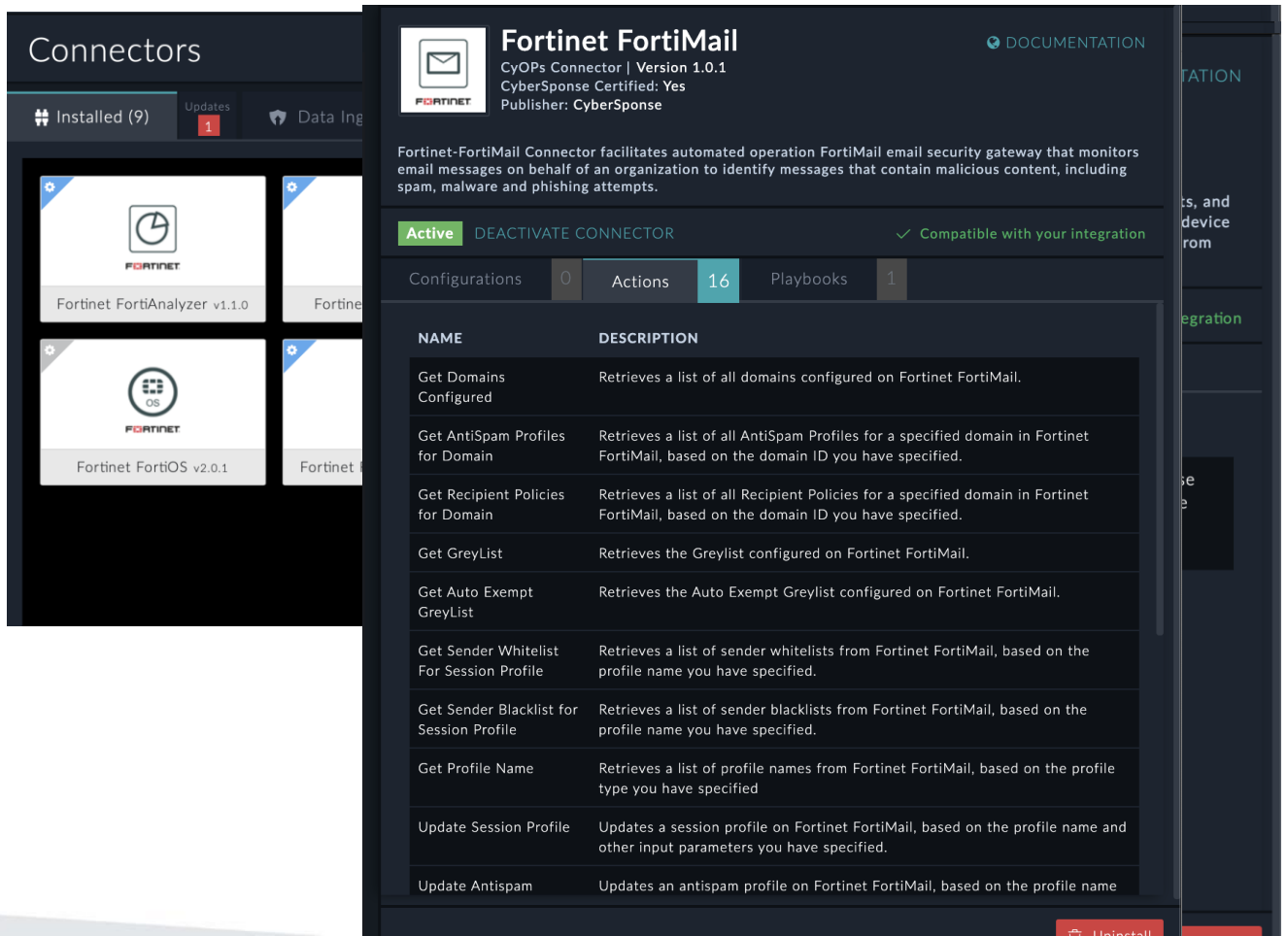
Дополнительные интеграции разрабатываются каждые 3 недели

