FortiEDR: средство обнаружения комплексных атак на рабочие станции

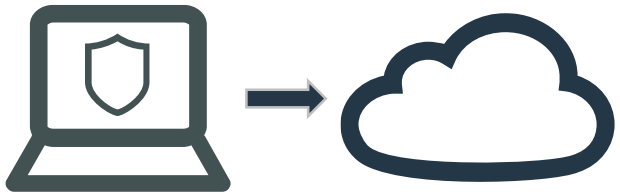
Кирилл Михайлов, Fortinet

Зачем?

Зачем?

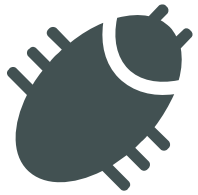
Эволюция атак

Управление уязвимостями

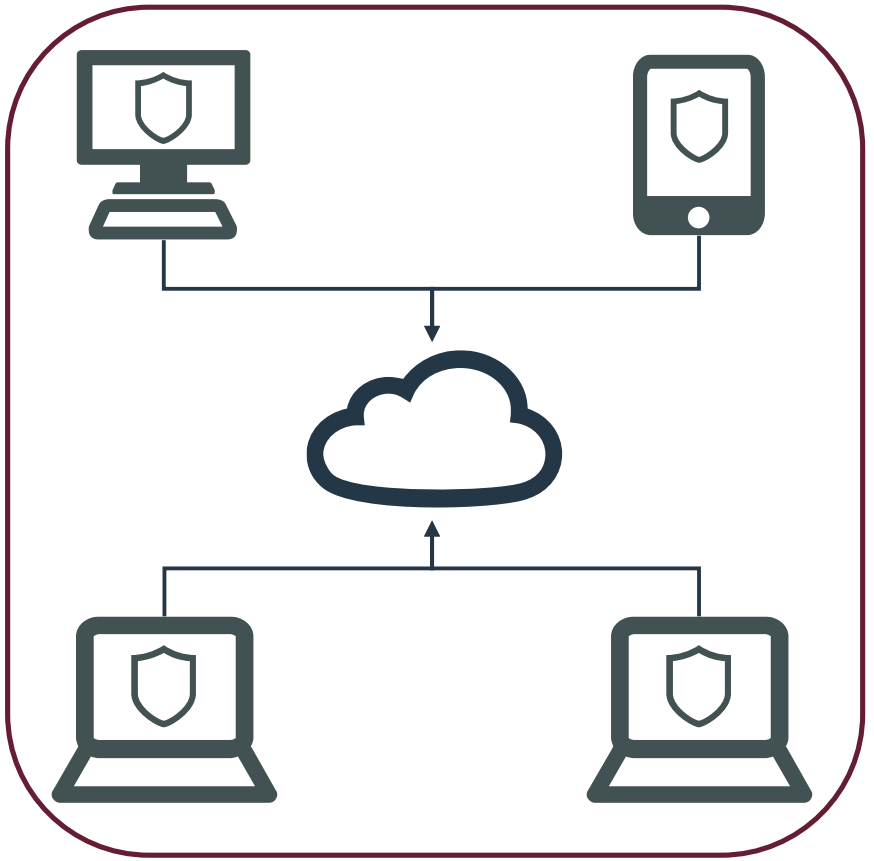


Размытие границ сети

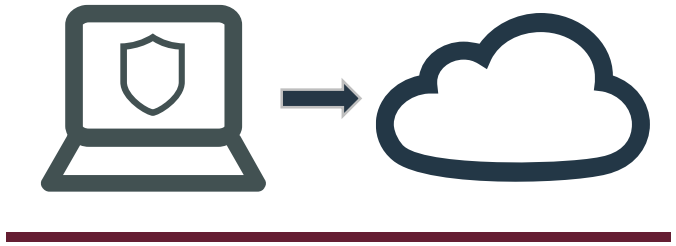
Управление уязвимостями



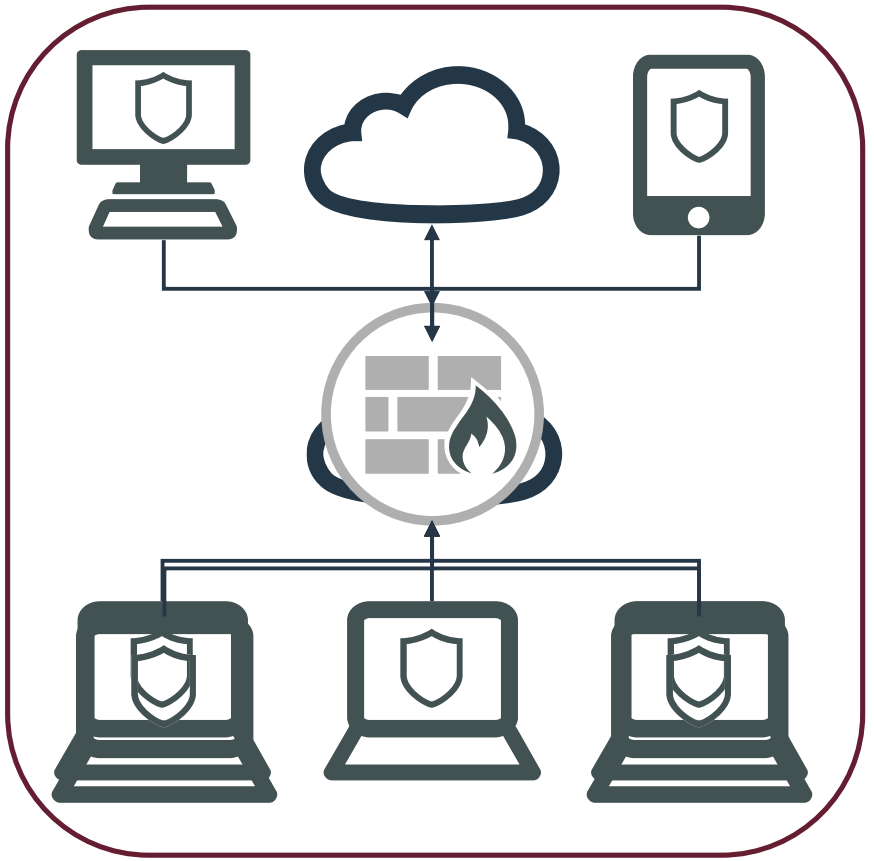
Управление уязвимостями



Размытие границ сети



Размытие границ сети



Эволюция атак

Эволюция атак

Целевой фишинг

Атаки с использованием легитимного ПО

Вредоносное программное обеспечение

Угрозы нулевого дня

Вирусы-вымогатели

Охота за угрозами

Охота за угрозами

Антивирусное ПО необходимо

Антивирусное ПО необходимо, но не достаточно

FortiClient как EDR?

Функционал	FortiClient	FortiEDR
Защитные механизмы	+	+
Безопасный удаленный доступ	+	-
Проведение расследований	-	+
Проактивный поиск угроз	-	+
Реагирование на инциденты	-	+

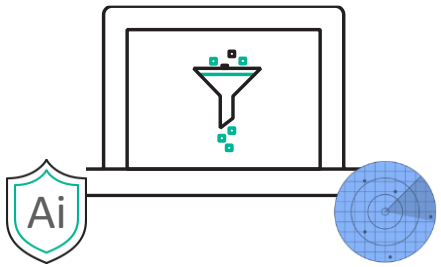
Автоматизация EDR

FortiEDR vs. неавтоматизированный EDR

Схема работы FortiEDR

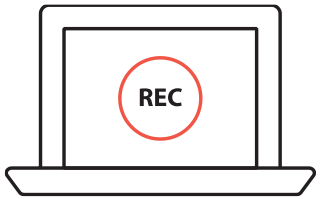
Защита: pre-infection | **Защита: post-infection** | **Реагирование**

Префильтрация | Запись | Сбор данных | Центральный компонент

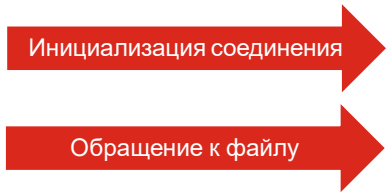


Шаг 1:
Коллектор блокирует известные угрозы

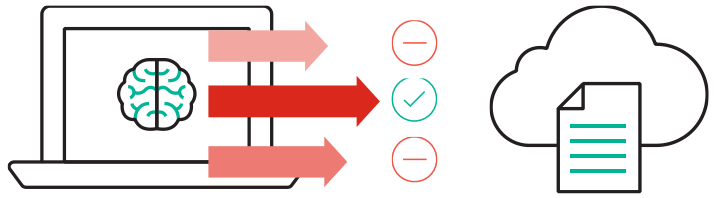
Шаг 2:
Коллектор реагирует на угрозы в соответствии с заранее заданными политиками



Шаг 3:
Коллектор собирает метаданные ОС



Шаг 4:
Коллектор передает снэпшот запроса и метаданные ОС центральному компоненту



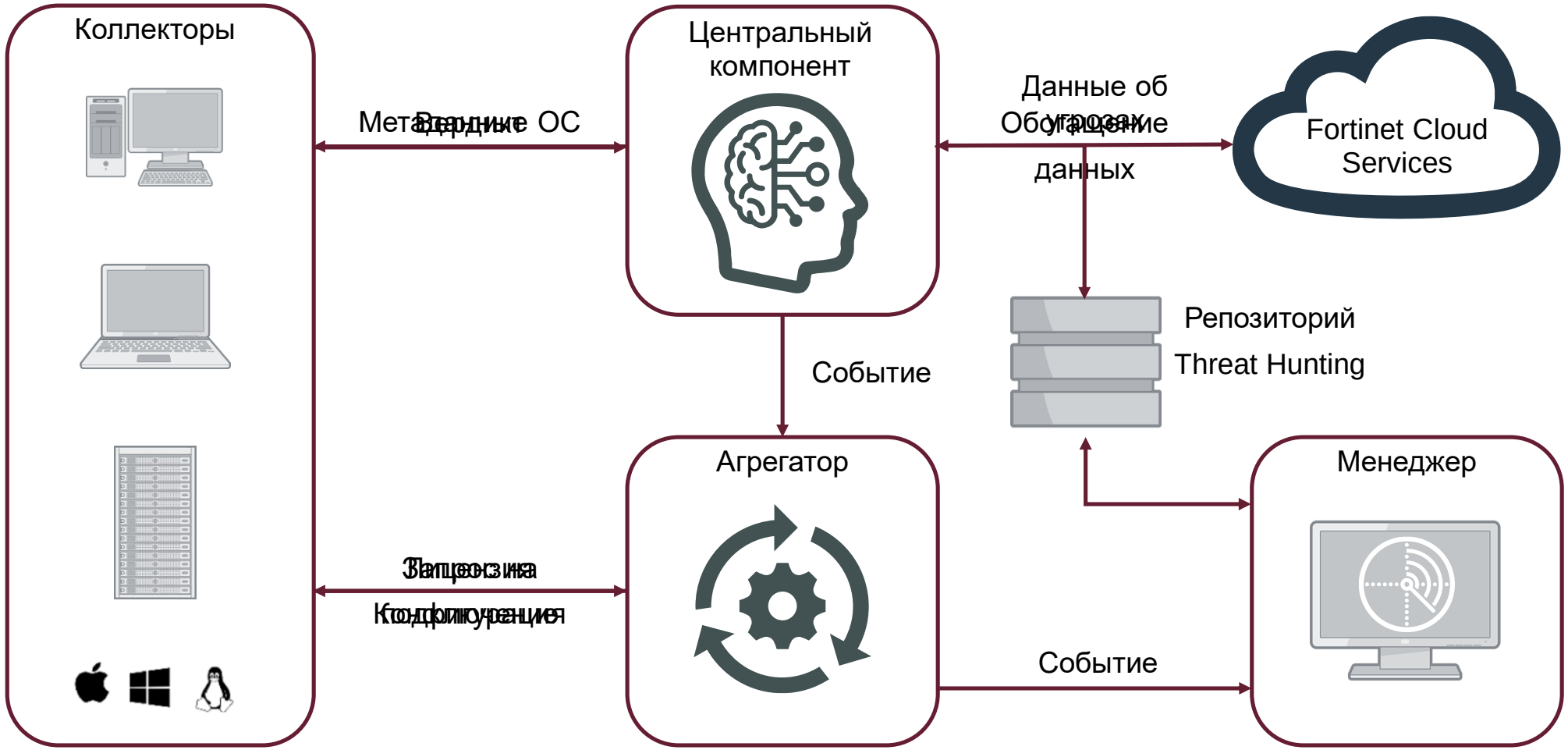
Шаг 5:
Центральный компонент анализирует данные, полученные от коллектора

Шаг 6:
Центральный компонент запускает плейбук для реагирования на обнаруженную нелигитмную активность

