



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

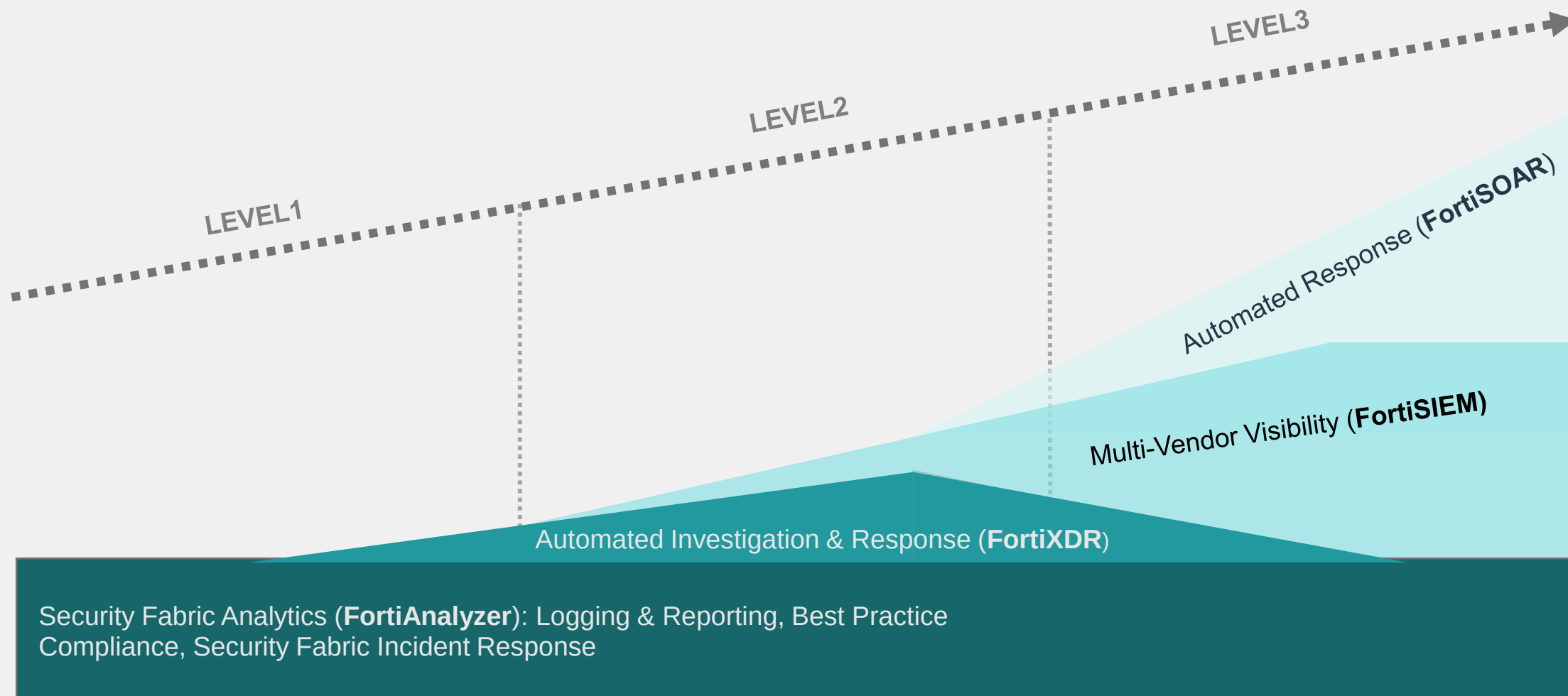


Организации сталкиваются с все более агрессивными угрозами ... где требуется быстрое реагирование в лучшем случае всего за несколько минут ... Это вынуждает организации сокращать время на реагирование, обычно путем делегирования большего количества задач машинам..²



Упростите операции по обеспечению безопасности

Выберите предложение, соответствующее вашей зрелости SOC



FortiSOAR – это независимое решение класса SOAR

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

Платформа управления SOC

- Управление кейсами организации
- Рольное управление доступом
- Мультиотенантность