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

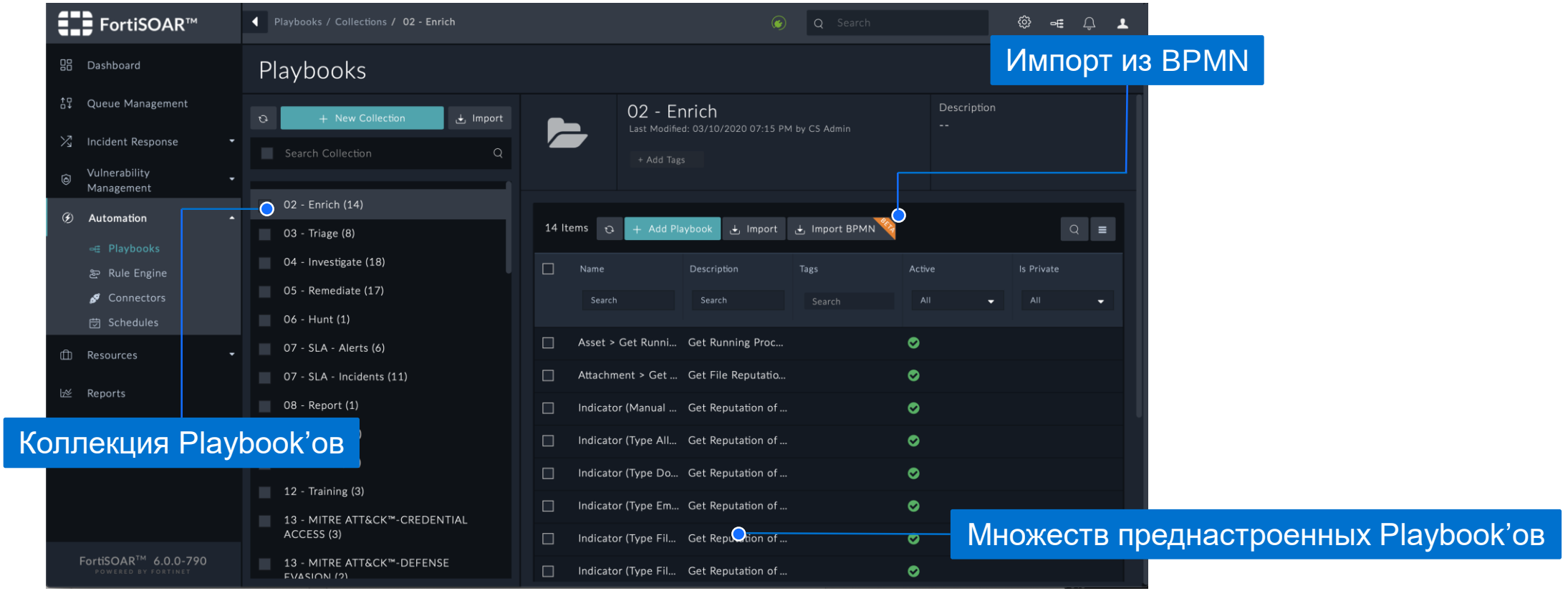
Оркестрация – Data Ingestion

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

