DIGITAL EDITION

FORTINET®

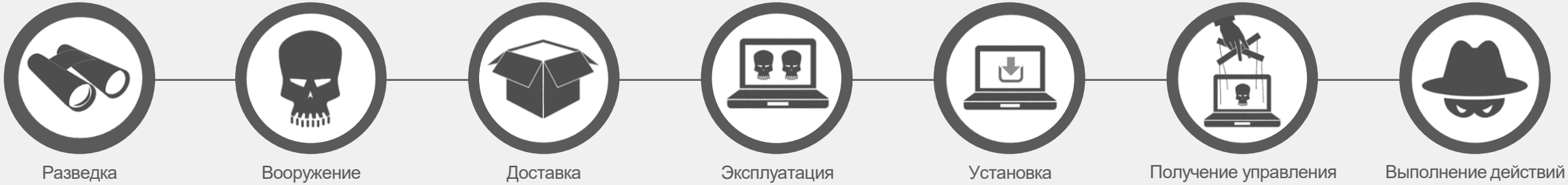
SECURITY DAY

Минимизация времени обнаружения и реагирования на кибератаки

Кирилл Михайлов, системный инженер

6 апреля 2021 | Киев | Минск

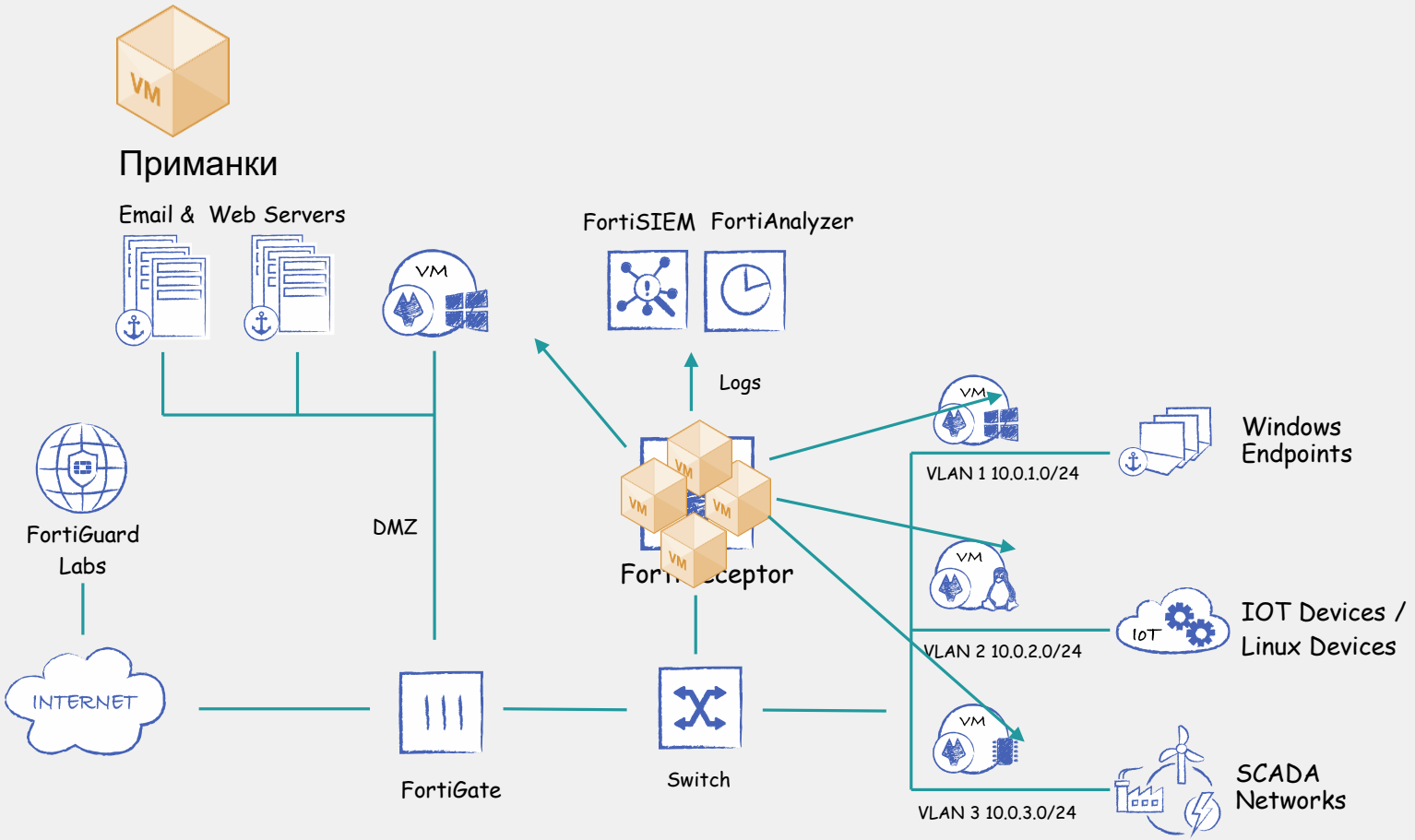
Минимизация издержек



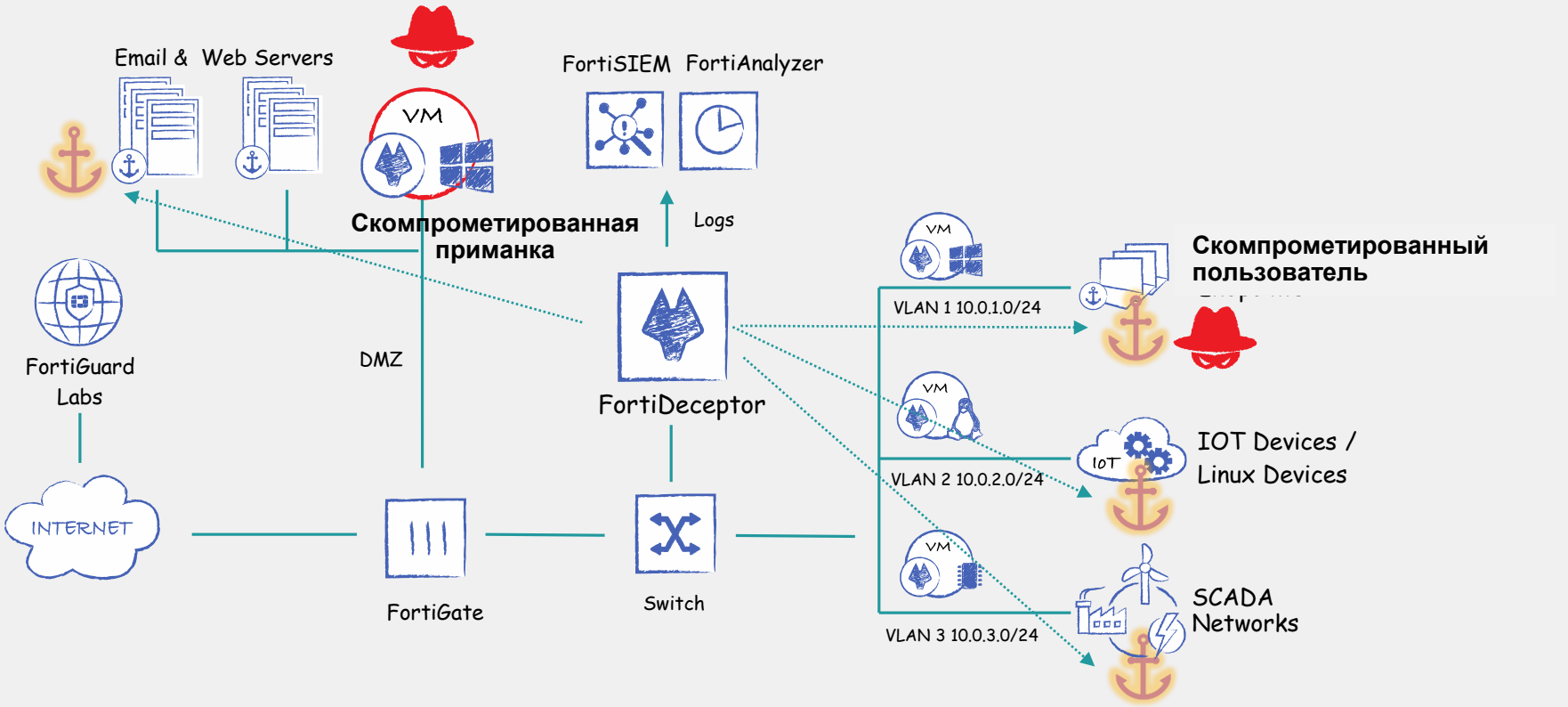
Обнаружение атаки

на стадии разведки

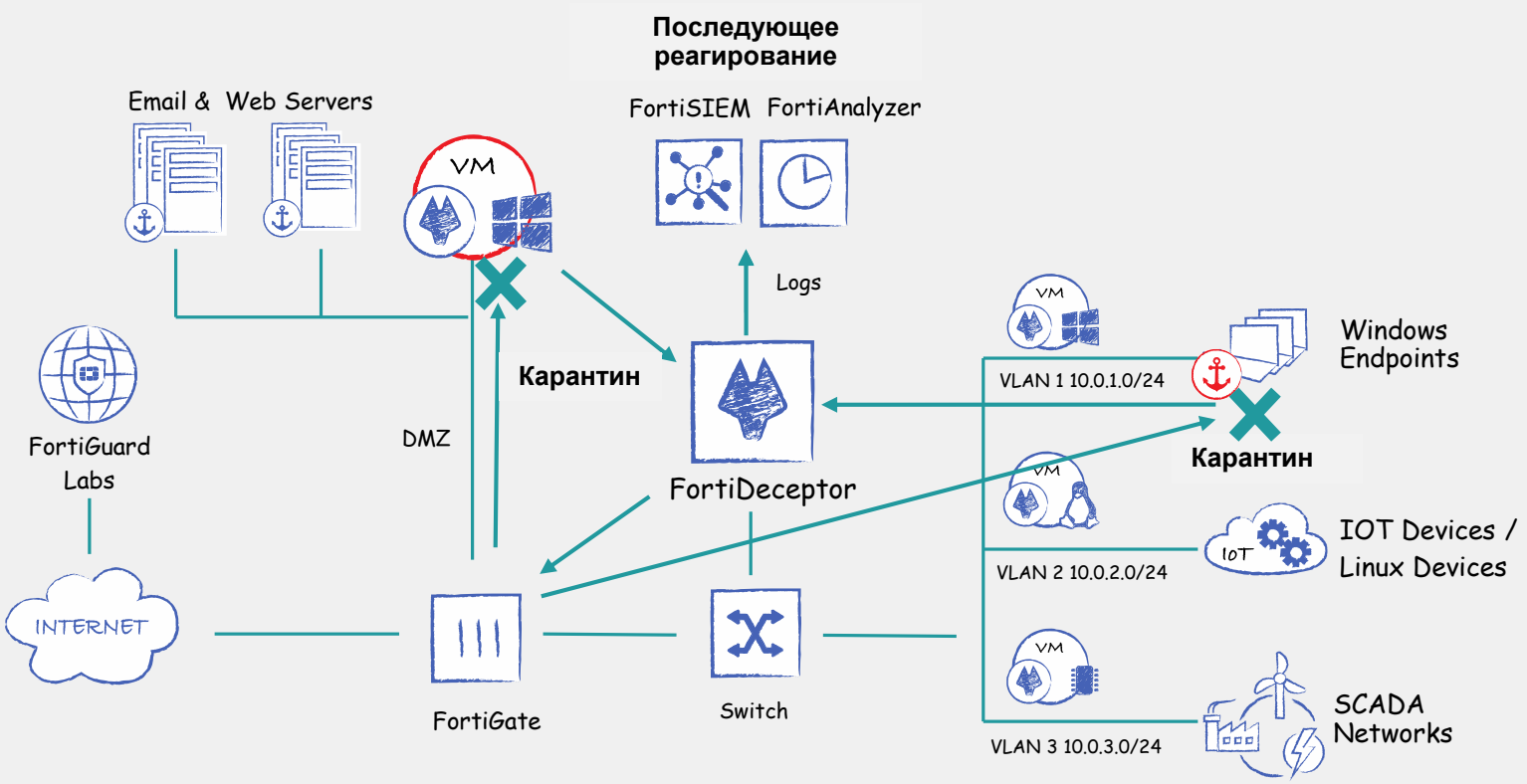
FortiDeceptor: разведка



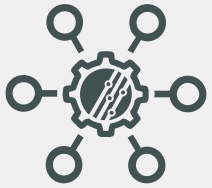
FortiDeceptor: доставка и эксплуатация



