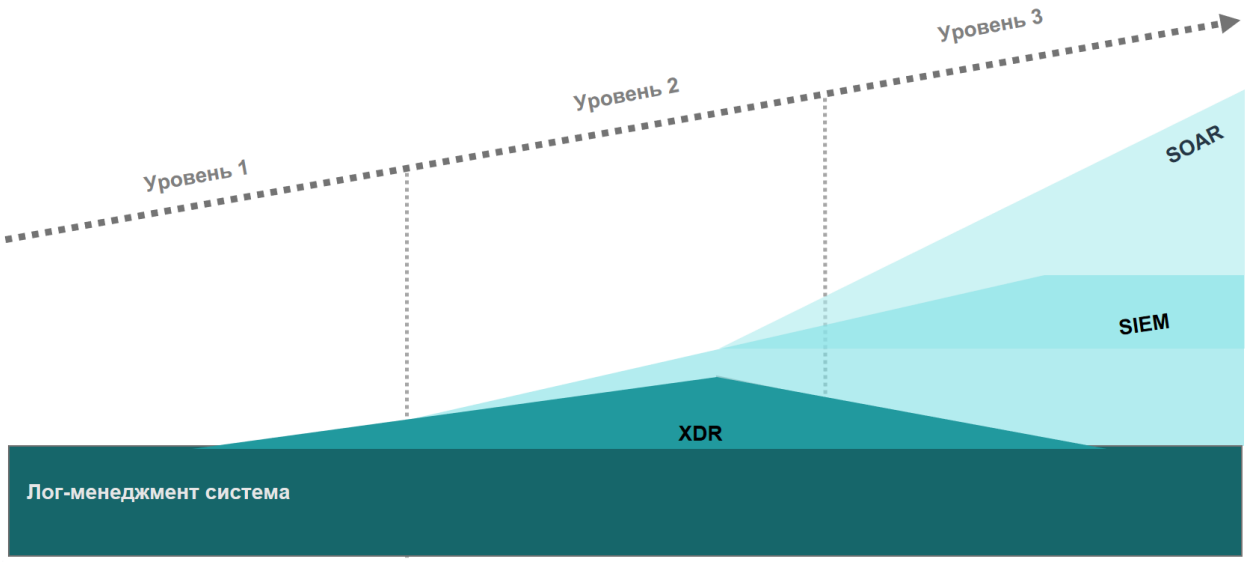
Сравнение решений XDR, SIEM, SOAR

Решения классов XDR (extended detection and response), SIEM (security information and event management) и SOAR (security orchestration, automation and response), лог-менеджмент системы решают схожую задачу – упрощение security operations.



Упрощение операций по обеспечению безопасности достигаются за счет автоматизации рутинных процессов, корреляции различных событий для получения комплексных событий. Для разграничения возможностей перечисленных выше систем, а также зон их применения рассмотрим их функционал подробнее:

- Log-management
- SIEM
- SOAR
- XDR

Log-management

Лог-менеджмент системы позволяют выполнять сбор, обработку и хранение логов с различных устройств. Если говорить о решениях Fortinet – таким решением является FortiAnalyzer. Помимо функции сбора и хранения логов FortiAnalyzer является обязательным компонентом Fortinet Security Fabric – экосистемы Fortinet объединяющей все решения Fortinet. Более подробно описание функционала FortiAnalyzer доступно по следующей ссылке: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/ru_ru/fortianalyzer.pdf

SIEM

SIEM (security information and event management) как и лог-менеджмент система позволяет в том числе реализовать централизованный сбор и хранение журналов. Ключевым отличием SIEM от лог-менеджмент систем является возможность работы с практическими любыми источниками событий (базы данных, syslog, snmp и т.д.), а также возможность создания собственных парсеров для обработки логов. При это лог-менеджмент система является одним из источников событий для SIEM. Плюс ко всему важным функциональным блоком SIEM является возможность корреляции событий и последующее исполнение каких-либо действий – от создания нотификации до запуска скрипта на удаленном узле. Также в состав SIEM могут входить инструменты управлением активами (asset management), контроля действий пользователей (UEBA), а также создания различных отчетов. FortiSIEM – решений класса SIEM от Fortinet. Более подробная информация о решении доступна по следующей ссылке: https://www.fortinet.com/ru/products/siem/fortisiem

SOAR

SOAR (security orchestration, automation and response) – решение, позволяющее частично автоматизировать обработку и последующее реагирование на инциденты безопасности. По сути своей SOAR является единой консолью работы с инцидентами для аналитика/офицера безопасности.