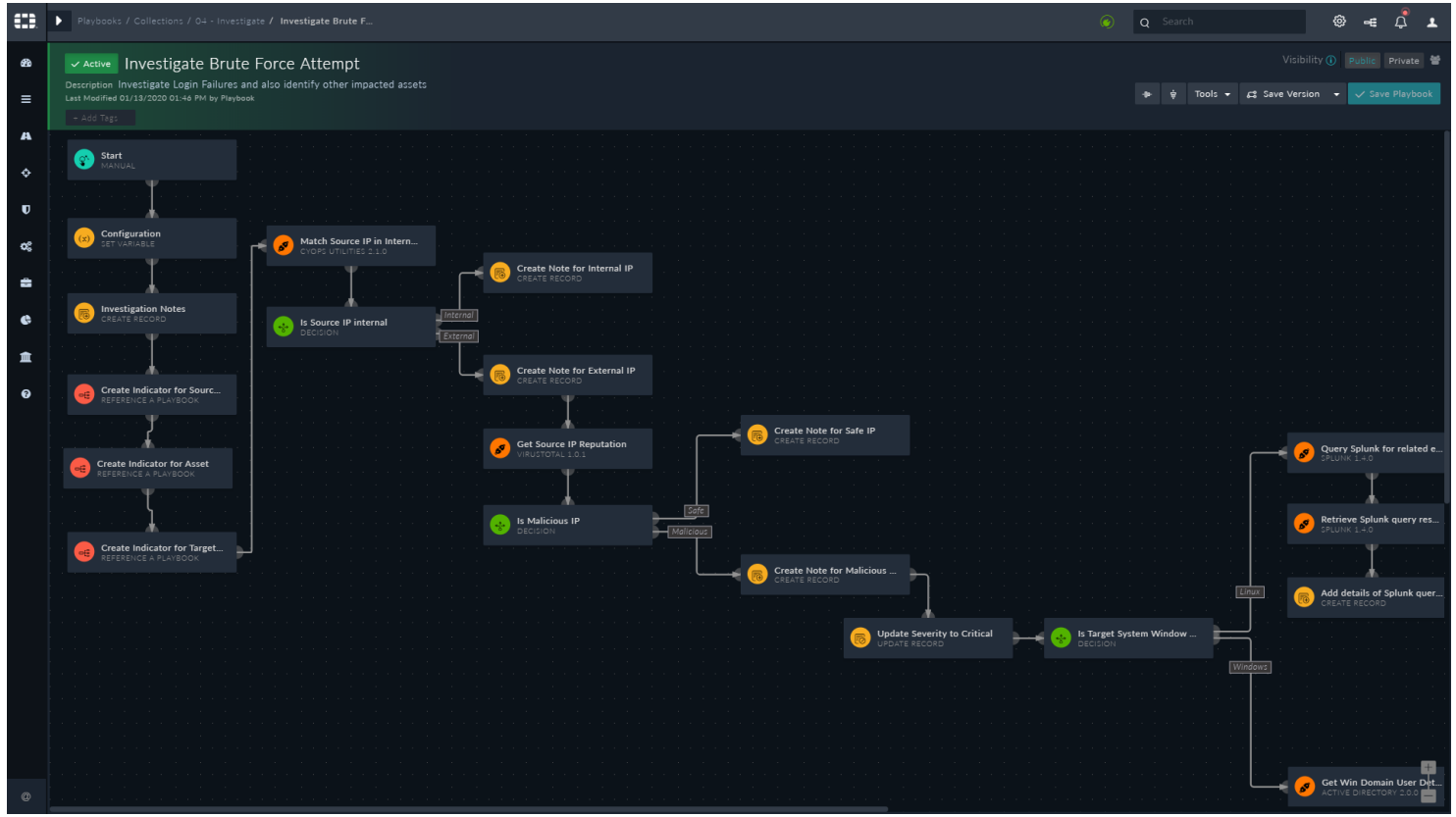


Orchestration & Automation

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

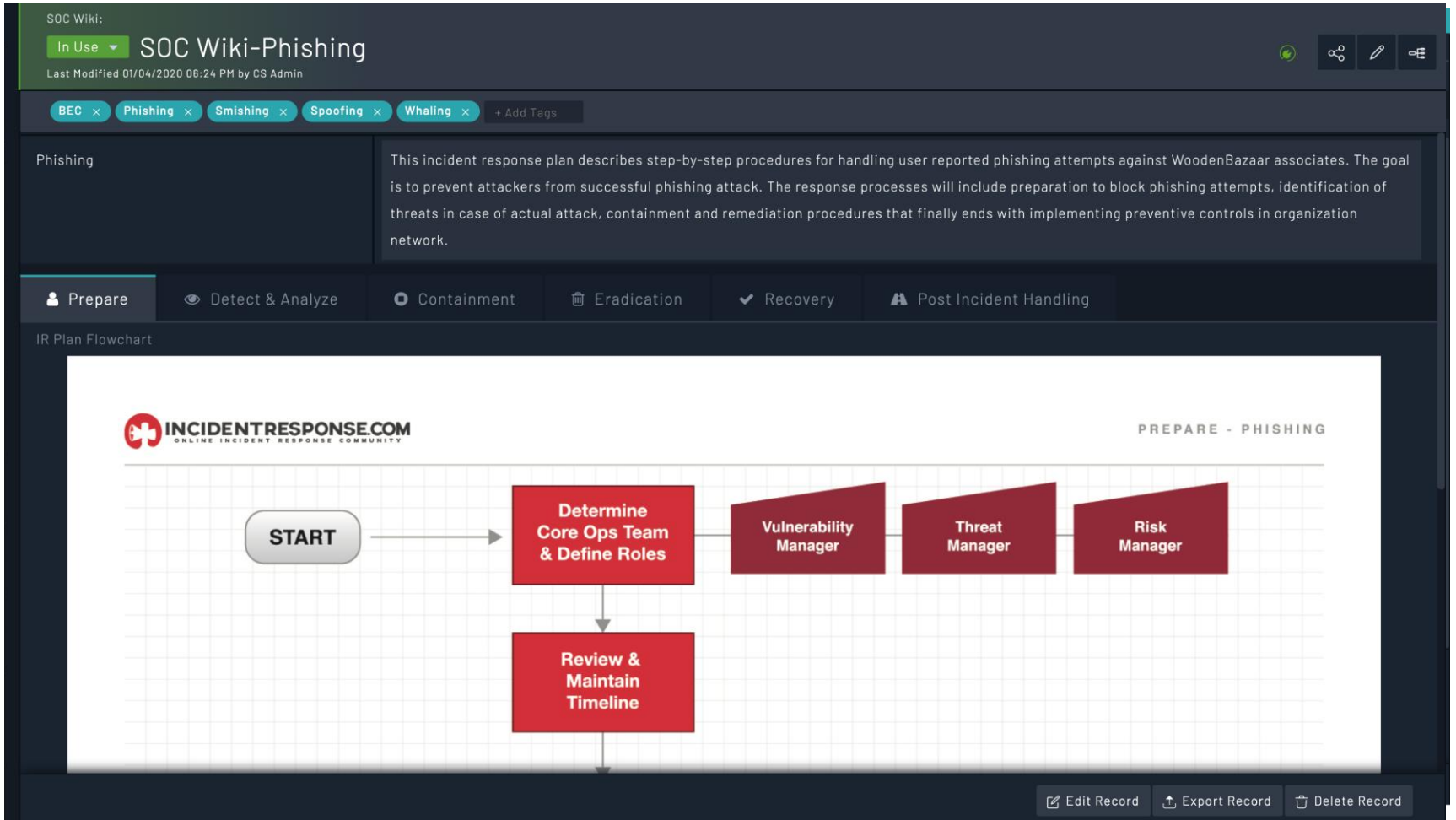


FORTINET

Workflow & Collaboration

Рабочая область для совместной работы & SOC Wiki

- Workspace Collaboration Panel
- SOC Wiki для хранения и управления документами и взаимодействия

