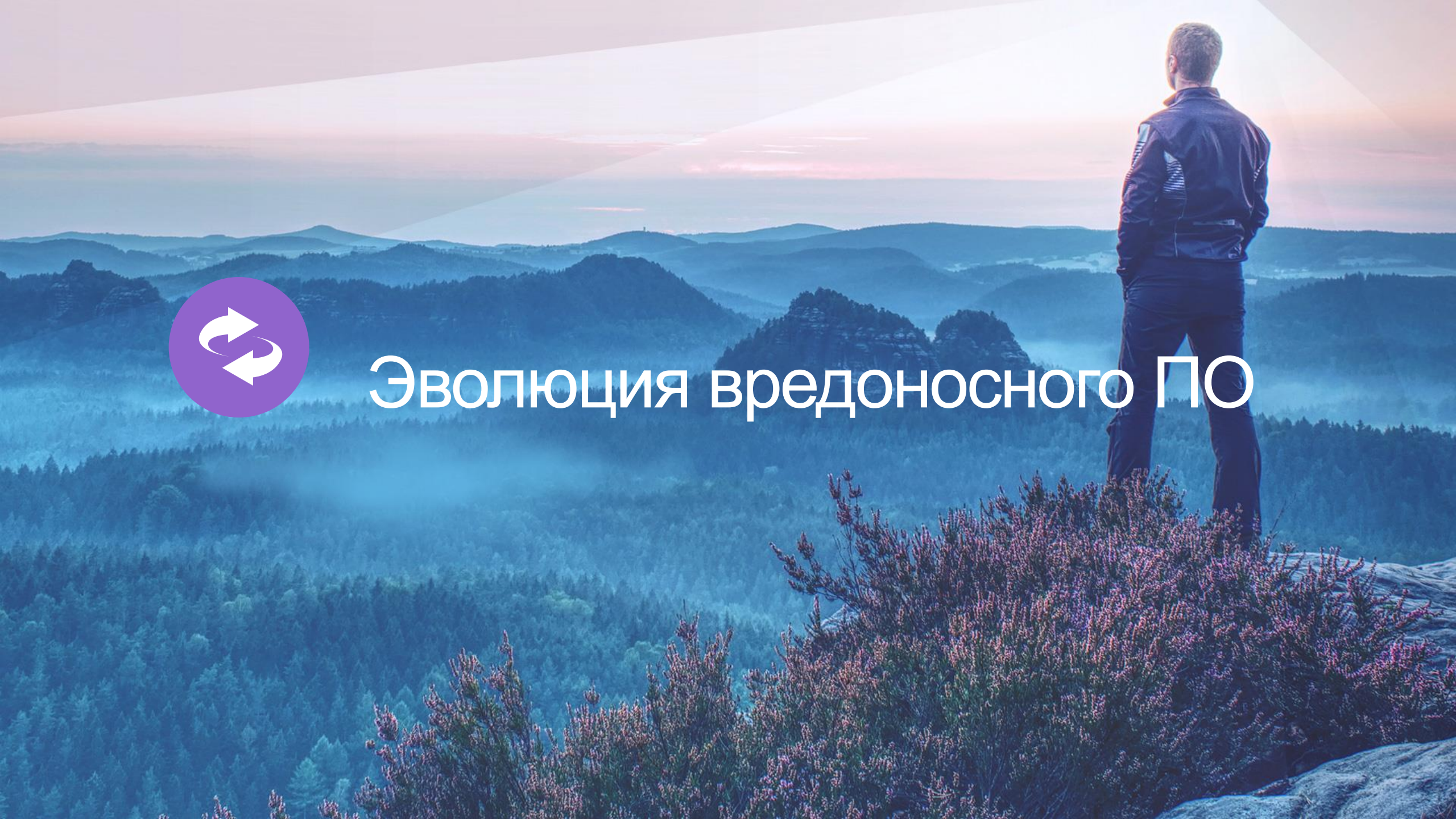
Обнаружение и предотвращение угроз с помощью поведенческого анализа и машинного обучения - UEBA, FortiAI, Deception

Кирилл Михайлов, Fortinet



Эволюция вредоносного ПО

Эволюция обнаружения ВПО

Методы и проблемы

1 Поколение

Сигнатурное обнаружение

- Задержка в обнаружении
- Высокие вычислительные затраты
- Статический анализ

Эволюция обнаружения ВПО

Методы и проблемы

2 Поколение

ATP

- ВПО эволюционирует
- Появление автоматизированного анализа ВПО
- Время обнаружения - минуты

1st Поколение

Сигнатурное обнаружение

- Задержка в обнаружении
- Высокие вычислительные затраты
- Статический анализ

Эволюция обнаружения ВПО

Методы и проблемы

3 Поколение — Искусственный интеллект

- Машинное обучение
- Виртуальный аналитик безопасности
- Время обнаружения – менее секунды

2nd Gen — ATP

- ВПО эволюционирует
- Появление автоматизированного анализа ВПО
- Время обнаружения - минуты

1st Gen — Сигнатурное обнаружение

- Задержка в обнаружении
- Высокие вычислительные затраты
- Статический анализ

Обнаружение вредоносного кода

Решения ATP

AV движок

Проверю сердцевину…

Вердикт - плохое.

FortiSandbox

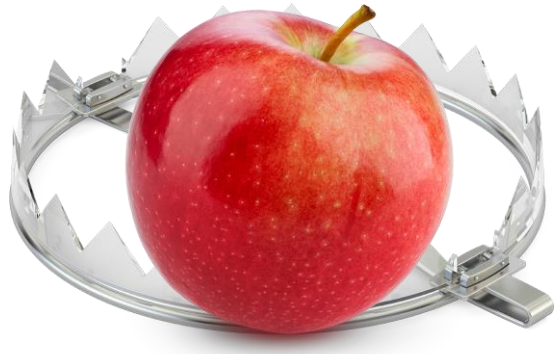
Надо откусить…

Вердикт - плохое.

FortiAI

Опишу яблоко - гнилое...

Вердикт - плохое.



FortiDeceptor

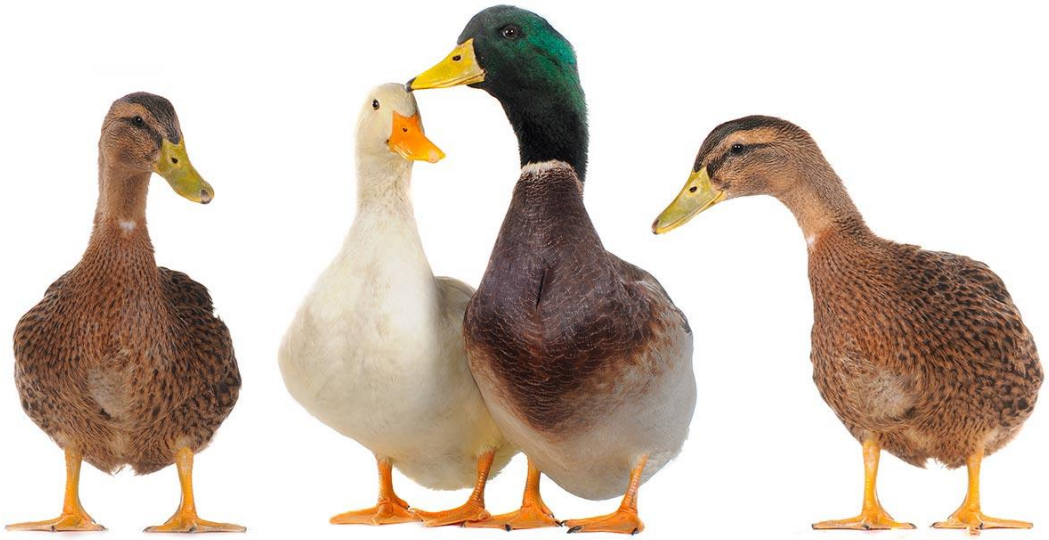
Разложу больше яблок…

…с ловушками.

FortiAI
Введение

ИИ / машинное обучение: что мы ожидаем?