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

Мультиотенантность

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



FortiSOAR

4 ключевых сценария использования



**Единое
управление
реагированием
на инциденты**



**Автоматизация
упорядочивания
алертов**



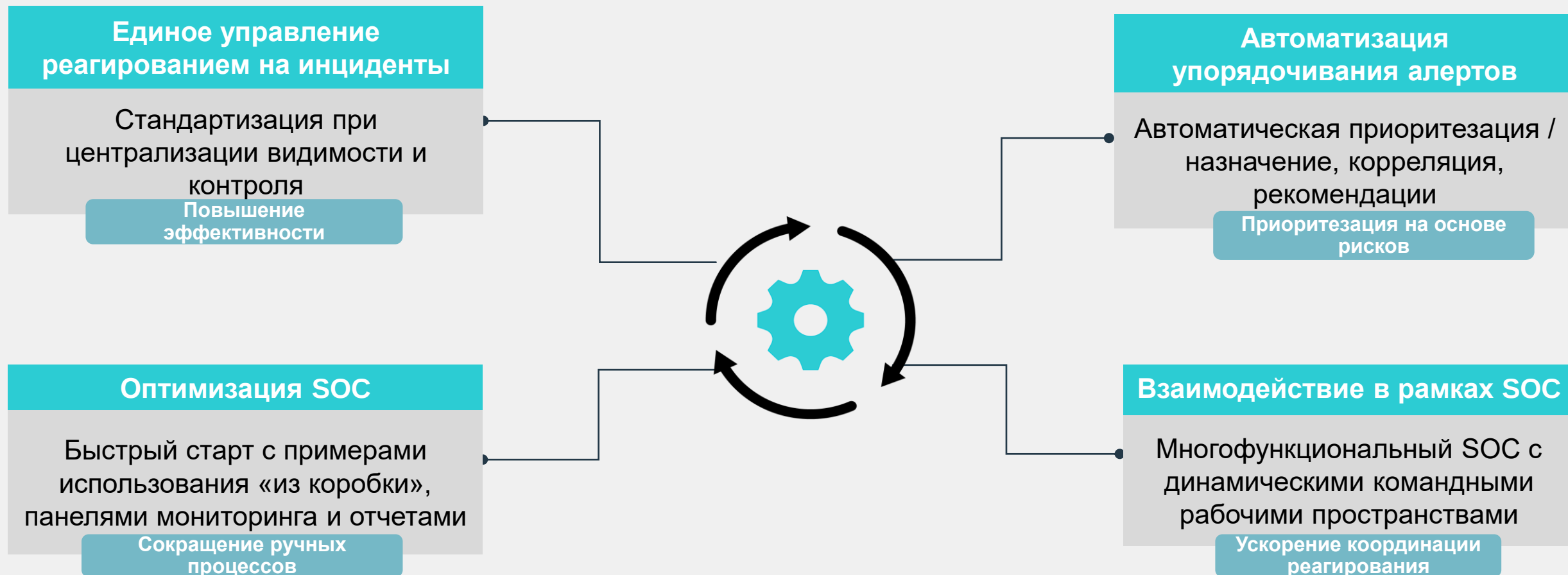
**Оптимизация
SOC**



**Взаимодействие
в рамках SOC**

Типовые сценарии применения FortiSOAR

Максимизируйте эффективность с помощью оркестрации и автоматизации



1. Единое управление реагированием на инциденты

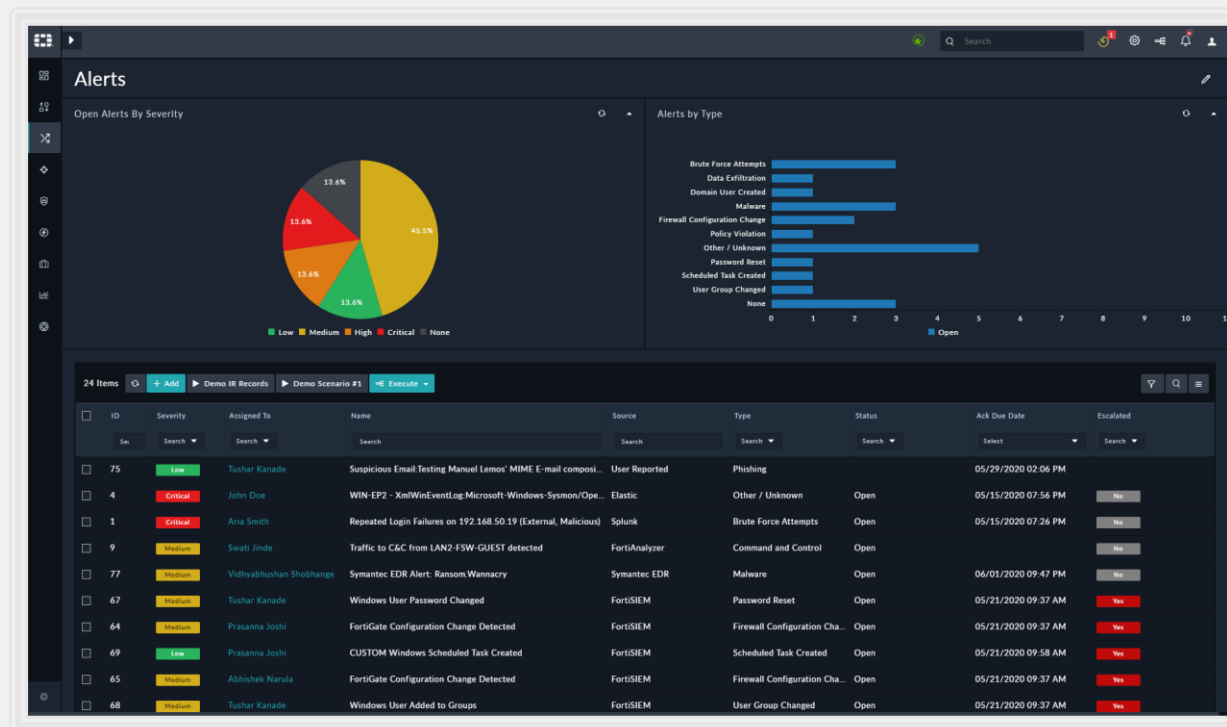
БИЗНЕС ДРАЙВЕР

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

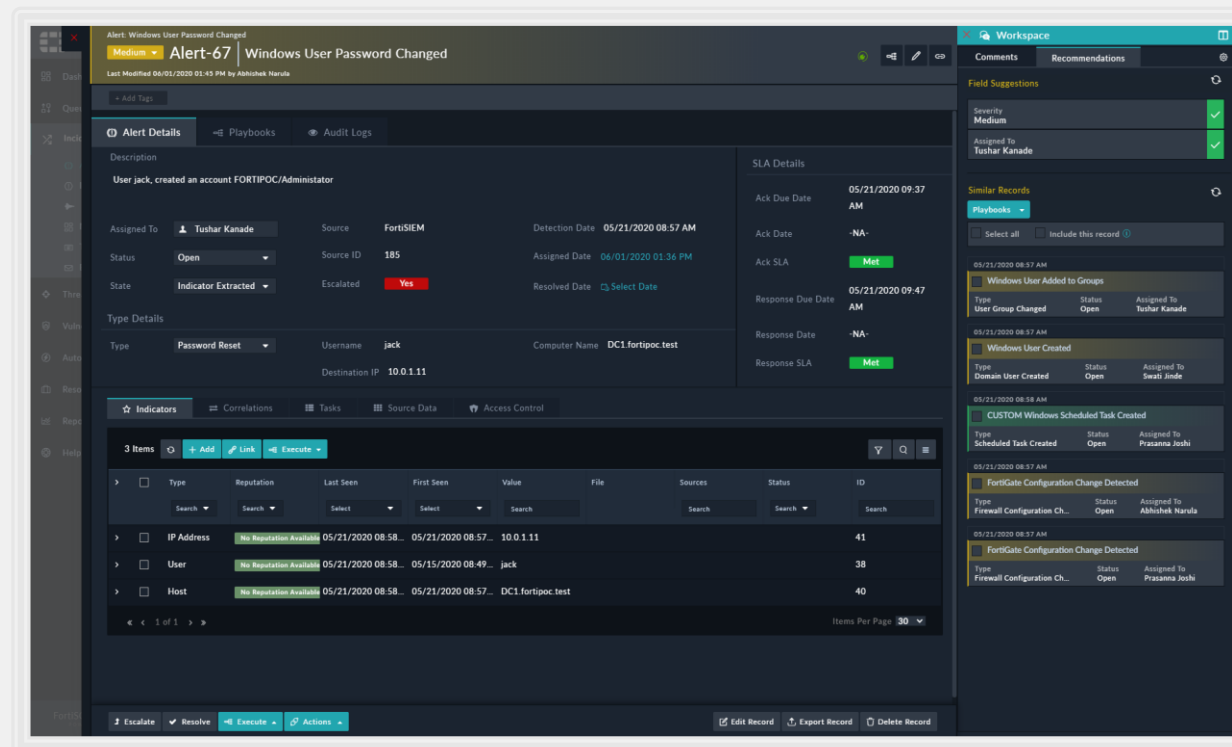