С помощью встроенных коннекторов и API SOAR позволяет подключить различные источники для получения данных о событиях безопасности. В процессе обработки событий с помощью коннекторов и API SOAR позволяет в ручном, либо автоматическом режиме выполнить классификацию инцидента, запросив информацию из сторонних источников. Последующие действия по обработке инцидента и реагированию на него также могут быть реализованы с помощью интеграции SOAR со сторонними системами.

Автоматизация как первой, так и последующей стадий работы с инцидентами достигается с помощью т.н. плэйбуков – сценариев реагирования на инцидент, описанных в системе в виде, например, блок-схем. В рамках плэйбуков SOAR позволяет, например, запросить данные о хэшах файлов или IP адресах из сторонних систем, передать какой-либо файл на анализ в песочницу или заблокировать обнаруженный вредоносный url на МСЭ и т.д.

Важно заметить, что SOAR, как и SIEM, не является заменой защитных решений для рабочих станций или сети т.к. сам не реализует какие-либо защитные механизмы, но позволяет управлять сторонними системами с помощью функционала коннекторов и API.

FortiSOAR – решение класса SOAR от Fortinet. Более подробная информация о решении доступна по следующей ссылке: https://www.fortinet.com/ru/products/fortisoar

XDR

XDR (extended detection and response) позволяет автоматизировать процесс обнаружения и реагирования на угрозы и, тем самым, существенно разгрузить команду безопасности. Gartner определяет XDR как “Моновендорное SaaS решение для обнаружения и реагирования на угрозы, объединяющее различные решения для обеспечения безопасности с единую систему”.

Решения XDR являются в первую очередь решениями по обнаружению и реагированию на угрозы. XDR является “поставщиком” событий для SIEM и SOAR, а также одним из инструментов по реализации реагирования на инциденты, который может использоваться в связке с SIEM и SOAR.

Важным отличием XDR от SOAR и SIEM является то, что правила и логика обнаружения вредоносных активностей зачастую заложены вендором (например, правила корреляции и обнаружения вредоносных активностей в FortiXDR заложены в функционал решения и на постоянной основе обновляются) и не требуют какой-либо дополнительной настройки, и последующего “тюнинга”. Администрирование и сопровождение решений XDR также заметно проще SOAR и SIEM. В свою очередь SOAR и SIEM системы “из коробки” несут в себе базовый функционал и требуют постоянного внимания со стороны аналитиков/офицеров безопасности.

FortiXDR – решение Fortinet класса XDR. FortiXDR базируется на двух компонентах:

- FortiEDR
- FortiAnalyzer (а если быть точнее – событиях решений Fortinet, входящих в Fortinet Security Fabric)

Компоненты FortiXDR

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”.

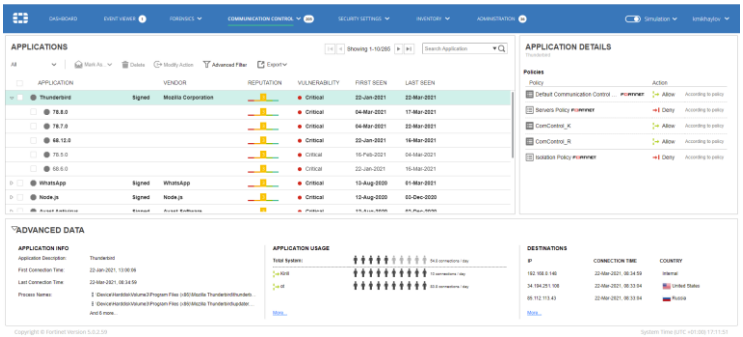
Модуль **“Discover and predict”** позволяет в автоматическом режиме блокировать сетевые подключения приложений, имеющих какие-либо известные уязвимости.

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.