☑ ходит ☑ крякает ☑ плавает



Утки

Не утки

ИИ / машинное обучение: FortiAI

Производительность

- Уменьшение время обнаружения до секунды и меньше
- Аппаратное ускорение ANN

Развитие

Эволлюция FortiGuard AI

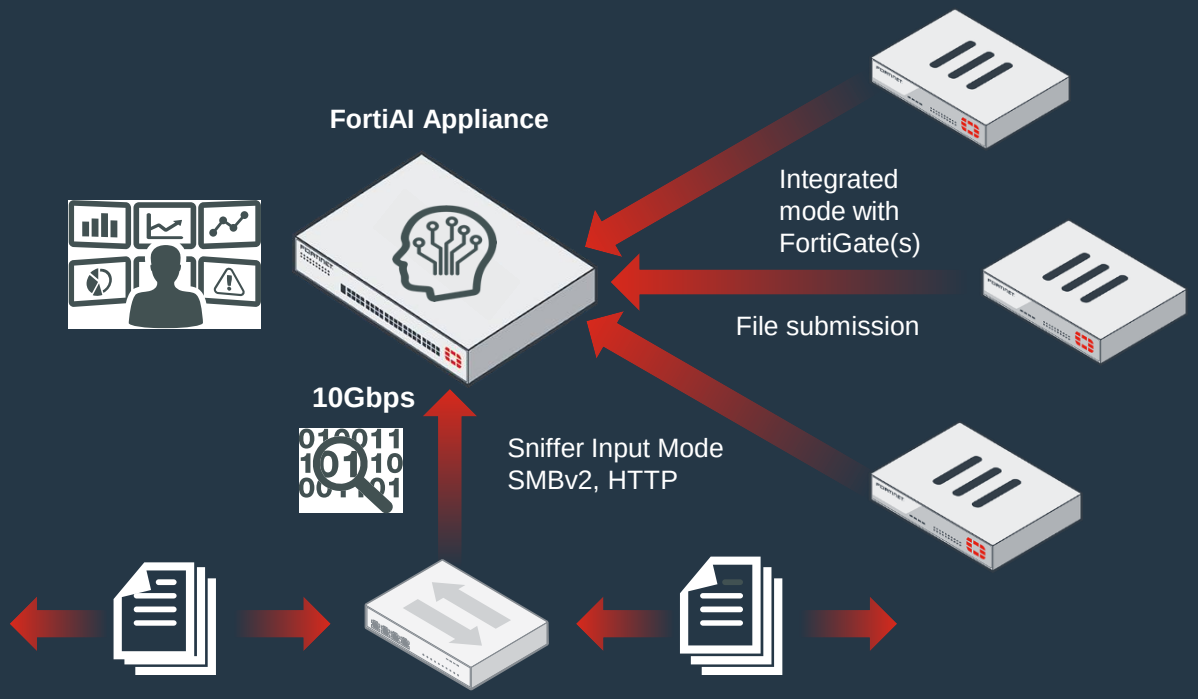
- Сигнатуры (CRPL)
- Сгенерированные машиной сигнатуры (AutoCPRL)
- Обучение DNN (Deep Neural Network)
- Самообучение (локально)

Преимущества

Преимущества для бизнеса

- Изменение функционала работников
- Virtual Security Analyst TM

FortiAI в Fortinet Security Fabric

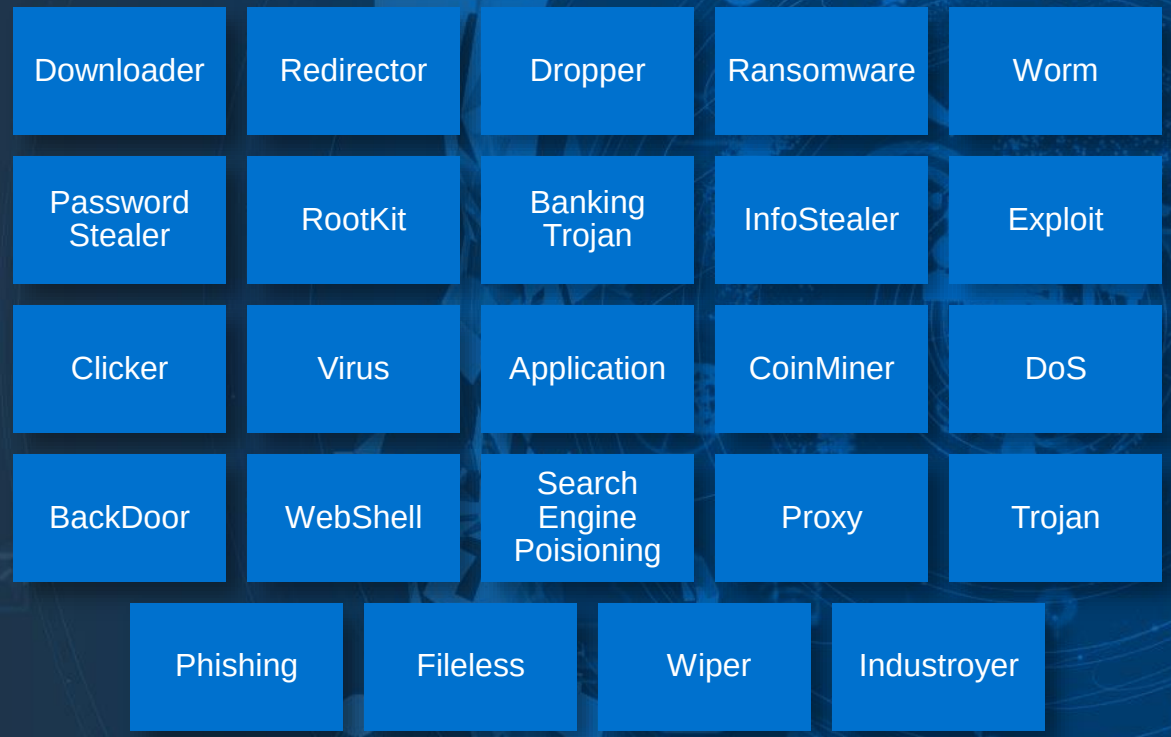


Virtual Security Analyst ™

FortiAI Virtual Security Analyst ™

Анализатор ВПО – идентифицирует более 20 сценариев атак

- Ransomware, Dropper, PWS (Password Stealing Trojan), CoinMiner, Banking Trojan, Fileless attack etc
- Отвечает на вопросы:
  - Какое ВПО используется в атаке?
  - Функционал ВПО?
  - Почему данное ПО вредоносное?