БИЗНЕС ДРАЙВЕР

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

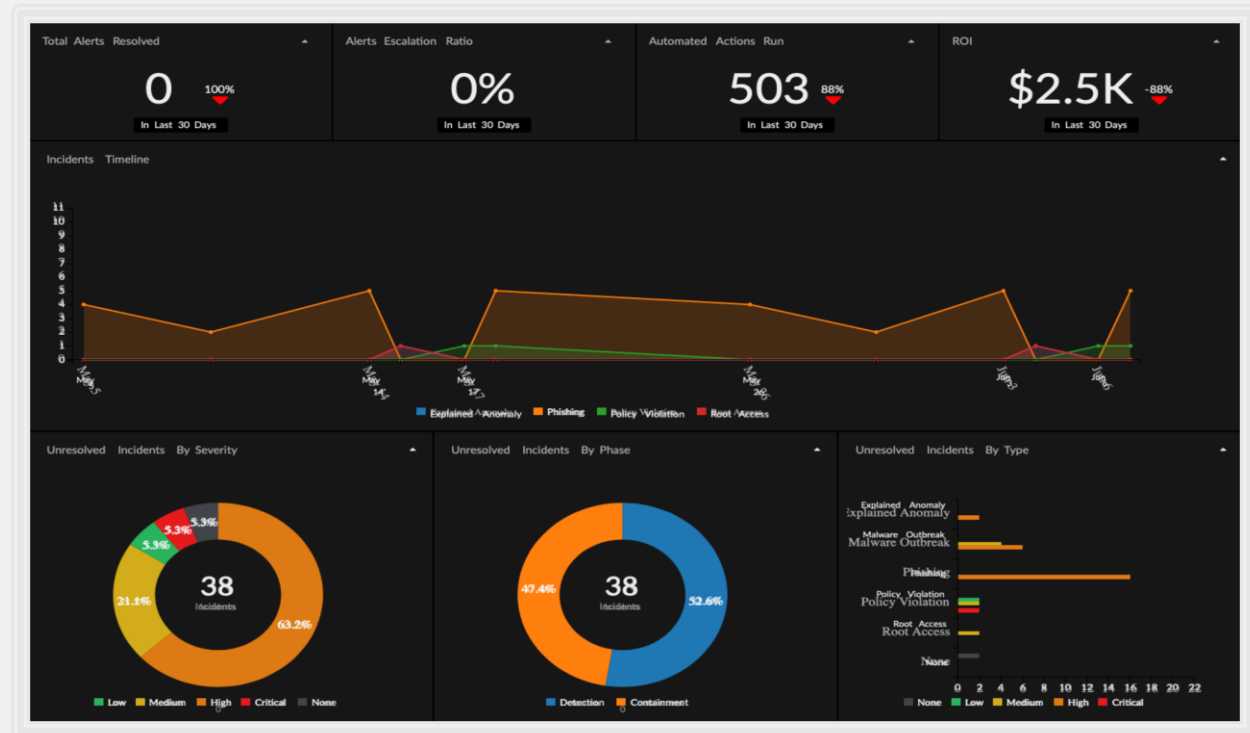
БИЗНЕС ДРАЙВЕР

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

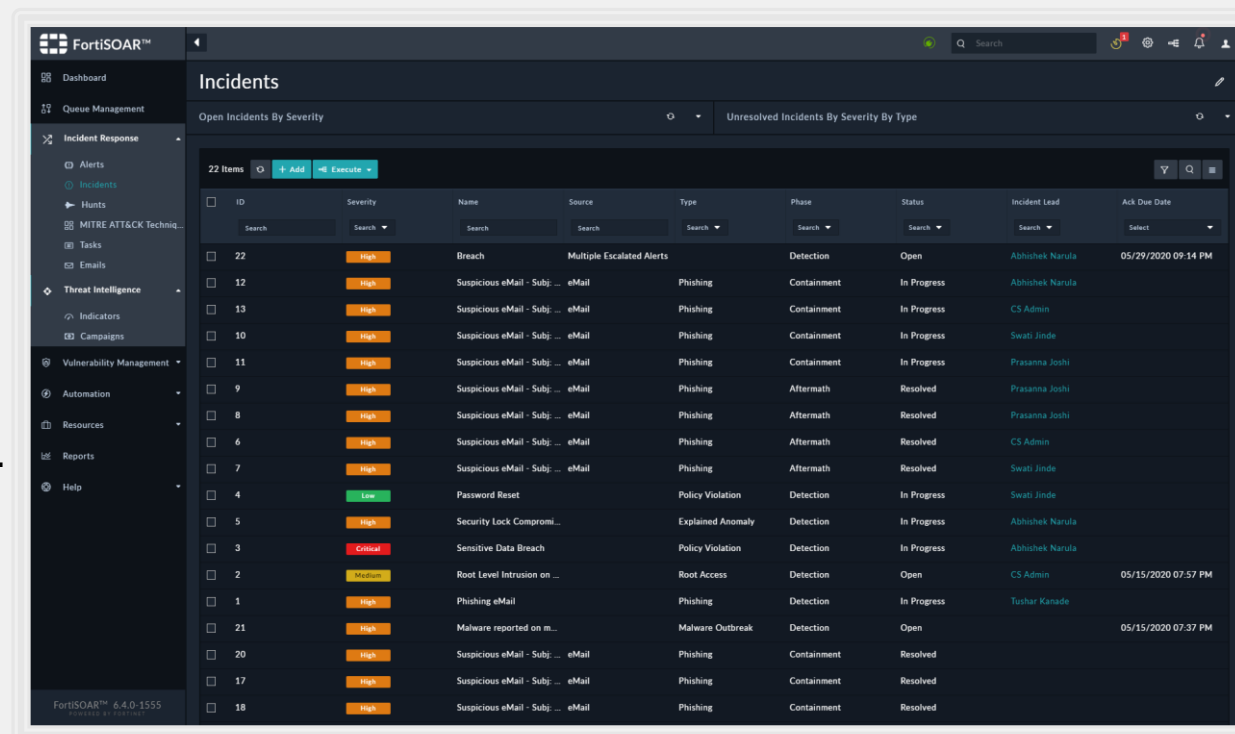
БИЗНЕС ДРАЙВЕР

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

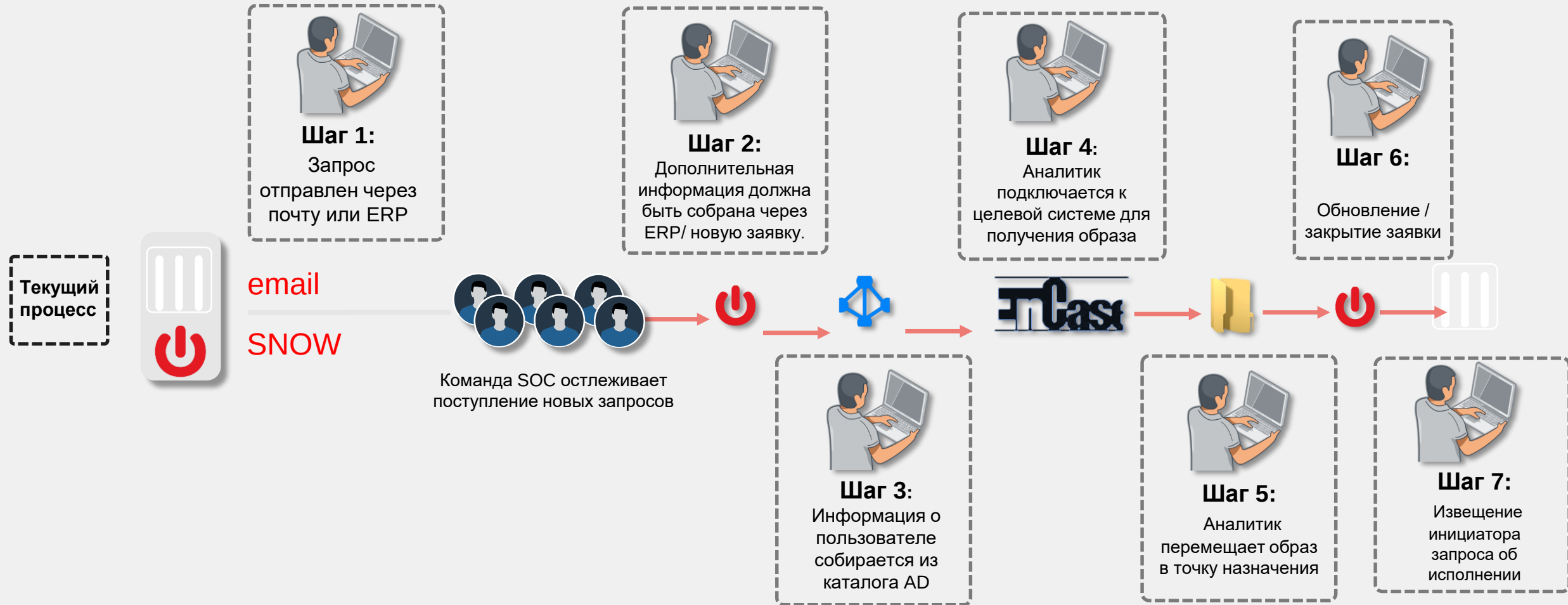


Ручное управление процессами

Запросы на получение образа машины



1 час на обработку события (x20 в неделю)



Автоматизация процесса с использованием FortiSOAR

Запросы на получение образа машины с использованием FortiSOAR

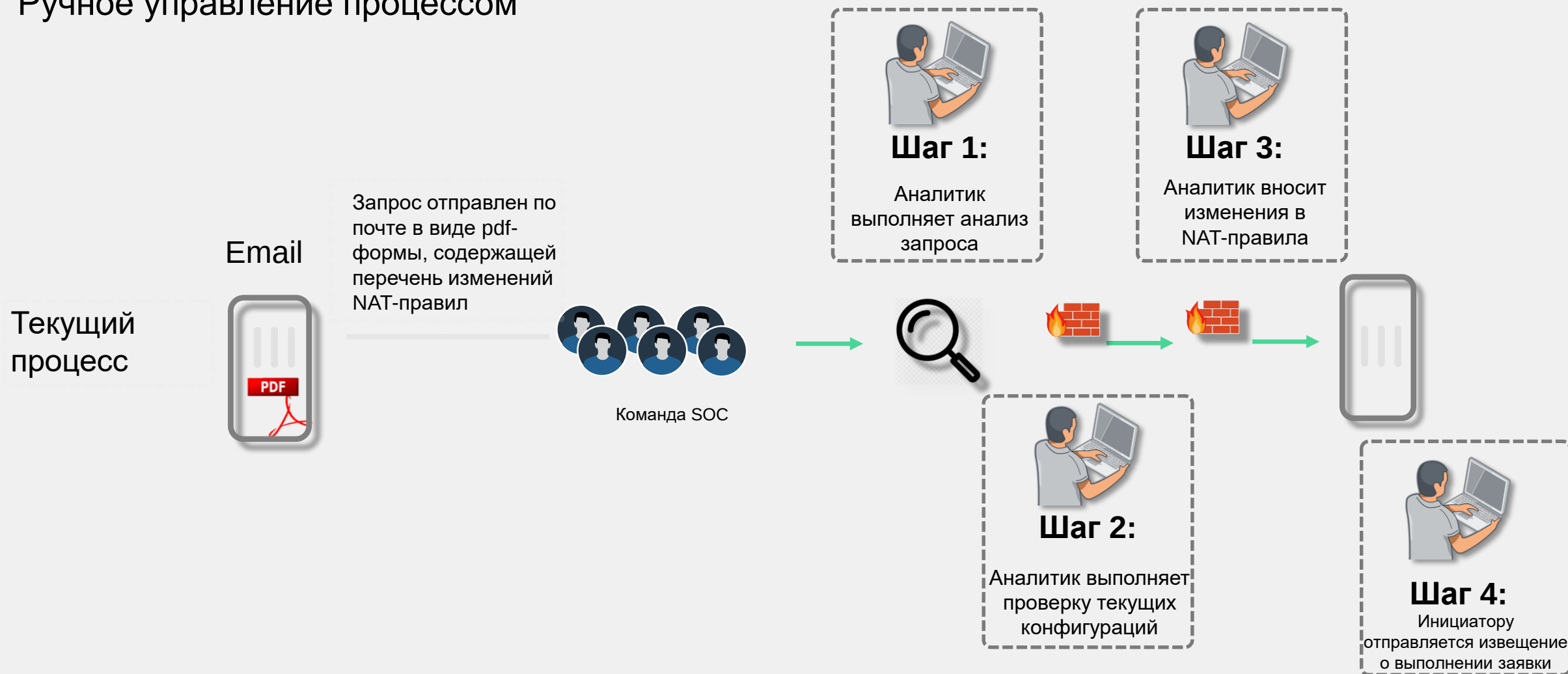
5 минут на обработку события (x20 в неделю)





