



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**



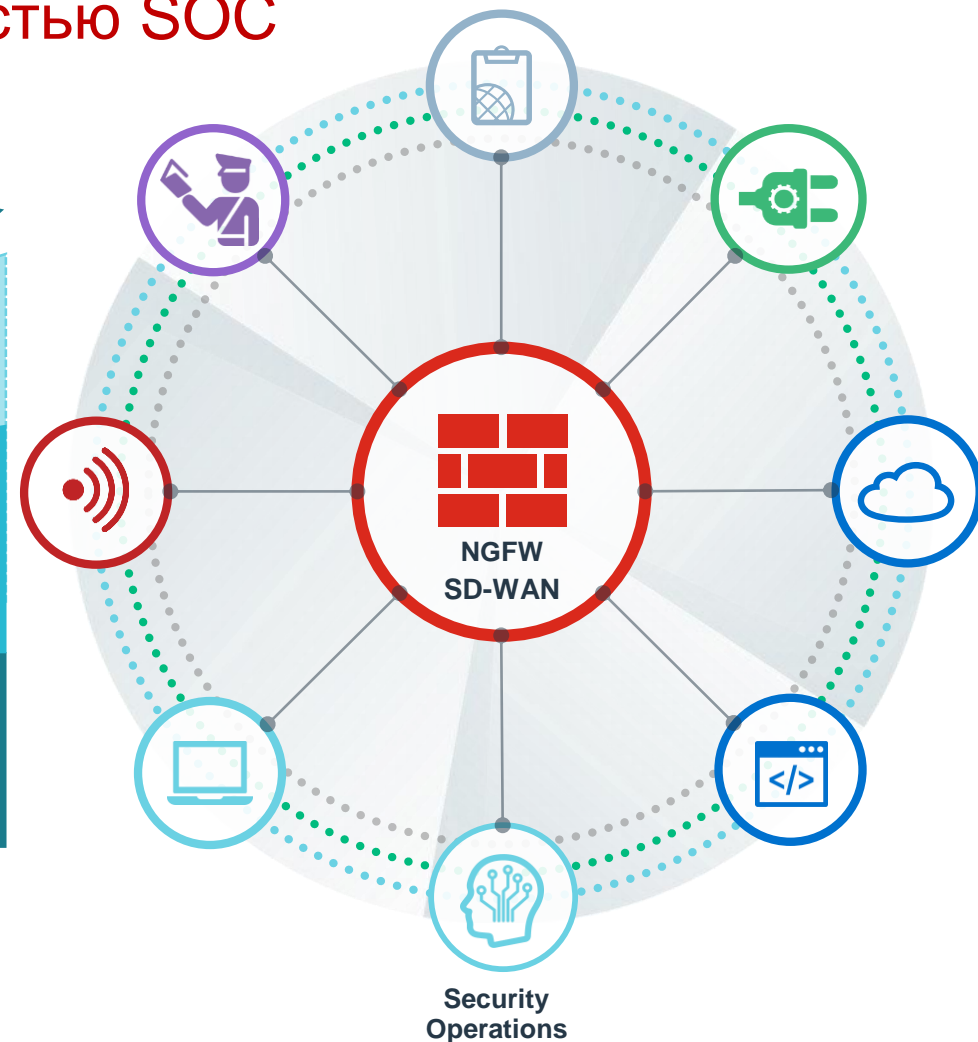
**Ручной и
медленный
ответ**



**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 <u>службы безопасности</u>)	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	<ul style="list-style-type: none"> Logging & Reporting Automated Detection & Response 	Уровень 1 плюс: <ul style="list-style-type: none"> Multi-Vendor Incident Detection 	Уровень 2 плюс: <ul style="list-style-type: none"> 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 централизовать 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 безопасности. 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