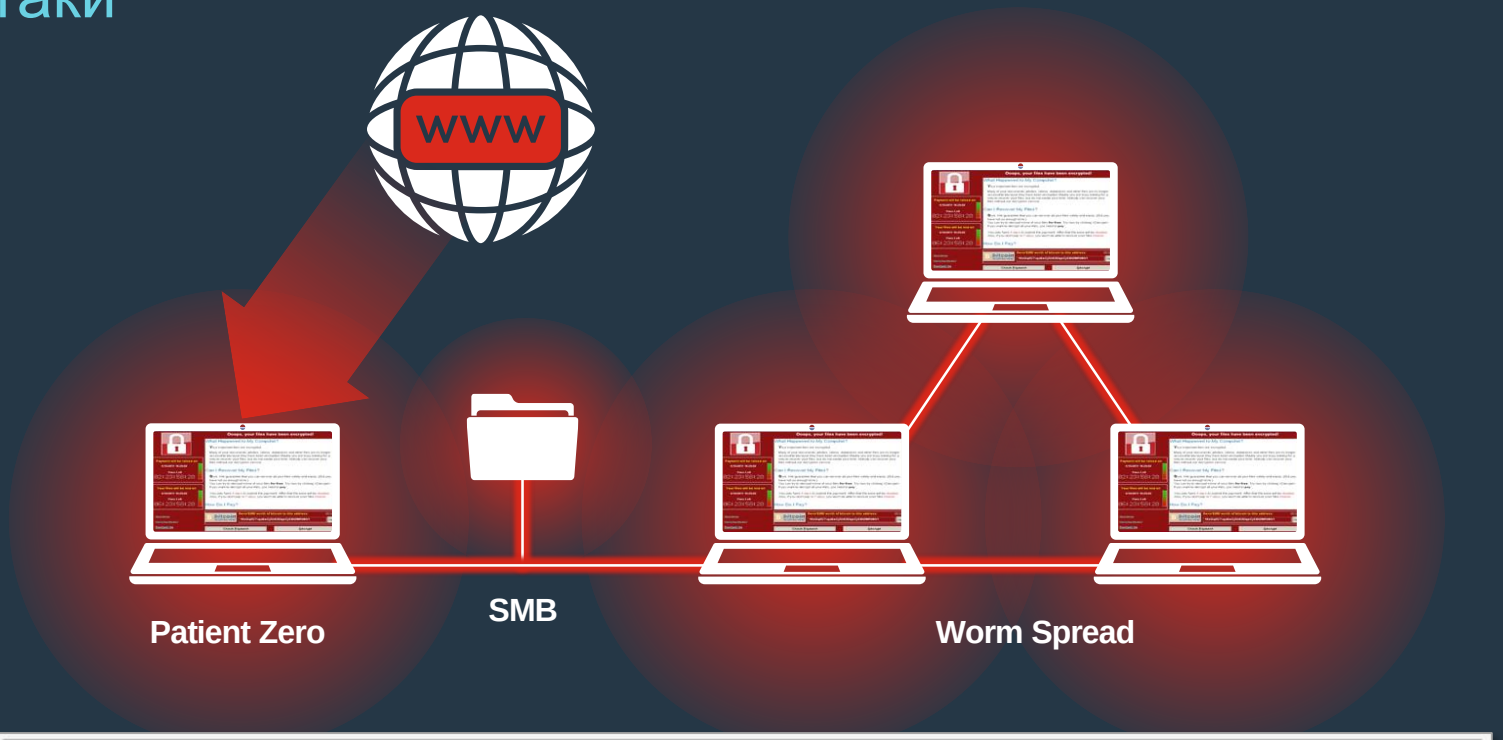
FortiAI Virtual Security Analyst ™

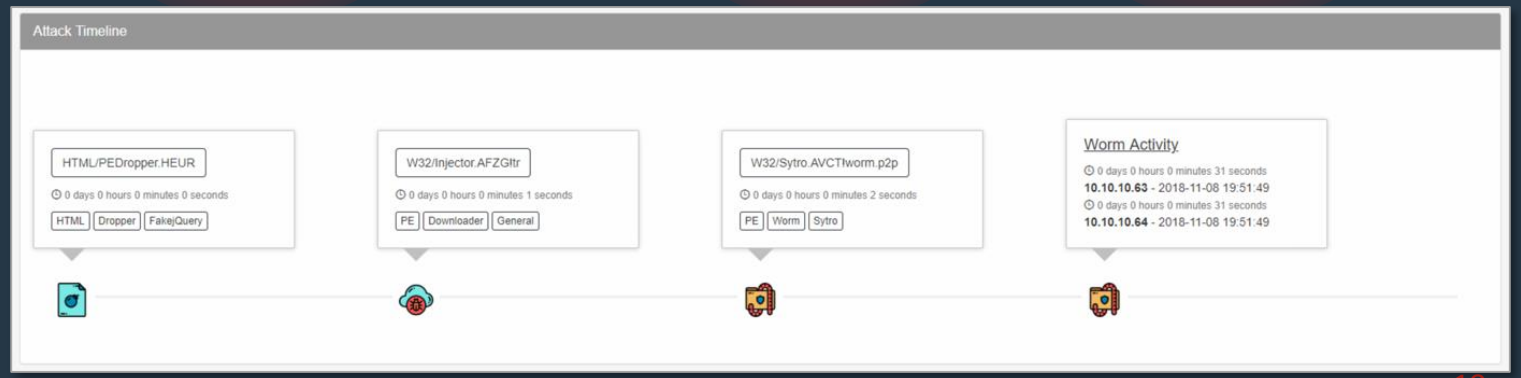
Определение источника атаки

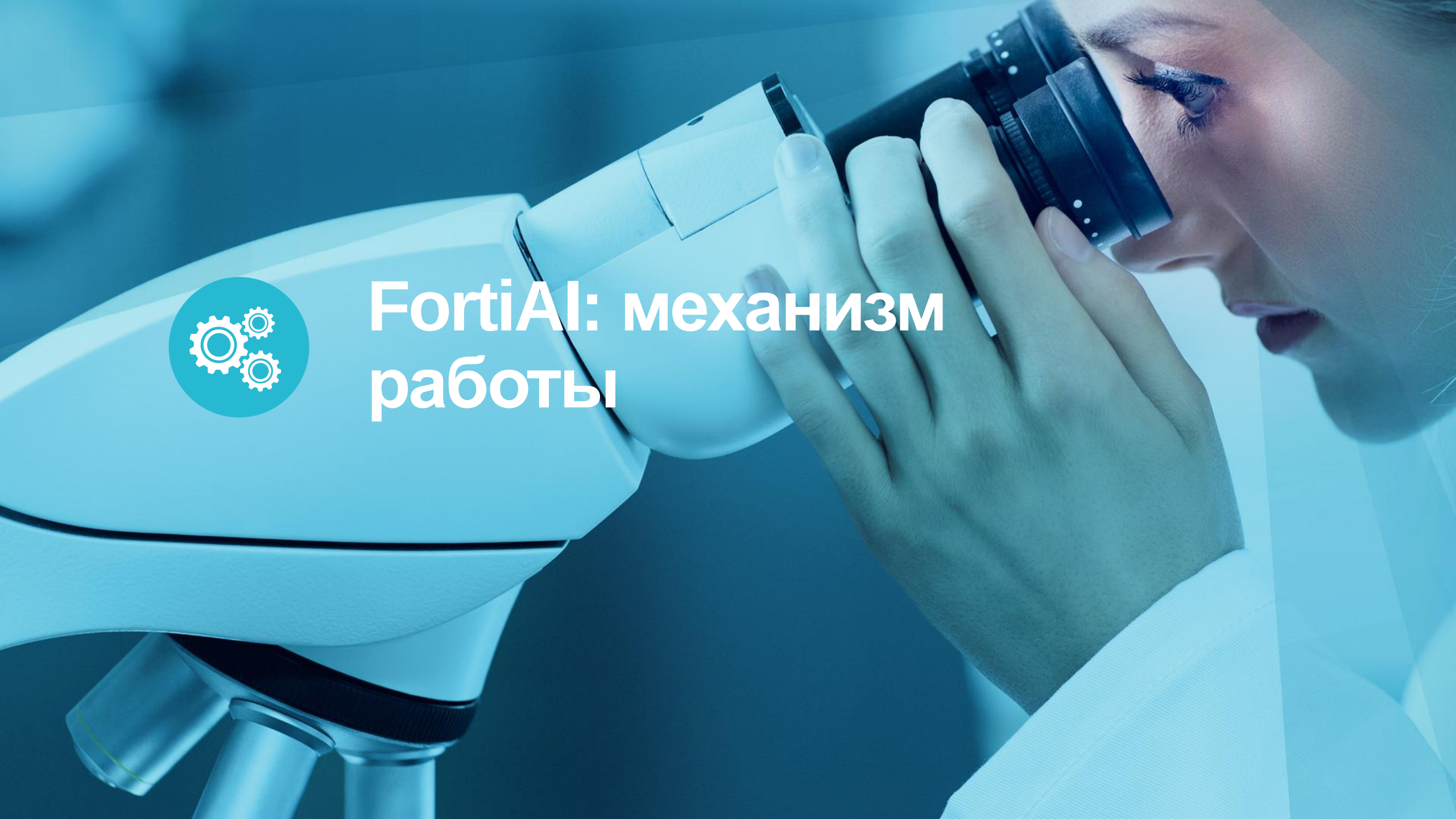
Определение “нулевого пациента”

Сценарий атаки

- Сколько ВПО проникло в сеть
- Специализированный движок связывает события заражения
- Менее секунды на получение вердикта







FortiAI: механизм работы

FortiAI Virtual Security Analyst ™
С помощью FortiAI Artificial Neural Networks (ANN), обнаруживает **неизвестное ВПО и** нулевого пациента