Пример: запрос на изменение NAT правил в конфигурации МЭ

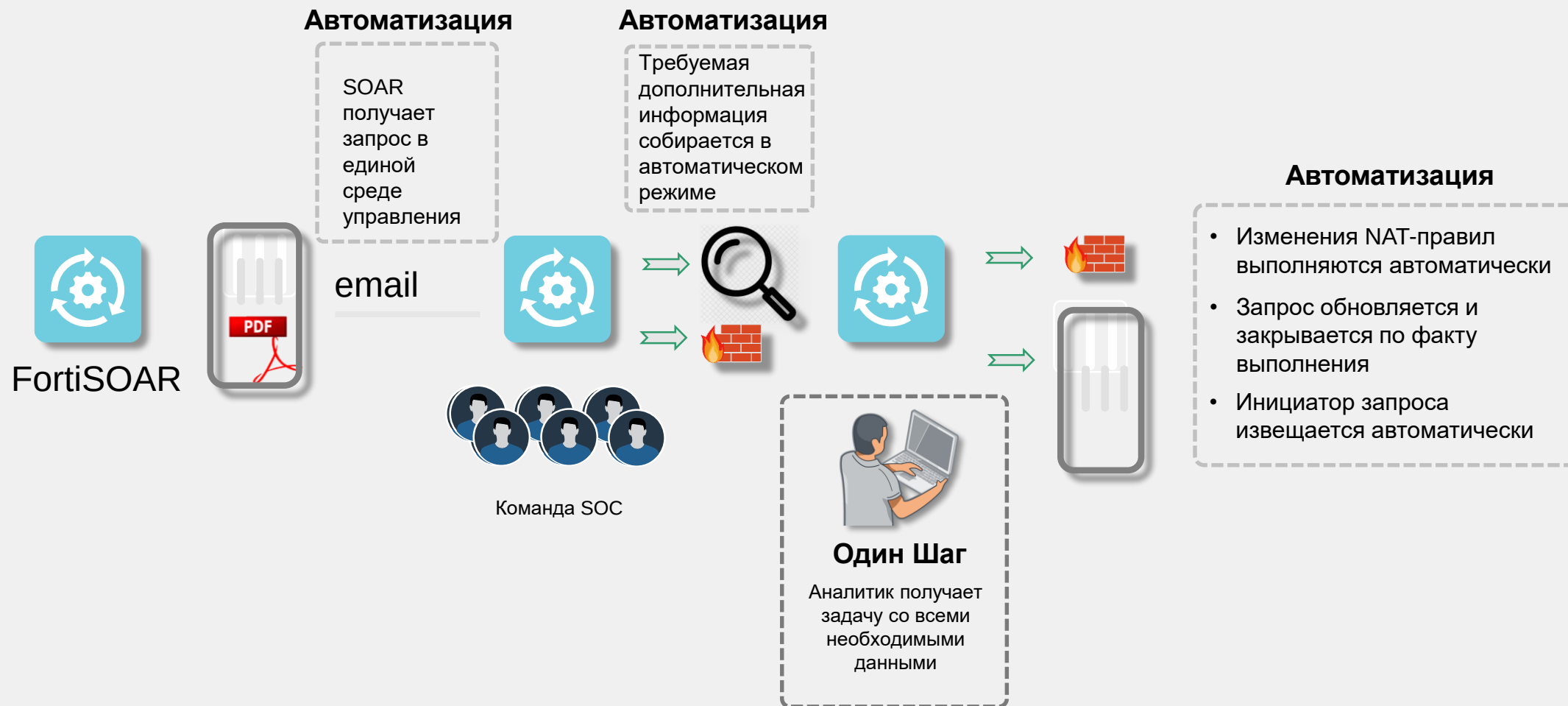
Ручное управление процессом





Пример: запрос на изменение NAT правил в конфигурации МЭ

Автоматизированный процесс



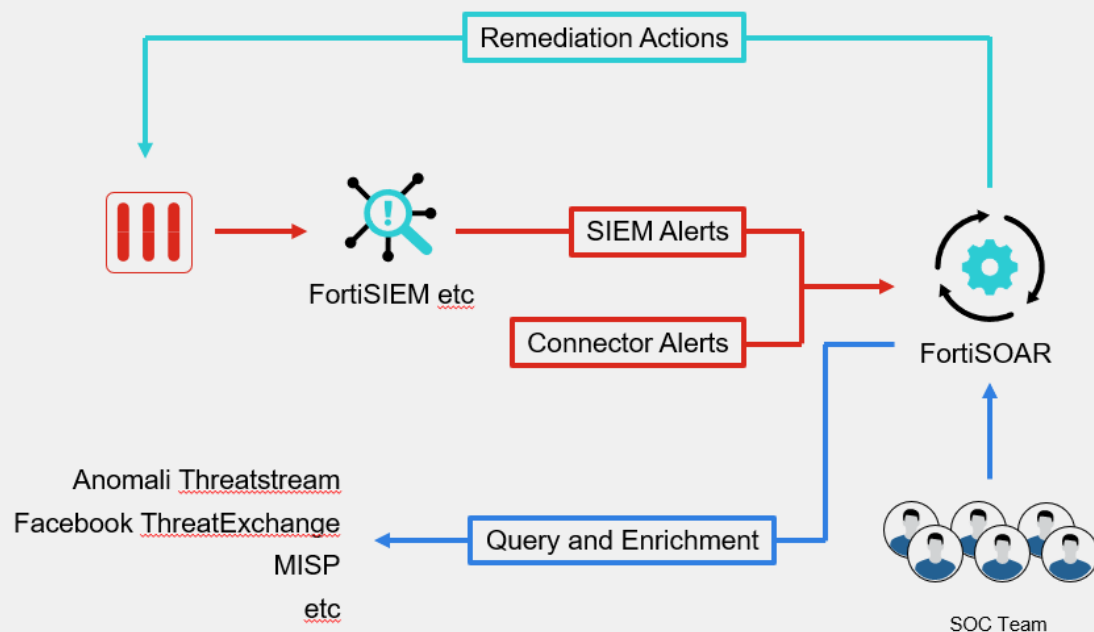


Архитектура

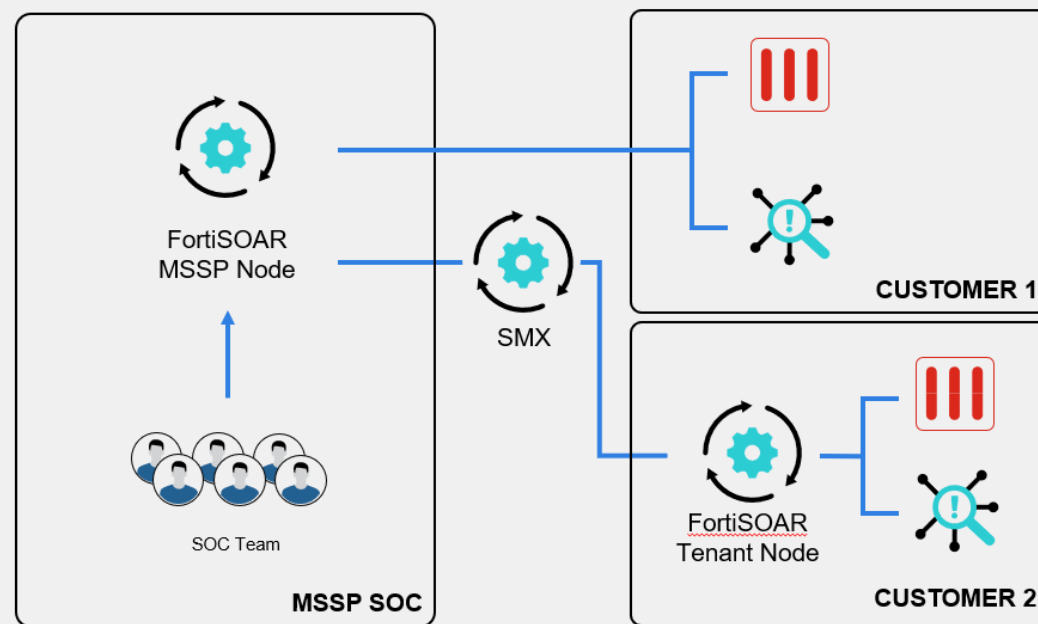


Гибкая и масштабируемая архитектура

Enterprise

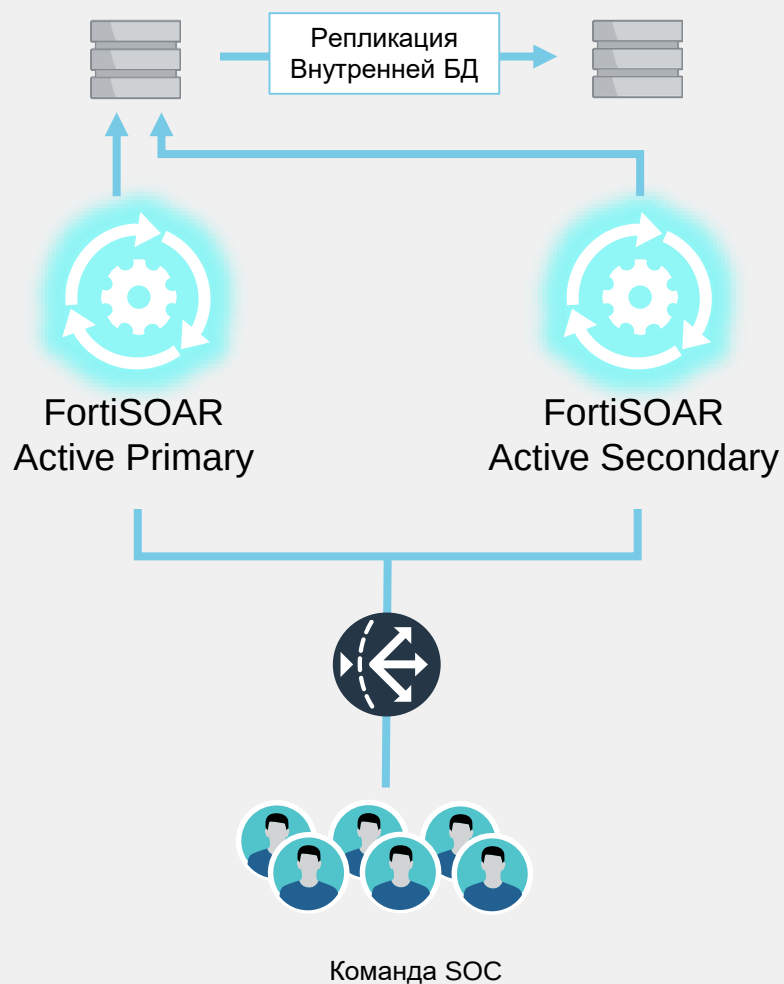


Multi-Tenant



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