FortiDeceptor: выполнение действий



Видимость и контроль конечных узлов



Fortinet Security Fabric

Рабочие станции / серверы

Видимость и контроль

конечных узлов

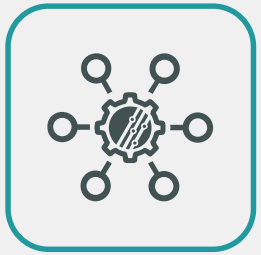
Функционал EPP

FortiClient

Модуль защиты от ВПО

Модуль VPN

Модуль Compliance



Модуль интеграции со сторонними системами

Функционал EDR

FortiEDR

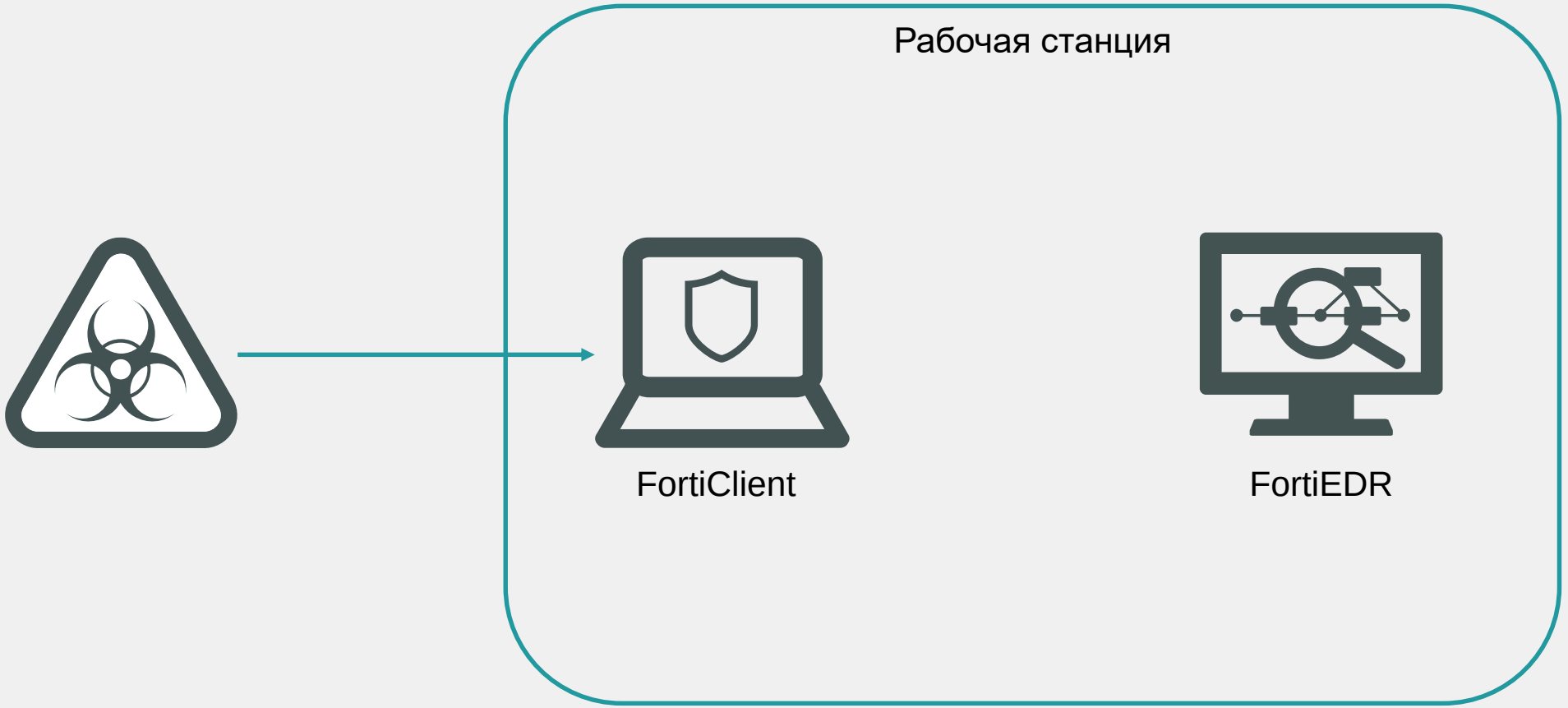
Антивирусный модуль

Модуль анализа активности

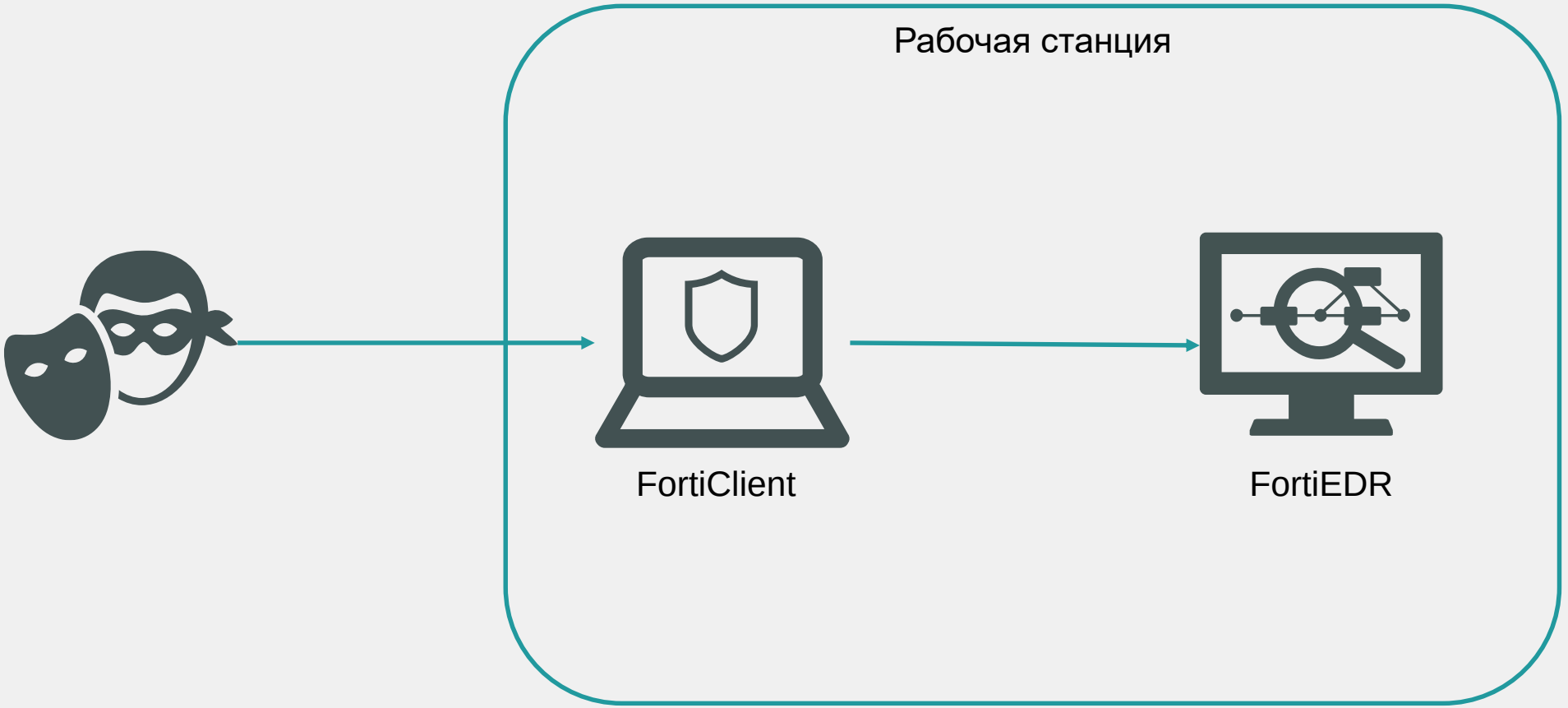
Модуль реагирования и восстановления системы

