FortiEDR

Автоматизация обнаружения и реагирования на угрозы

Решение FortiEDR обеспечивает видимость всей цепочки атаки и выявление действий злоумышленников, не обнаруженных традиционными средствами защиты конечных узлов (Endpoint Protection), а также позволяет автоматизировать процесс реагирования на инциденты информационной безопасности и, тем самым, значительно снизить время реакции на инцидент.

Обнаружение и реагирование

Заложенные в FortiEDR технологии обнаружения и реагирования на угрозы реализуются на основе гибких политик. FortiEDR позволяет администратору безопасности создавать шаблоны политик, определять реакцию на сработку того или иного правила (логирование/блокировка), включать либо отключать определенные правила для групп агентов.

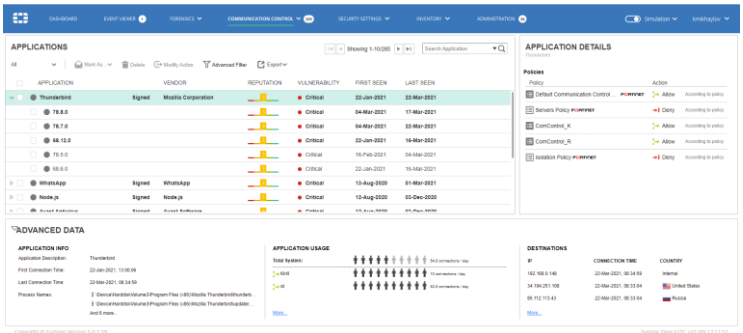
Технологии обнаружения и реагирования можно разделить на два направления: pre-infection и post-infection.

Pre-infection

К технологиям pre-infection относятся модули “Discover and predict”, “Prevent”.

Модуль **“Discover and predict”** позволяет в автоматическом режиме блокировать сетевые подключения приложений, имеющих какие-либо известные уязвимости.

После установки на конечный узел, агент FortiEDR собирает данные о приложениях, открывающих сетевые соединения. Данные о приложениях передаются в центральный компонент (Core) и сопоставляются со списком известных уязвимостей MITRE CVE.



На основе данных о приложениях и уязвимостях FortiEDR позволяет создавать политики автоматической блокировки сетевых соединений уязвимых приложений и тем самым проактивно предотвращать эксплуатацию злоумышленниками уязвимостей в приложениях.

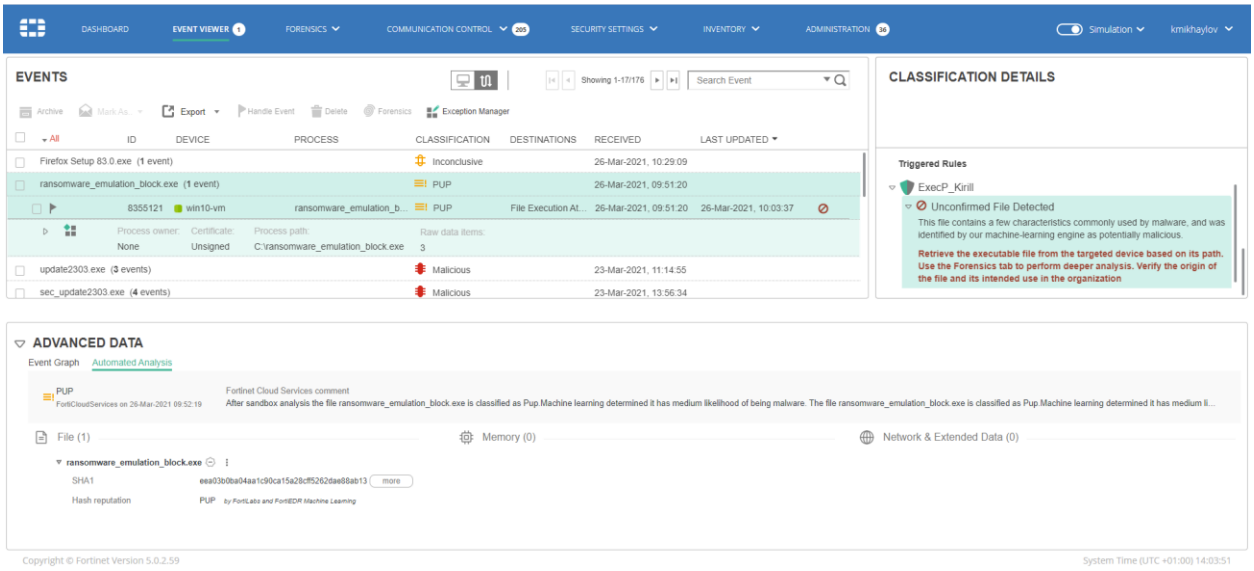
Помимо этого модуль **“Discover and predict”** позволяет обнаруживать подключенные к сети IoT устройства, устройства на которых не установлен агент FortiEDR.