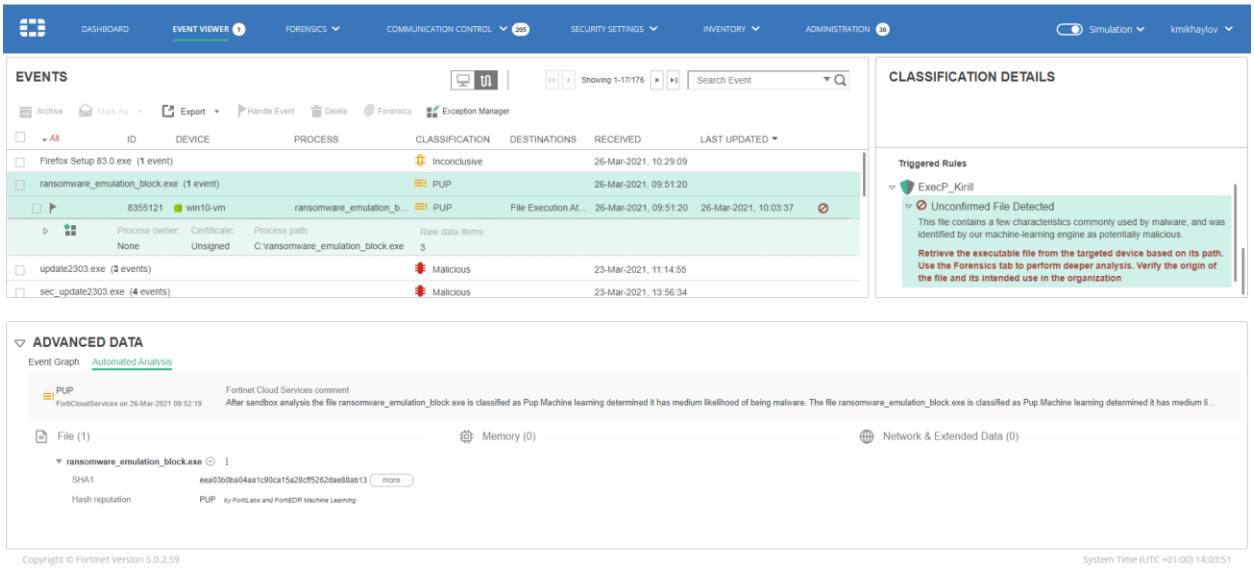


Антивирусный движок FortiEDR позволяет:

- 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).

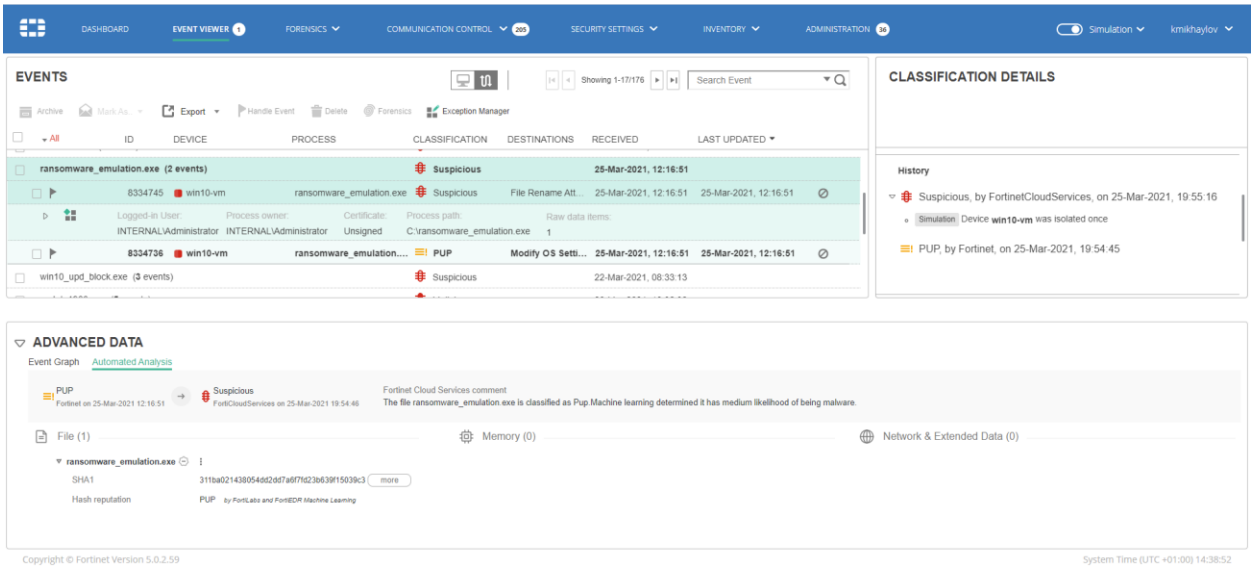
Для анализа агент FortiEDR собирает следующую телеметрию:

- 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.



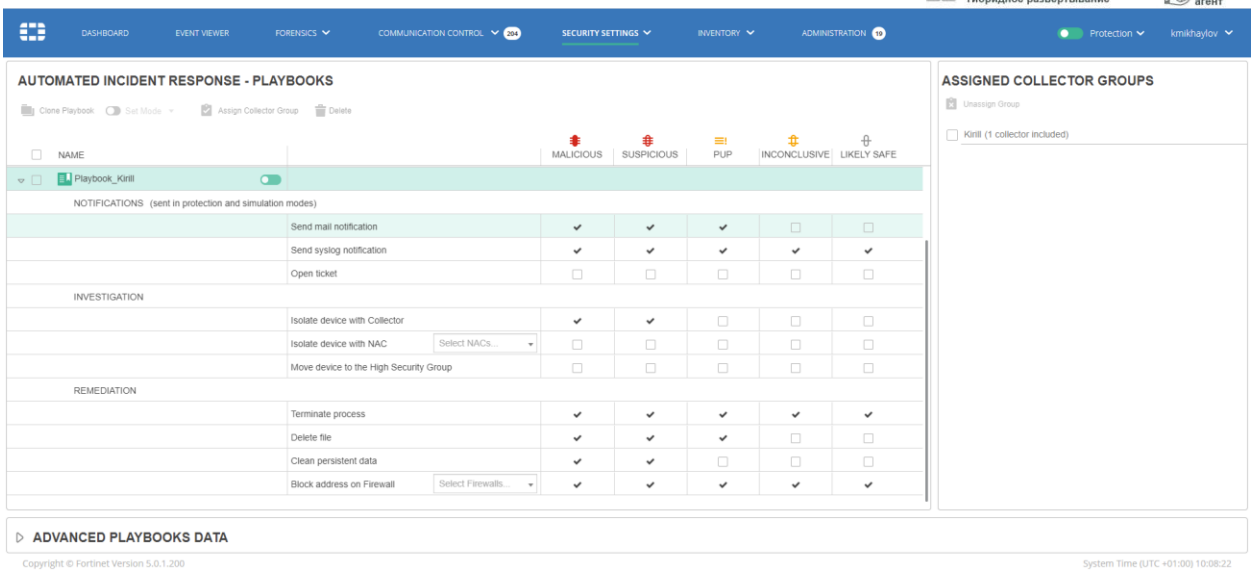
Модуль **“Respond and Remediate”** позволяет автоматизировать реагирование на обнаруженные FortiEDR инциденты безопаности, а также выполнять threat hunting.

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:

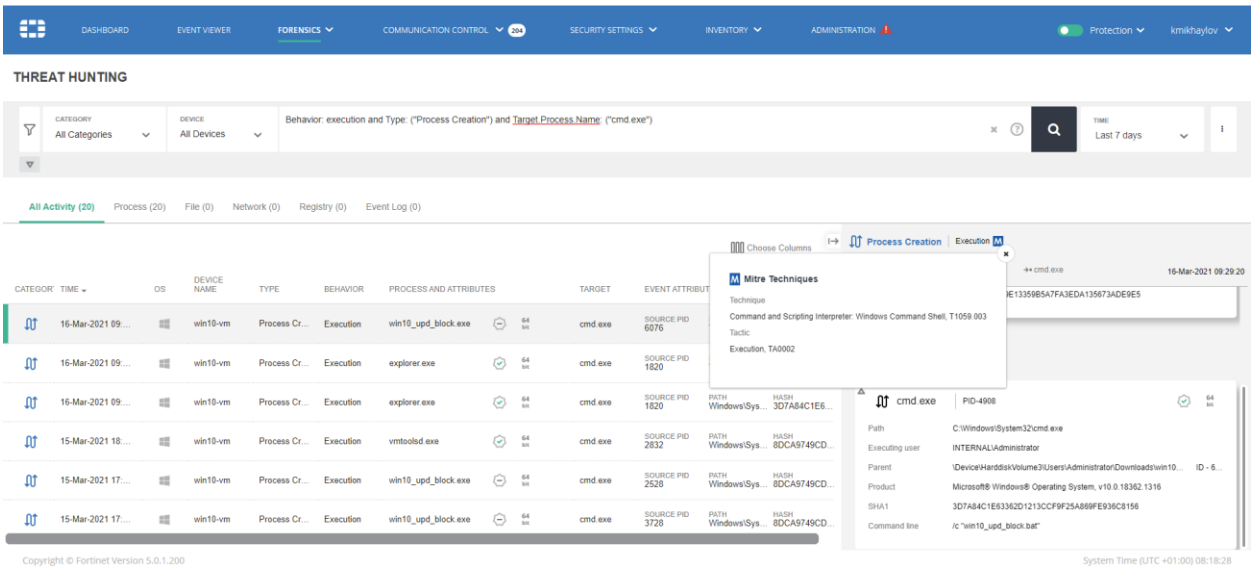
- Остановка процесса, выполняющего вредоносные действия
- Удаление файла, породившего вредоносный процесс

- 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



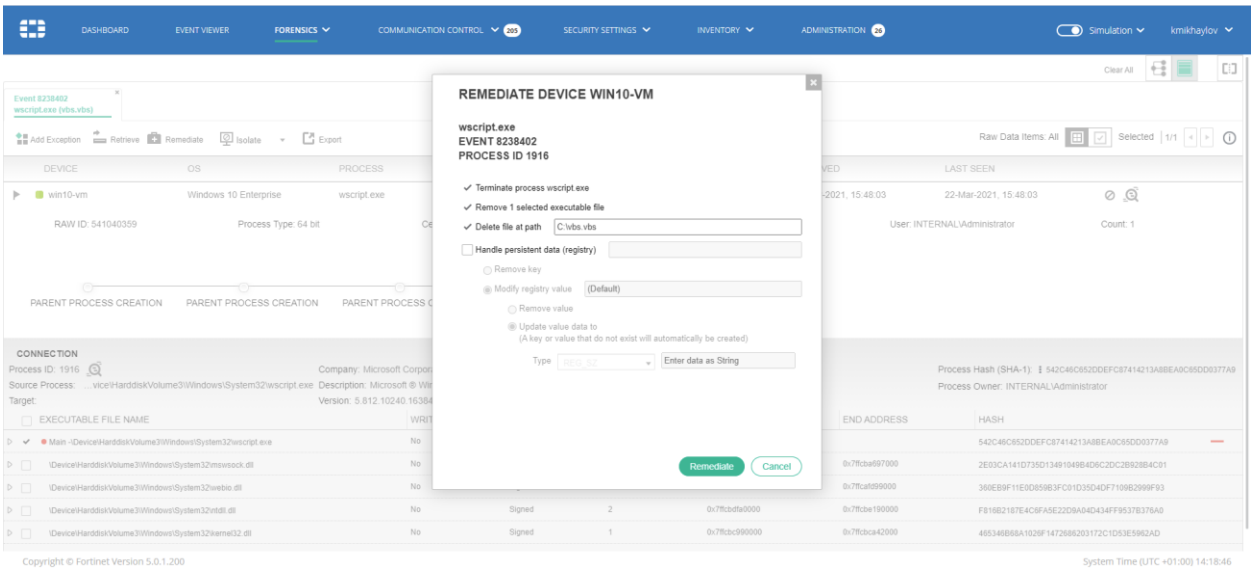
FortiEDR позволяет выполнять проактивный поиск угроз – threat hunting по базе телеметрии, собранной с конечных узлов. Поиск осуществляется с помощью гибкого языка запросов. Язык запросов позволяет создавать сложные поисковые запросы по всем типам данных, обрабатываемых центральным компонентом (Core),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