Модуль анализа и закрытия уязвимостей

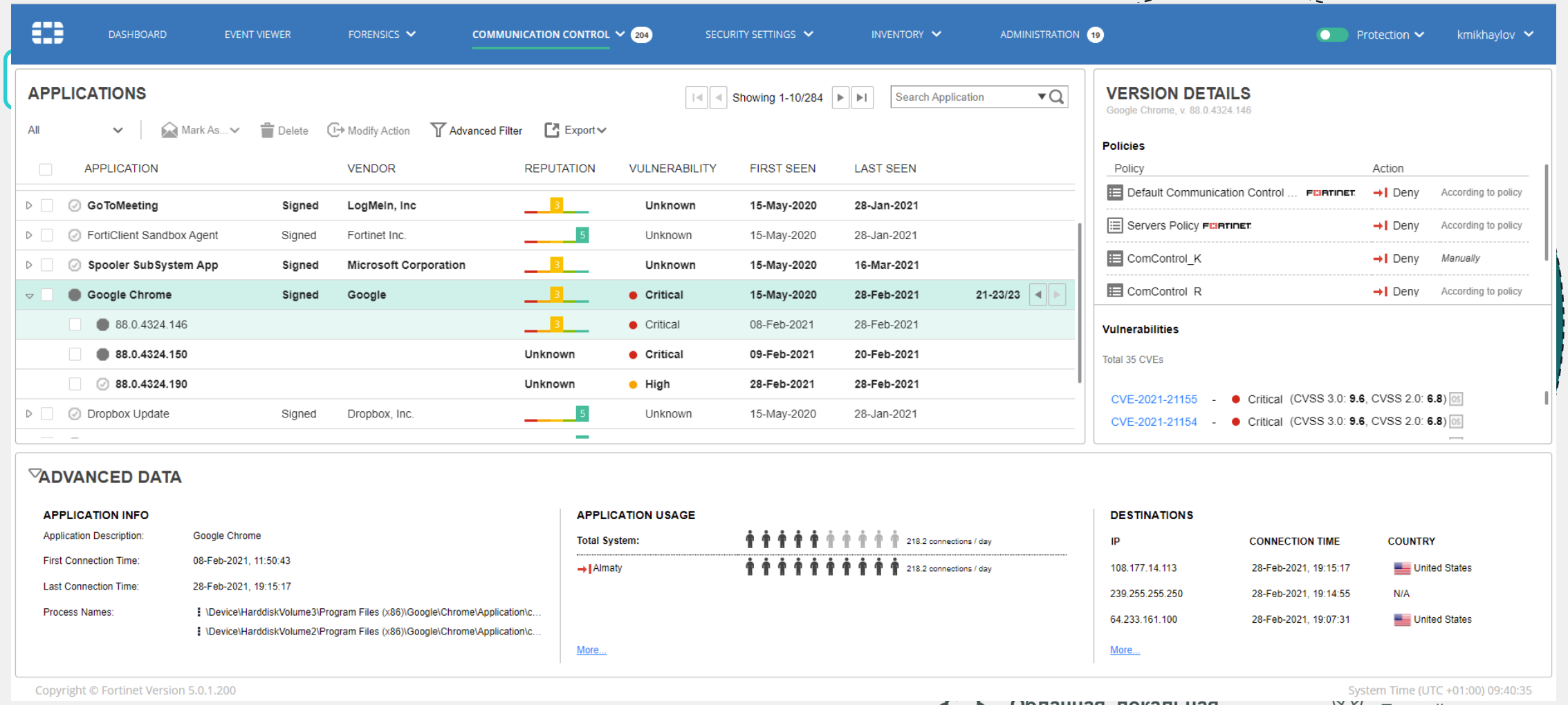
EPP: защита от известных угроз



EDR: обнаружение продвинутых атак



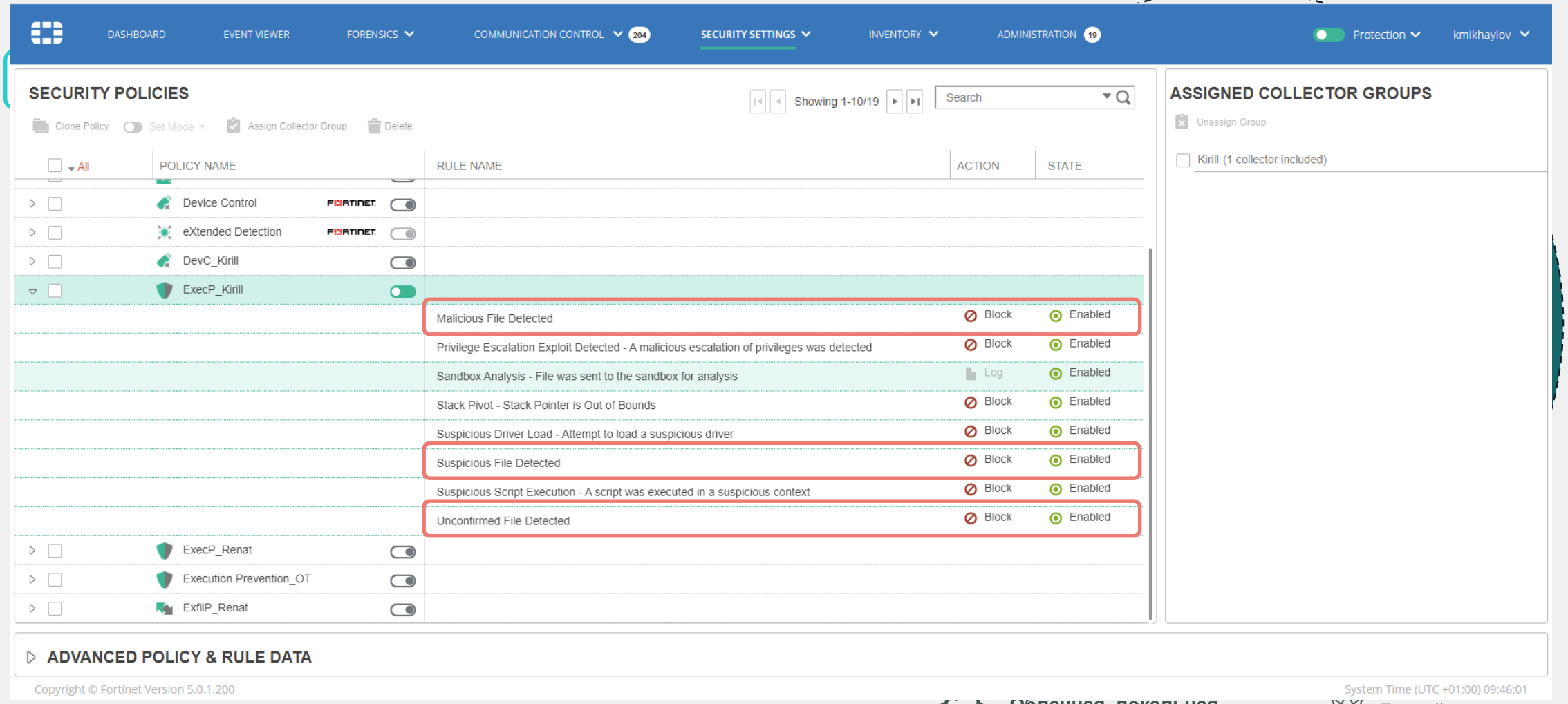
FortiEDR: гипотеза



Облачная, локальная, Гибридная архитектура

Легкий агент

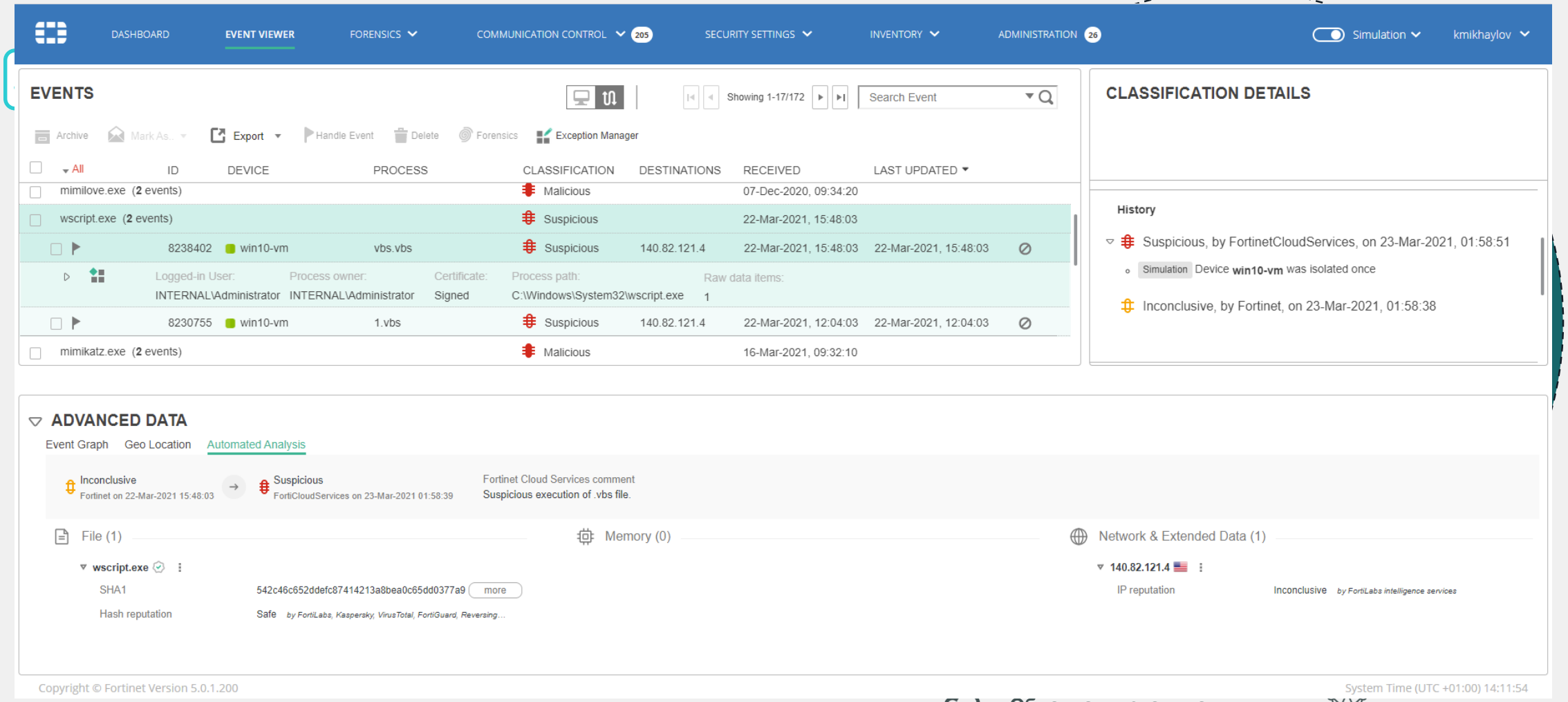