Модуль **“Prevent”** - это встроенный в агент FortiEDR антивирусный движок. Антивирусный движок FortiEDR базируется на технологиях машинного обучения, работает на уровне ядра системы.

Антивирусный движок FortiEDR позволяет:

- Автоматически блокировать запуск вредоносного программного обеспечения (на основе политик execution prevention)
- Реализовать интеграцию с локальной песочницей FortiSandbox
- Осуществлять контроль подключаемых USB устройств (на основе политик device control)

В случае, если агент FortiEDR не подключен к серверной части решения (работает в так называемом автономном режиме) антивирусный движок реализует защиту конечного узла от вредоносного программного обеспечения.



Post-infection

К технологиям Post-infection относятся модули “Detect and defuse”, “Respond and Remediate”.

Данные модули выполняют анализ данных, собранных с конечных узлов (далее телеметрии) агентами FortiEDR. Анализ выполняется центральным компонентом (Core).

Для анализа агент FortiEDR собирает следующую телеметрию:

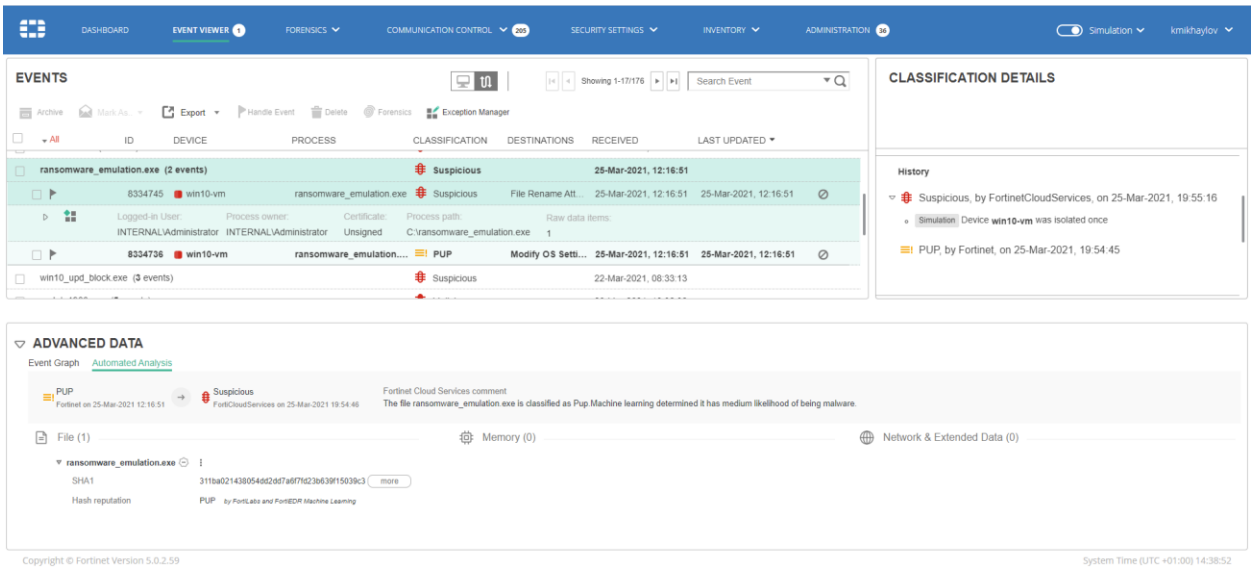
- Данные об активности процессов

- Данные о сетевой активности
- Данные об операциях с файловой системой
- Данные об операциях с реестром
- Записи Windows Event Log

Модуль **“Detect and defuse”** выполняет:

- Автоматизированный анализ данных, собранных с конечных узлов
- Обогащение данных, собранных с конечных узлов информацией об угрозах из облака Fortinet Cloud Services
- Обнаружение вредоносных активностей на конечных узлах на основе анализа телеметрии

После получения данных о какой-либо активности, FortiEDR присваивает данной активности определённый уровень критичности. Всего в системе заложены 5 уровней критичности: от наименьшего – likely safe, до наивысшего – malicious. В зависимости от результатов анализа конкретного события, например, после обогащения данных информацией из облака Fortinet Cloud Service, либо в результате эмуляции файла в песочнице FortiSandbox, критичность инцидента может быть изменена. В случае изменения критичности инцидента действия по автоматизированному реагированию, настроенные для указанного уровня будут применены автоматически.