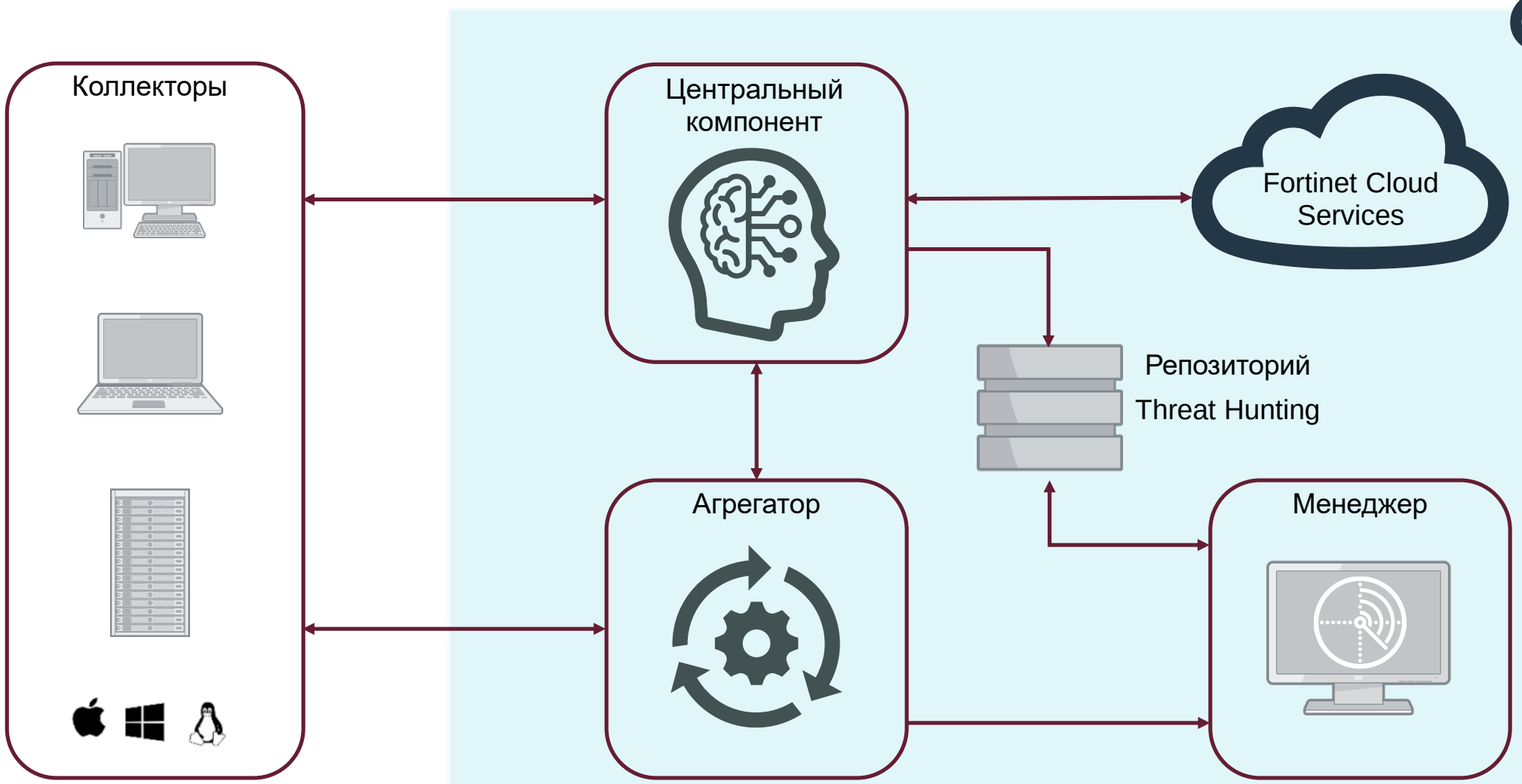
FortiEDR

Архитектура

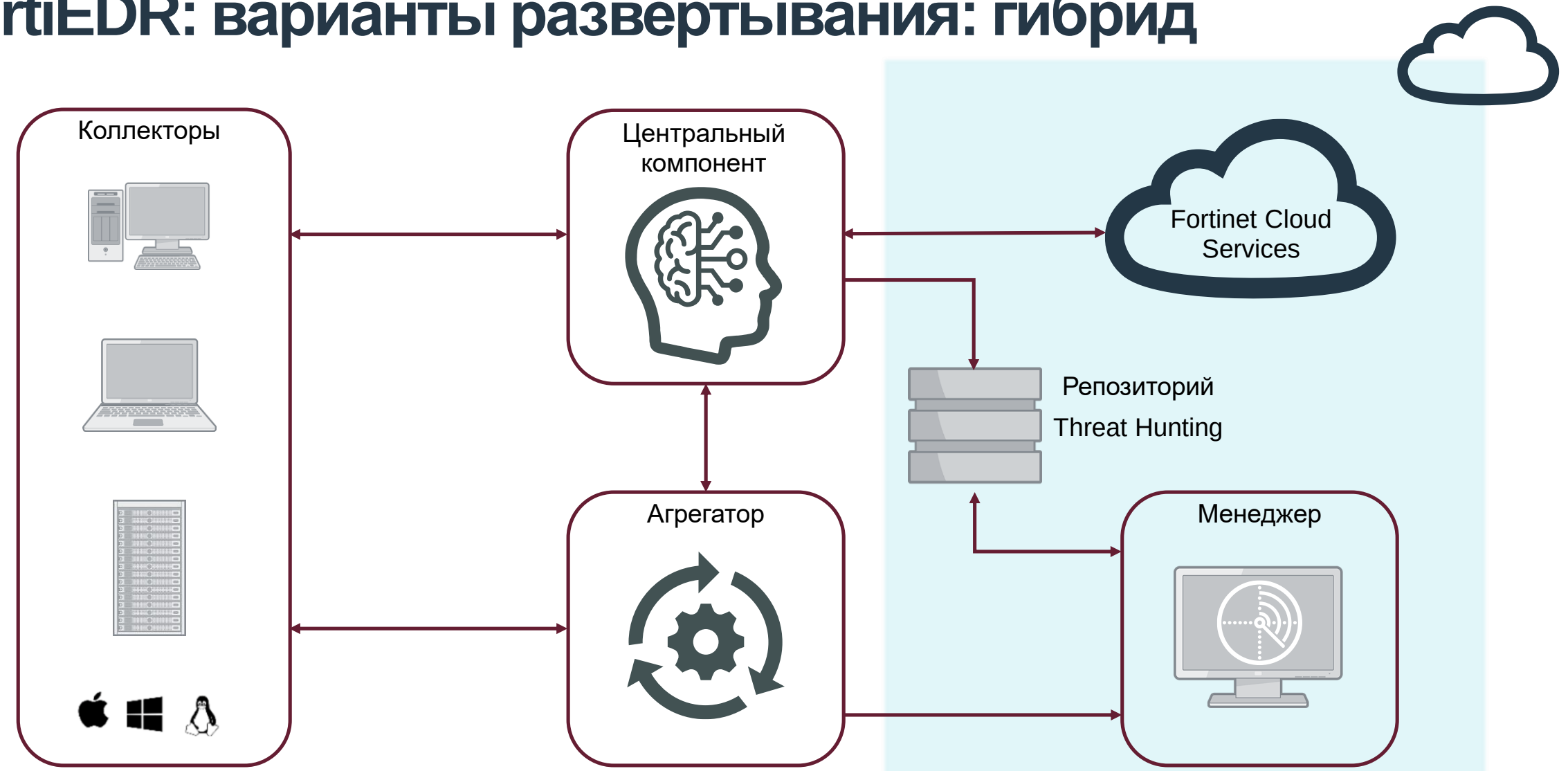
FortiEDR: компоненты



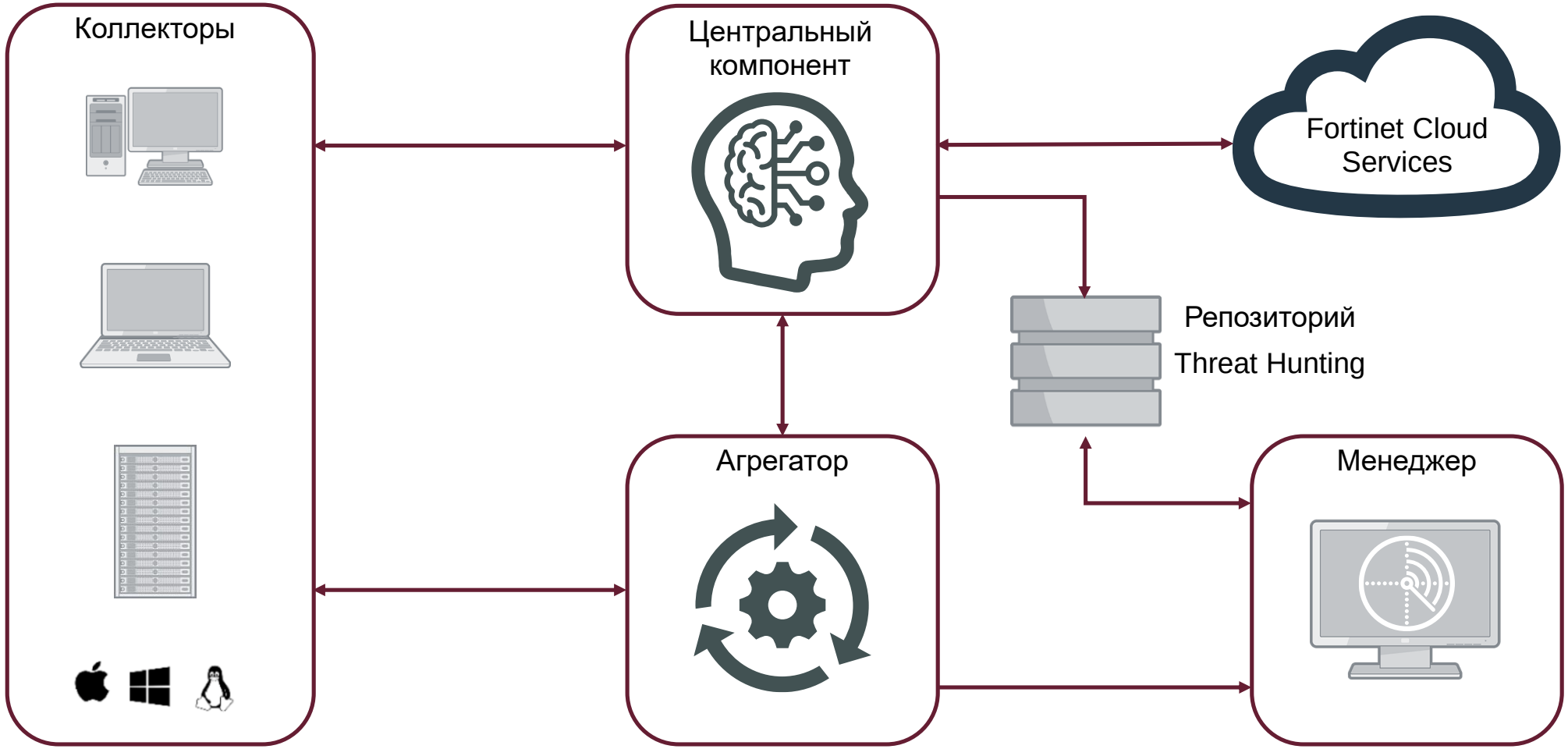
FortiEDR: варианты развертывания: облако