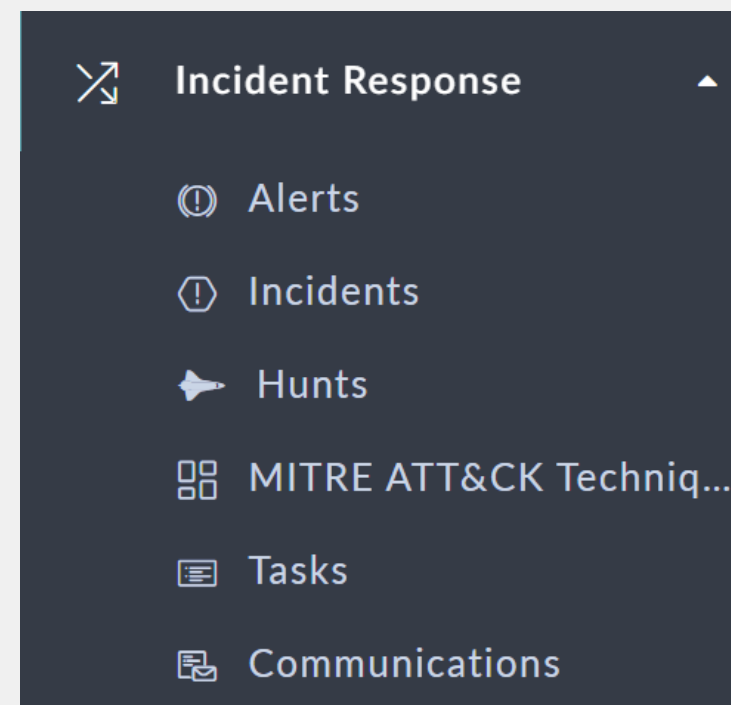


Incident & Case Management

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

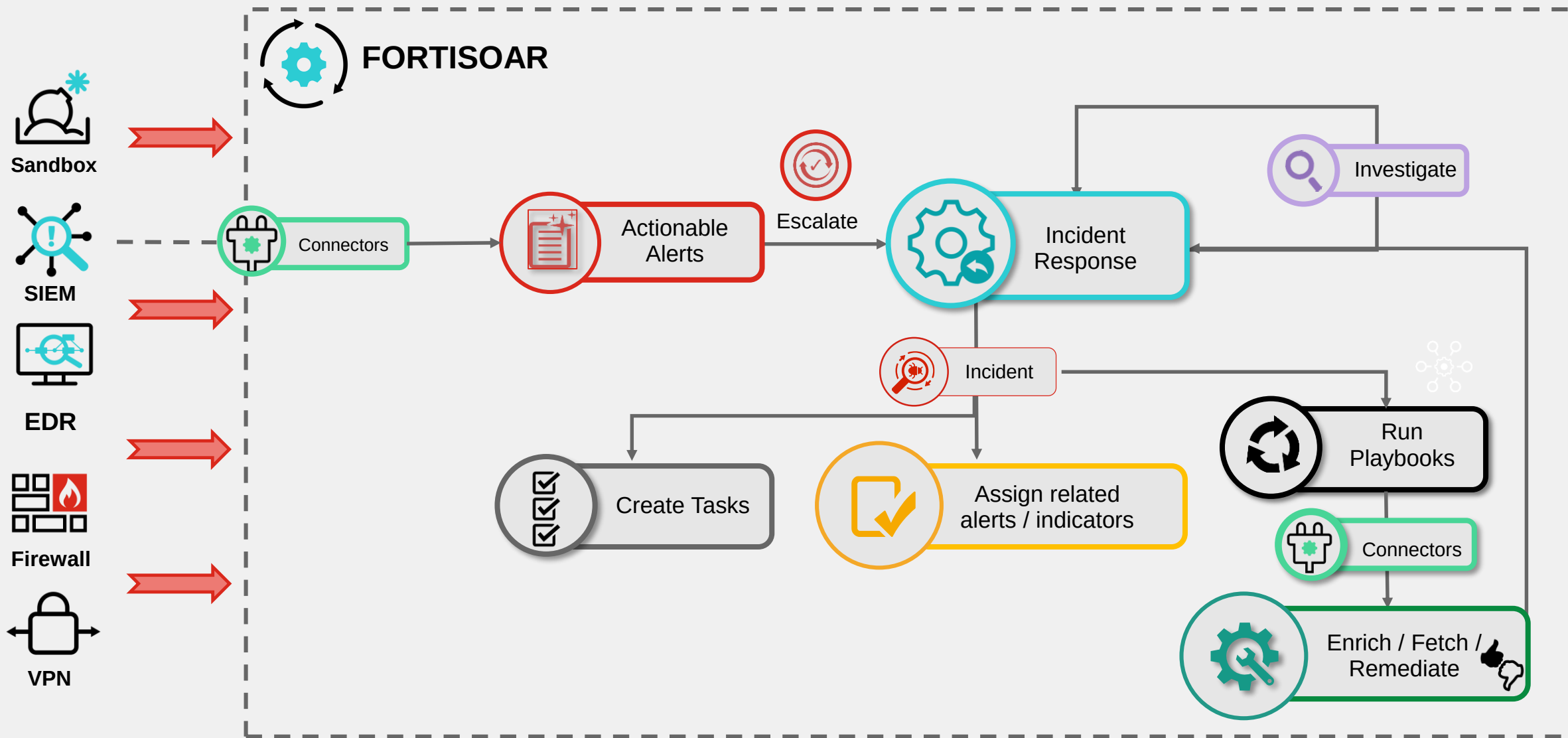


Incident & Case Management

Реагирование на инциденты – Пример типового процесса

П
Р
Я
М
А

И
Н
Т
Е
Г
Р
А
Ц
И
Я

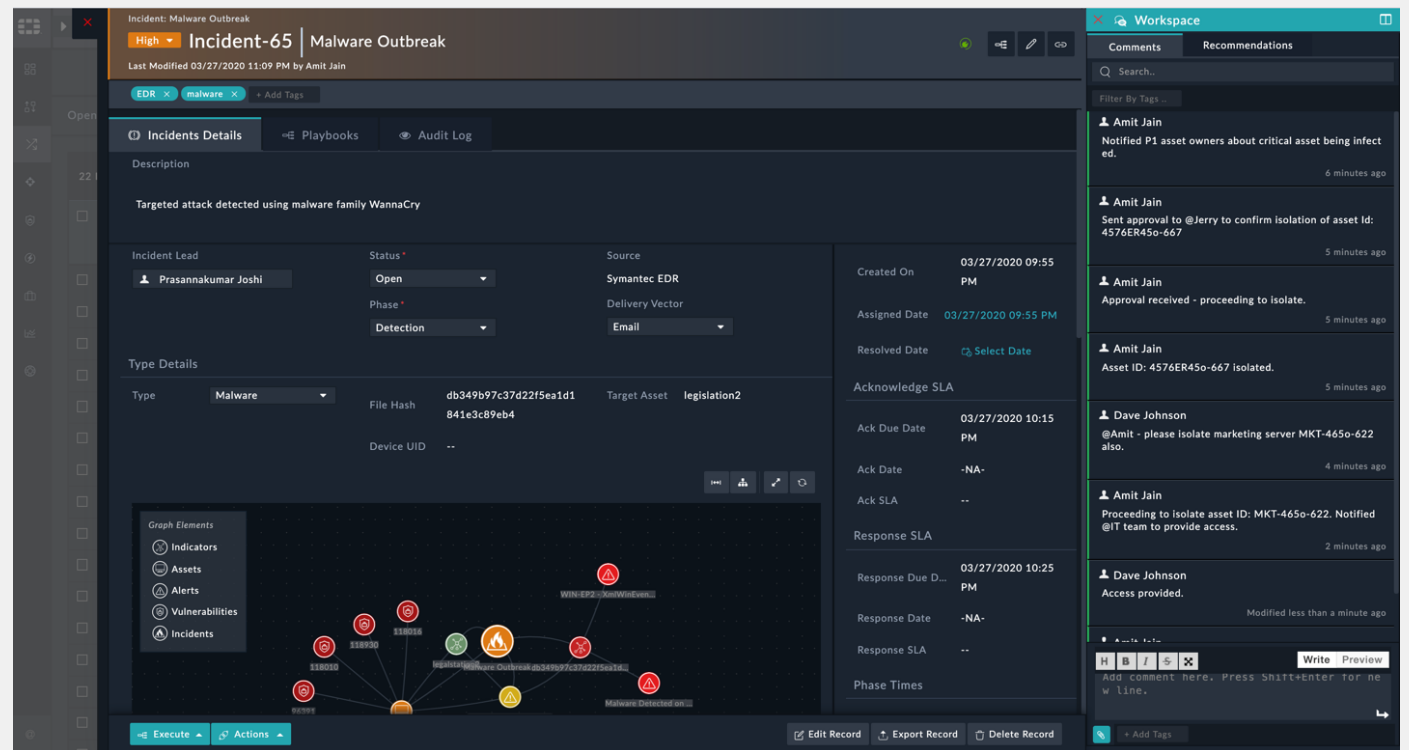


Incident & Case Management

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 аналитик, 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