99.9%

Уровень обнаружения*

<100 мс

Время обнаружения

10G

Производительность

200 млрд

Обнаруженных признаков

20+

Сценарии атак

* Measured by Breaking Point malware strike pack

Forti AI: что внутри

Патент # U.S. Serial No.: 16/053,479

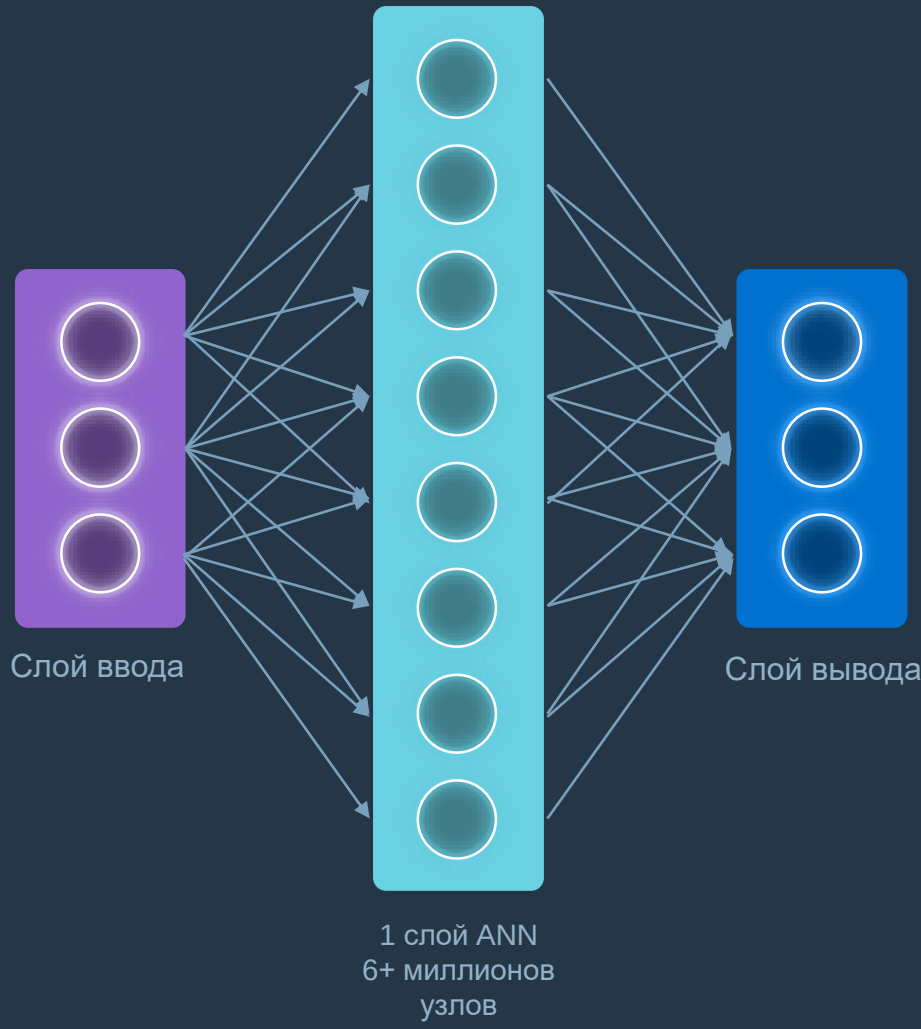
Нейронная сеть

- **Обучена на** 200+ миллионах файлов
- Изучены миллиарды **признаков**

Каждый узел обозначает “аналитика”

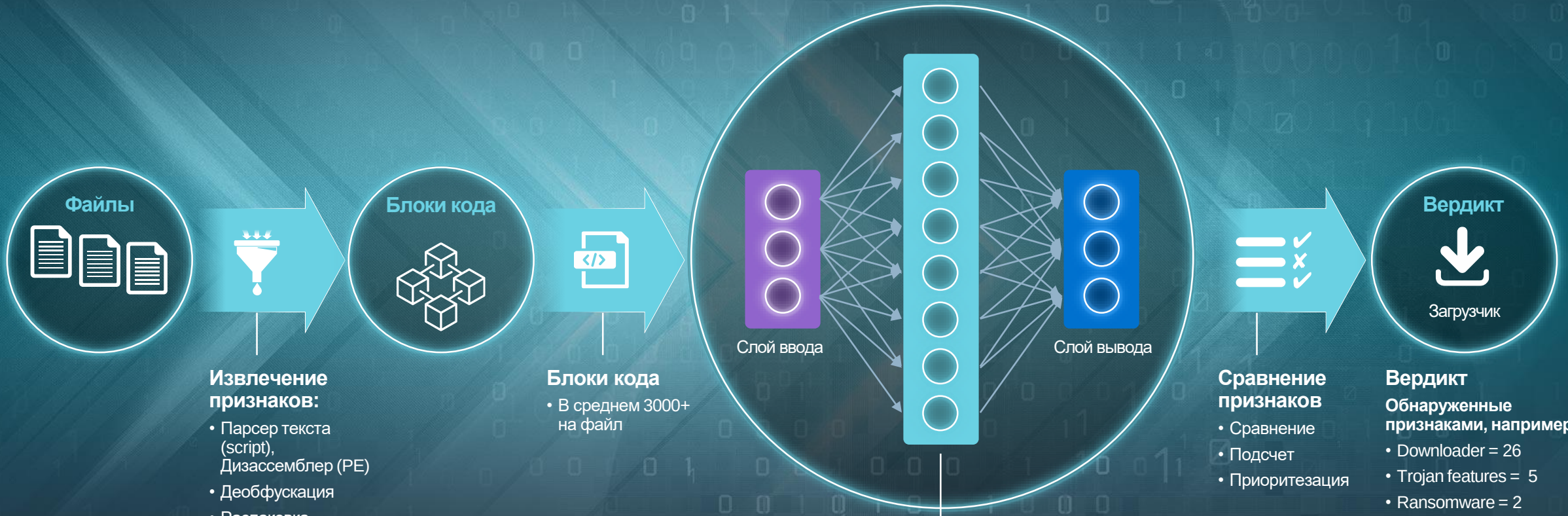
- **Функция** – сравнение с признаками ВПО
- База **признаков** состоит из:
  - PE признаким (Portable Executables) & Non-PE признаки
  - Техник, таких как анализ файлом значений реестра, запущенных процессов и т.д.

Не **требует запуска файла**



FortiAI

Процесс обнаружения ВПО



Извлечение признаков:

- Парсер текста (script), Дизассемблер (PE)
- Деобфускация
- Распаковка

Блоки кода

- В среднем 3000+ на файл

Нейронные сети

- База признаков
- Более 6 миллионов признаков
- Аппаратное ускорение

Сравнение признаков

- Сравнение
- Подсчет
- Приоритезация

Вердикт

Обнаруженные признаками, например

- Downloader = 26
- Trojan features = 5
- Ransomware = 2

FortiAI: обнаружение бестелесного ВПО

Что такое бестелесное ВПО?