FortiEDR: блокировка



Облачная, локальная, Гибридная архитектура

Легкий агент

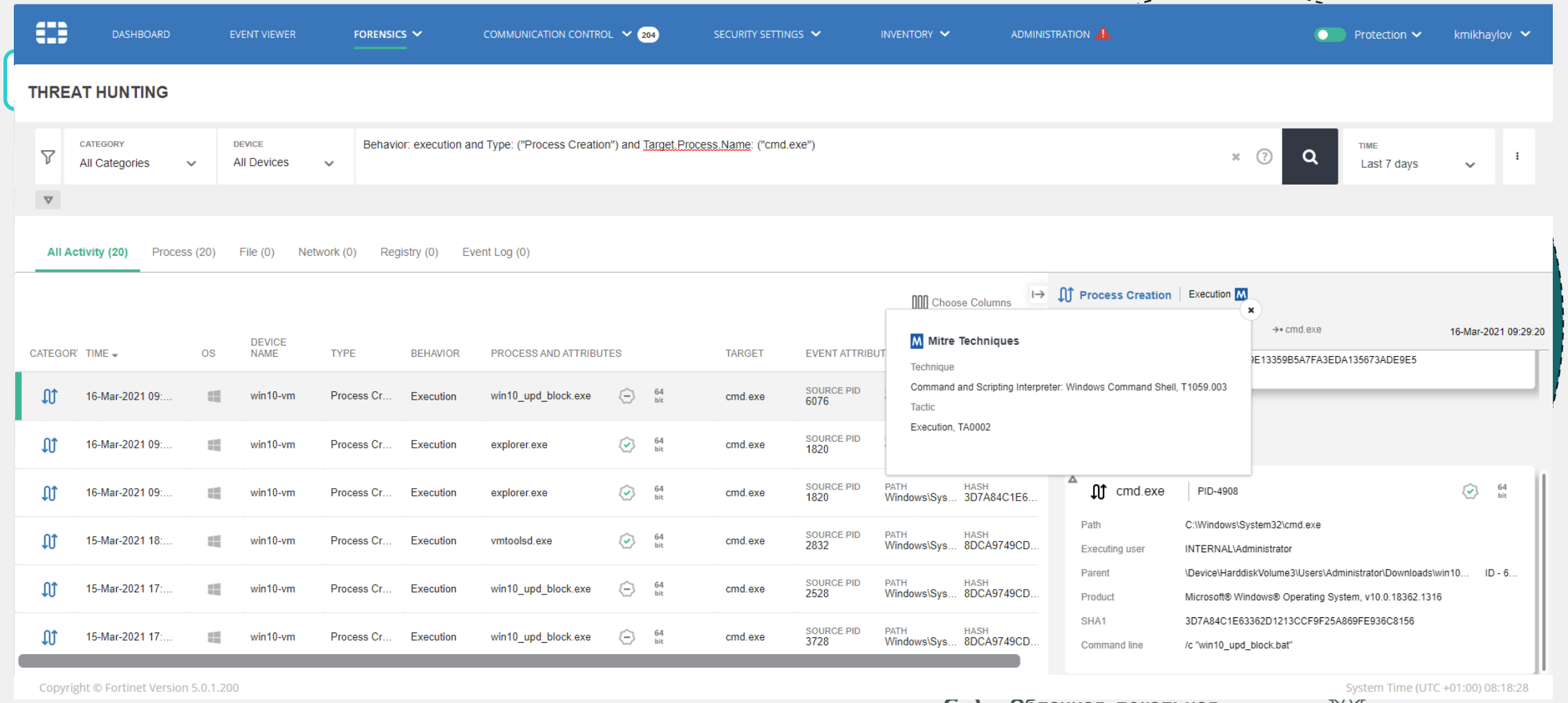
FortiEDR: обнаружение



Облачная, локальная, Гибридная архитектура

Легкий агент

FortiEDR: реагирование



Облачная, локальная, Гибридная архитектура

Легкий агент