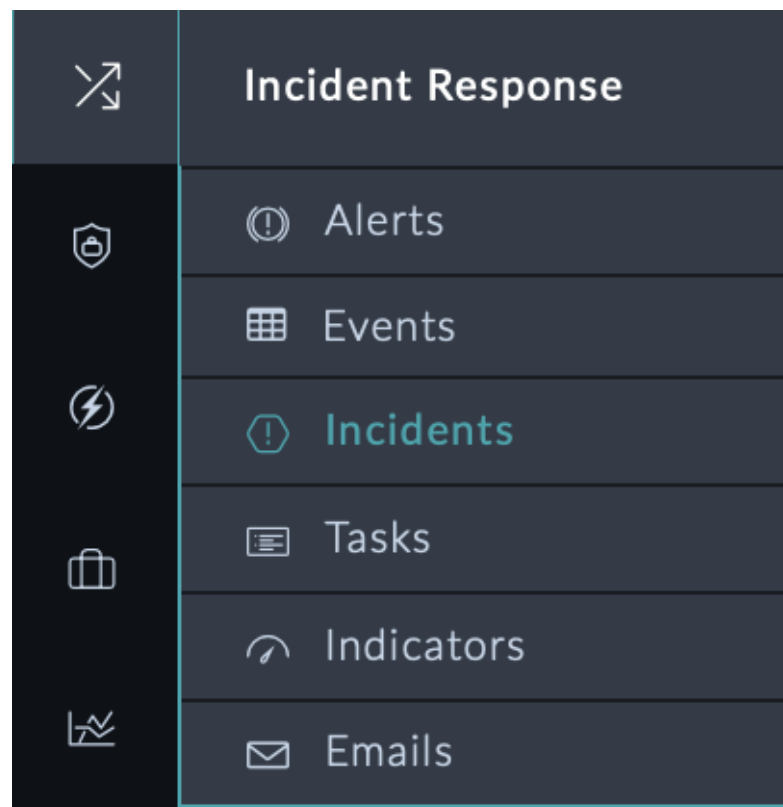


Incident & Case Management

Компонент реагирования на инциденты

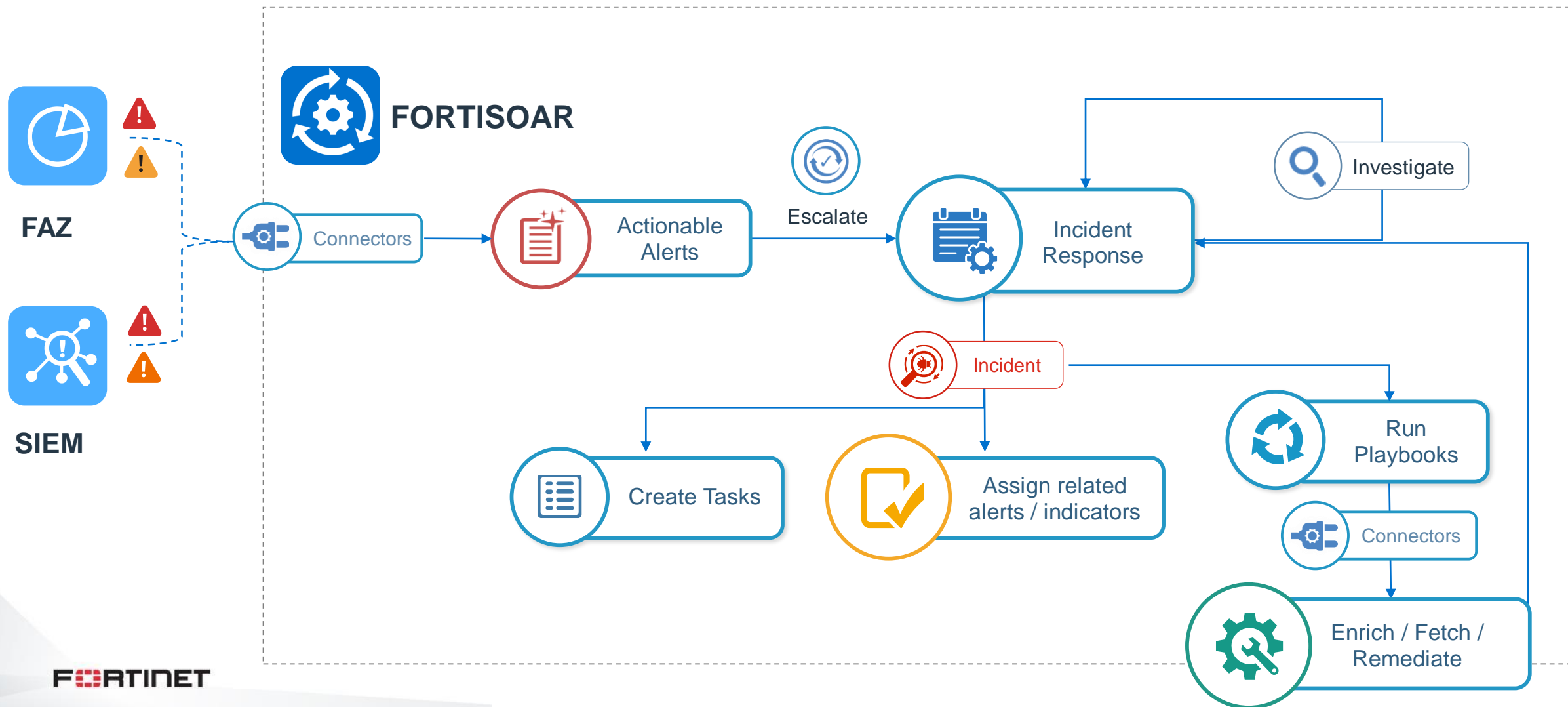
Компонент реагирования на инциденты содержит коллекцию всех модулей, связанных с инцидентами безопасности.

- 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 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

The screenshot displays the Fortinet Security Fabric interface for an incident titled 'Malware Outbreak' (Incident-65). The interface is divided into several sections:

- Incident Details:** Shows the incident lead (Prasannakumar Joshi), status (Open), phase (Detection), and source (Symantec EDR). It also displays the incident description: 'Targeted attack detected using malware family WannaCry'.
- Type Details:** Lists the type (Malware), file hash (db349b97c37d22f5ea1d1841e3c89eb4), target asset (legislation2), and device UID.
- Timeline:** A vertical list of events including 'Created On', 'Assigned Date', 'Resolved Date', 'Acknowledge SLA', 'Ack Due Date', 'Ack Date', 'Ack SLA', 'Response SLA', 'Response Due Date', 'Response Date', and 'Response SLA'.
- Workspace:** A chat window showing a series of messages from users like Amit Jain and Dave Johnson, detailing the response process, including approvals and asset isolation.
- Graph Elements:** A network diagram at the bottom showing connections between various assets and indicators.