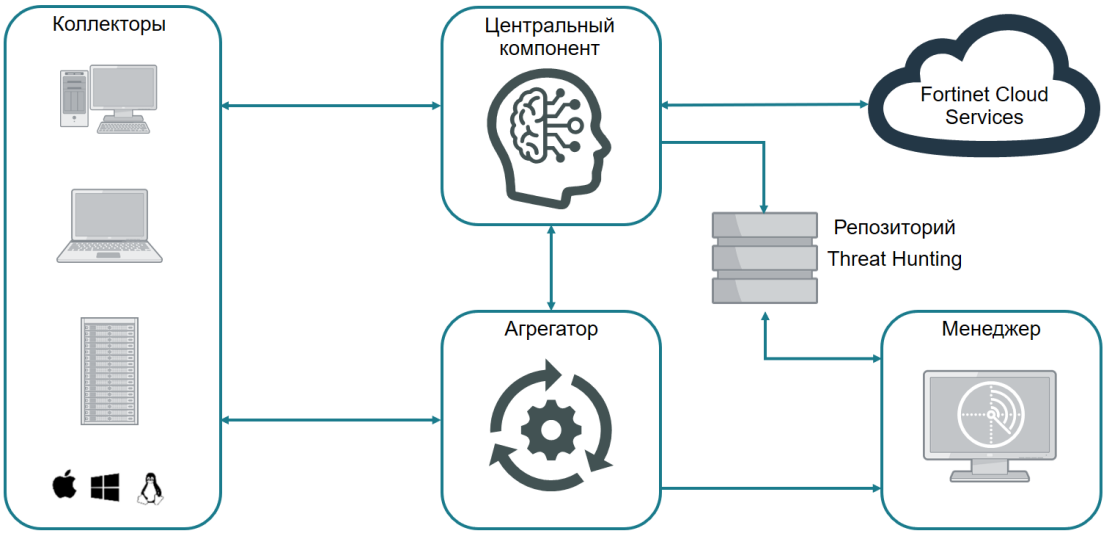
Помимо автоматического реагирования на инцидент, FortiEDR позволяет выполнять реагирование в ручном режиме. В дополнение к указанным выше действиям администратор решения может:



- 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:

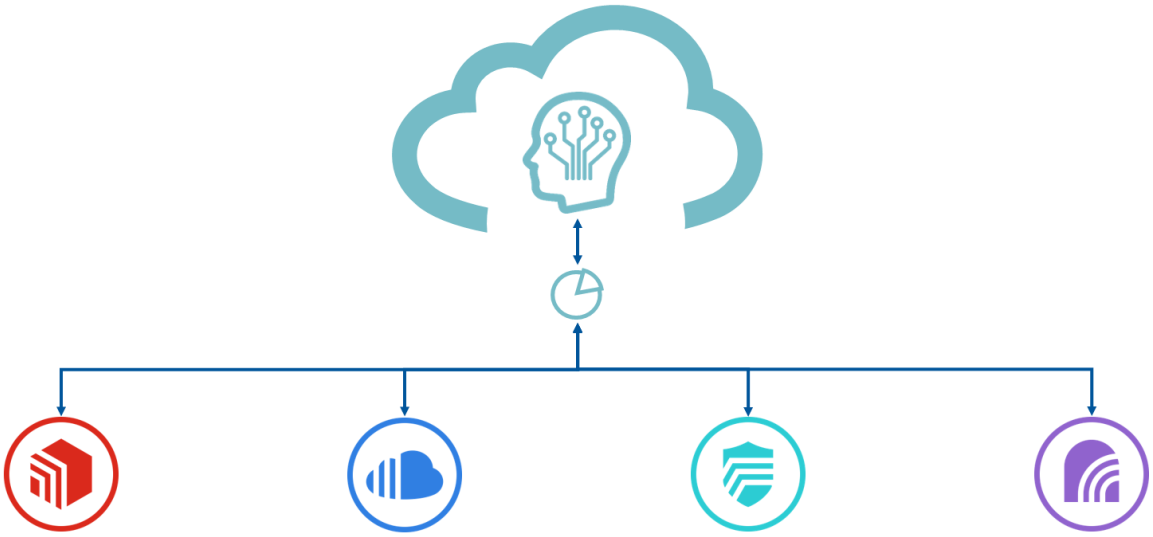
- FortiGate
- FortiSandbox
- FortiNAC
- FortiSIEM (syslog)
- FortiSOAR (API)

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.