Расширенные обнаружение и реагирование

FortiEDR

Fortinet Security Fabric



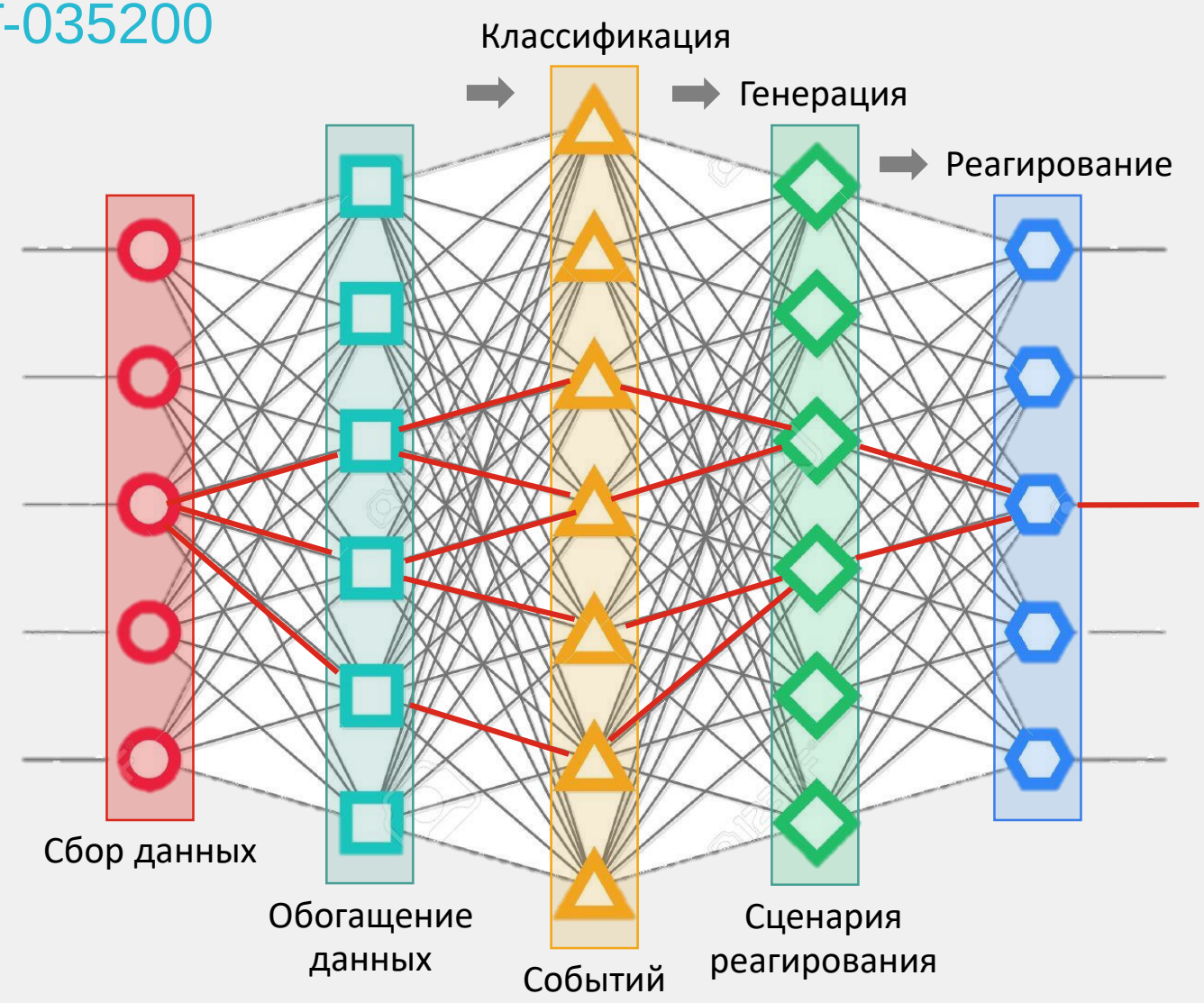

Автоматизация обнаружения

и реагирования на угрозы

FortiXDR

FortiXDR: ANN

Патент: #FORT-035200

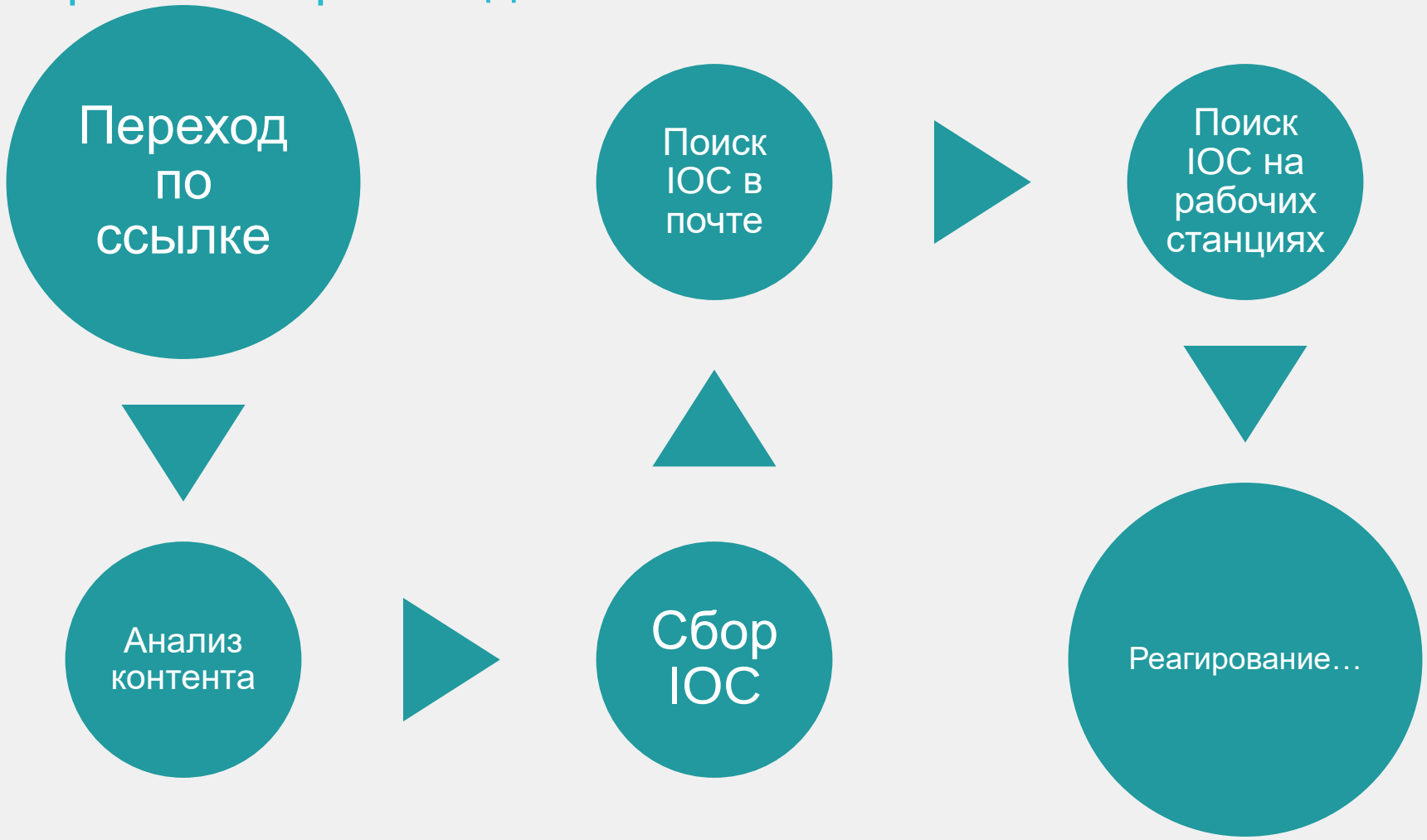


FortiXDR

Пример: целевой фишинг