Маскирующееся

Использующее легитимное ПО

Скрывающее следы

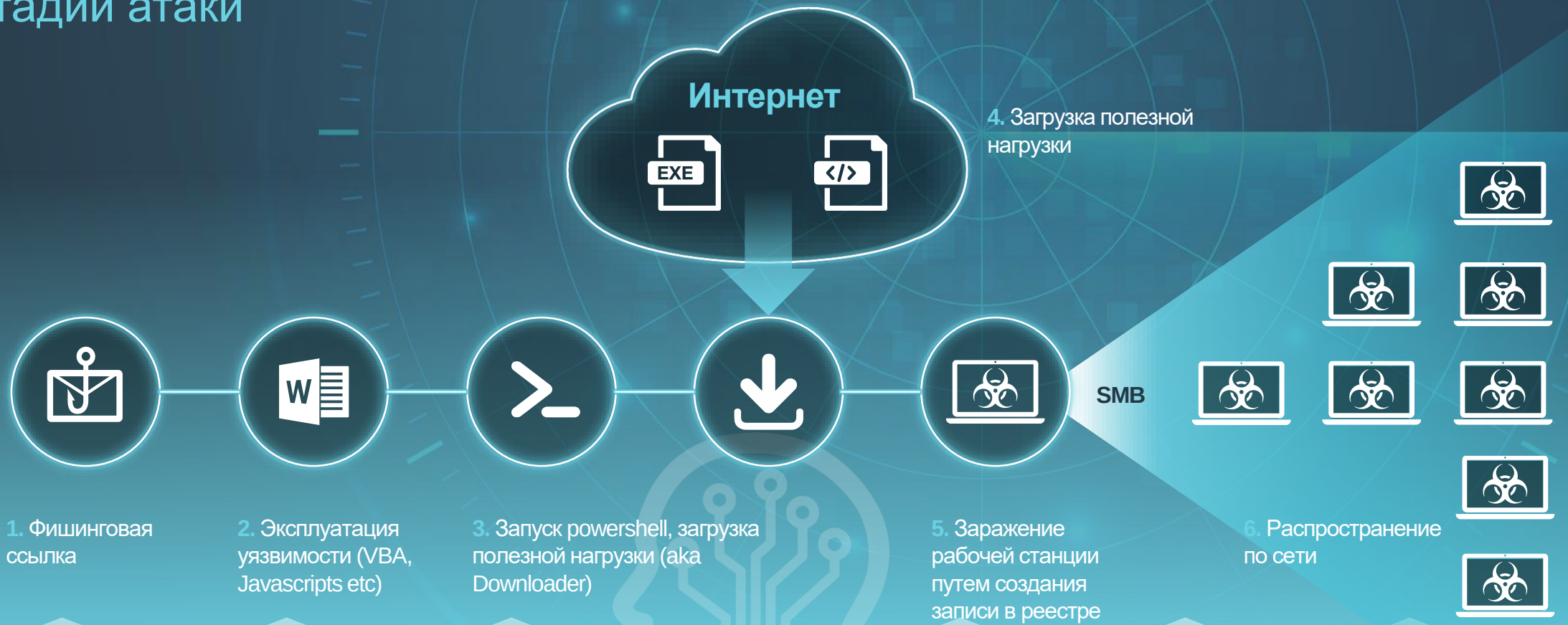
Не оставляющее следов запуска

Вредоносное

Скрипт, запускающий вредоносный код в памяти

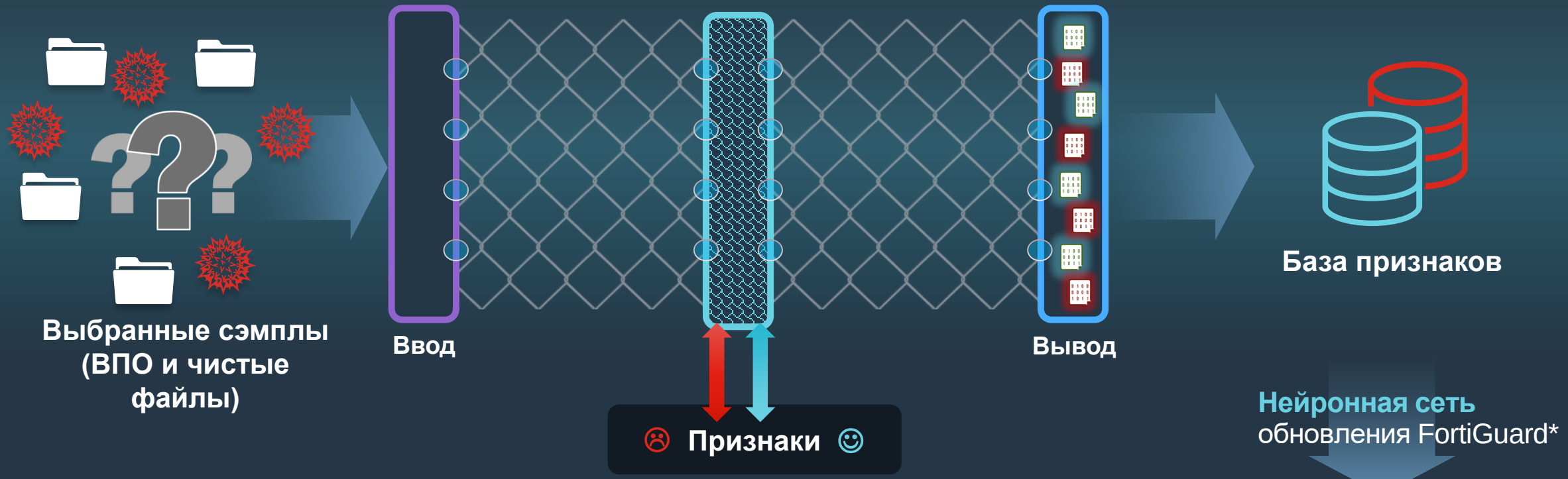
FortiAI: обнаружение бестелесного ВПО

Стадии атаки



FortiAI e.g. Downloader, Network worm

FortiAI: обучение



Нейронная сеть обновления FortiGuard*

- **Предварительное обучение** в FortiGuard ~ 20 миллионами чистых и вредоносных файлов
- Обучение и обновления на регулярной основе

”Локальное” обучение

На реальном трафике

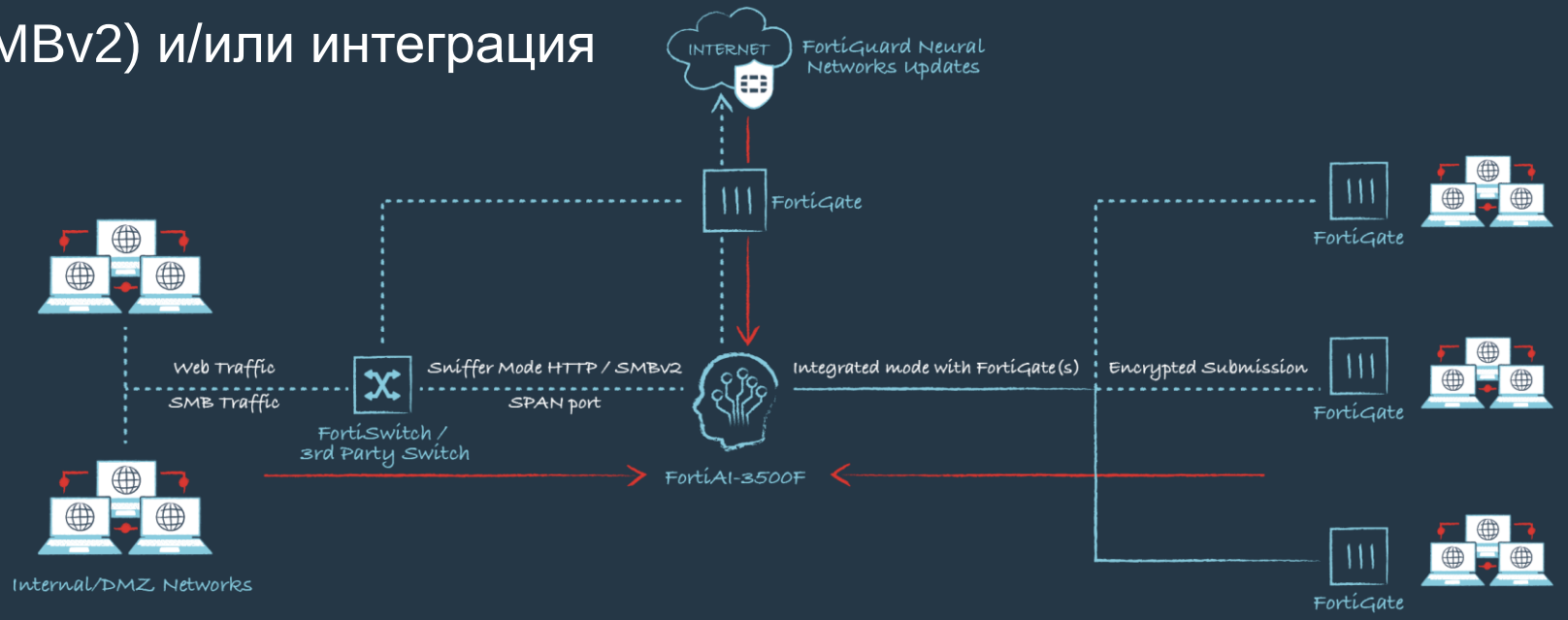
Цель:
Снижение ложных сработок и получение новых черт