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

The screenshot displays the 'Queue Management' interface. On the left, under 'Unassigned Action Items', there is a list of incidents:

Severity	Title	ID NO.	Status	Action
HIGH	PHISHING EMAIL	162	IN PROGRESS	DRAG & DROP TO ASSIGN
HIGH	SUSPICIOUS EMAIL - SUBJ: RESPONSE N...	129	IN PROGRESS	DRAG & DROP TO ASSIGN
HIGH	SUSPICIOUS EMAIL - SUBJ: FREE MEMBE...	133	IN PROGRESS	DRAG & DROP TO ASSIGN
CRITICAL	SENSITIVE DATA BREACH	122	IN PROGRESS	DRAG & DROP TO ASSIGN
MEDIUM	METASPLOIT METERPRETER CONNECTIO...	96	OPEN	DRAG & DROP TO ASSIGN
MEDIUM	OUTBOUND UNENCRYPTED PII DETECTED	95	OPEN	DRAG & DROP TO ASSIGN

On the right, under 'Assigned Action Items', there is a list of queues:

Queue Name	Modified by	Modified Time	Alerts	Team
Mid Night Shift	Ling Lu	04/21/2020 11:14 AM	3 Alerts	--NA--
Day Shift	Ling Lu	04/21/2020 11:12 AM	3 Alerts	
Night Shift	Ling Lu	04/21/2020 11:12 AM	4 Incidents	
SOC Workflow	CS Admin	03/09/2020 11:49 AM	2 Incidents 39 Alerts	

Orchestration & Automation

Разве оркестрация и автоматизация не одно и то же?

Orchestration: возможность управлять или контролировать внешние системы через определенные коннекторы

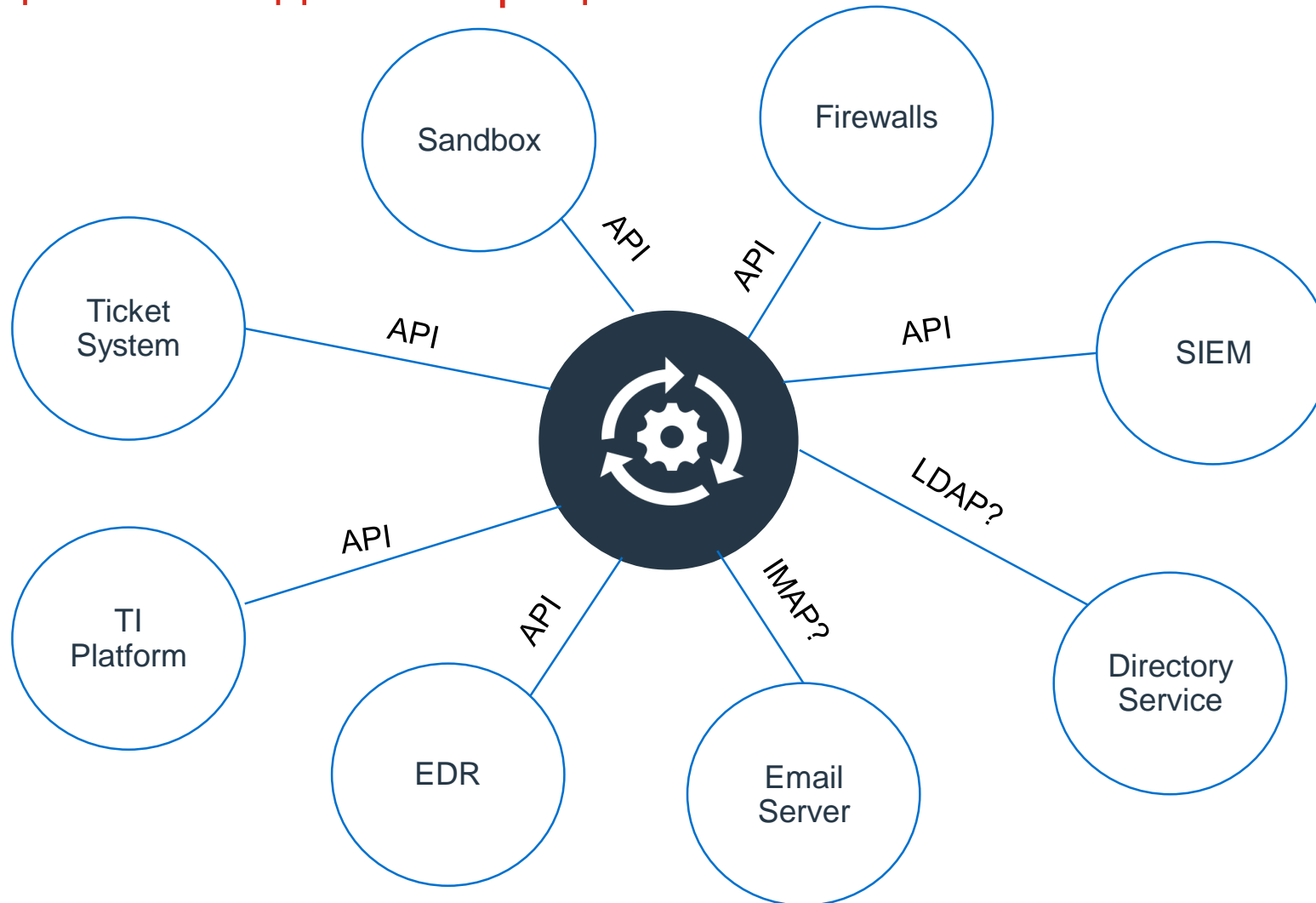
Automation: выполнение сценария реагирования (playbook) при выполнении определенных условий

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 привлечь оператора-аналитика.