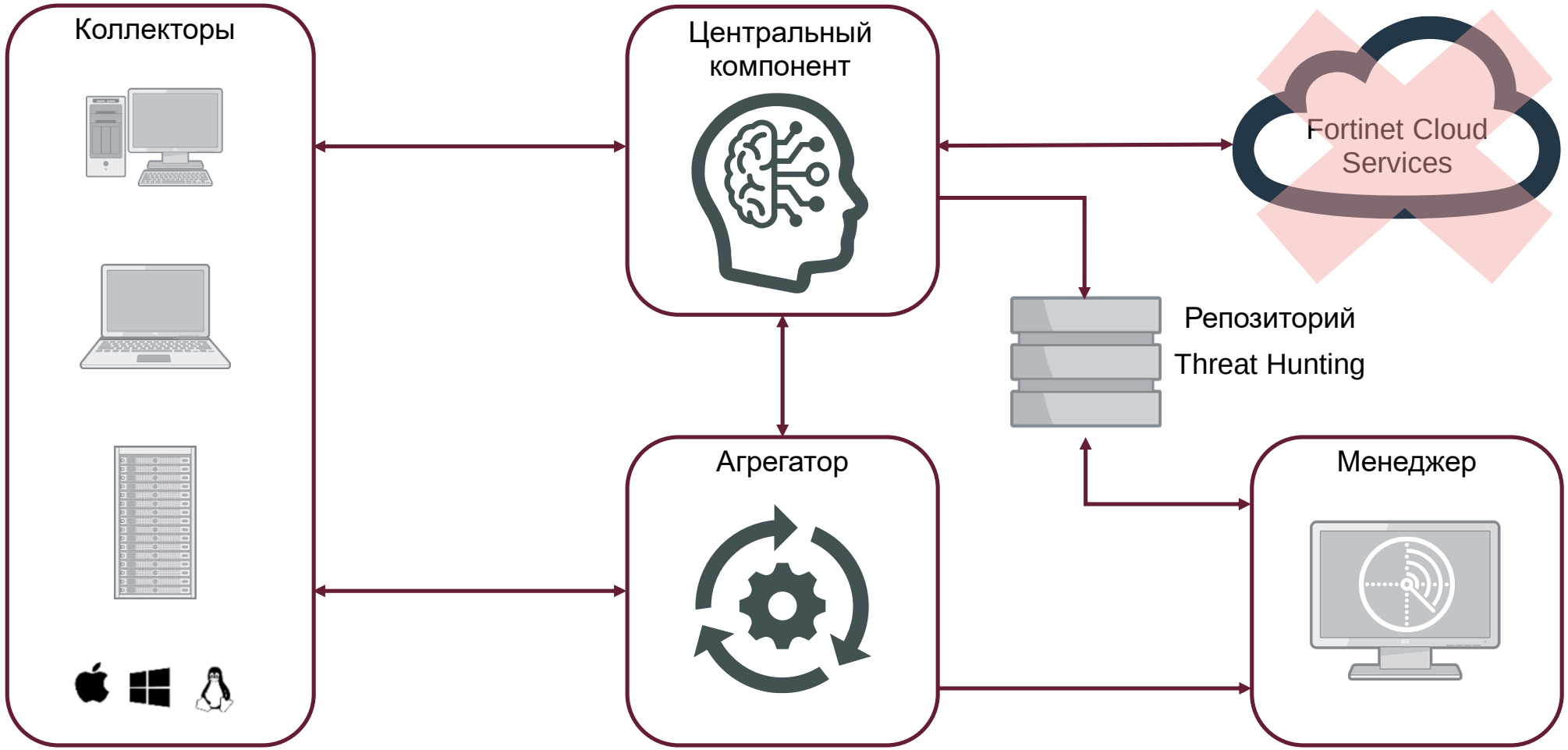
FortiEDR: варианты развертывания: гибрид



FortiEDR: варианты развертывания: локальный



FortiEDR: варианты развертывания: offline



FortiEDR

Системные требования

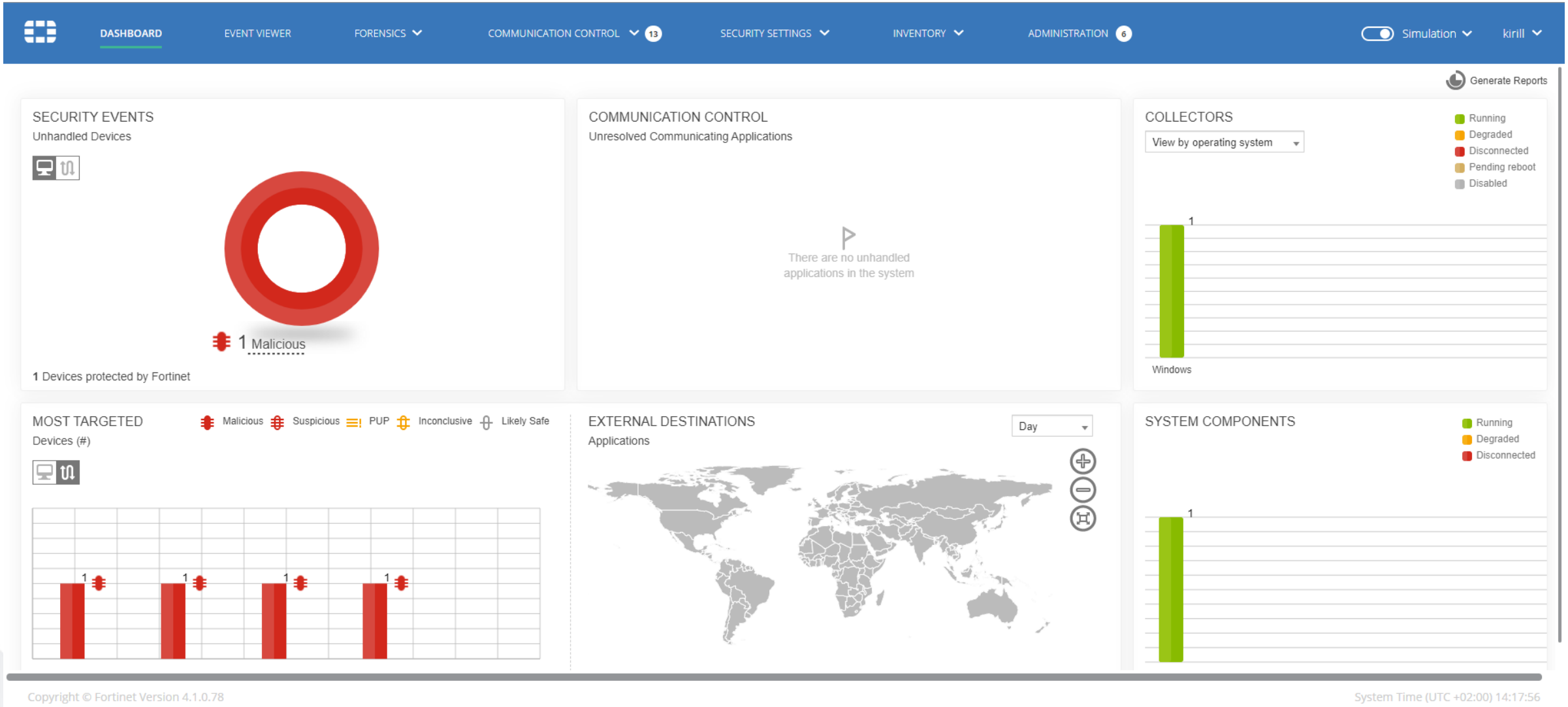
FortiEDR: минимальные системные требования

Компонент	Поддерживаемая платформа	Требования
Коллектор	Windows, MacOS, Linux, VDI	< 1% cpu; 120MB memory; 20MB Disk usage
Центральный компонент (Core)	VM/Bare metal	2 CPUs; 8GB RAM; 80GB Disk size
Агрегатор		2 CPUs; 16GB RAM; 40GB Disk size
Менеджер		2 CPUs; 16GB RAM; 80GB Disk size
Репозиторий Threat Hunting		# CPUs (Cores) eq. #of Cores 8GB 250 GB Disk size and up