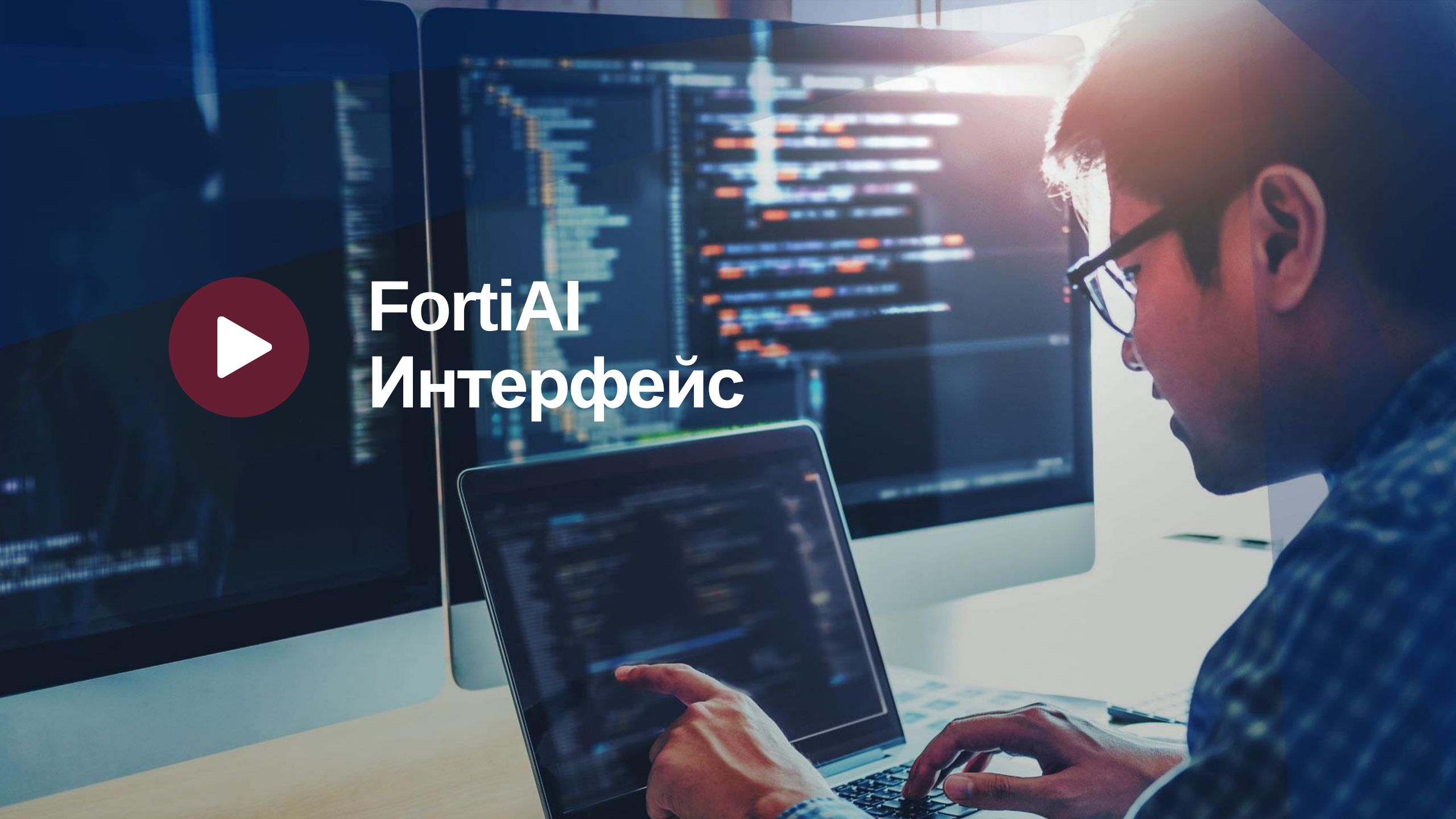
1. Обнаружение ВПО
2. Идентификация
3. Обновление базы признаков
4. Новые признаки помогают обнаруживать новое ВПО

FortiAI: развертывание

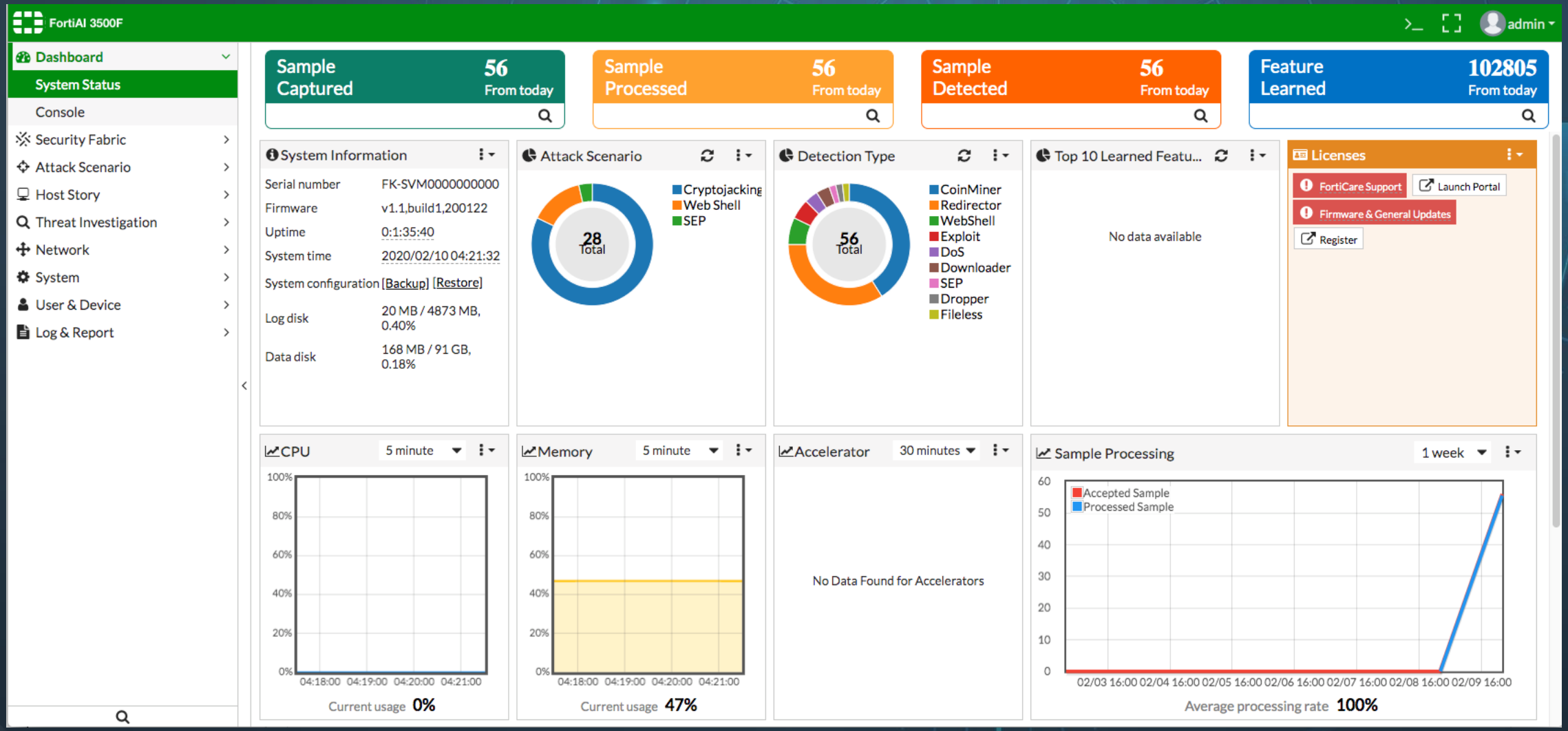
Архитектура

- Не требуются сенсоры
- Поддержка FortiGate 6.4+
- Сниффер (HTTP & SMBv2) и/или интеграция
- 10G