Orchestration & Automation

Оркестрация – Методы интеграции



Connectors

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

Orchestration & Automation

Оркестрация – Connectors



280+ коннекторов, 3000+ действий

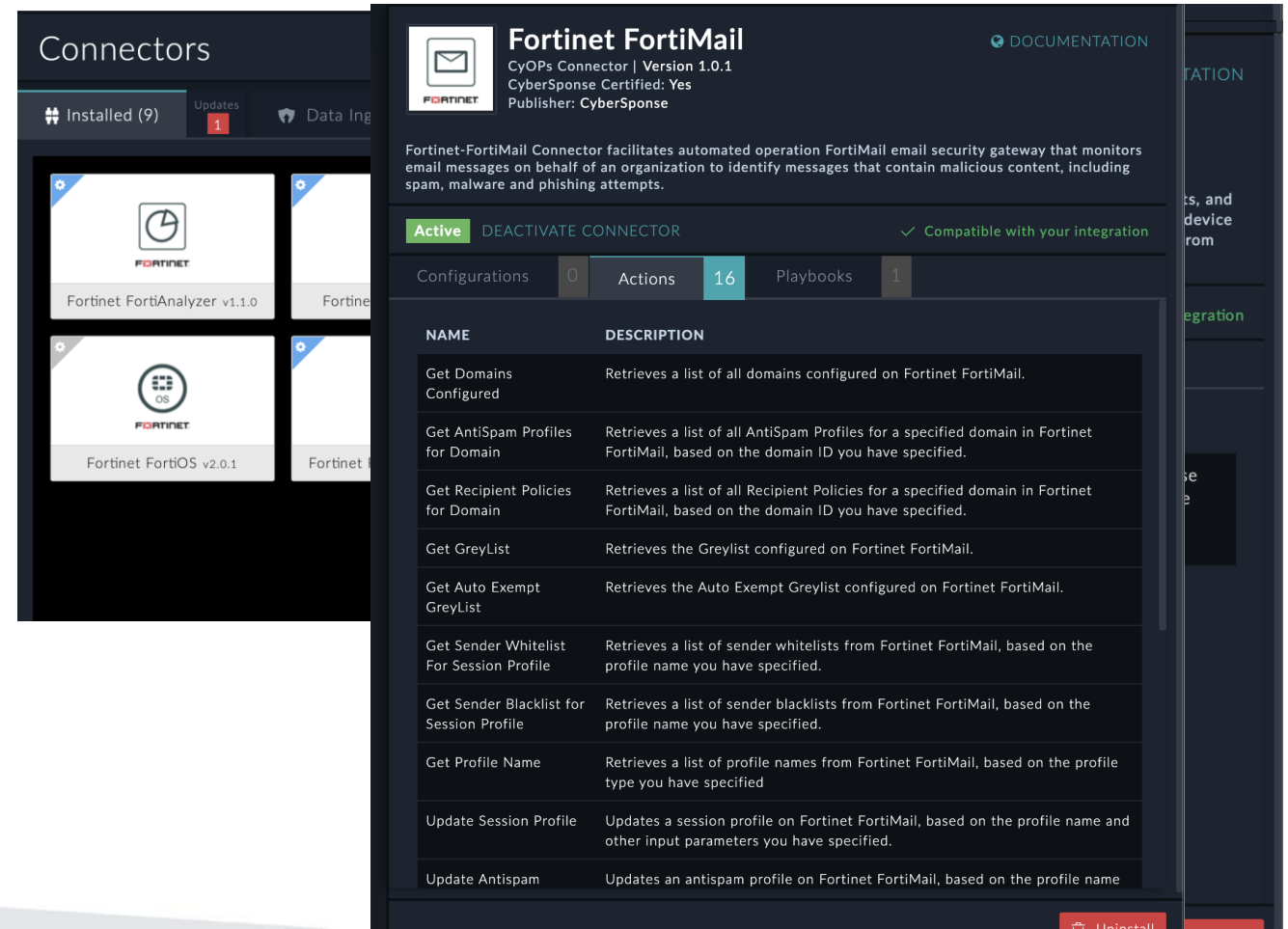
Дополнительные интеграции разрабатываются каждые 3 недели

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



The screenshot displays the Fortinet Connectors Store interface. On the left, a grid shows installed connectors, including Fortinet FortiAnalyzer v1.1.0 and Fortinet FortiOS v2.0.1. The main panel shows the details for the Fortinet FortiMail connector, which is active and compatible with the integration. Below the connector details is a table of actions available for this connector.

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

The screenshot shows the 'Data Ingestion - Anomali ThreatStream' configuration wizard. At the top, a progress bar indicates the steps: Start, Fetch Data, Field Mapping, Scheduling, and Summary. The 'Fetch Data' step is currently active. Below the progress bar, there is a 3D visualization of server racks connected to a central data ingestion point, with a green checkmark indicating success. To the right, a message states 'Data Ingestion Successfully Configured!' and provides a link to the playbook collection. Below this, a 'Quick Summary' section lists the following steps with green checkmarks: Connector 'Anomali ThreatStream' Configured, Sample Data Fetched Successfully, Field Mappings Added, Schedule Created, and Ingestion Playbooks Created Successfully. The last item includes a sub-entry: 'Anomali ThreatStream > Ingest' with an 'ACTIVE' status. A 'Done' button is visible in the bottom right corner.

Orchestration & Automation

Автоматизация – Репозиторий сценариев реагирования

The screenshot displays the FortiSOAR Playbooks management interface. On the left, a sidebar menu includes sections for Dashboard, Queue Management, Incident Response, Vulnerability Management, Automation (with sub-items like Playbooks, 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 playbooks is visible, including 'Asset > Get Runni...', 'Attachment > Get ...', and several 'Indicator' types. A blue callout box points to the 'Import BPMN' button in the top right of the main area. Another blue callout box points to the '02 - Enrich' collection in the left sidebar. A third blue callout box points to the 'Indicator (Type Fil...' entry in the list.