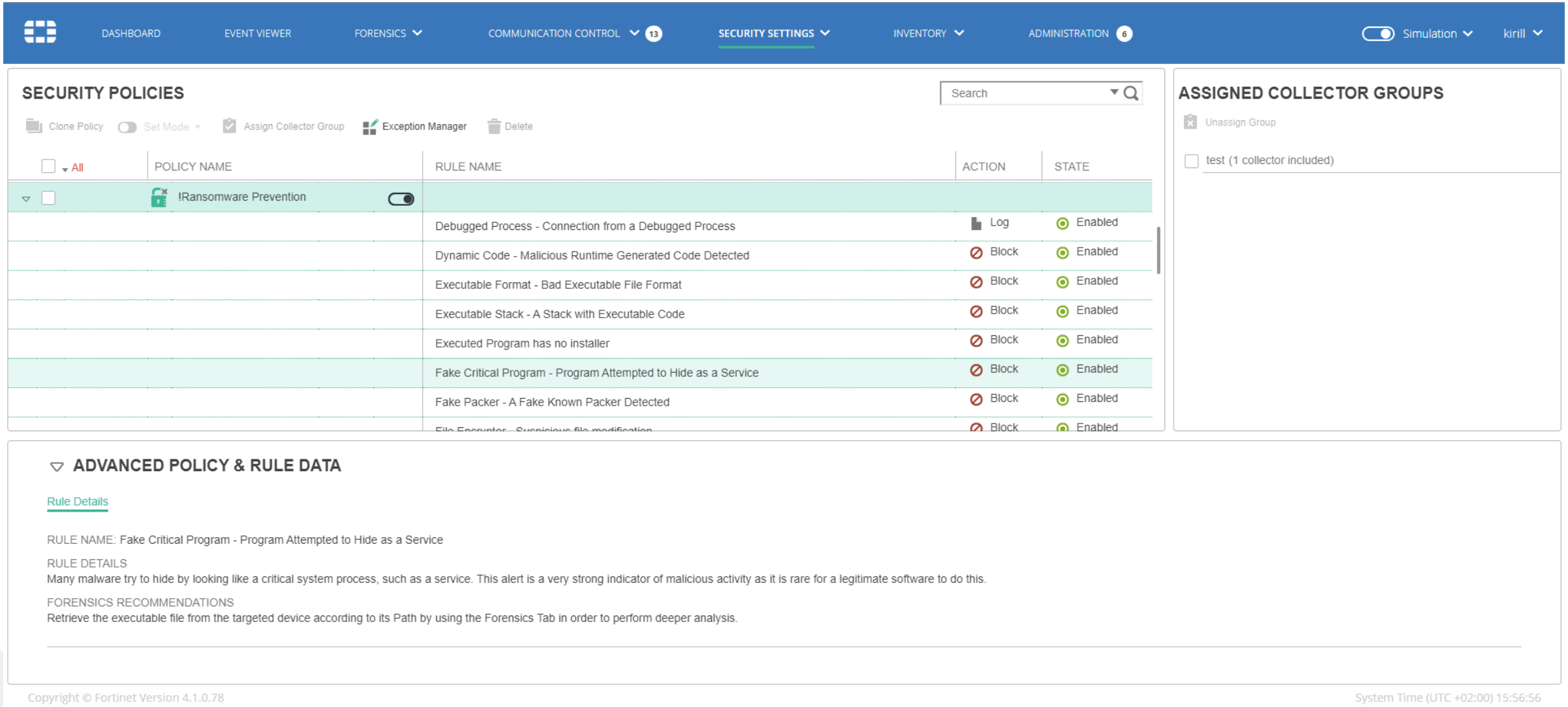
FortiEDR

Интерфейс

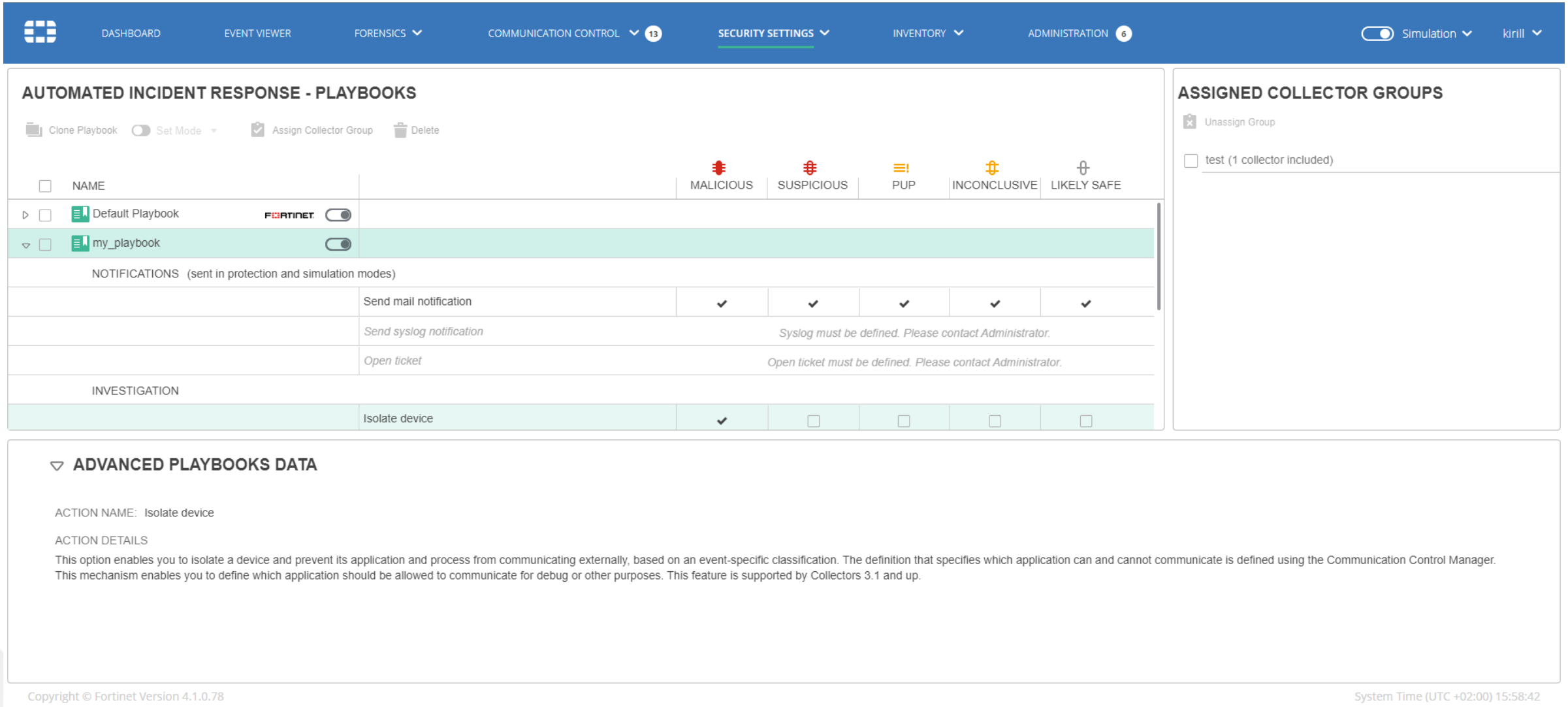
FortiEDR: главный экран



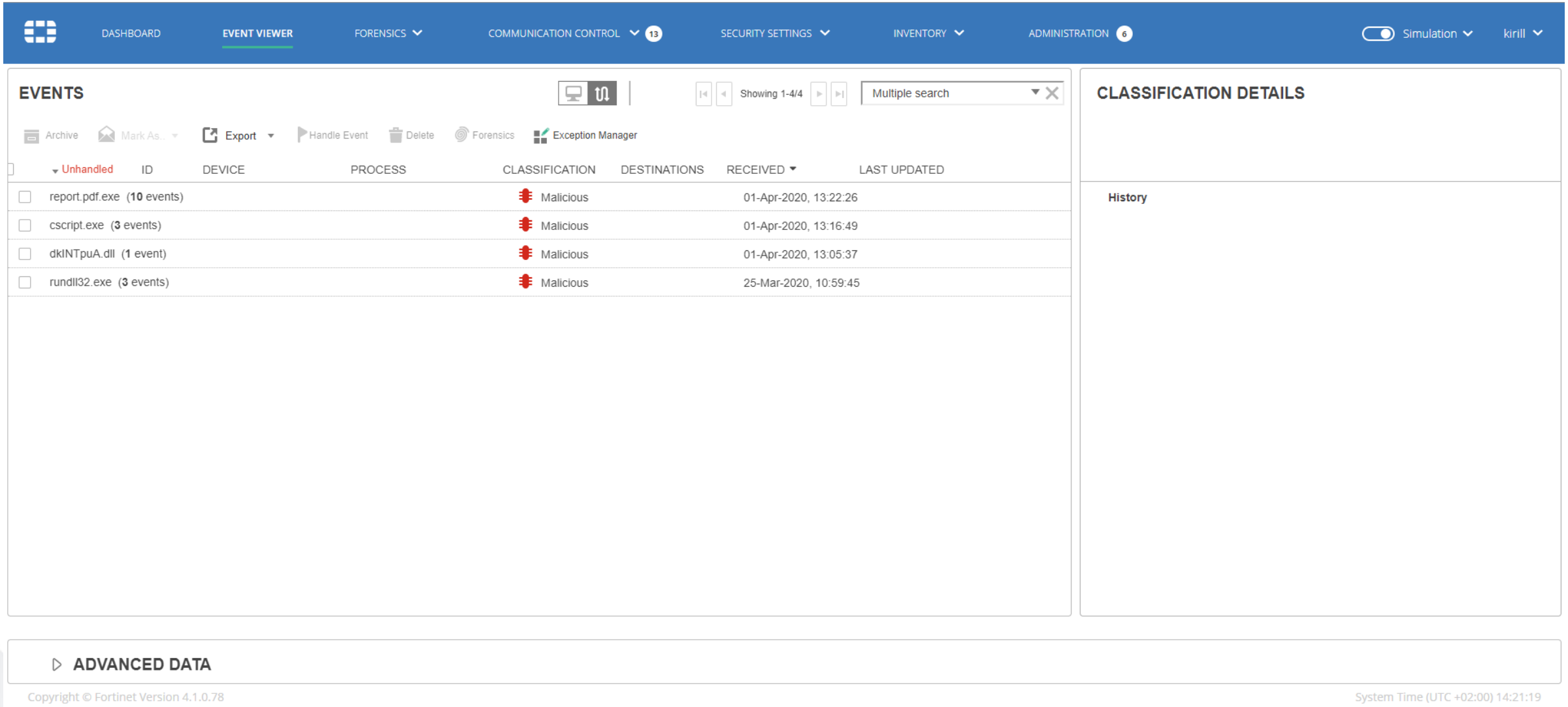
FortiEDR: политики безопасности



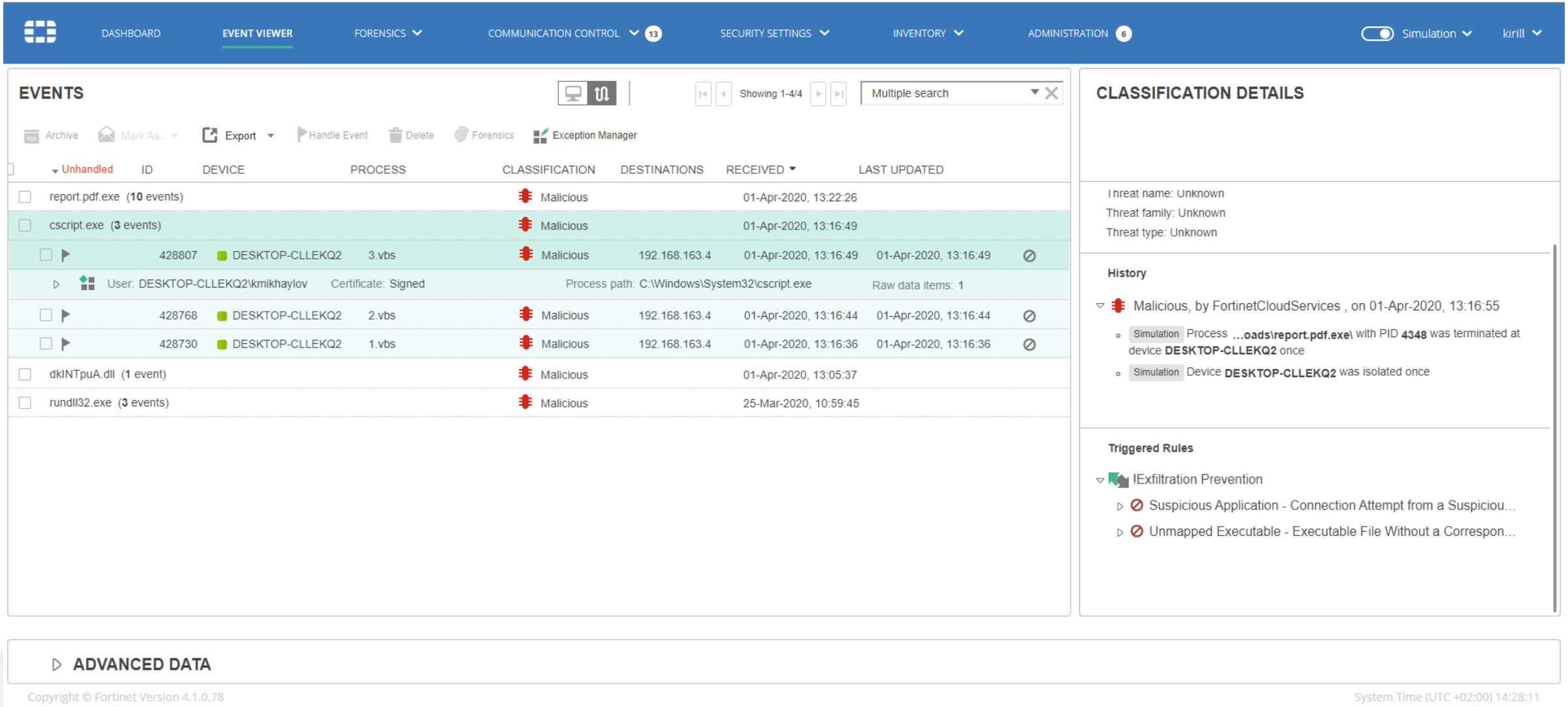
FortiEDR: автоматизация



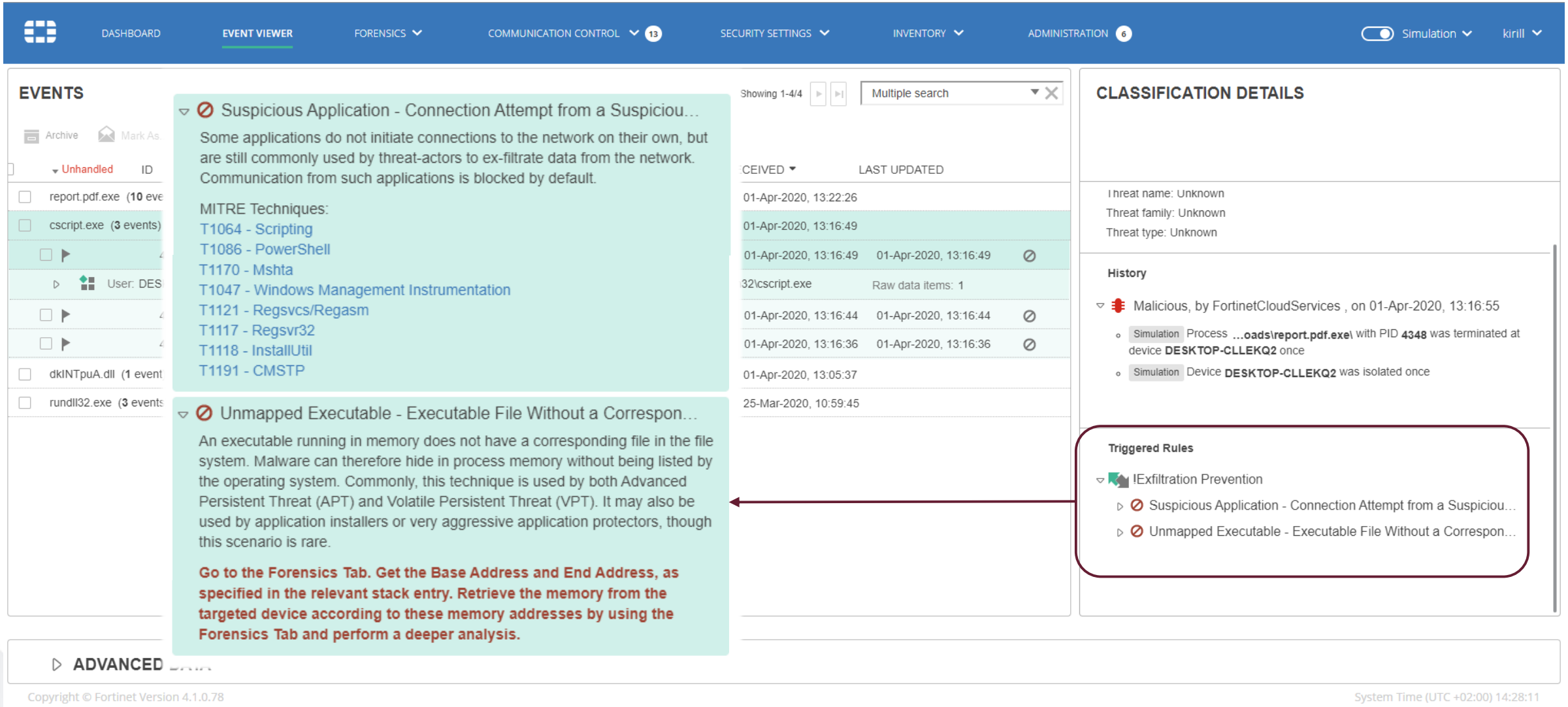
FortiEDR: события



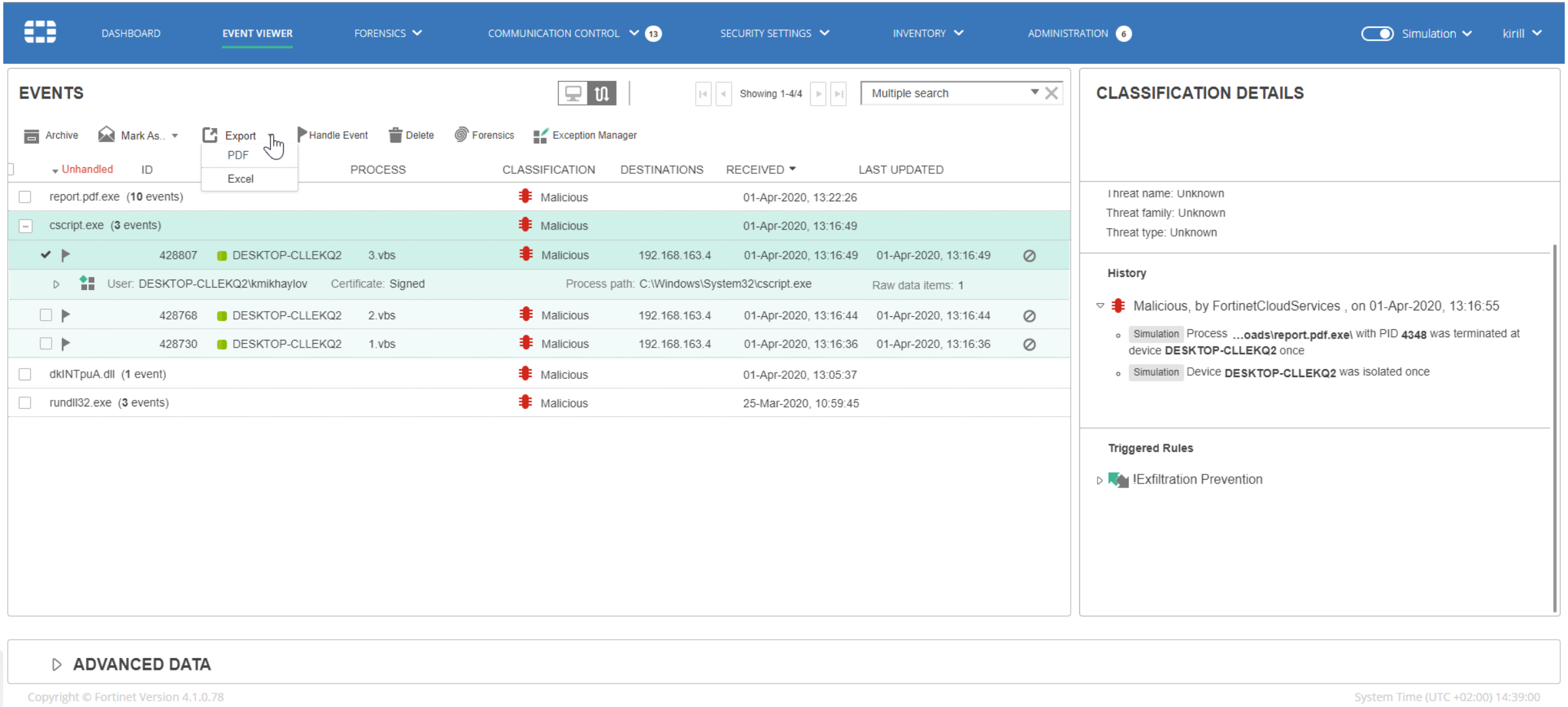
FortiEDR: события



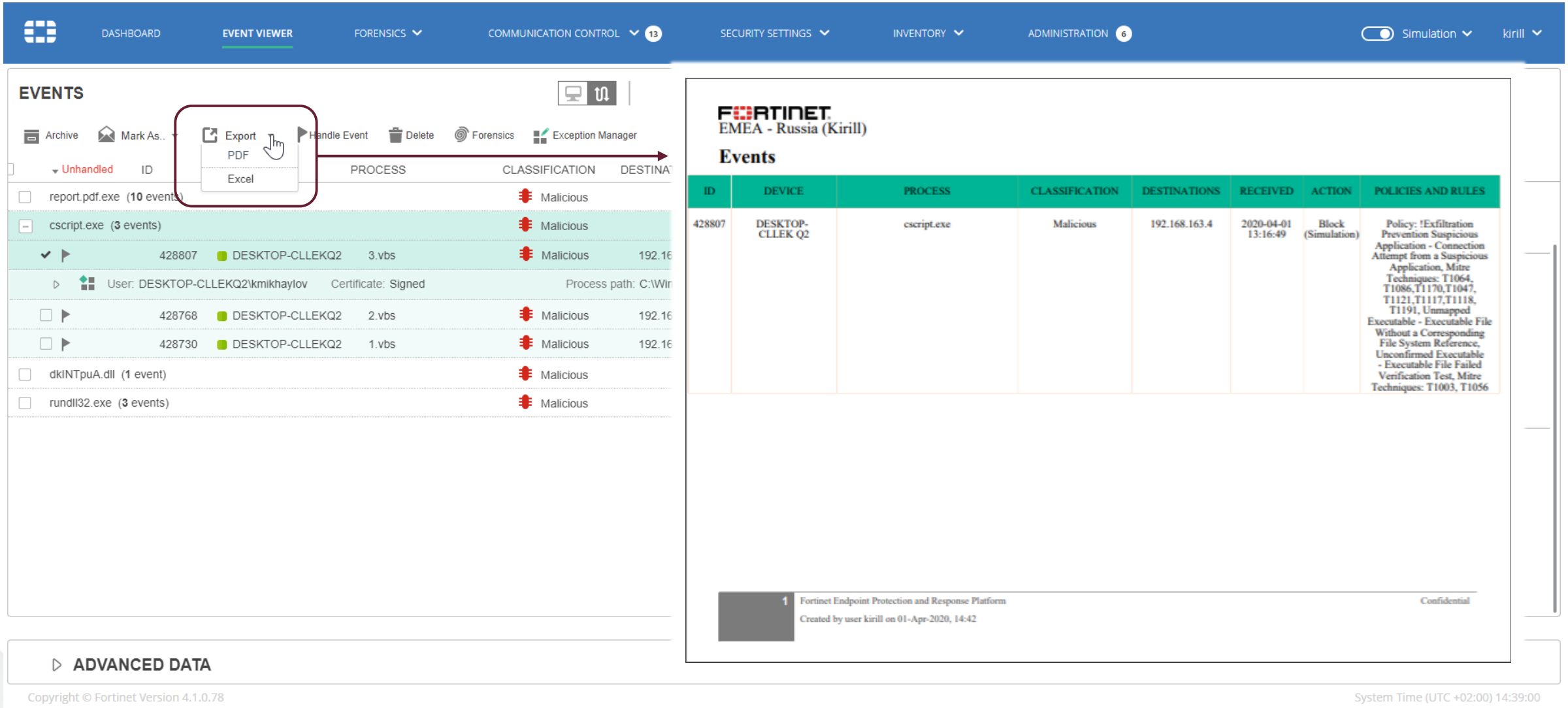
FortiEDR: события



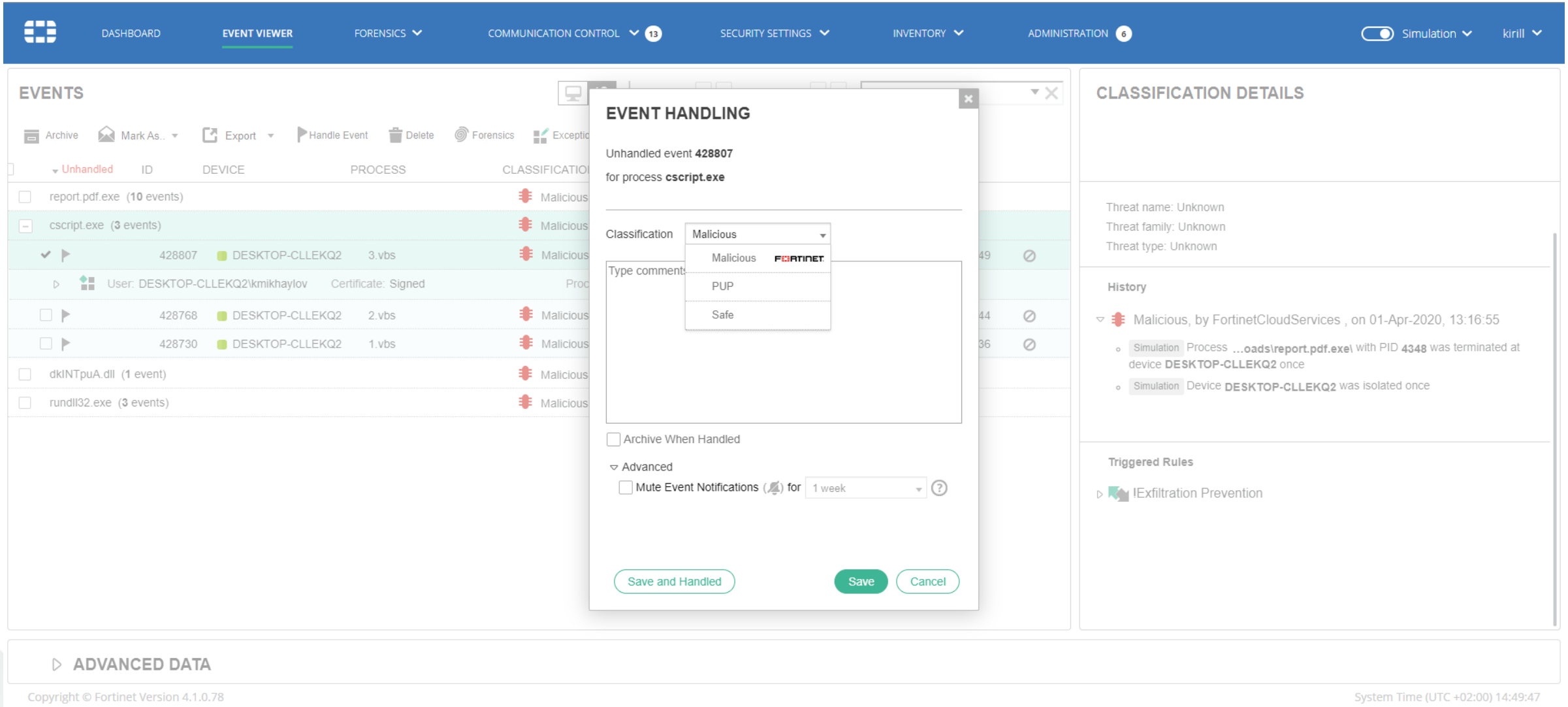
FortiEDR: события



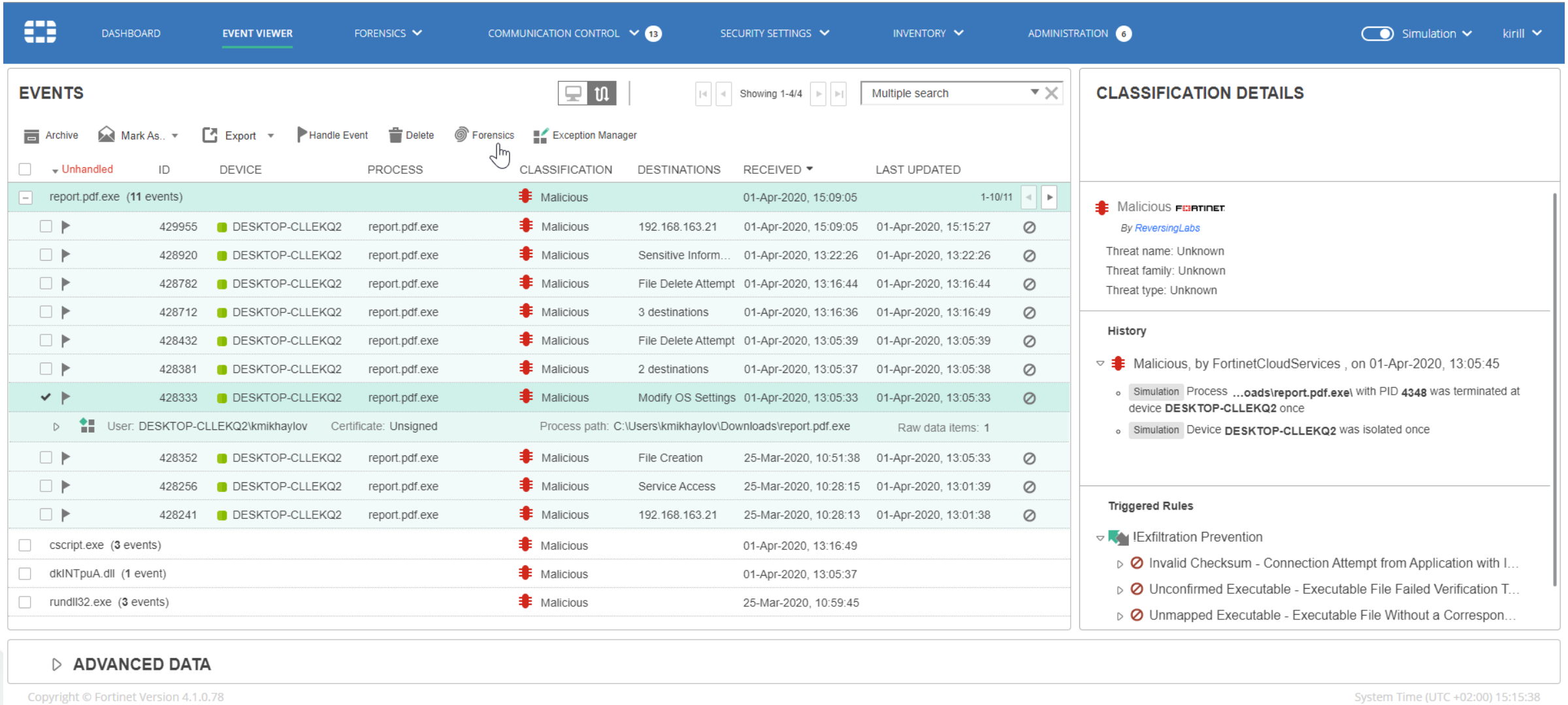
FortiEDR: события