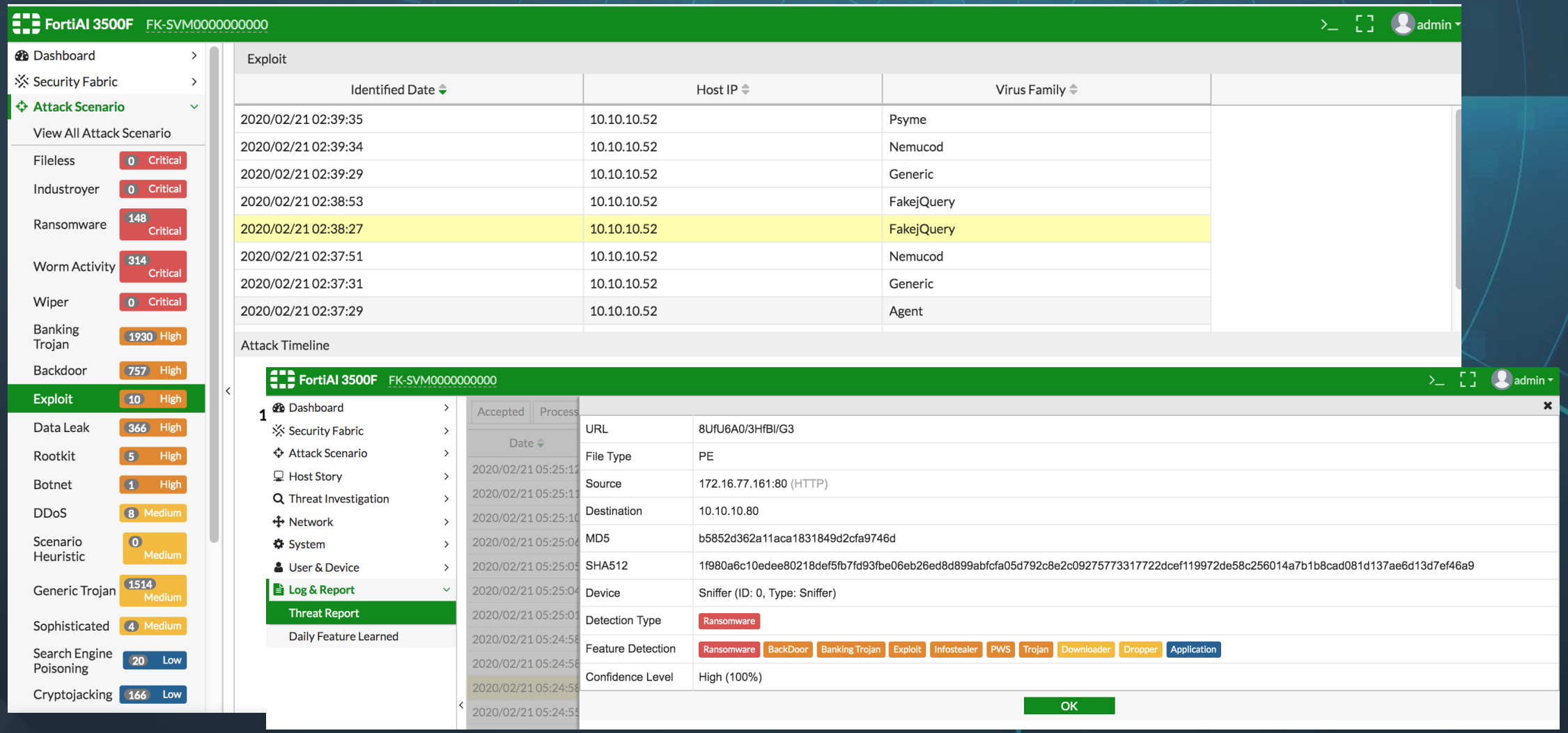



FortiAI
Интерфейс

FortiAI: главный экран

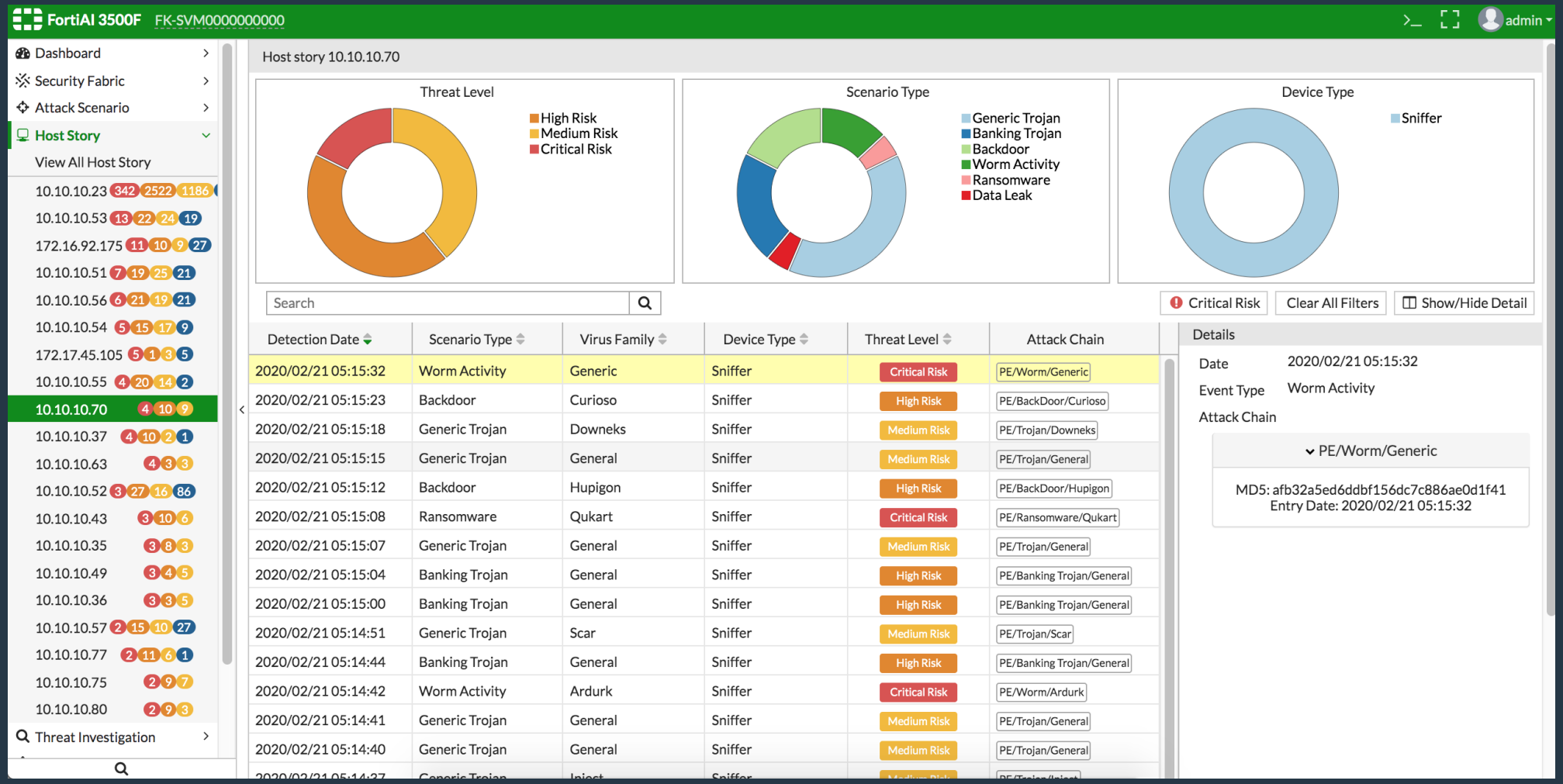


FortiAI – VSA – классификация ВПО



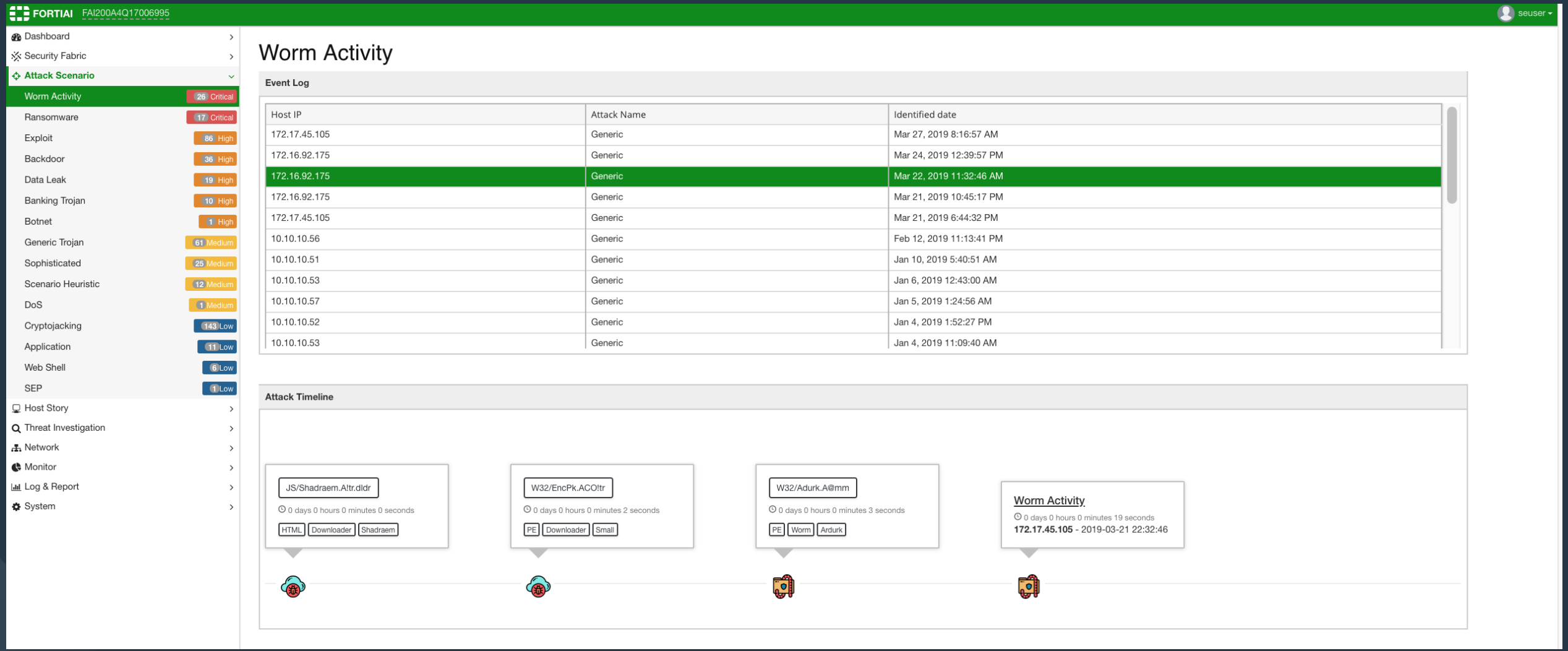
FortiAI: Host Story

Группировка по узлу и времени

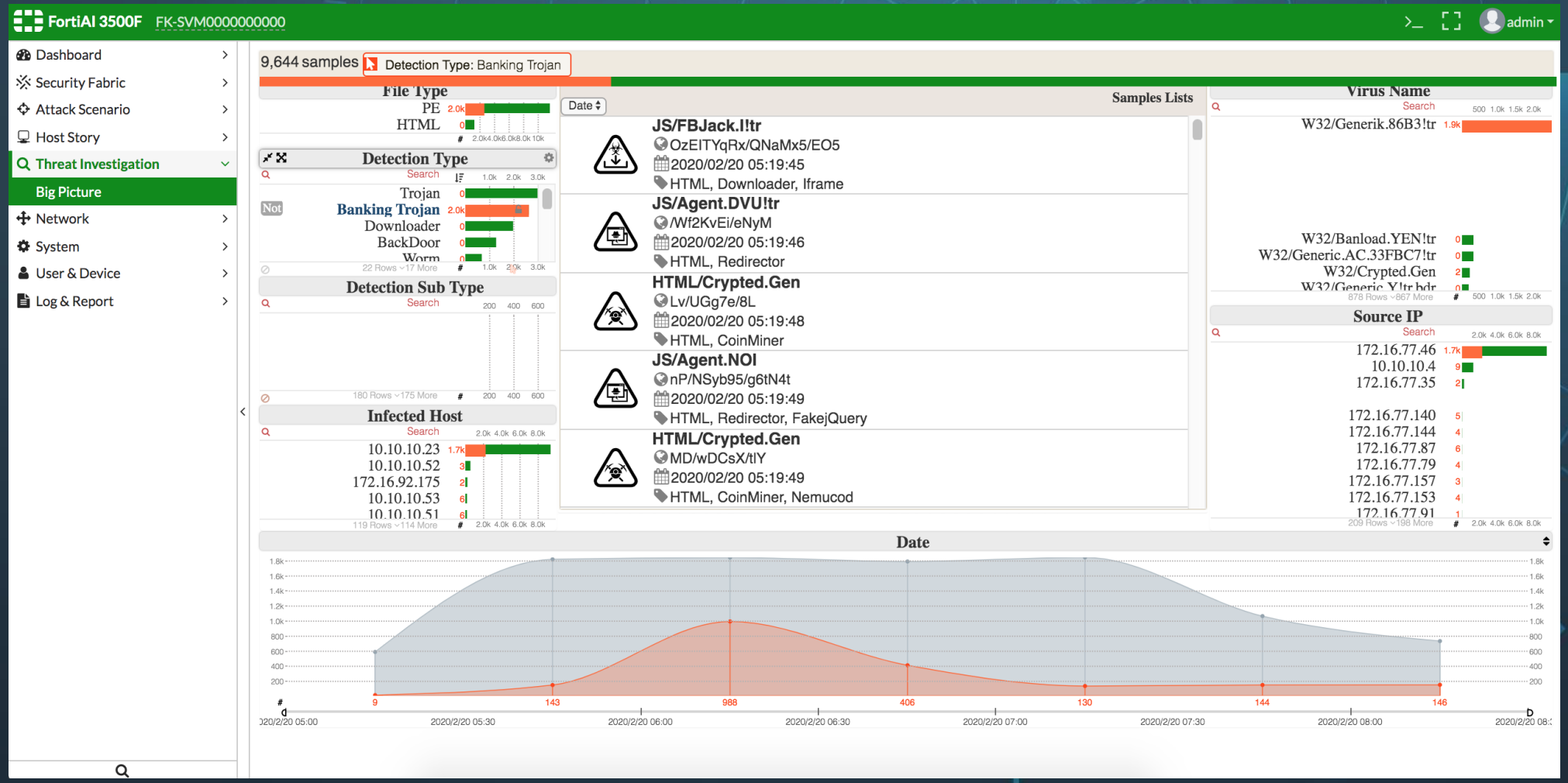