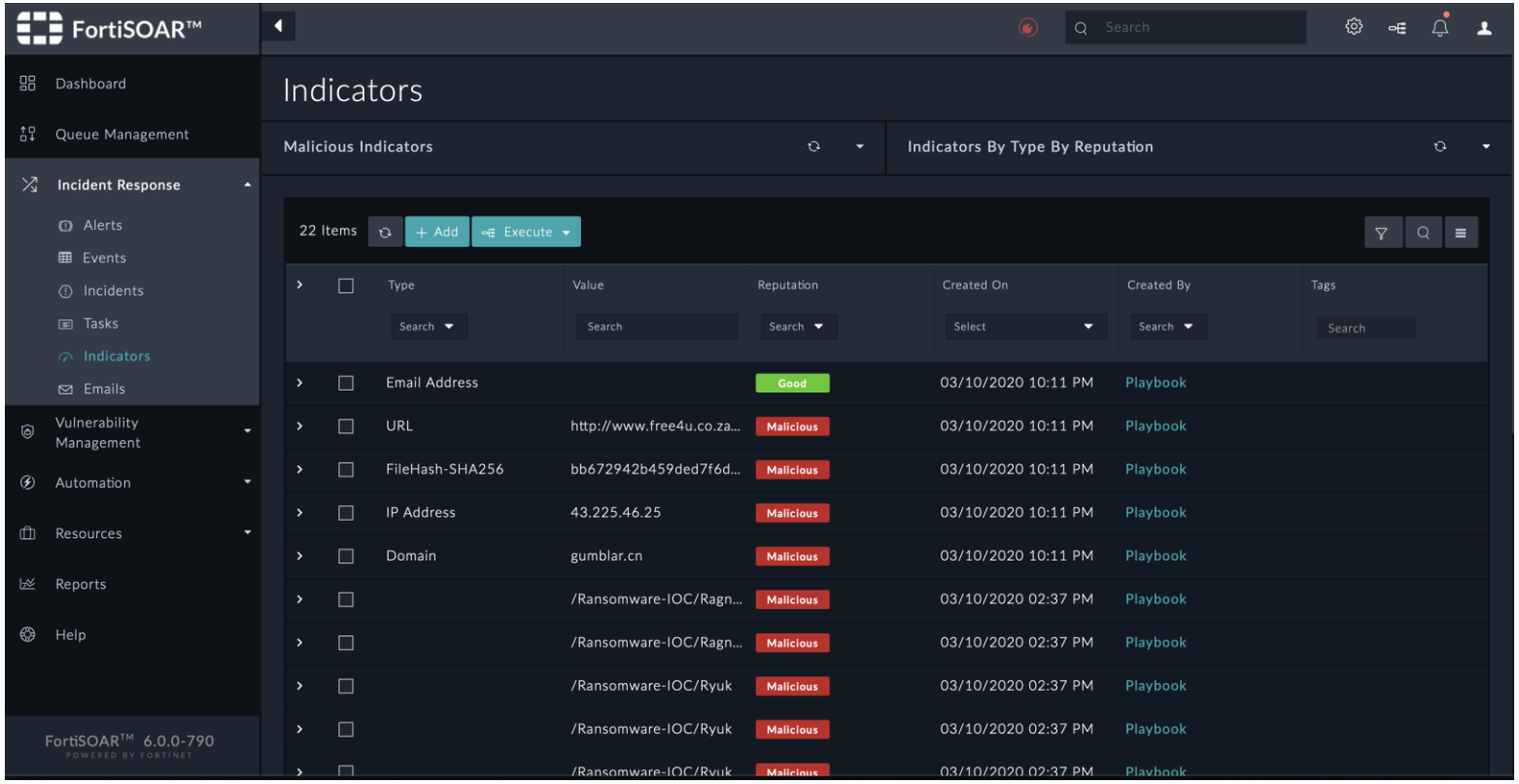


Threat Intelligence Management

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