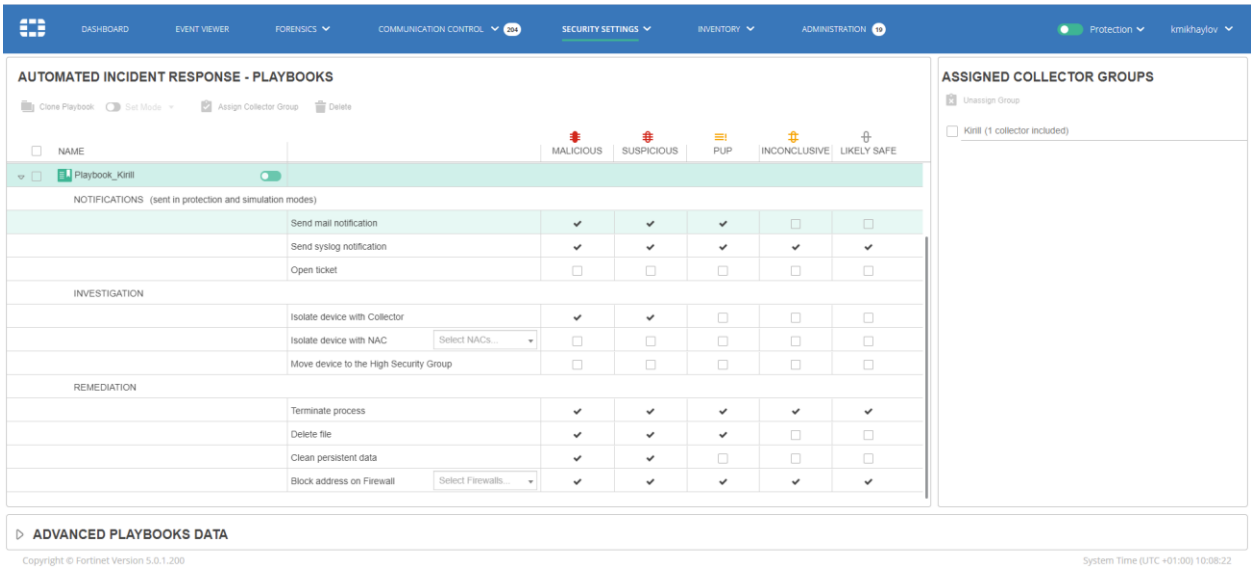
Модуль **“Respond and Remediate”** позволяет автоматизировать реагирование на обнаруженные FortiEDR инциденты безопаности, а также выполнять threat hunting.

Автоматизация реагирования реализуется с помощью политик – Playbooks. Как и политики обнаружения вредоносных активностей, политики реагирования могут гибко

настраиваться администратором безопасности. Помимо возможности выбора определенной реакции в зависимости от критичности инцидента, реагирование также можно настраивать для различных групп агентов FortiEDR.

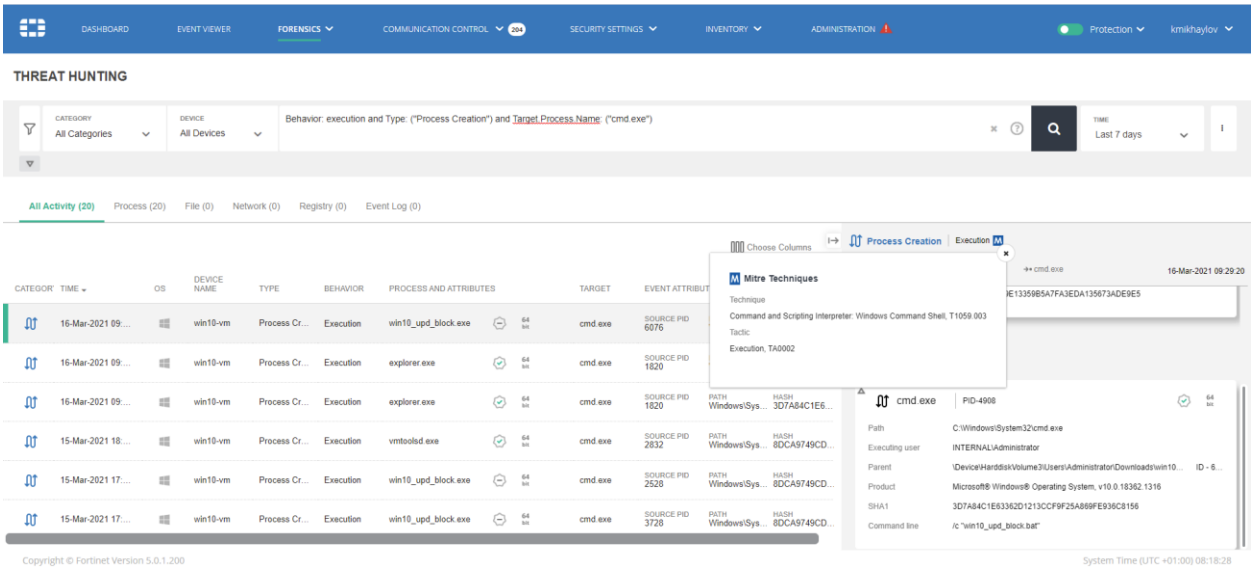
FortiEDR позволяет автоматизировать следующие действия:

- Остановка процесса, выполняющего вредоносные действия
- Удаление файла, породившего вредоносный процесс
- Восстановление модифицированных ключей реестра
- Изоляция рабочей станции от сети
- Перевод агента в более строгую группу
- Блокировка обнаруженного вредоносного IP (требуется интеграция с FortiGate)
- Изоляция рабочей станции от сети с помощью решения FortiNAC (требуется интеграция с FortiNAC)
- Создание почтовой нотификации, syslog
- Открытие тикета в сторонней системе



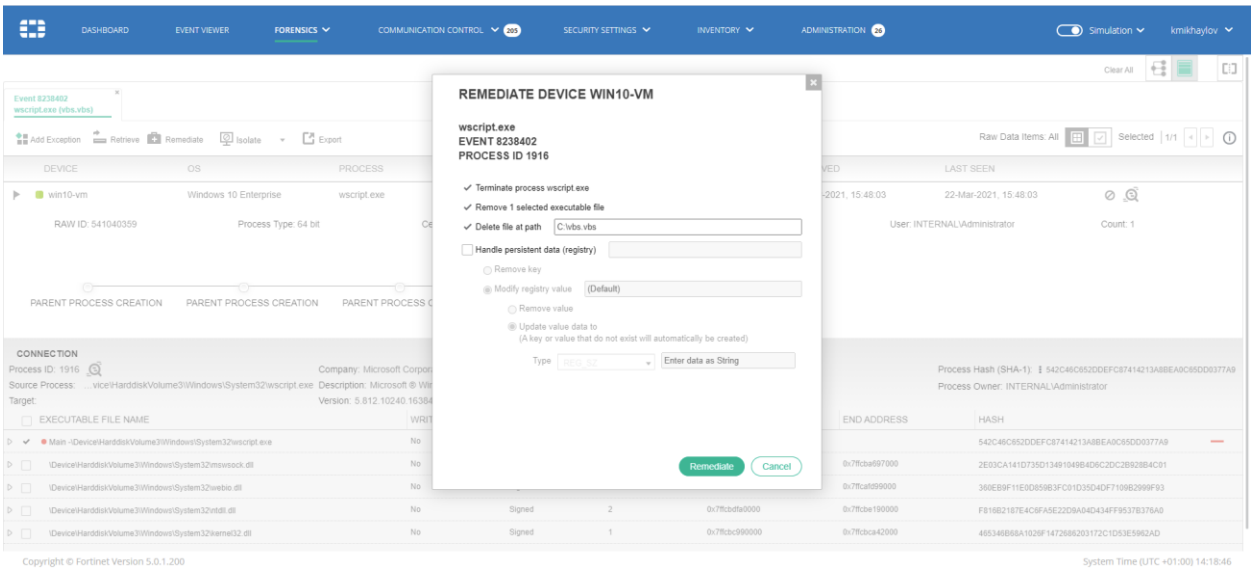
FortiEDR позволяет выполнять проактивный поиск угроз – threat hunting по базе телеметрии, собранной с конечных узлов. Поиск осуществляется с помощью гибкого языка запросов. Язык запросов позволяет создавать сложные поисковые запросы по всем типам данных, обрабатываемых центральным компонентом (Core), а также поддерживает логические операторы для объединения запросов.