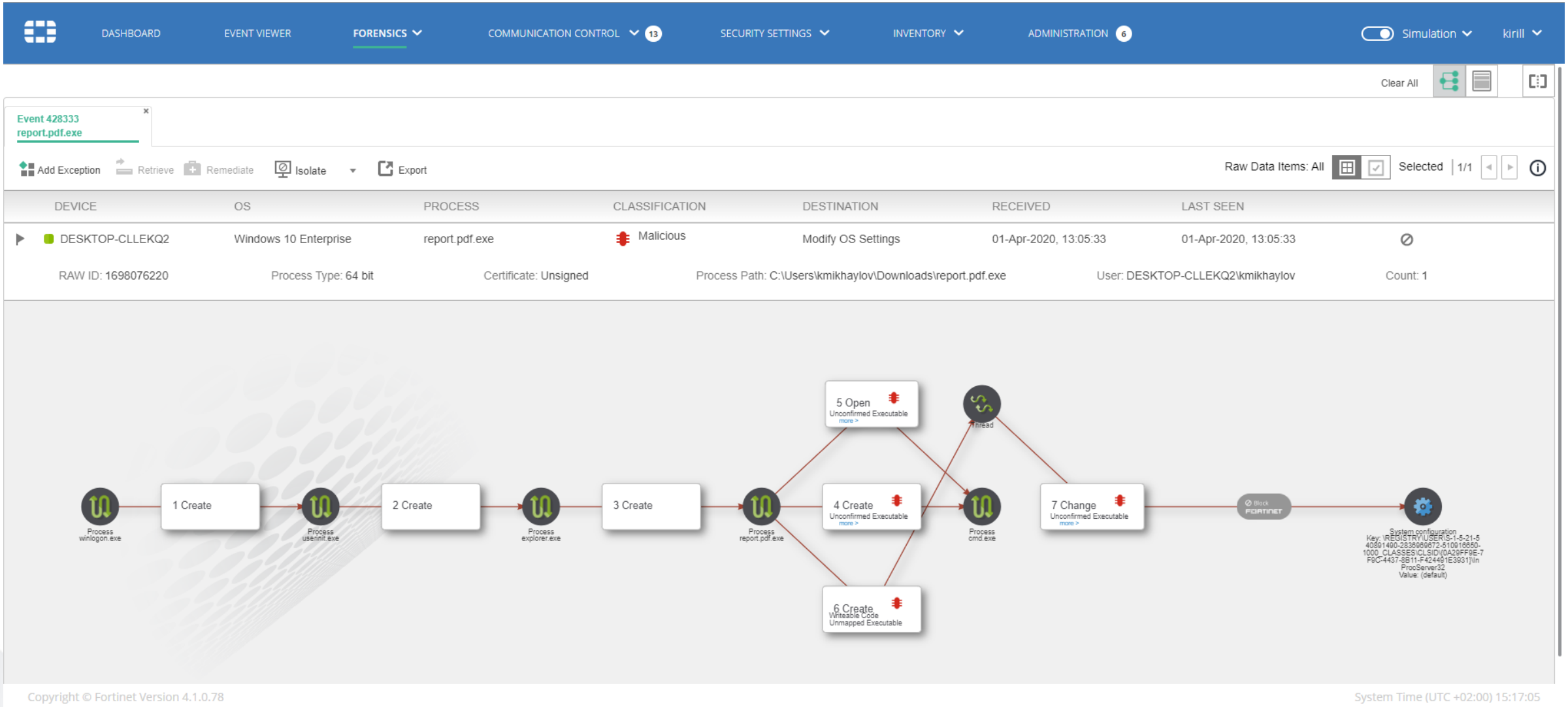
FortiEDR: события



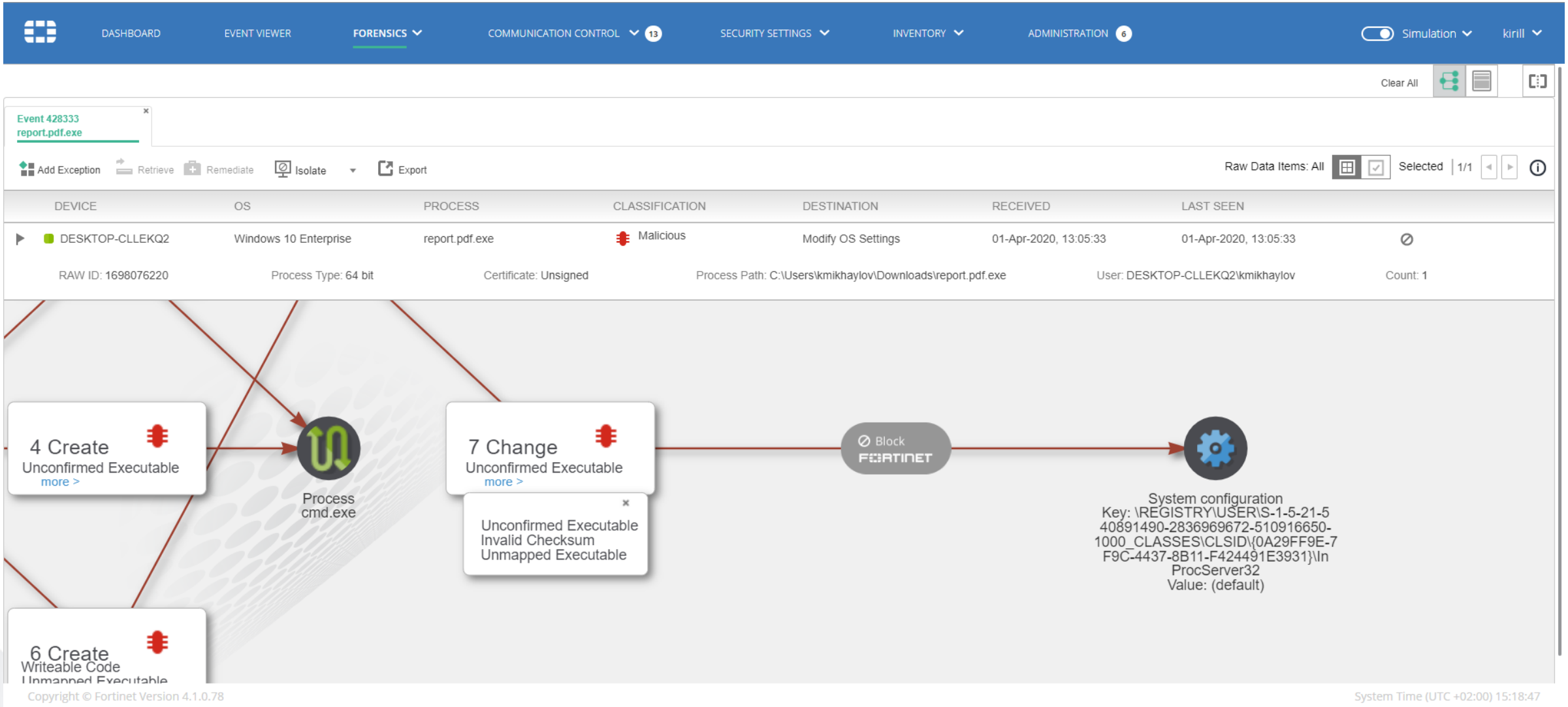
FortiEDR: события



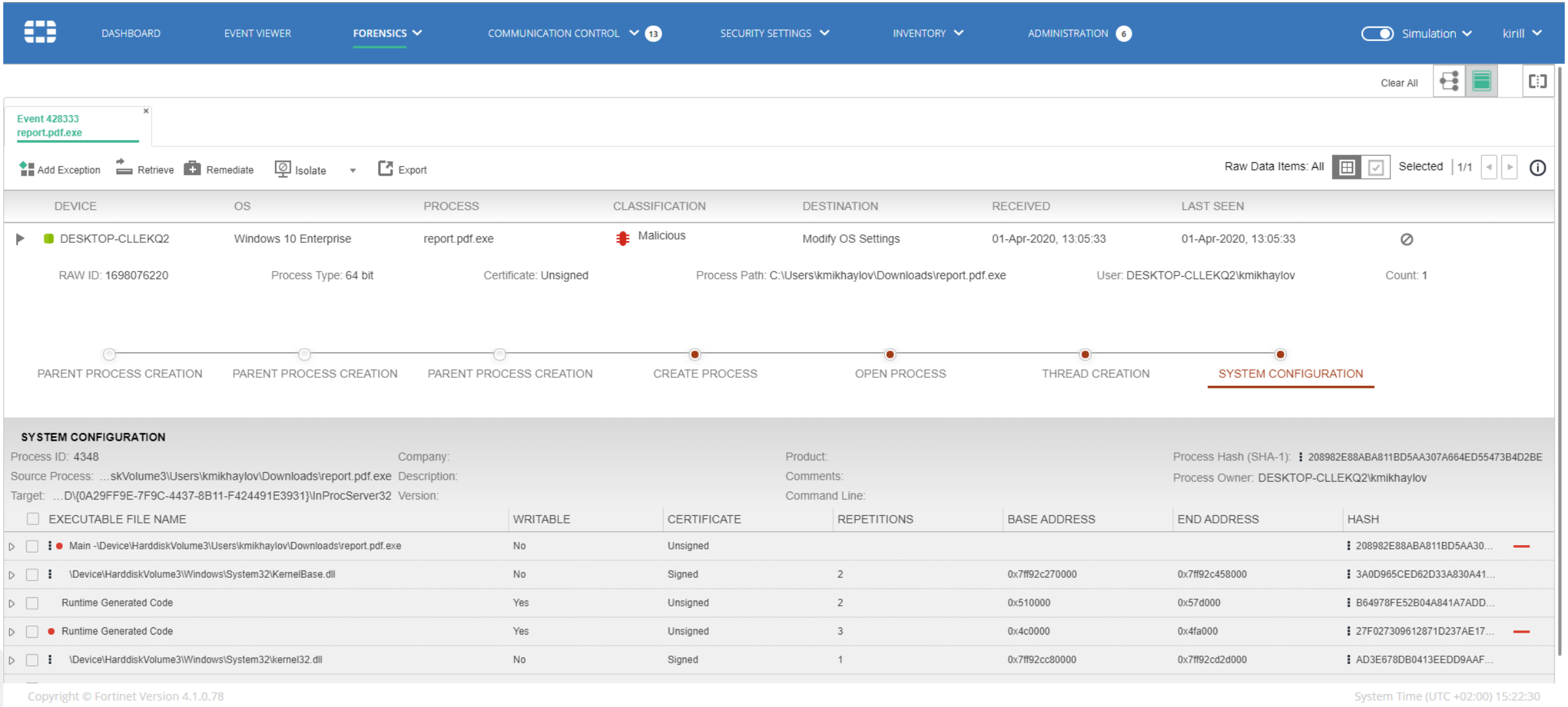
FortiEDR: события



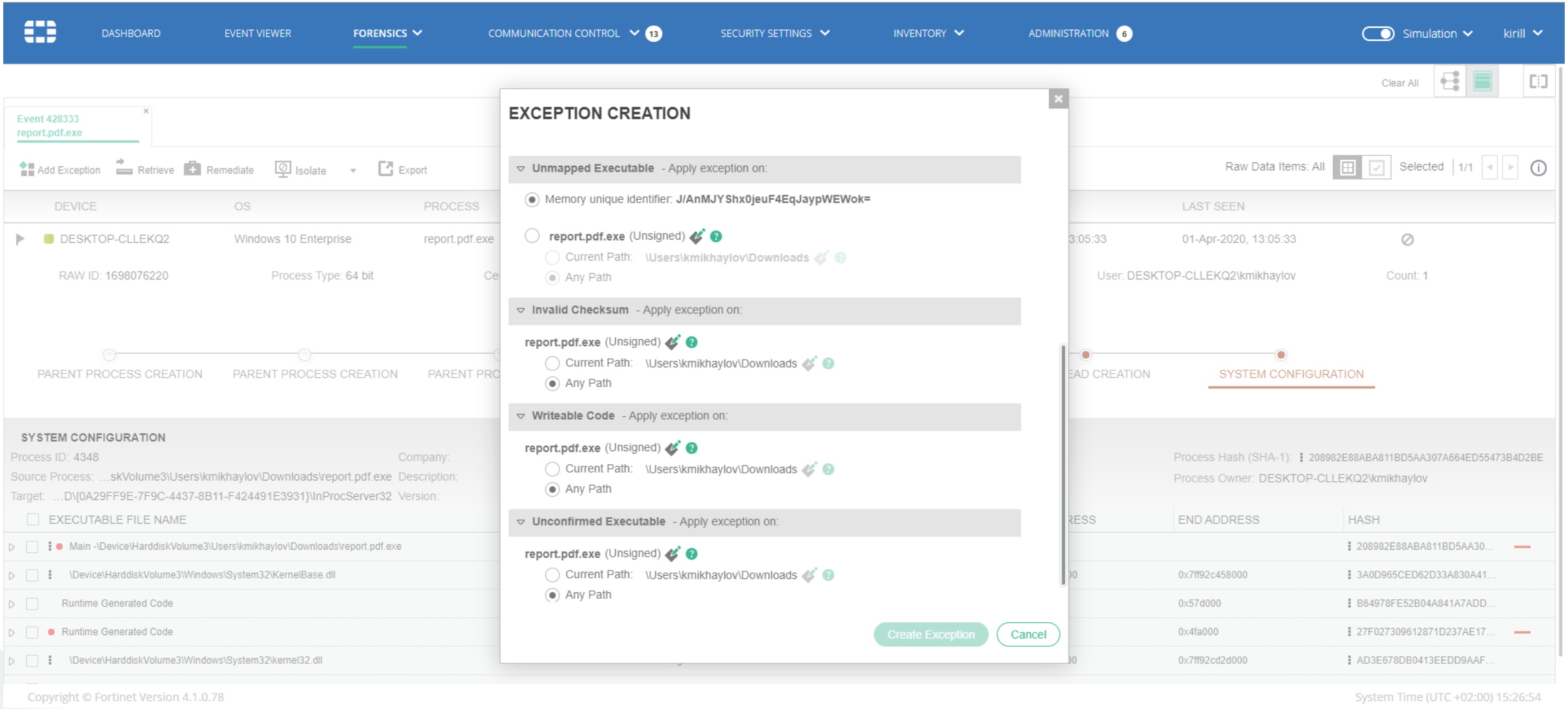
FortiEDR: события



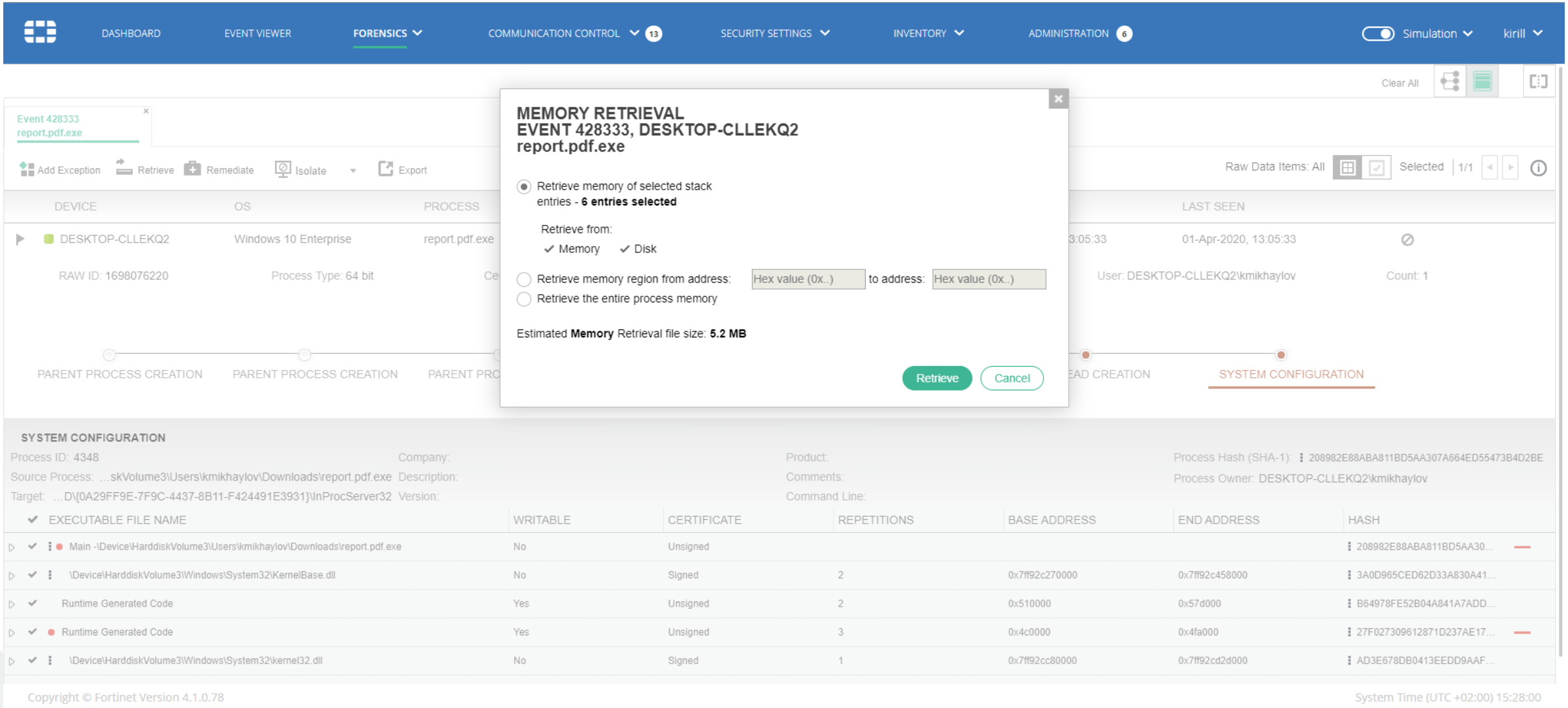
FortiEDR: события



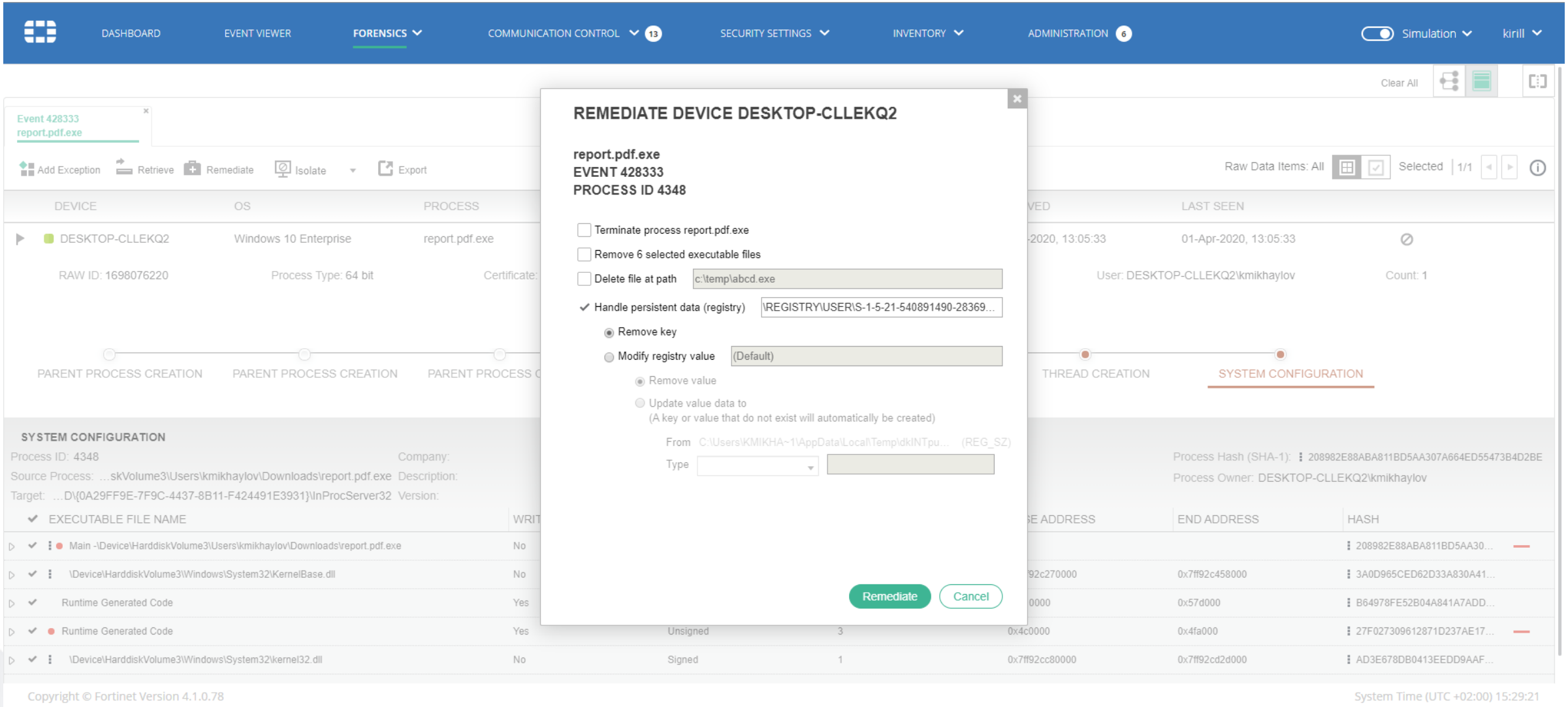
FortiEDR: события



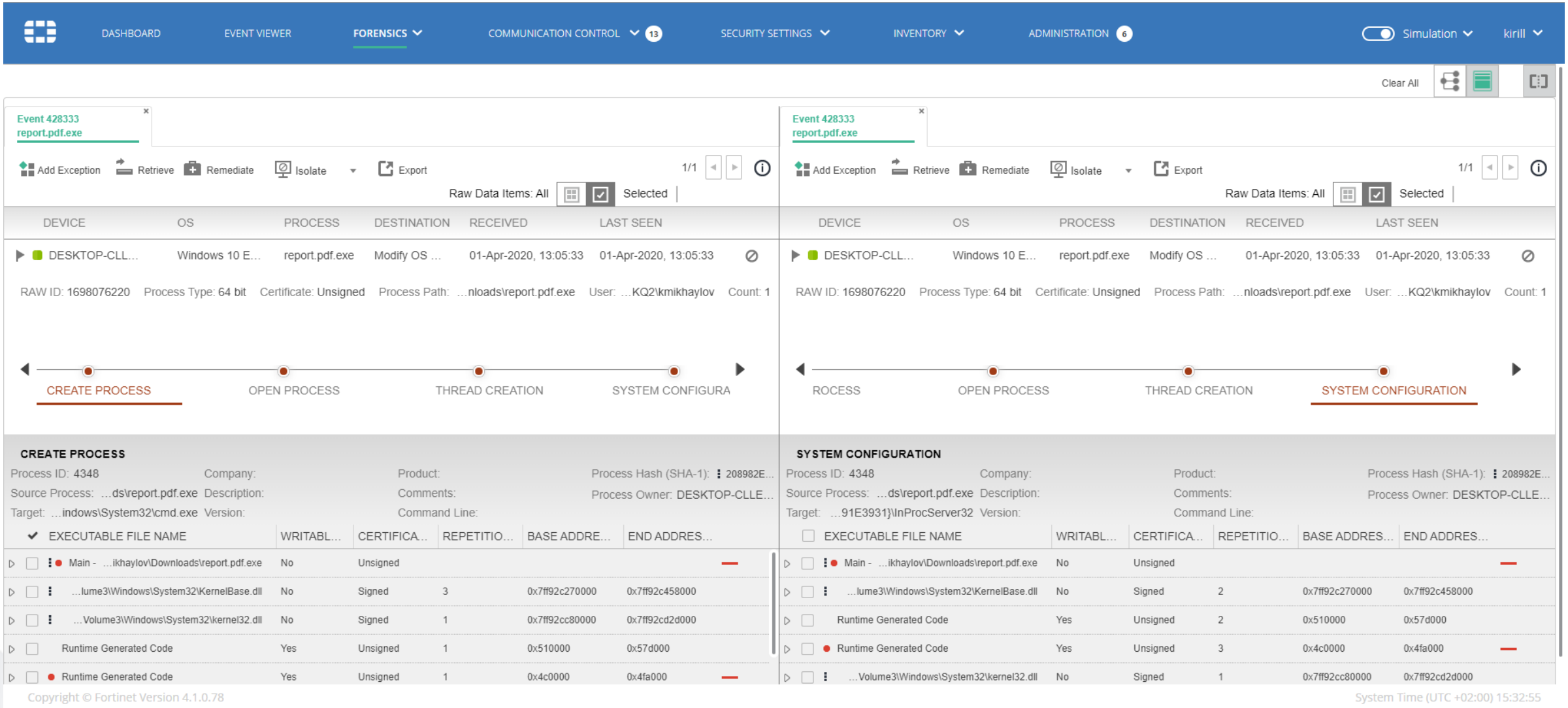
FortiEDR: события



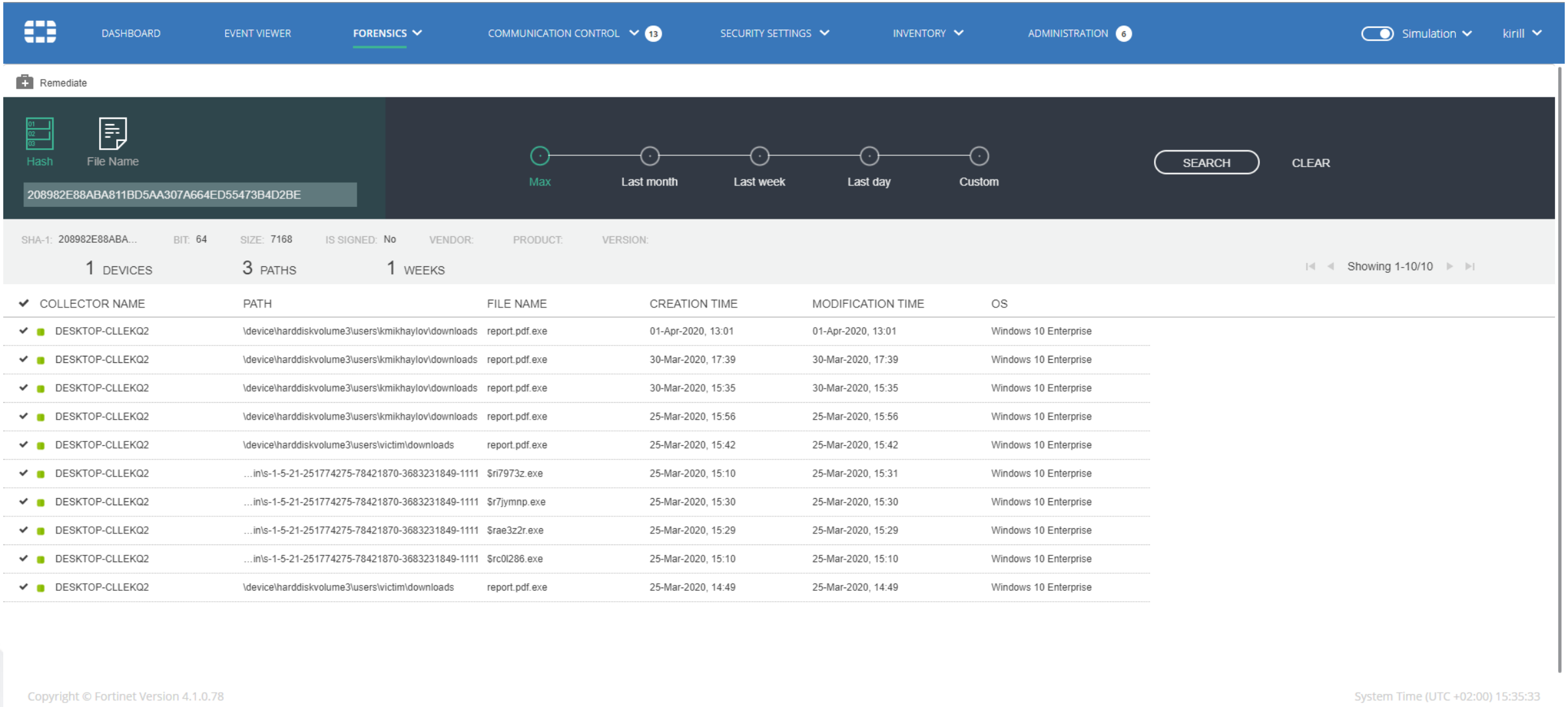
FortiEDR: события



FortiEDR: события

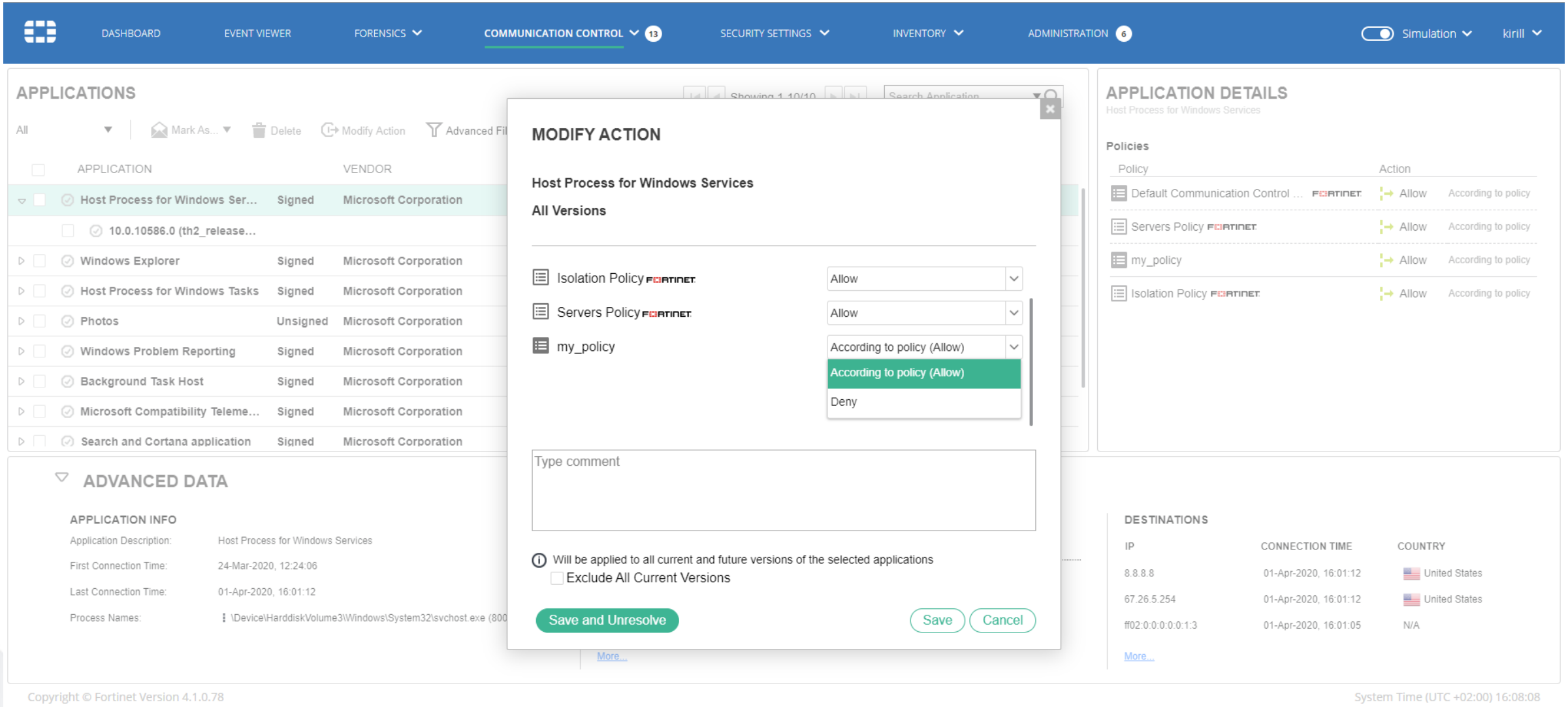


FortiEDR: события