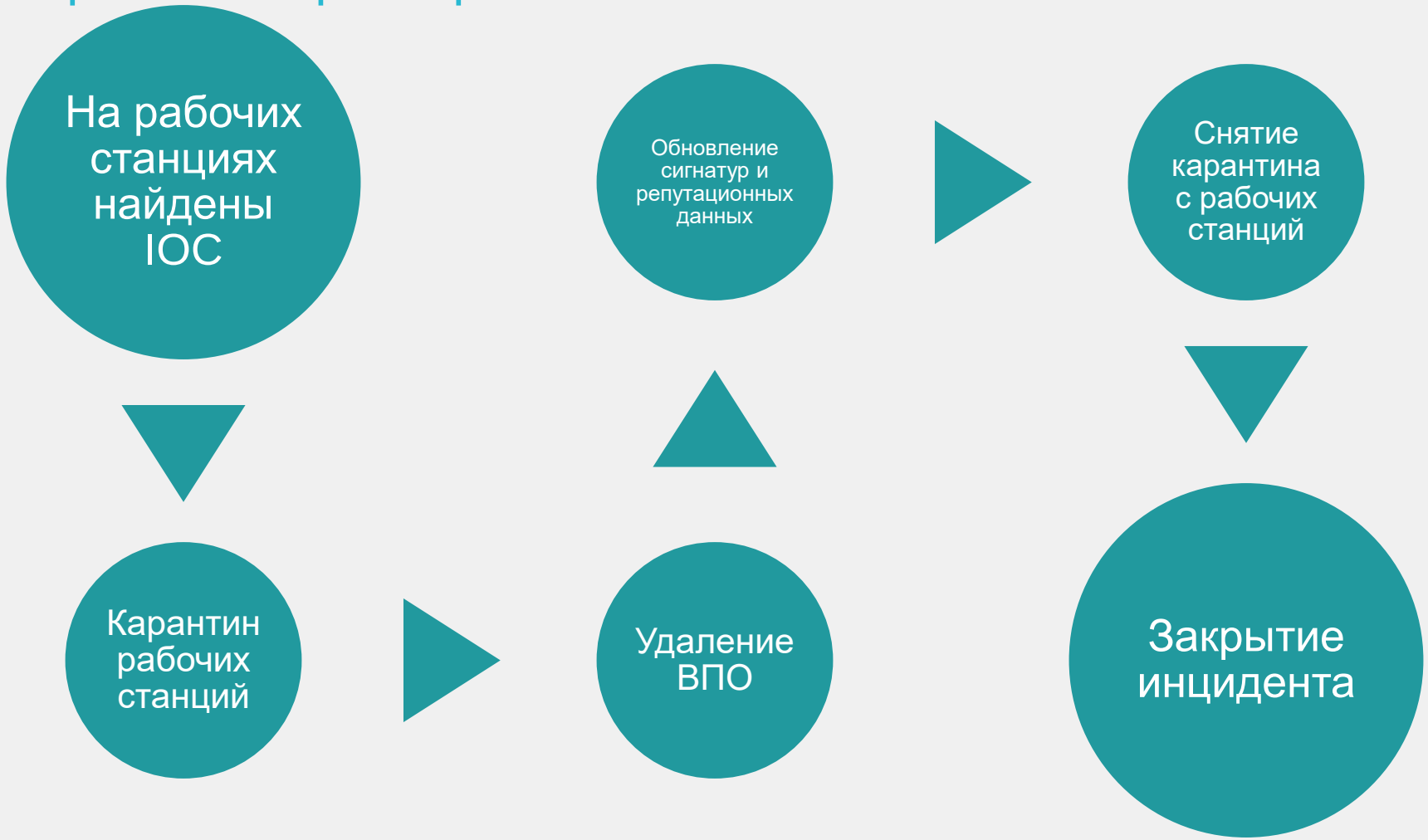
FortiXDR

Автоматизированное расследование



FortiXDR

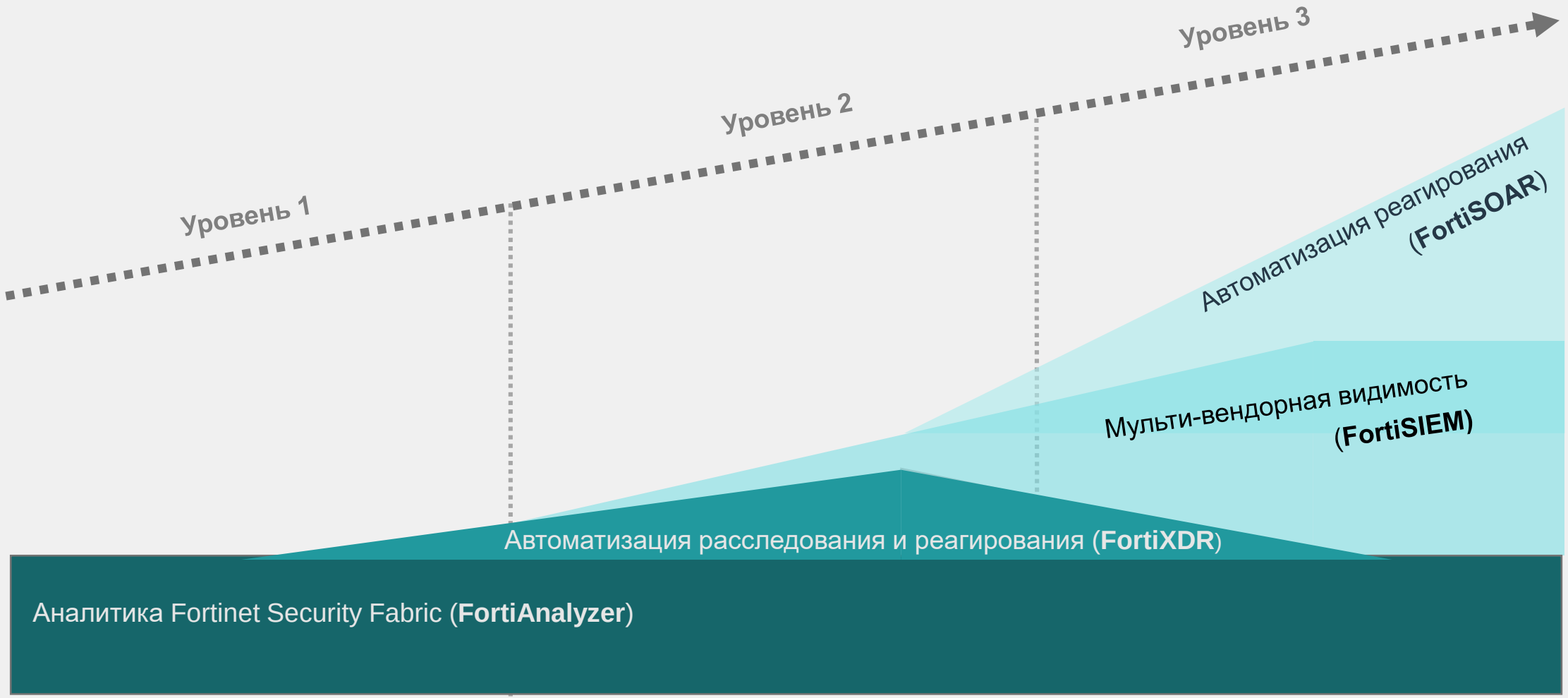
Автоматизированное реагирование



Автоматизация расследования

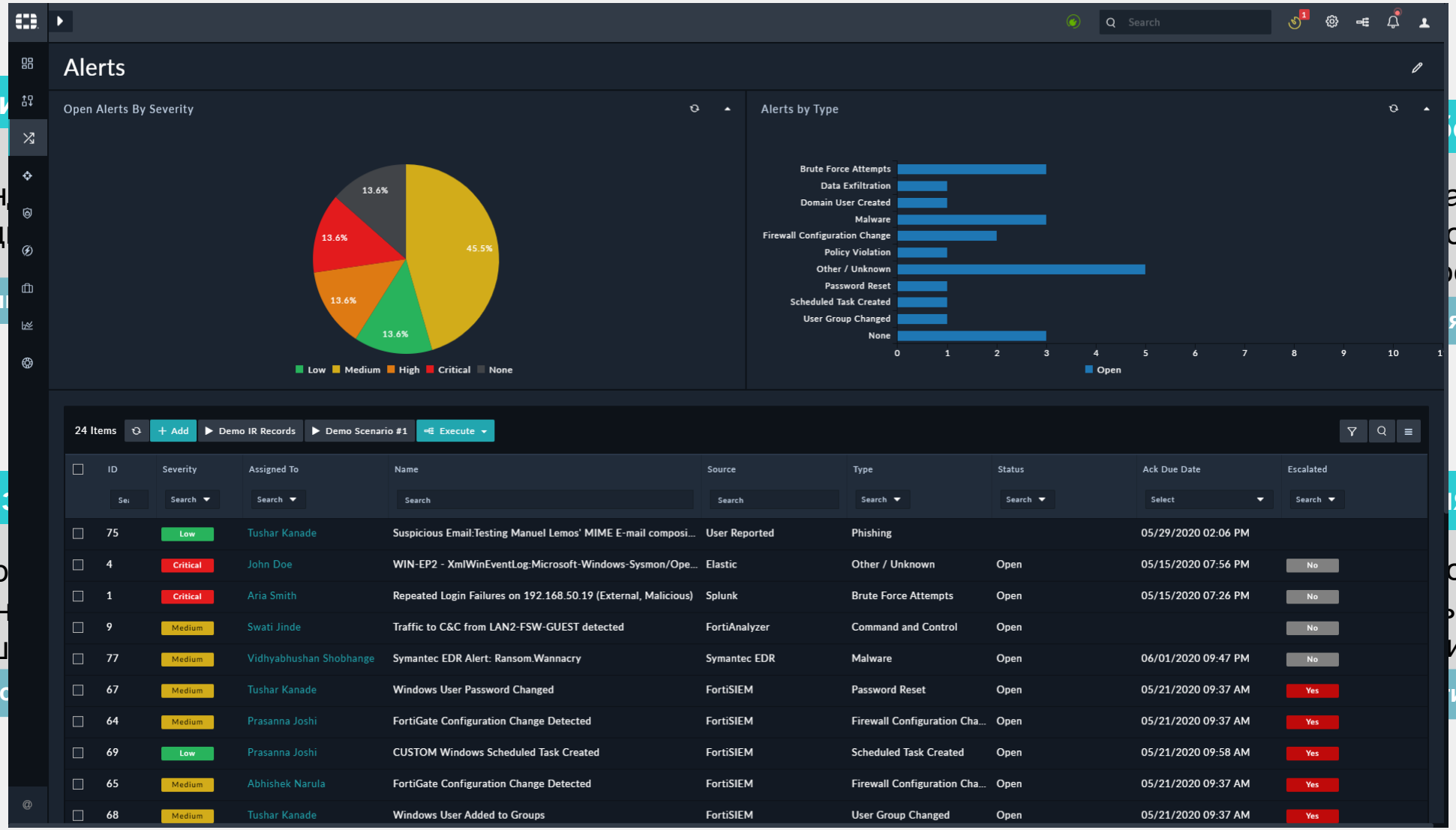
и реагирования на инциденты в мультивендорной среде