FortiEDR позволяет сохранять запросы в виде правил и выполнять сканирование базы по расписанию. В случае обнаружения событий, подходящих под запрос, FortiEDR создает инцидент заданного уровня критичности.



События, хранящиеся в базе телеметрии также маркируются согласно базе тактик и техник MITRE.

Помимо автоматического реагирования на инцидент, FortiEDR позволяет выполнять реагирование в ручном режиме. В дополнение к указанным выше действиям администратор решения может:

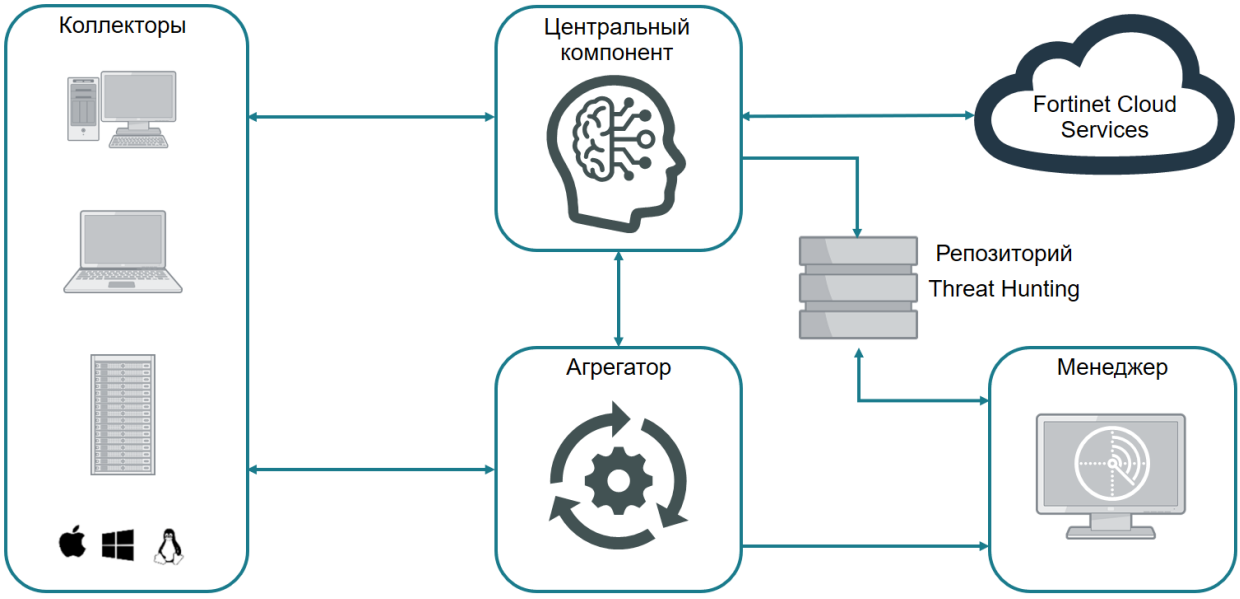


- Выгрузить файл из файловой системы целевой машины для анализа
- Создать дамп памяти процесса
- Удалить файл по заданному пути

- Создать/модифицировать/удалить ключи реестра

Архитектура FortiEDR

FortiEDR состоит из 5 компонентов (см. схему ниже).



Серверные компоненты системы могут быть развернуты как в **облаке** (на серверных мощностях Fortinet), так и **локально** в среде виртуализации.

Коллекторы (агенты) поддерживают операционные системы Windows, Linux, MacOS различных версий, также поддерживаются VDI.

В случае необходимости FortiEDR может быть развернут в полностью изолированном от внешней сети сегменте (т.н. air-gap), с поправкой на отсутствие доступа к облачным сервисам Fortinet.

Интеграция FortiEDR со сторонними решениями

FortiEDR “из коробки” поддерживает интеграцию со следующими решениями Fortinet:

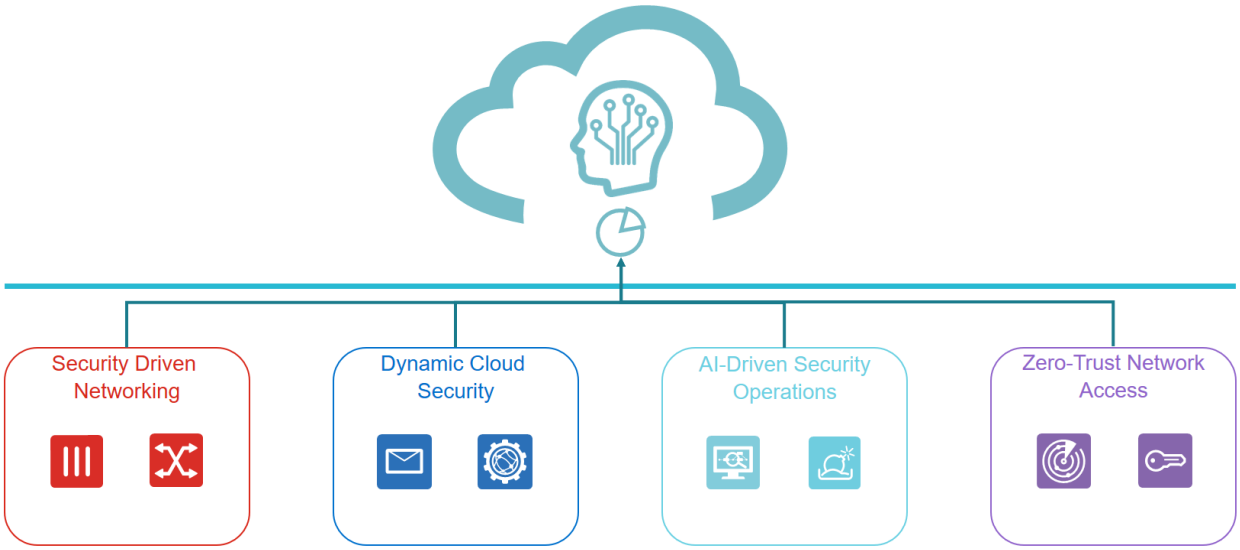
- FortiGate
- FortiSandbox
- FortiNAC
- FortiSIEM (syslog)
- FortiSOAR (API)

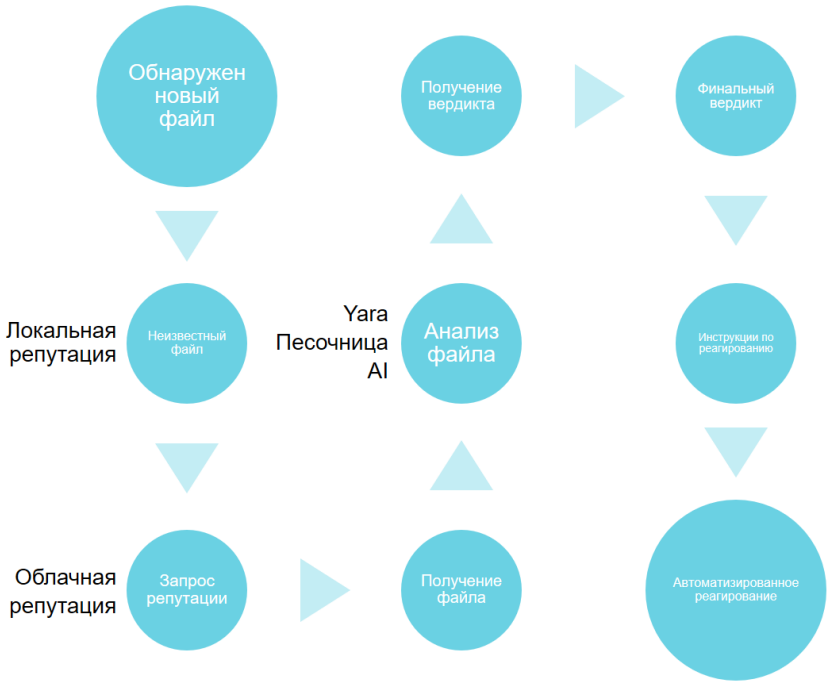
Также на базе FortiEDR реализуется решение FortiXDR, которое позволяет интегрировать FortiEDR с Fortinet Security Fabric.

Для интеграции с решениями сторонних вендоров FortiEDR имеет развитый API.

FortiXDR

FortiXDR позволяет расширить возможности по обнаружения и реагированию на угрозы с рабочих станций на всю Fortinet Security Fabric.



Интеграция с Fortinet Security Fabric реализуется за счет подключения FortiAnalyzer к облачной платформе Fortinet. В рамках облачной платформы, с помощью технологий искусственного интеллекта, происходит обогащение собранных данных, их корреляция, формирование сценария реагирования.

На последнем этапе, с помощью агентов FortiEDR, производит автоматизированное реагирование на обнаруженные угрозы.