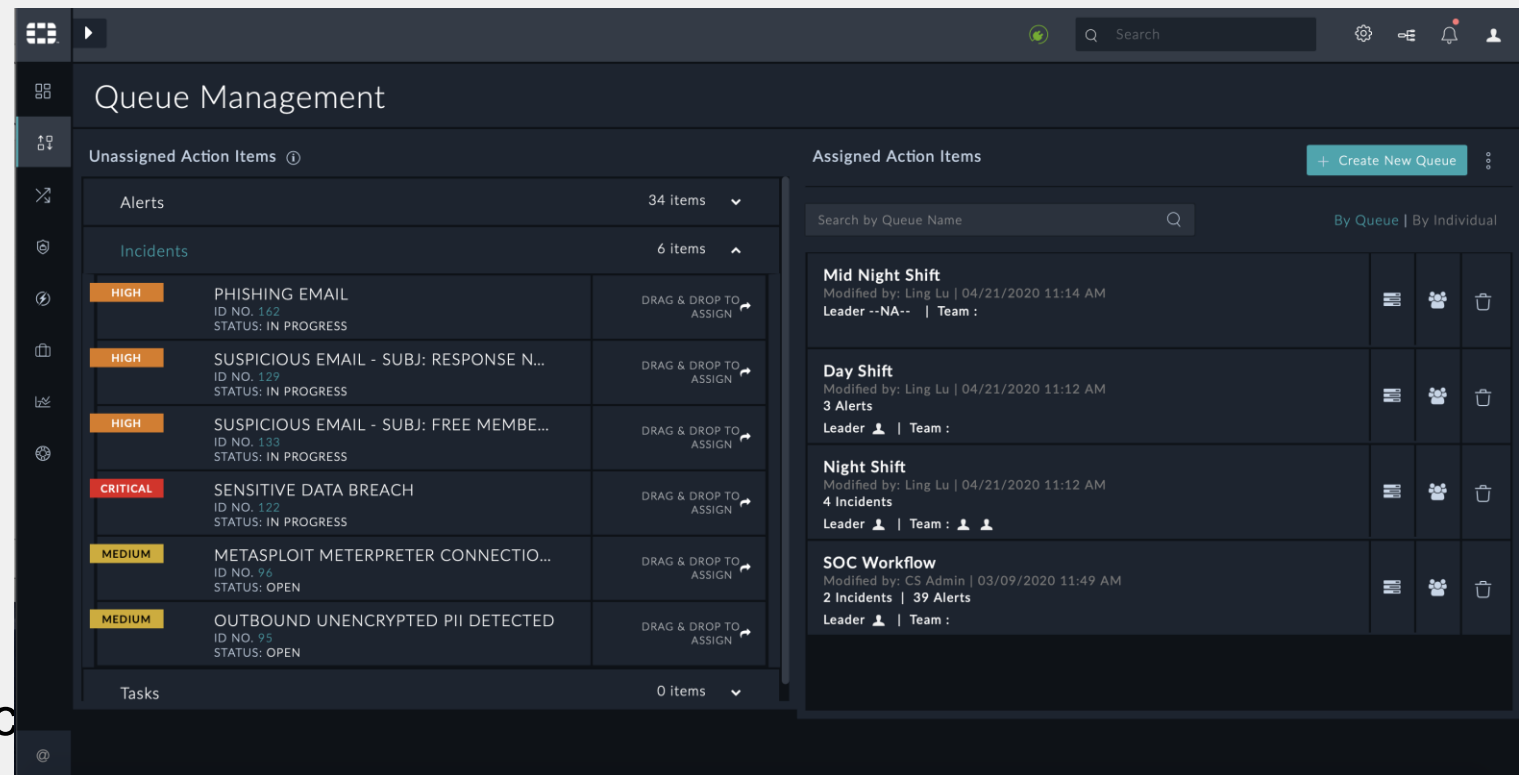


Incident & Case Management

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

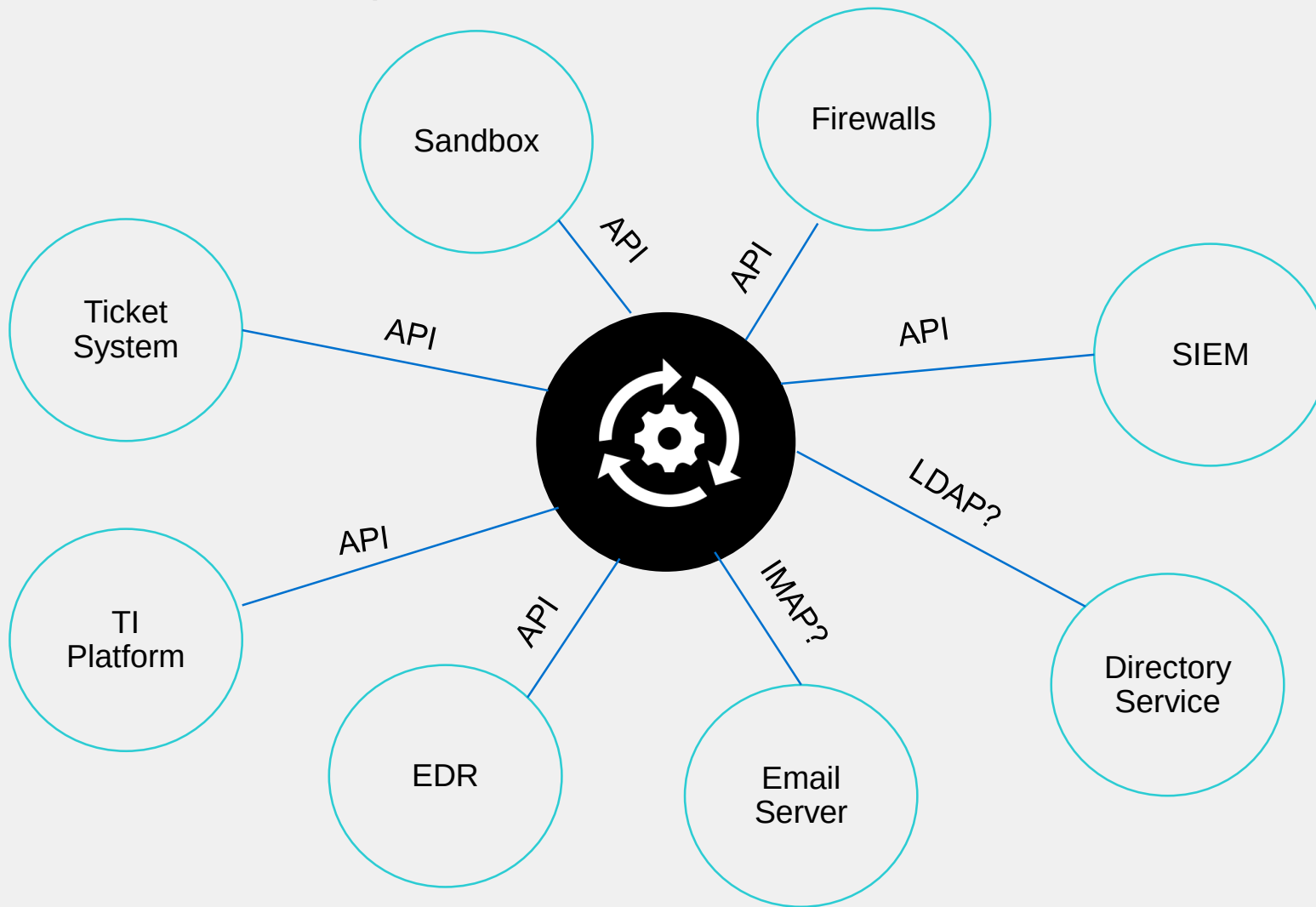
Playbooks: коллекция действий на основании скриптов

Например, может быть создан playbook, который срабатывает 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

The screenshot displays the Fortinet Connectors Store interface. On the left, a sidebar shows 'Connectors' with tabs for 'Installed (9)', 'Updates' (1), and 'Data Ing'. The main area shows the 'Fortinet FortiMail' connector details. The connector is 'Active' and 'Compatible with your integration'. It has 0 configurations, 16 actions, and 1 playbook. A table lists the available actions:

NAME	DESCRIPTION
Get Domains Configured	Retrieves a list of all domains configured on Fortinet FortiMail.
Get AntiSpam Profiles for Domain	Retrieves a list of all AntiSpam Profiles for a specified domain in Fortinet FortiMail, based on the domain ID you have specified.
Get Recipient Policies for Domain	Retrieves a list of all Recipient Policies for a specified domain in Fortinet FortiMail, based on the domain ID you have specified.
Get GreyList	Retrieves the Greylist configured on Fortinet FortiMail.
Get Auto Exempt GreyList	Retrieves the Auto Exempt Greylist configured on Fortinet FortiMail.
Get Sender Whitelist For Session Profile	Retrieves a list of sender whitelists from Fortinet FortiMail, based on the profile name you have specified.
Get Sender Blacklist for Session Profile	Retrieves a list of sender blacklists from Fortinet FortiMail, based on the profile name you have specified.
Get Profile Name	Retrieves a list of profile names from Fortinet FortiMail, based on the profile type you have specified.
Update Session Profile	Updates a session profile on Fortinet FortiMail, based on the profile name and other input parameters you have specified.
Update Antispam	Updates an antispam profile on Fortinet FortiMail, based on the profile name

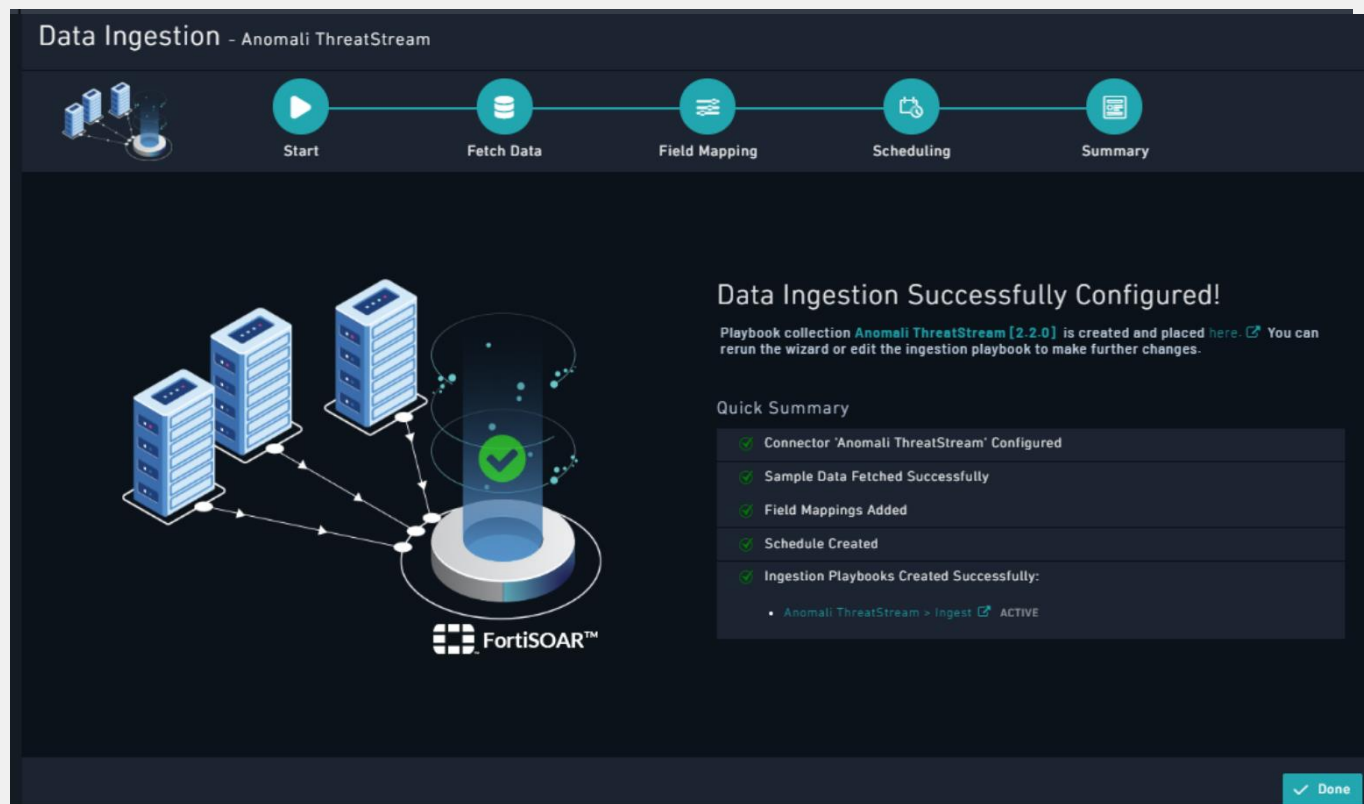


Orchestration & Automation

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

The screenshot shows the FortiSOAR Playbooks interface. The left sidebar contains navigation options: Dashboard, Queue Management, Incident Response, Vulnerability Management, Automation (selected), Rule Engine, Connectors, Schedules, Resources, and Reports. The main area is titled 'Playbooks' and shows a collection named '02 - Enrich' with 14 items. A list of collections is visible on the left: 02 - Enrich (14), 03 - Triage (8), 04 - Investigate (18), 05 - Remediate (17), 06 - Hunt (1), 07 - SLA - Alerts (6), 07 - SLA - Incidents (11), 08 - Report (1), 12 - Training (3), 13 - MITRE ATT&CK™-CREDENTIAL ACCESS (3), and 13 - MITRE ATT&CK™-DEFENSE EVASION (?). The right pane shows details for the '02 - Enrich' collection, including a description and a list of 14 items. The items are listed in a table with columns: Name, Description, Tags, Active, and Is Private. The 'Import BPMN' button is highlighted in the top right corner. The 'Automation' menu item is highlighted in the left sidebar. The 'Import BPMN' button is highlighted in the top right corner. The '02 - Enrich' collection is highlighted in the left sidebar. The '14 Items' button is highlighted in the top right corner. The 'Add Playbook' button is highlighted in the top right corner. The 'Import' button is highlighted in the top right corner. The 'Import BPMN' button is highlighted in the top right corner. The 'Name' column is highlighted in the table. The 'Description' column is highlighted in the table. The 'Tags' column is highlighted in the table. The 'Active' column is highlighted in the table. The 'Is Private' column is highlighted in the table. The 'Asset > Get Runni...' item is highlighted in the table. The 'Attachment > Get ...' item is highlighted in the table. The 'Indicator (Manual ...)' item is highlighted in the table. The 'Indicator (Type All...' item is highlighted in the table. The 'Indicator (Type Do...' item is highlighted in the table. The 'Indicator (Type Em...' item is highlighted in the table. The 'Indicator (Type Fil...' item is highlighted in the table. The 'Indicator (Type Fil...' item is highlighted in the table.