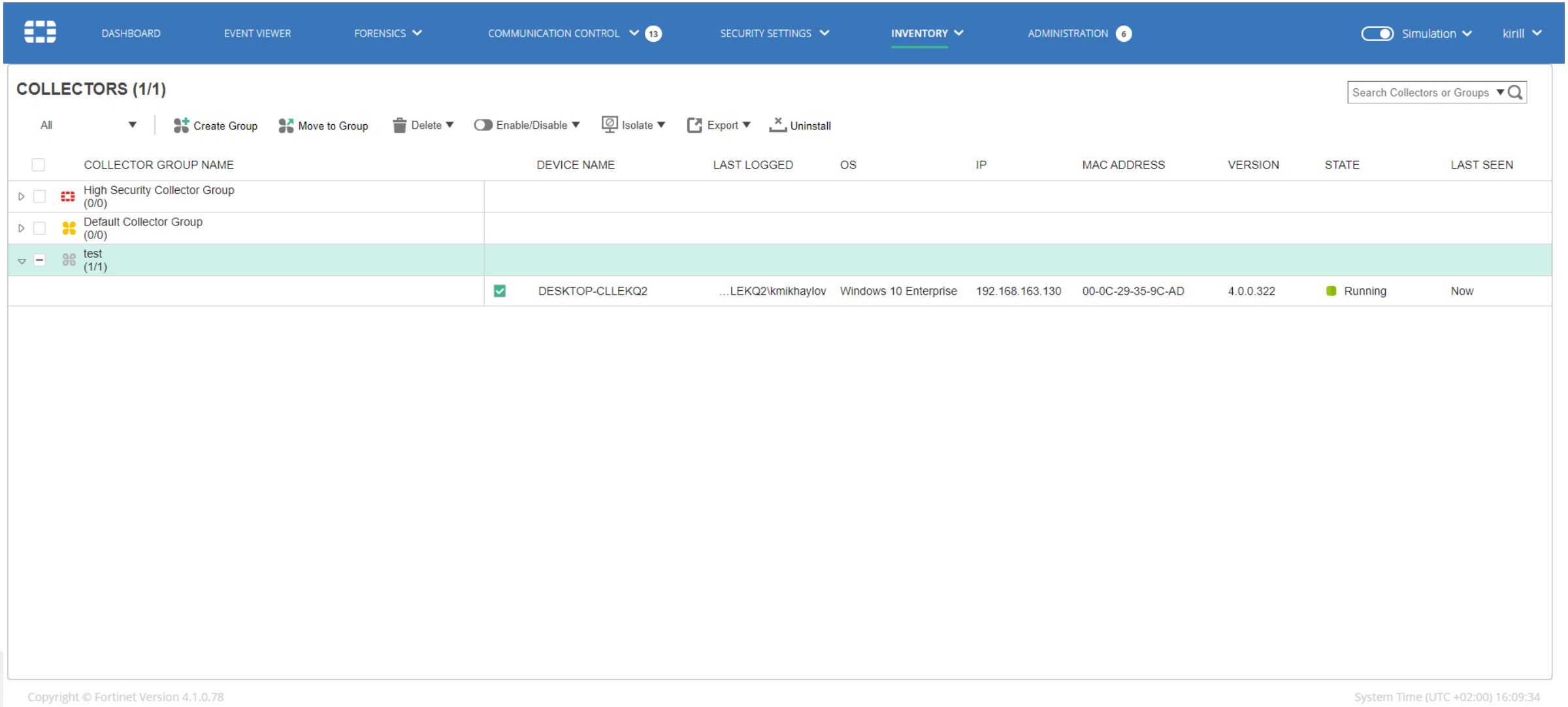


COLLECTOR NAME	PATH	FILE NAME	CREATION TIME	MODIFICATION TIME	OS
DESKTOP-CLLEKQ2	\device\harddiskvolume3\users\kmikhaylov\downloads	report.pdf.exe	01-Apr-2020, 13:01	01-Apr-2020, 13:01	Windows 10 Enterprise
DESKTOP-CLLEKQ2	\device\harddiskvolume3\users\kmikhaylov\downloads	report.pdf.exe	30-Mar-2020, 17:39	30-Mar-2020, 17:39	Windows 10 Enterprise
DESKTOP-CLLEKQ2	\device\harddiskvolume3\users\kmikhaylov\downloads	report.pdf.exe	30-Mar-2020, 15:35	30-Mar-2020, 15:35	Windows 10 Enterprise