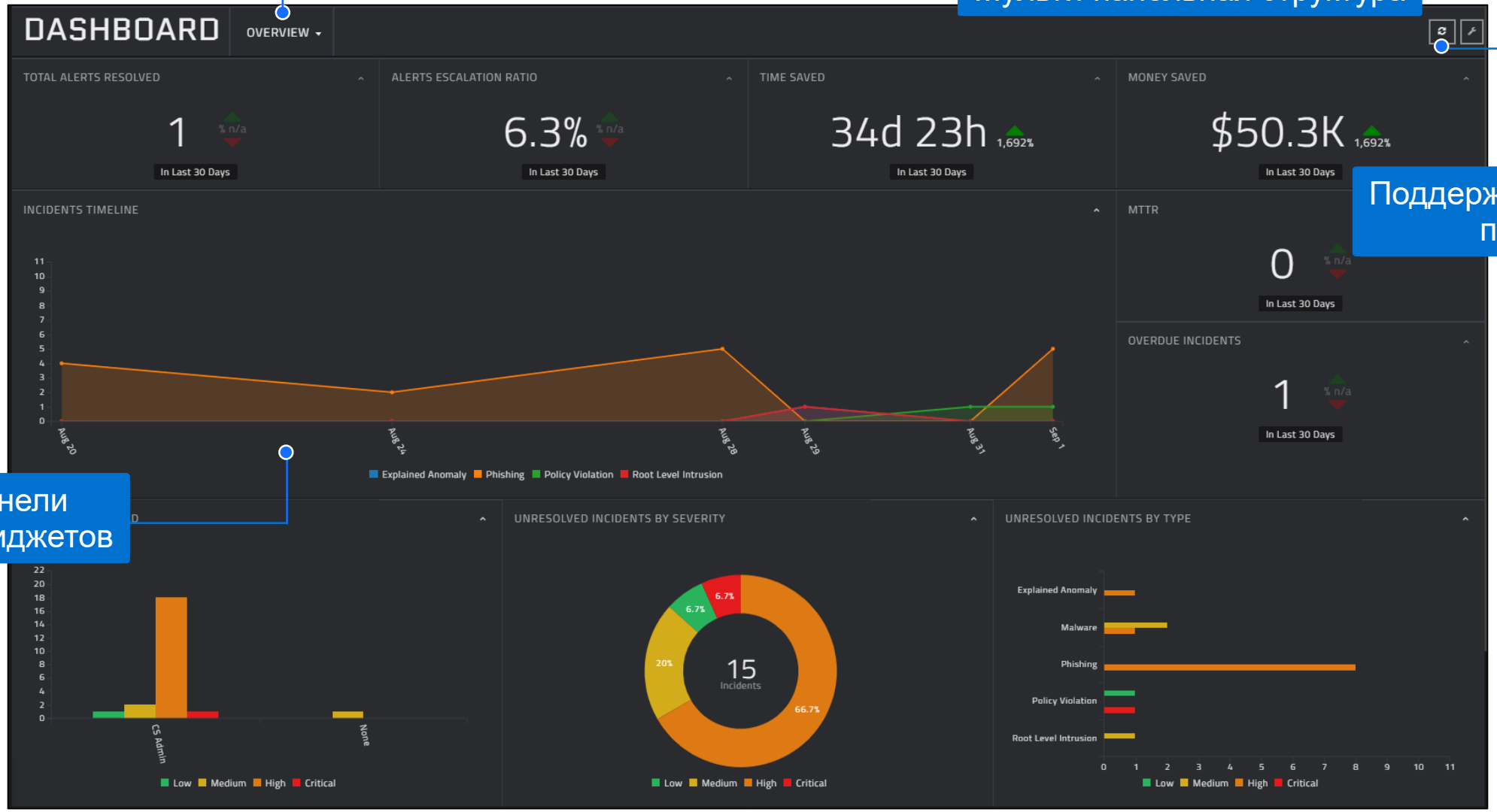


Панели управления (Dashboards)