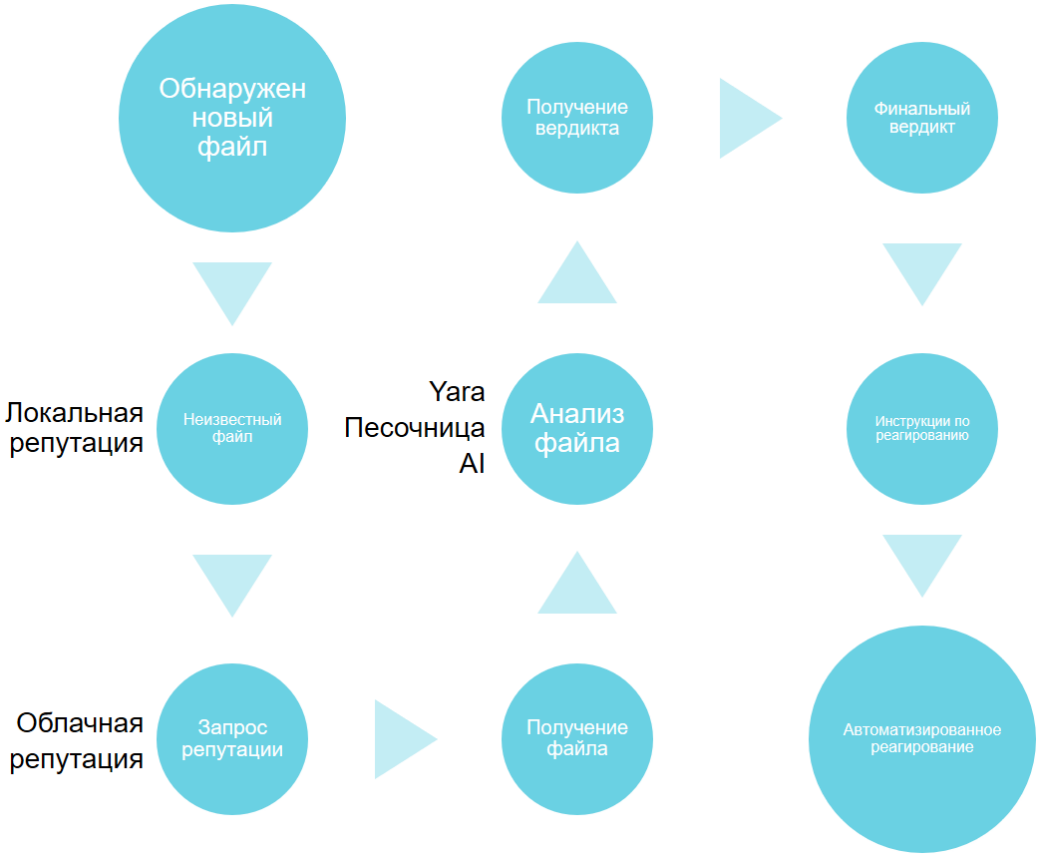
FortiXDR

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 FortiXDR. В рамках облачной платформы, с помощью технологий искусственного интеллекта, происходит обогащение собранных данных, их корреляция, формирование сценария реагирования.

В рамках расследования система автоматически анализирует полученные из



подключенных к FortiAnalyzer источников данные, а также коррелирует их с телеметрией, полученной от коллекторов FortiEDR с конечных узлов.

На следующем шаге FortiXDR, опять же в автоматическом режиме, производит обогащение данных в сторонних источниках (FortiGuard cloud services и база данных партнеров), а также может дополнительно запросить с конечного узла файл для дополнительного его анализа в песочнице. В результате анализа FortiXDR формирует вердикт о вредоносности той или иной обнаруженной активности, а также план автоматизированного реагирования.

На последнем этапе, с помощью встроенного в коллекторы FortiEDR функционала по реагированию на инциденты, производит автоматизированное реагирование на обнаруженные угрозы.