Name	Description	Tags	Active	Is Private
Asset > Get Runni...	Get Running Proc...		✓	
Attachment > Get ...	Get File Reputatio...		✓	
Indicator (Manual ...	Get Reputation of ...		✓	
Indicator (Type All...	Get Reputation of ...		✓	
Indicator (Type Do...	Get Reputation of ...		✓	
Indicator (Type Em...	Get Reputation of ...		✓	
Indicator (Type Fil...	Get Reputation of ...		✓	
Indicator (Type Fil...	Get Reputation of ...		✓	

Импорт из BPMN

Коллекция Playbook'ов

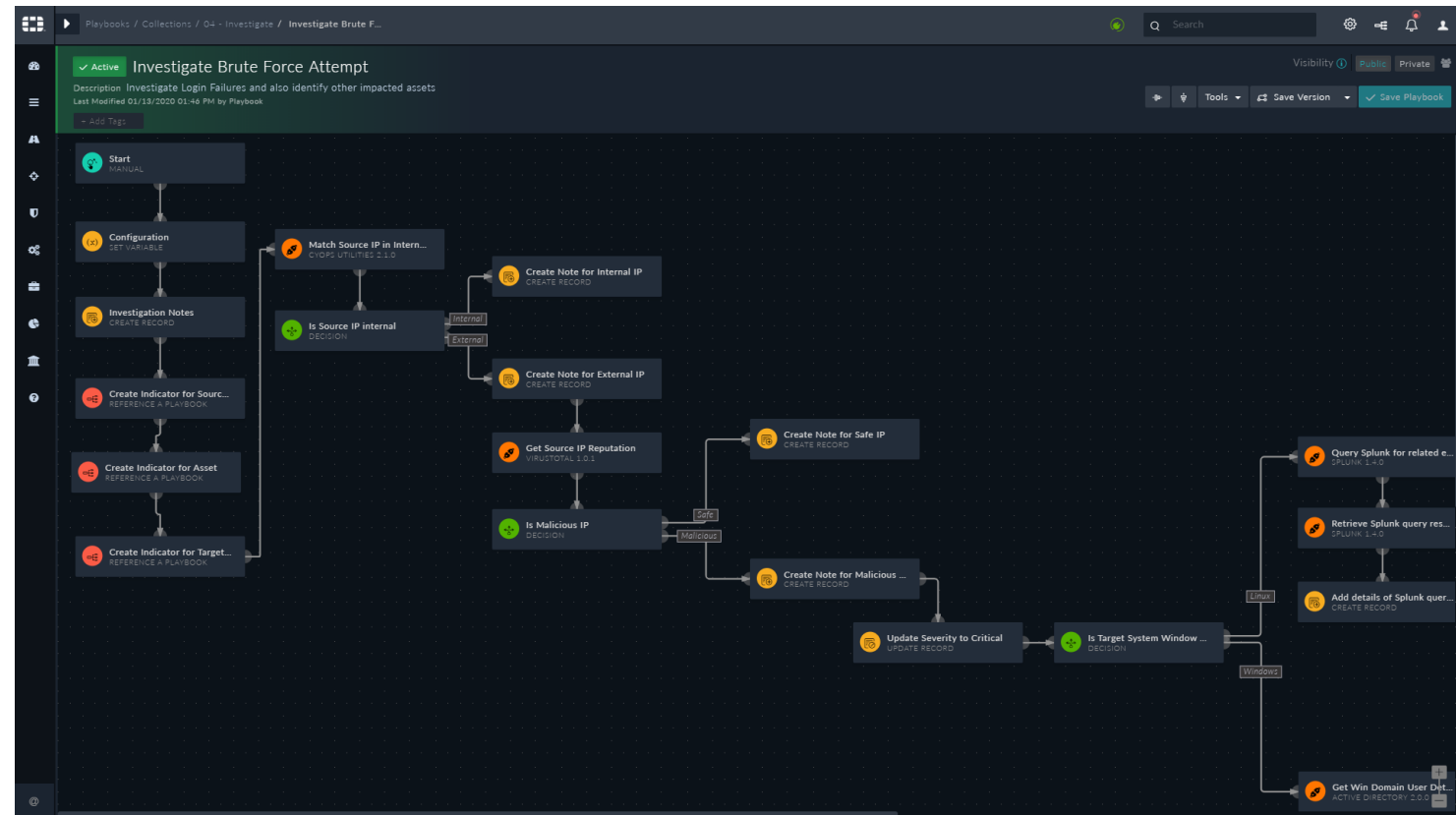
Множество предустановленных Playbook'ов

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 Wiki

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

The screenshot displays the SOC Wiki interface for a Phishing incident response plan. The page title is "SOC Wiki-Phishing" and it is marked as "In Use". The last modified date is 01/04/2020 06:24 PM by CS Admin. The page content includes a description of the incident response plan and a flowchart titled "IR Plan Flowchart".

The flowchart, titled "PREPARE - PHISHING", is a process flow diagram. It starts with a "START" node, followed by a red box "Determine Core Ops Team & Define Roles". From this box, the flow goes to three red boxes: "Vulnerability Manager", "Threat Manager", and "Risk Manager". Below the "Determine Core Ops Team & Define Roles" box is another red box "Review & Maintain Timeline". The flowchart is displayed on a grid background.