Импорт из BPMN

Коллекция Playbook'ов

Множество предустановленных Playbook'ов

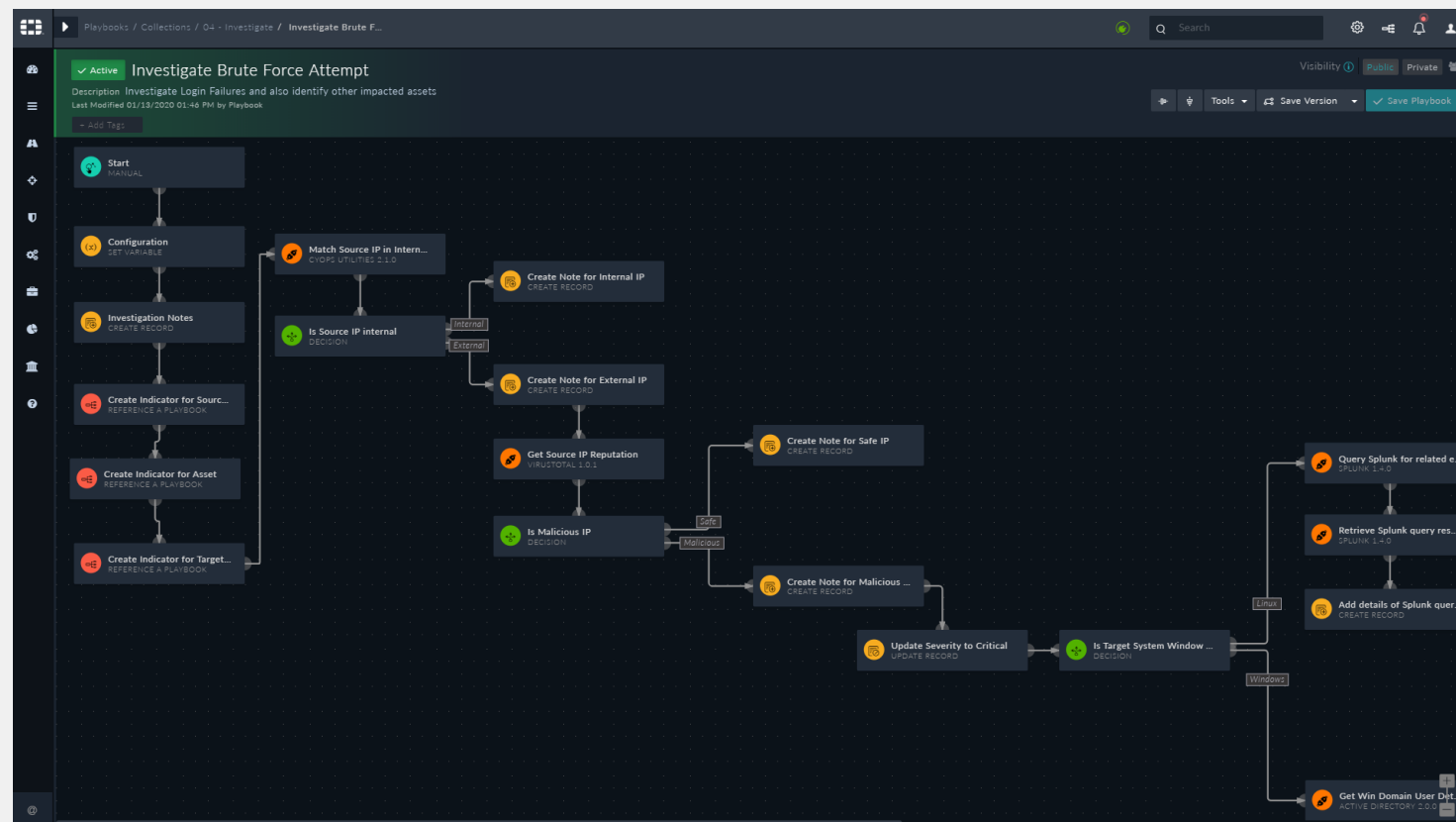


Orchestration & Automation

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

The screenshot displays the Splunk SOAR interface. The main panel shows an alert titled "Alert-27 | Repeated Login Failures on 192.168.50.19 (External, Malicious)" with a critical severity. Below the alert, the "Playbooks" tab is active, showing a workflow for "Investigate Brute Force Attempt". The workflow steps include: Start, Configuration (Set Variable), Investigation Notes (Create Record), Create Indicator for Source (Reference a Playbook), Create Indicator for Asset (Reference a Playbook), Create Indicator for Target (Reference a Playbook), Match Source IP in Internal, Is Source IP Internal (Decision), Create Note for Internal IP (Create Record), Is Source IP External (Decision), Create Note for External IP (Create Record), Get Source IP Reputation (Create Record), Is Malicious IP (Decision), and Create Note (Create Record). The workflow is marked as "FINISHED" with an execution time of 42 seconds and 167 milliseconds.

The right sidebar, titled "Workspace", contains two tabs: "Comments" and "Recommendations". The "Recommendations" tab is active, showing "Field Suggestions" and "Similar Records".

Field Suggestions:

Field	Value	Status
Severity	Medium	✓
Assigned To	CS Admin	✓

Similar Records:

Playbooks

Select all ☐ Include this record ☐

Timestamp	Type	Status	Assigned To
02/25/2021 09:26 AM	Windows User Added to Groups	Open	CS Admin
02/25/2021 09:26 AM	Windows User Password Changed	Open	CS Admin
02/25/2021 09:26 AM	Windows User Created	Open	CS Admin
02/25/2021 09:26 AM	FortiGate Configuration Change Detected	Open	CS Admin

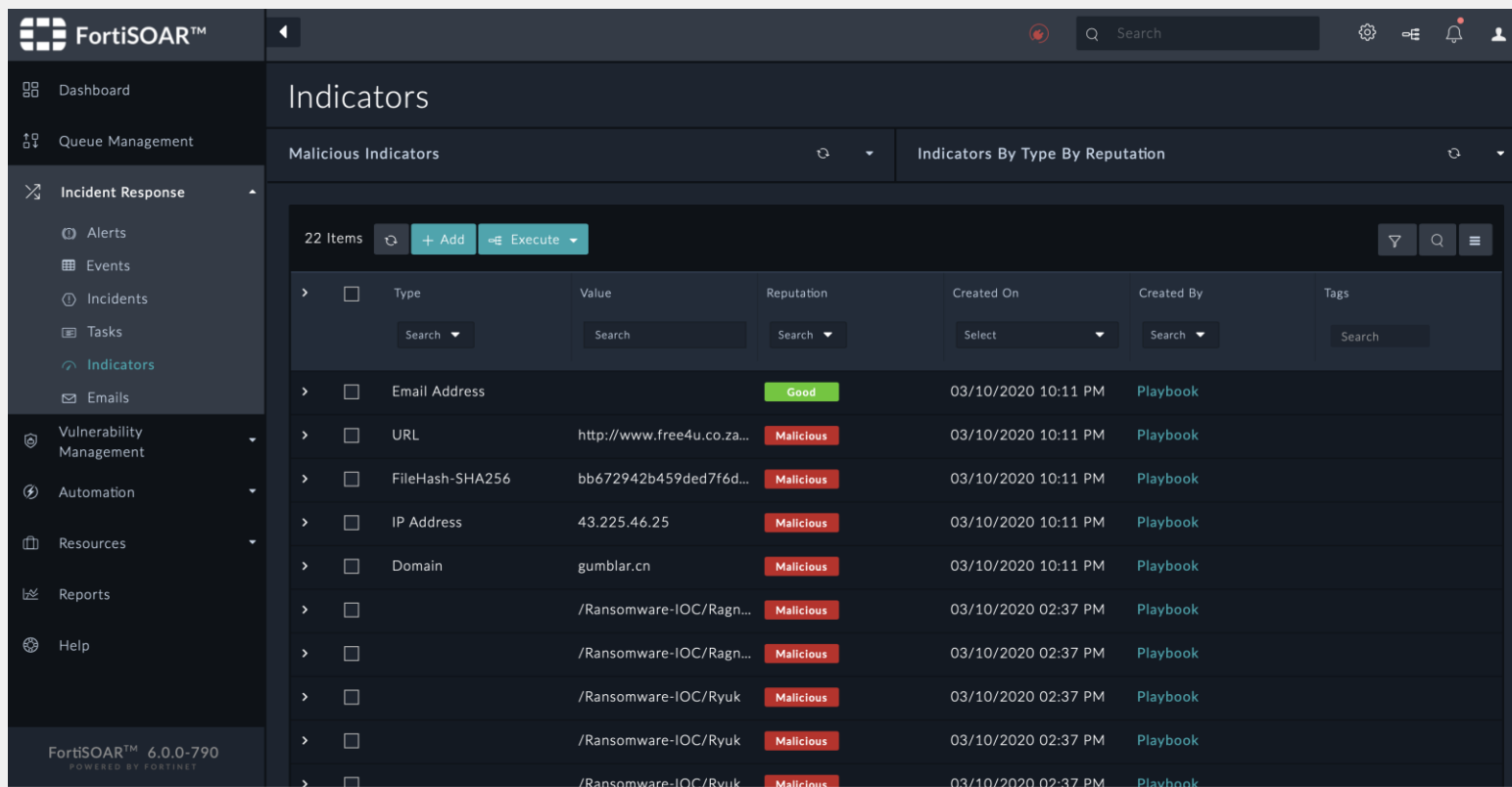


Threat Intelligence Management

Модуль Indicators

Управление несколькими форматами и источниками ТИ 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 (ТИ)
- Сохранение информации об угрозе в БД для использования другими модулями