DESKTOP-CLLEKQ2	\device\harddiskvolume3\users\kmikhaylov\downloads	report.pdf.exe	25-Mar-2020, 15:56	25-Mar-2020, 15:56	Windows 10 Enterprise
DESKTOP-CLLEKQ2	\device\harddiskvolume3\users\victim\downloads	report.pdf.exe	25-Mar-2020, 15:42	25-Mar-2020, 15:42	Windows 10 Enterprise
DESKTOP-CLLEKQ2	...in\s-1-5-21-251774275-78421870-3683231849-1111	$ri7973z.exe	25-Mar-2020, 15:10	25-Mar-2020, 15:31	Windows 10 Enterprise
DESKTOP-CLLEKQ2	...in\s-1-5-21-251774275-78421870-3683231849-1111	$r7jymnp.exe	25-Mar-2020, 15:30	25-Mar-2020, 15:30	Windows 10 Enterprise
DESKTOP-CLLEKQ2	...in\s-1-5-21-251774275-78421870-3683231849-1111	$rae3z2r.exe	25-Mar-2020, 15:29	25-Mar-2020, 15:29	Windows 10 Enterprise
DESKTOP-CLLEKQ2	...in\s-1-5-21-251774275-78421870-3683231849-1111	$rc0l286.exe	25-Mar-2020, 15:10	25-Mar-2020, 15:10	Windows 10 Enterprise
DESKTOP-CLLEKQ2	\device\harddiskvolume3\users\victim\downloads	report.pdf.exe	25-Mar-2020, 14:49	25-Mar-2020, 14:49	Windows 10 Enterprise

FortiEDR: контроль сетевых соединений



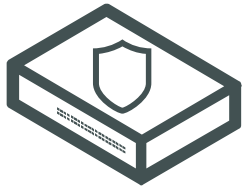
FortiEDR: инвентарь



Лицензирование

Лицензирование

Количество рабочих станций



Количество серверов

Сервисы и подписки

Демонстрация

Вопросы?

Кирилл Михайлов, kmikhaylov@fortinet.com