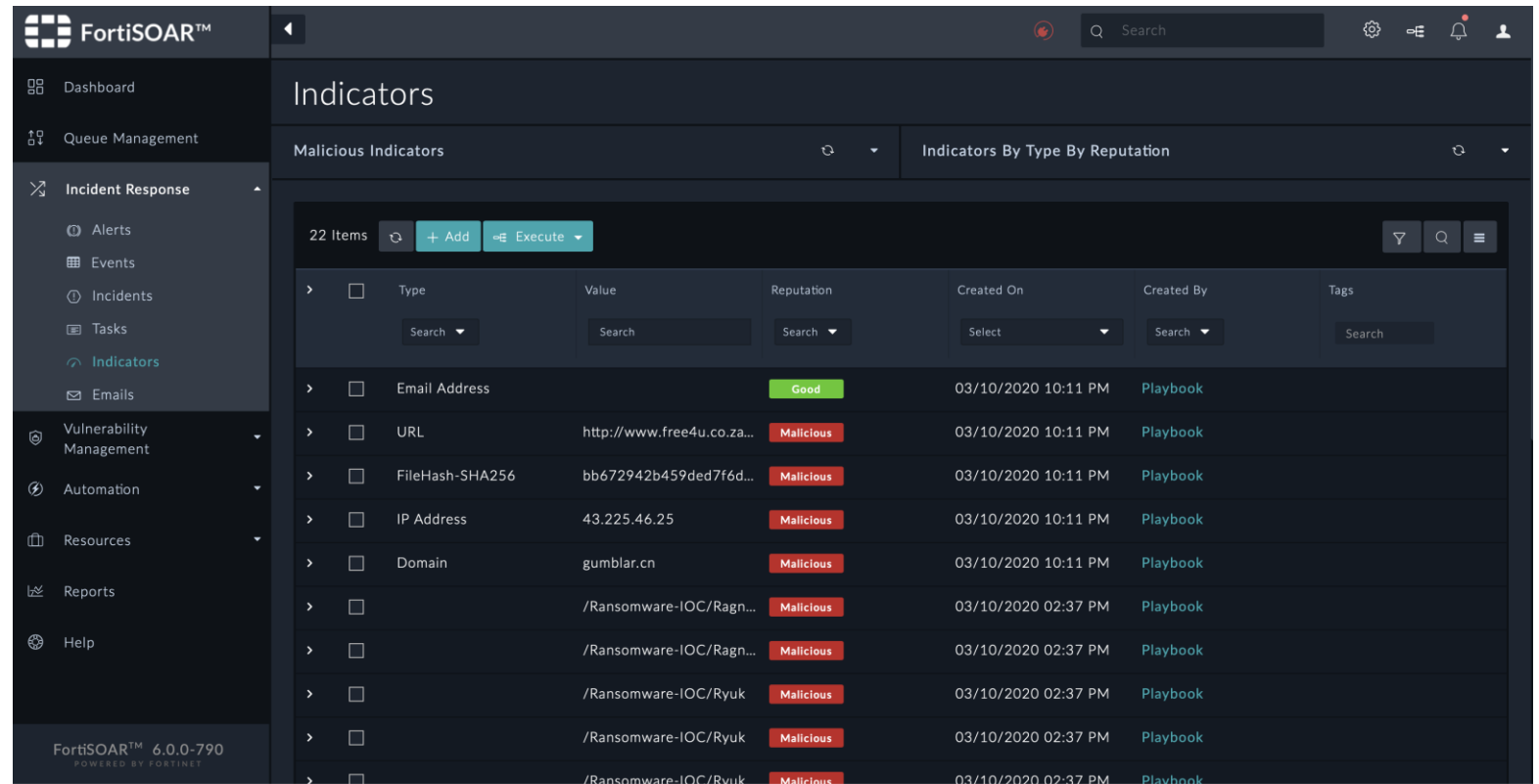
At the bottom of the interface, there are buttons for "Edit Record", "Export Record", and "Delete Record".

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



The screenshot displays the FortiSOAR interface for the Indicators module. The left sidebar contains navigation options: Dashboard, Queue Management, Incident Response (Alerts, Events, Incidents, Tasks, Indicators, Emails), Vulnerability Management, Automation, Resources, Reports, and Help. The main area shows a table of Malicious Indicators with columns for Type, Value, Reputation, Created On, Created By, and Tags. The table contains 22 items, with the first item being an Email Address with a 'Good' reputation and the rest being various types (URL, FileHash, IP Address, Domain, Ransomware-IOC) with 'Malicious' reputations.