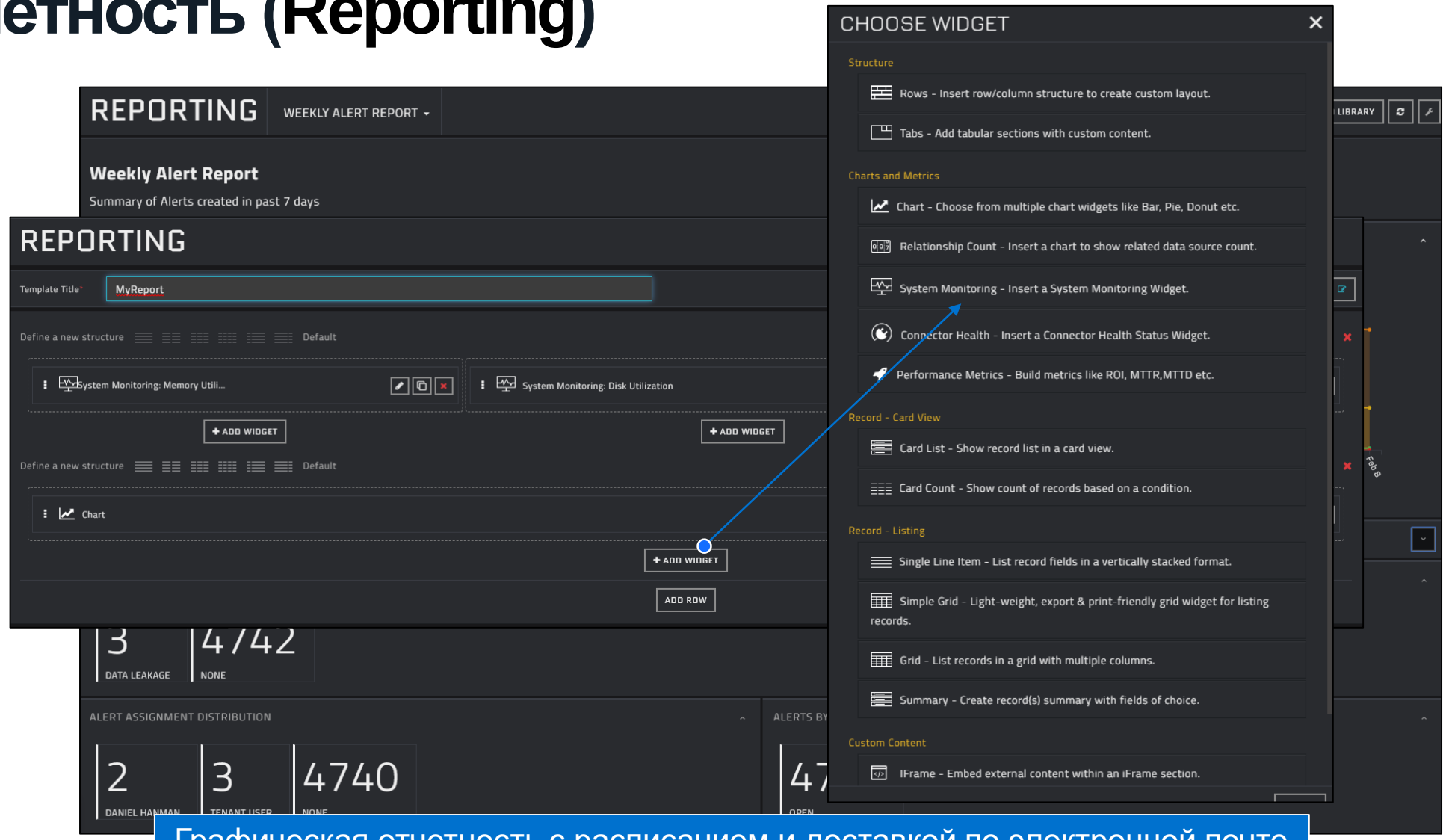
Мульти-панельная структура

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

Истории клиентов

Крупное нефтегазовое предприятие, SOAR для распредленного SOC

Мировой лидер по производству энергетических и химических веществ

ЦЕЛИ

- Отсутствие глобальной видимости и единообразия по всему Saudi Aramco – 6 SOC и более 130 SOC аналитиков

ПРОБЛЕМЫ

- Аналитики не успевали за объемами оповещений, которые обрабатывались локально по регионам
- Отсутствие обмена передовым опытом и непрерывность процесса 24/7 в ручном режиме
- Кастомизация существующего SOAR, т.е. локальная доработка, была сложной задачей.

РЕШЕНИЕ

- Мощная, масштабируемая, настраиваемая автоматизация и расширяемое управление кейсами
- Мультитенантная полностью распределенная архитектура
- Лучшая в своем классе поддержка и предоставляемые опции профессионального сервиса продемонстрированы в рамках POC

Строительная компания, переход на FortiSOAR

Комплексный поставщик услуг в сфере жилой недвижимости. Нацелен на расширение возможностей независимых агентов по продажам для лучшего обслуживания современных потребителей

ЦЕЛИ

- Работа с SOAR уже велась, но через год Заказчик захотел добавить новые функциональные возможности для автоматизации существующих рабочих процессов (команда SOC 10+ аналитиков)