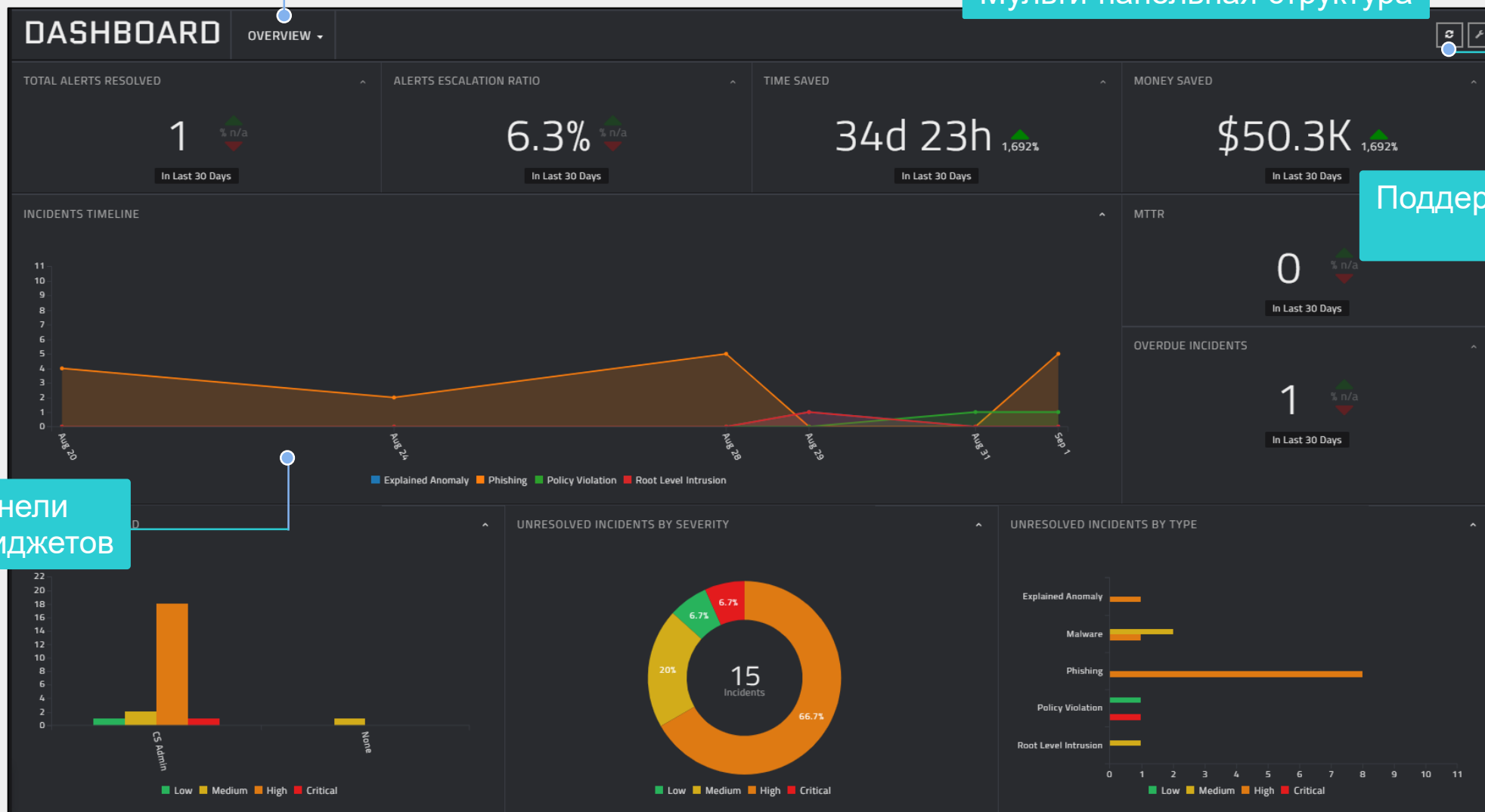
Type	Value	Reputation	Created On	Created By	Tags
Email Address		Good	03/10/2020 10:11 PM	Playbook	
URL	http://www.free4u.co.za...	Malicious	03/10/2020 10:11 PM	Playbook	
FileHash-SHA256	bb672942b459ded7f6d...	Malicious	03/10/2020 10:11 PM	Playbook	
IP Address	43.225.46.25	Malicious	03/10/2020 10:11 PM	Playbook	
Domain	gumblar.cn	Malicious	03/10/2020 10:11 PM	Playbook	
	/Ransomware-IOC/Ragn...	Malicious	03/10/2020 02:37 PM	Playbook	
	/Ransomware-IOC/Ragn...	Malicious	03/10/2020 02:37 PM	Playbook	
	/Ransomware-IOC/Ryuk	Malicious	03/10/2020 02:37 PM	Playbook	
	/Ransomware-IOC/Ryuk	Malicious	03/10/2020 02:37 PM	Playbook	
	/Ransomware-IOC/Rvuk	Malicious	03/10/2020 02:37 PM	Playbook	

Панели управления (Dashboards)

Мульти-панельная структура

Поддержка кастомных панелей

Гибкие панели
на основе виджетов



Отчетность (Reporting)

The screenshot displays the Fortinet Reporting interface. At the top, there's a 'REPORTING' header with a 'WEEKLY ALERT REPORT' dropdown. Below it, the 'Weekly Alert Report' section shows a summary of alerts created in the past 7 days. The main area is a report editor with a 'Template Title' field set to 'MyReport'. It features a 'Define a new structure' section with a grid of widgets, including 'System Monitoring: Memory Utilization' and 'System Monitoring: Disk Utilization'. A 'CHOOSE WIDGET' dialog box is open on the right, listing various widget categories: Structure (Rows, Tabs), Charts and Metrics (Chart, Relationship Count, System Monitoring, Connector Health, Performance Metrics), Record - Card View (Card List, Card Count), Record - Listing (Single Line Item, Simple Grid, Grid, Summary), and Custom Content (IFrame). A blue arrow points from the 'System Monitoring' widget in the dialog to the 'System Monitoring: Memory Utilization' widget in the report editor. The bottom of the image shows a preview of the report with data tables for 'DATA LEAKAGE' and 'ALERT ASSIGNMENT DISTRIBUTION'.

REPORTING WEEKLY ALERT REPORT ▾

Weekly Alert Report
Summary of Alerts created in past 7 days

REPORTING

Template Title:

Define a new structure: [Grid Icons] Default

System Monitoring: Memory Utilization [Edit] [Copy] [Delete]

+ ADD WIDGET

System Monitoring: Disk Utilization [Edit] [Copy] [Delete]

+ ADD WIDGET

Define a new structure: [Grid Icons] Default

Chart [Edit] [Copy] [Delete]

+ ADD WIDGET

ADD ROW

CHOOSE WIDGET [X]

Structure

- Rows - Insert row/column structure to create custom layout.
- Tabs - Add tabular sections with custom content.

Charts and Metrics

- Chart - Choose from multiple chart widgets like Bar, Pie, Donut etc.
- Relationship Count - Insert a chart to show related data source count.
- System Monitoring - Insert a System Monitoring Widget.
- Connector Health - Insert a Connector Health Status Widget.
- Performance Metrics - Build metrics like ROI, MTTR, MTDD etc.

Record - Card View

- Card List - Show record list in a card view.
- Card Count - Show count of records based on a condition.

Record - Listing

- Single Line Item - List record fields in a vertically stacked format.
- Simple Grid - Light-weight, export & print-friendly grid widget for listing records.
- Grid - List records in a grid with multiple columns.
- Summary - Create record(s) summary with fields of choice.

Custom Content

- IFrame - Embed external content within an iFrame section.

DATA LEAKAGE NONE

ALERT ASSIGNMENT DISTRIBUTION

2	3	4740
DANIEL HAMMAN	TENANT USER	NONE

ALERTS BY

47
OPEN

Графическая отчетность с расписанием и доставкой по электронной почте

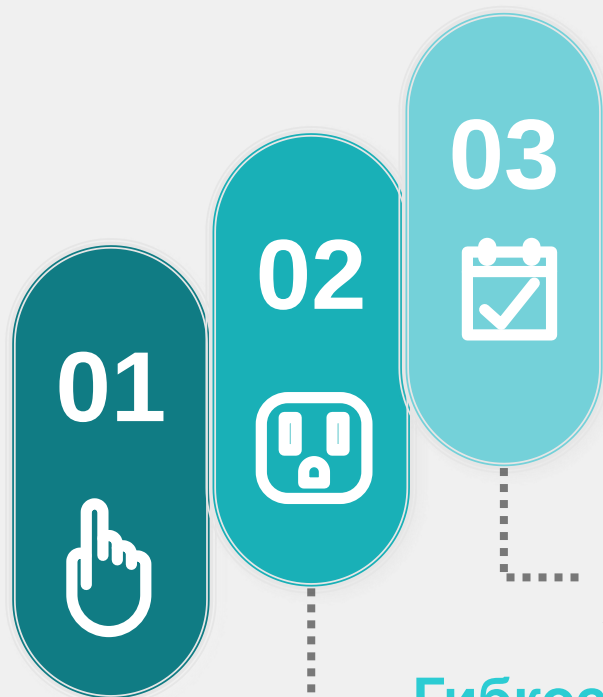
Построение пользовательских отчетов с помощью редактора отчетов на основе виджетов



Особенности



Ключевые особенности FortiSOAR



Продвинутое управление кейсами

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

Гибкость продукта

Automated beyond the investigation, Modify existing modules, Customize Modules

Масштабируемая архитектура

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

Комплексная автоматизация и оркестрация

- Повышение безопасности
- Перекрестное сотрудничество
- Разделение команд и обязанностей

Демонстрация





FORTINET®