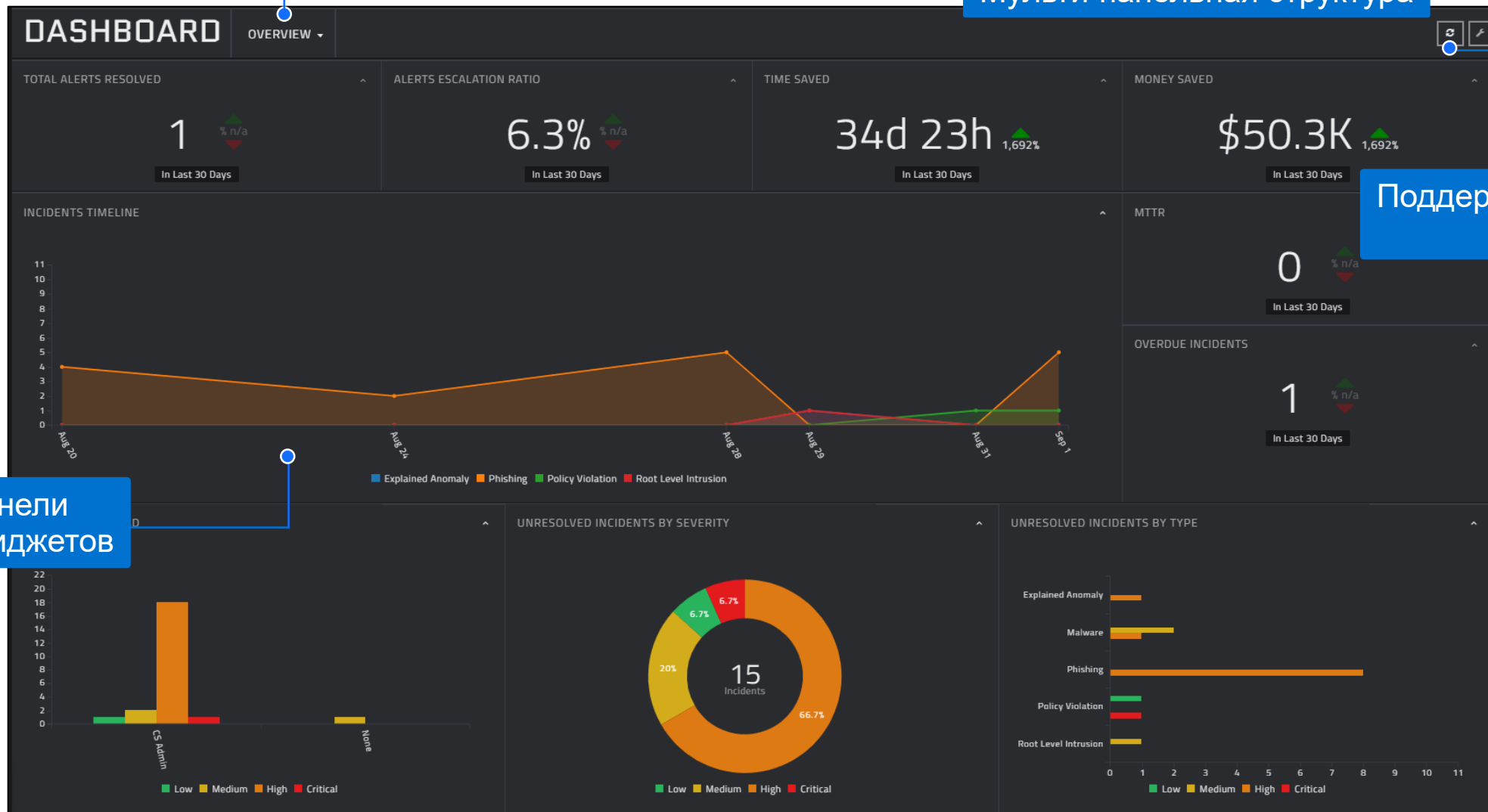
Type	Value	Reputation	Created On	Created By	Tags
Email Address		Good	03/10/2020 10:11 PM	Playbook	
URL	http://www.free4u.co.za...	Malicious	03/10/2020 10:11 PM	Playbook	
FileHash-SHA256	bb672942b459ded7f6d...	Malicious	03/10/2020 10:11 PM	Playbook	
IP Address	43.225.46.25	Malicious	03/10/2020 10:11 PM	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 image displays the Fortinet Reporting interface. At the top, there's a 'REPORTING' header with a 'WEEKLY ALERT REPORT' dropdown. Below it, a 'Weekly Alert Report' section shows a summary of alerts from the past 7 days. The main area is a template editor for 'MyReport', where users can define a new structure using various widgets. A 'CHOOSE WIDGET' modal is open, listing categories like 'Structure', 'Charts and Metrics', 'Record - Card View', 'Record - Listing', and 'Custom Content'. A blue arrow points from the 'ADD WIDGET' button in the editor to the 'System Monitoring' widget in the modal. Below the editor, there are summary cards for 'DATA LEAKAGE' (3) and 'TENANT USER' (2), and a table for 'ALERT ASSIGNMENT DISTRIBUTION'.

DATA LEAKAGE	TENANT USER
3	2

ALERT ASSIGNMENT DISTRIBUTION	TENANT USER	ALERTS BY
4 / 42	3	47
NONE	4740	OPEN

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 распределенного 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
- Мультиэнтная 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