Упрощение security operations



Ref: 2020 CISO Benchmark Study

FortiSOAR



FortiSOAR

Инцид

Станда
видим

Увелич

бора данных

назначение и
событий
ности

ция рисков

Оптимиза

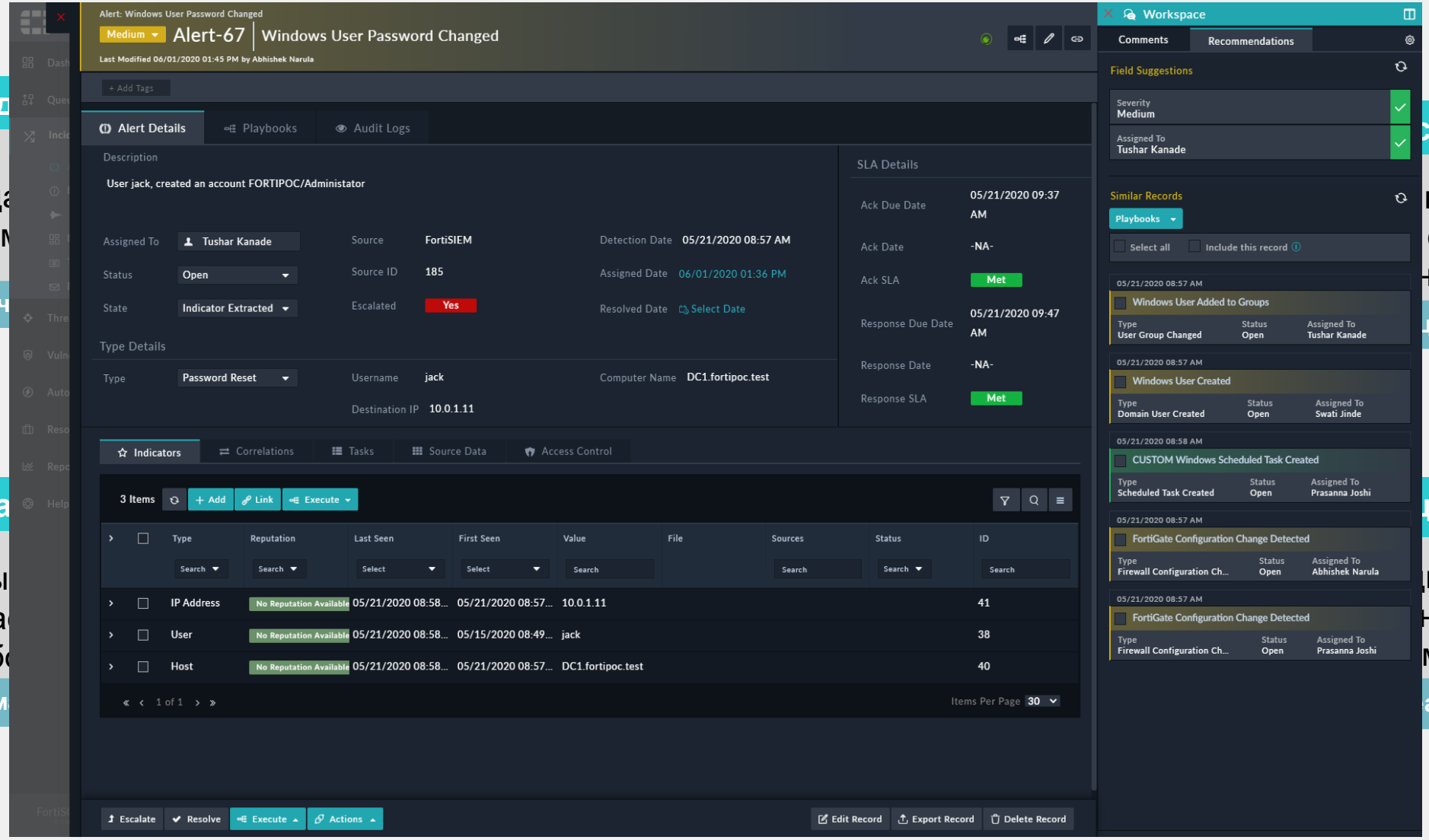
Быстры
предна
дашб

Автом

ция SOC

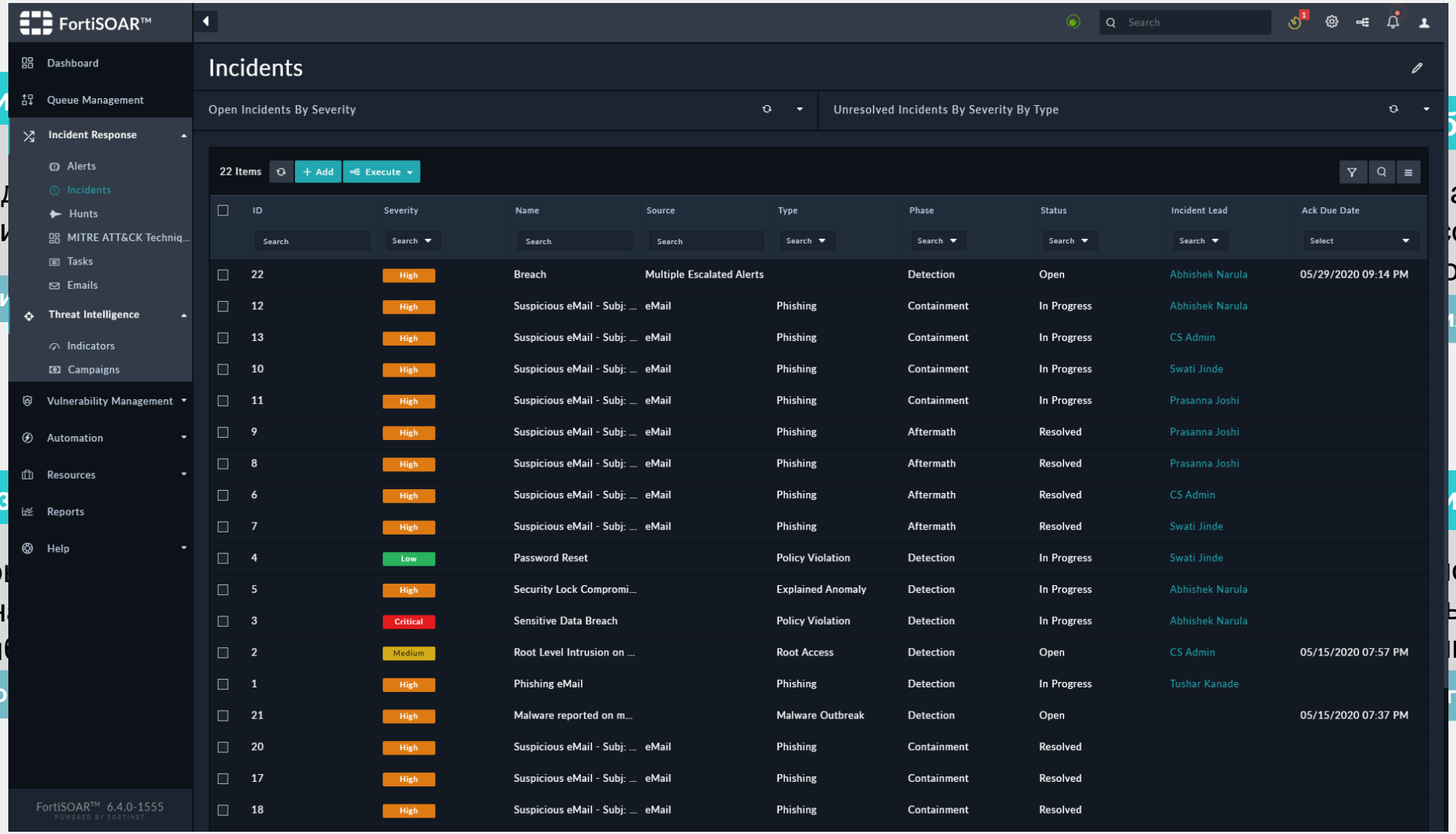