ПРОБЛЕМЫ

- Отсутствие масштабируемости действующего SOAR
- Playbook-движок действующего SOAR было очень сложно кастомизировать
- Отсутствие поддержки со стороны действующего поставщика SOAR

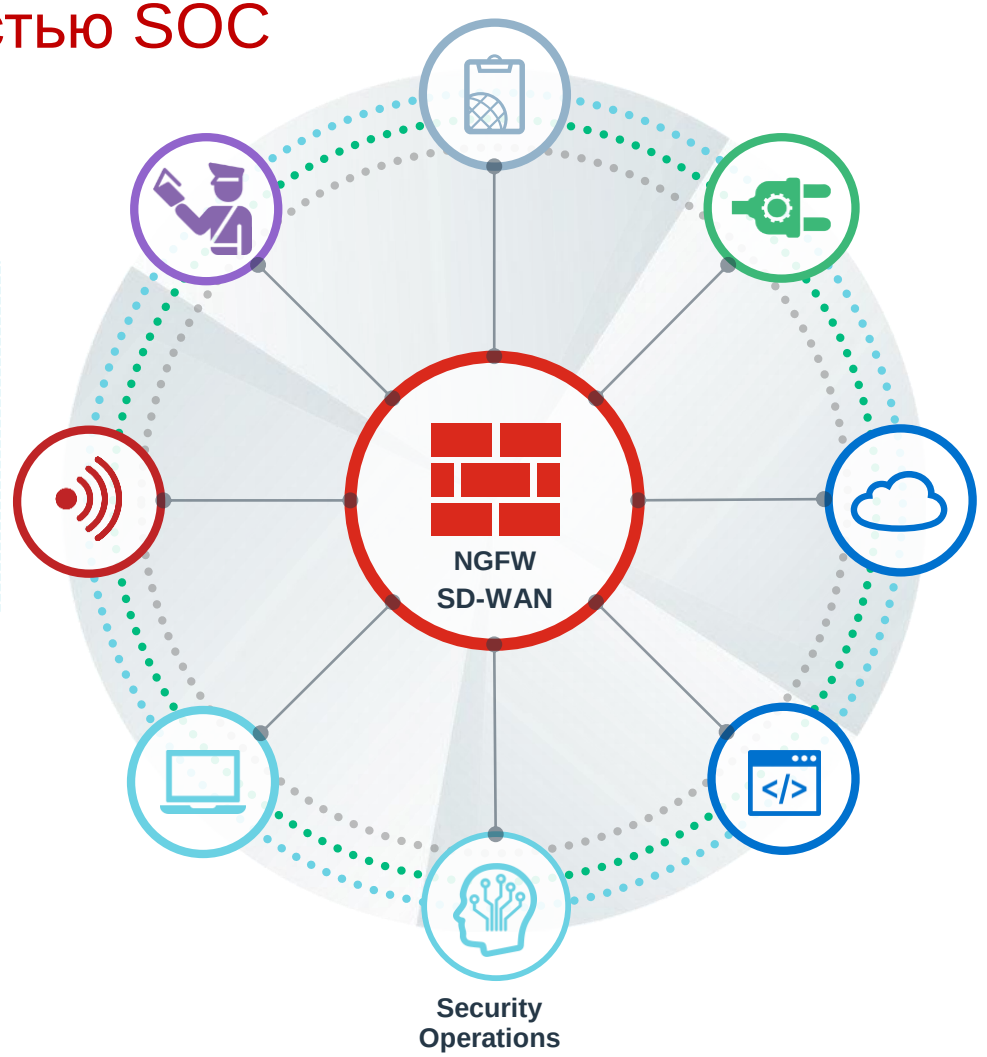
РЕШЕНИЕ

- Мощная, настраиваемая автоматизация и управление кейсами
- Глубокая поддержка предприятия и предоставление услуг профессионального сервиса
- Настраиваемый интерфейс и модули

Резюме

Упрощение операций безопасности

Выбор предложения в соответствии со зрелостью SOC




FORTINET