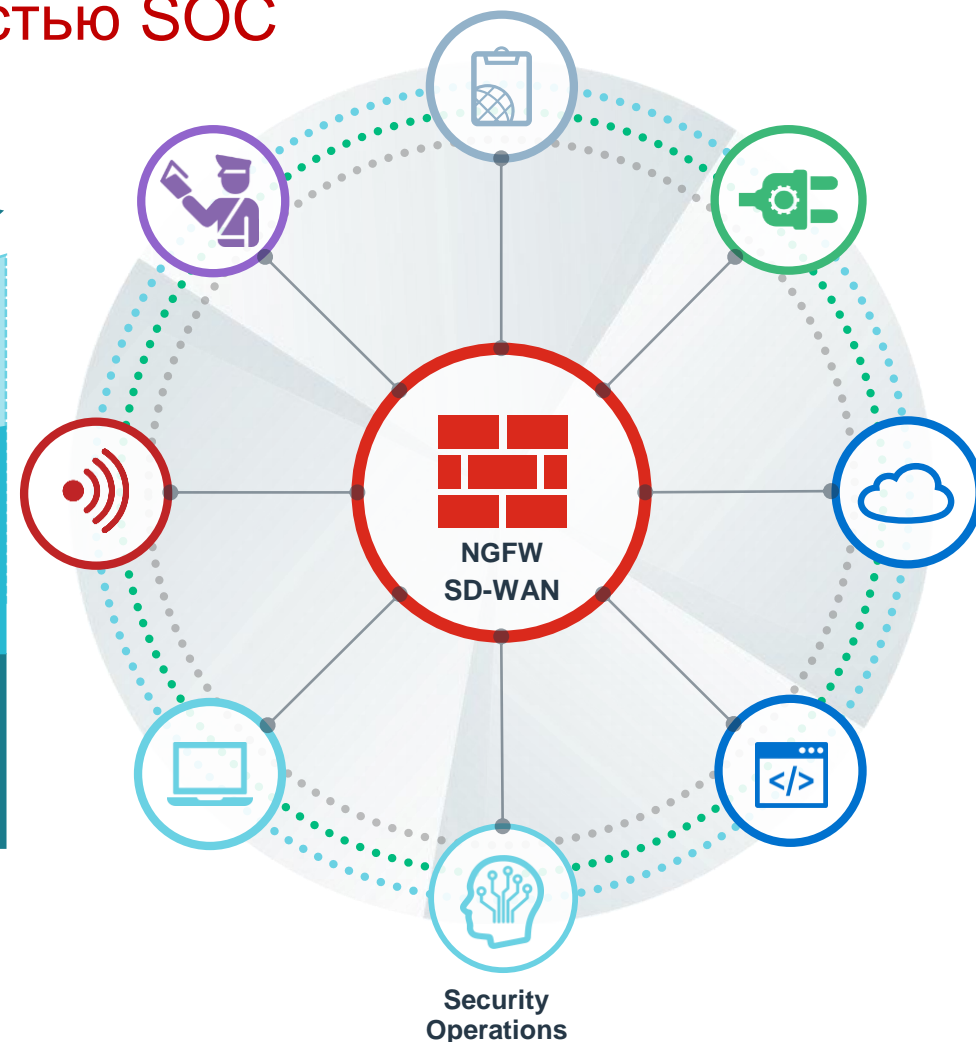
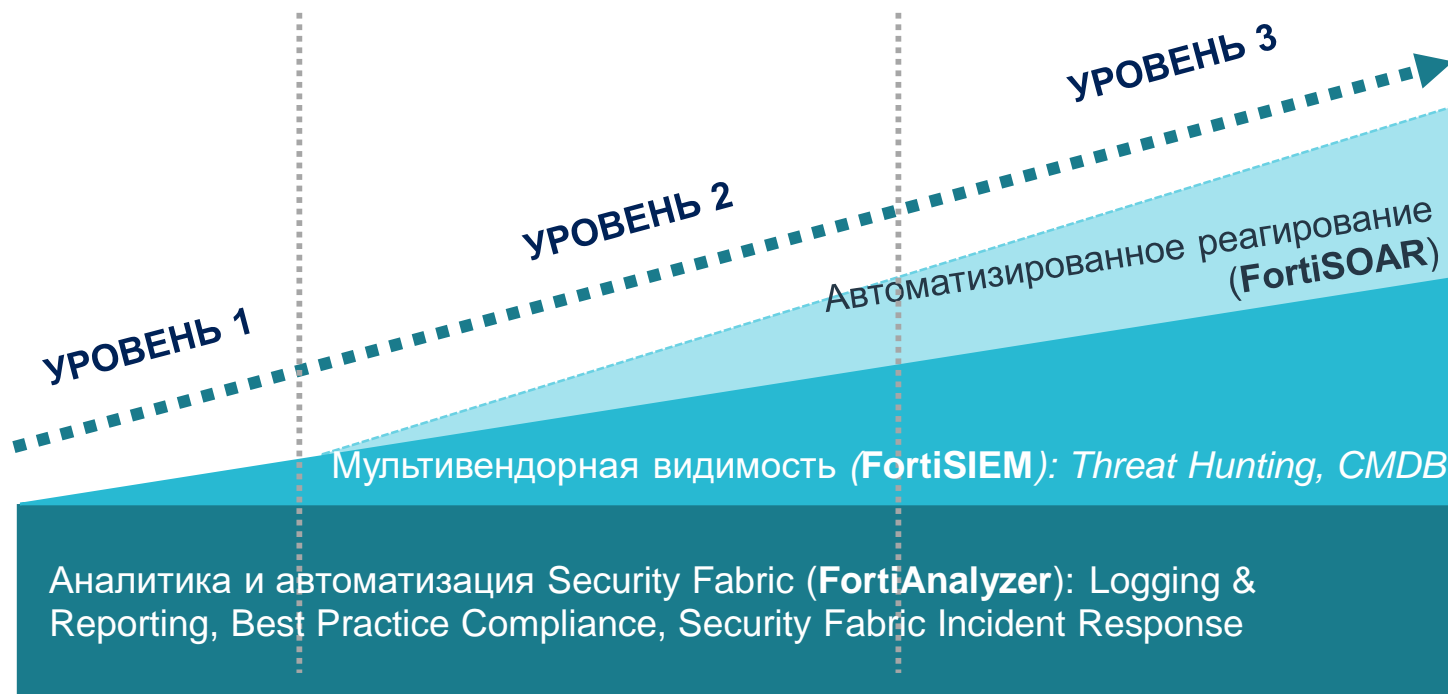
РЕШЕНИЕ

- 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®