циональный
ный SOC с
ми зонами

агирования

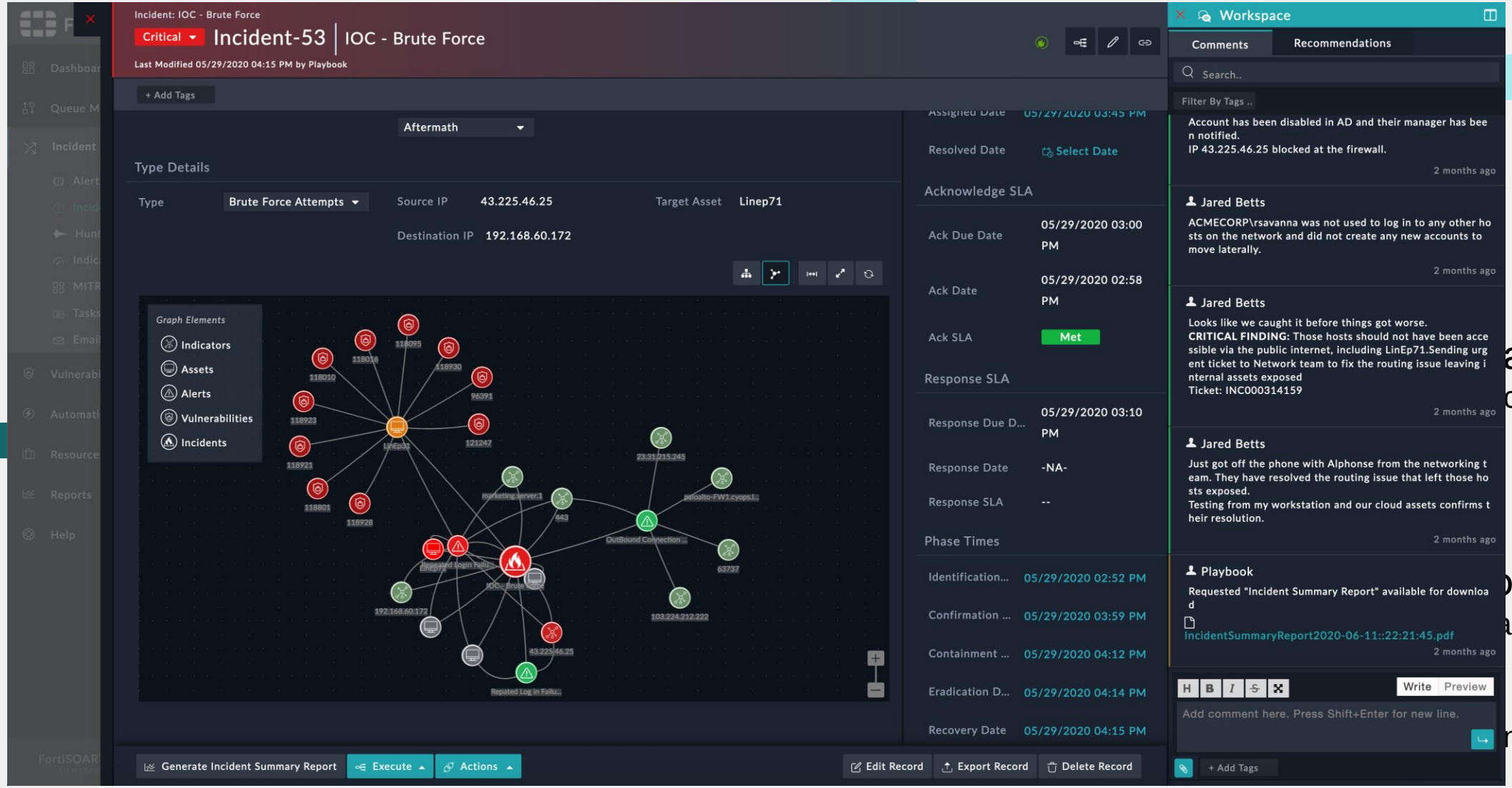


FortiSOAR

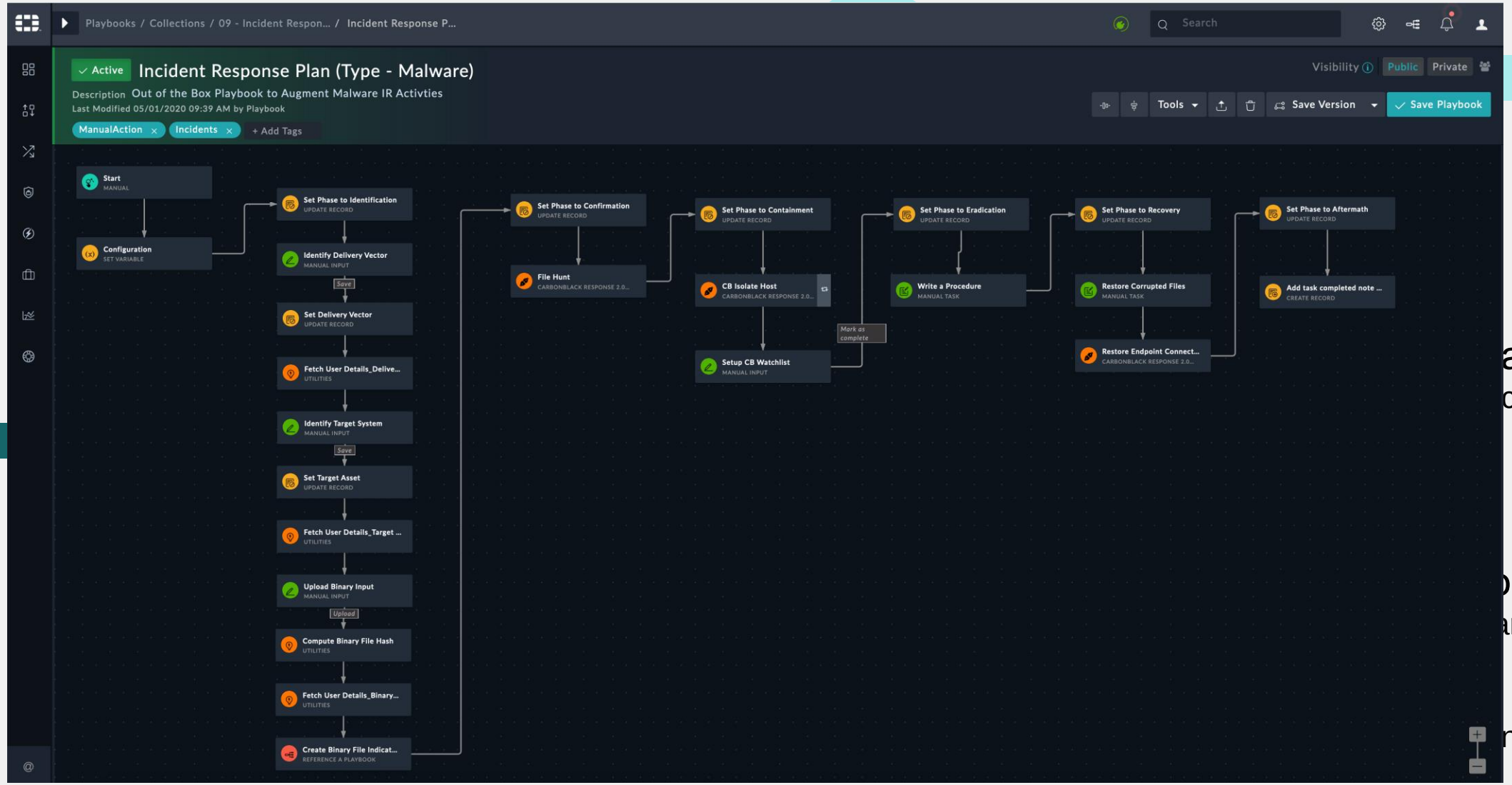
FortiSOAR



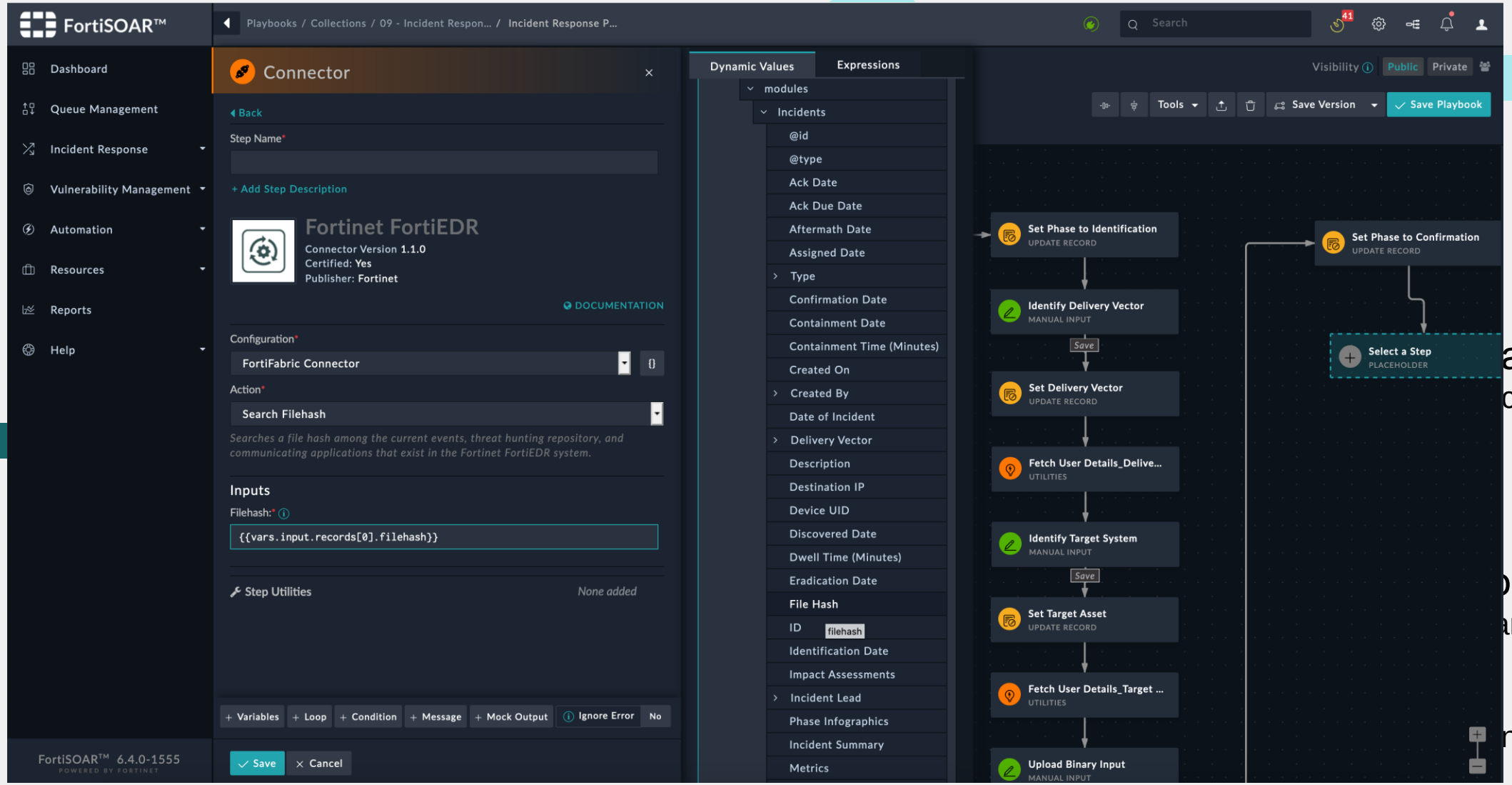
FortiSOAR



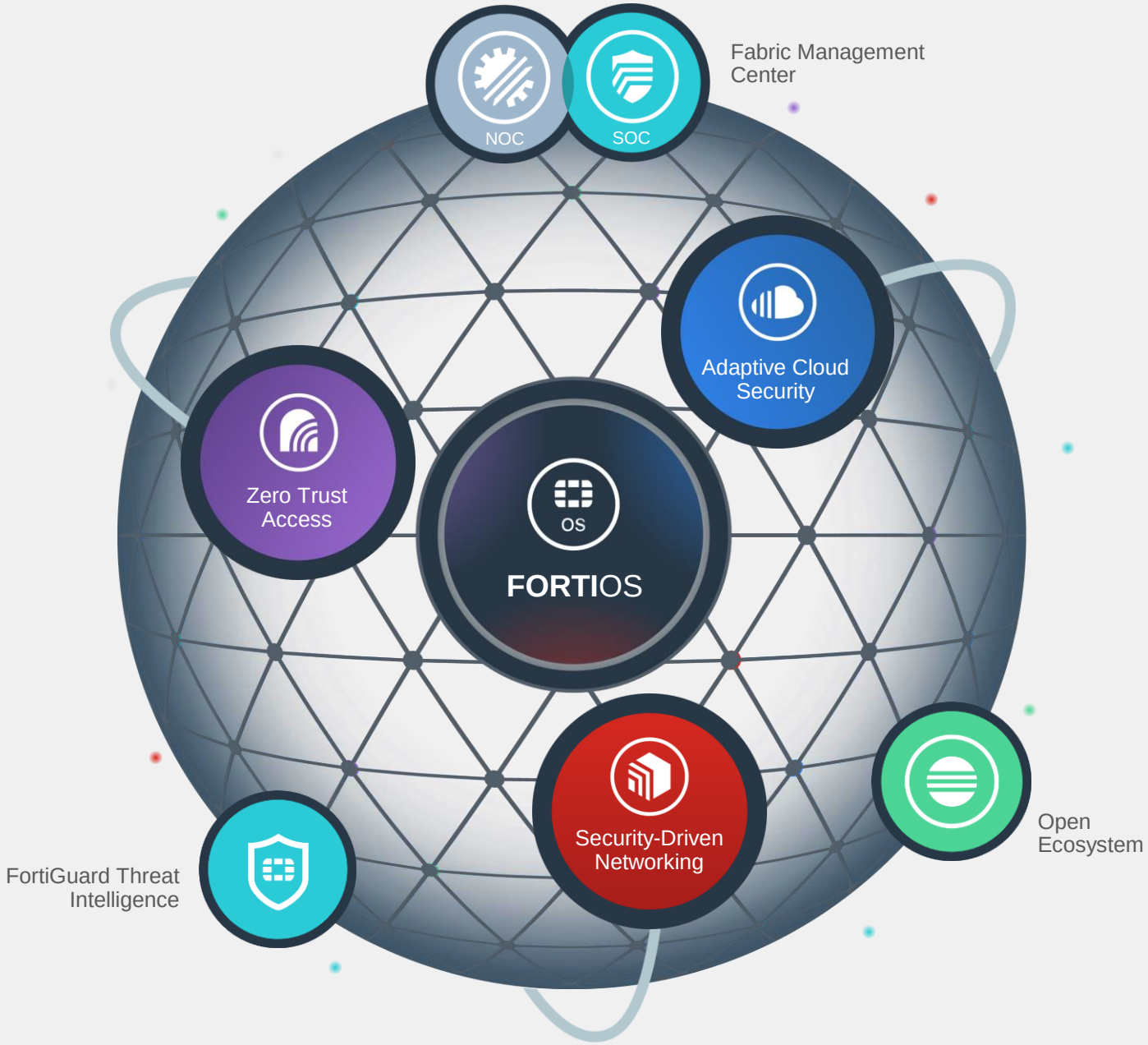
FortiSOAR



FortiSOAR



Заключение



36


FORTINET