FortiAI: Attack Scenario AI engine

Группировка по сценарию атаки



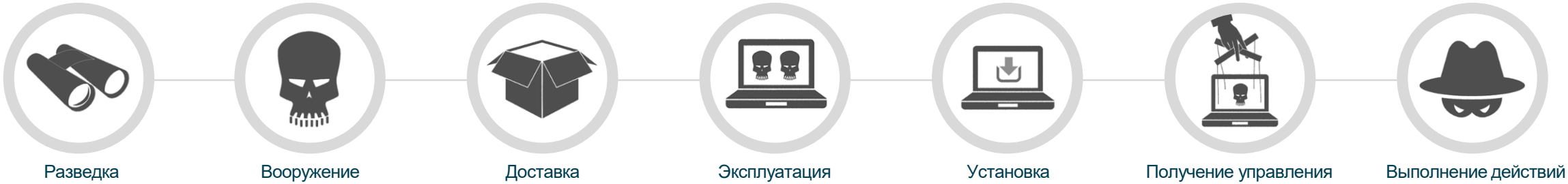
FortiAI: Big picture



FortiDeceptor

Стратегия защиты

Модель Lockheed Martin Cyber Kill-Chain



Стратегия защиты

Где Deception эффективен?

Разведка: FortiDeceptor

- Создание приманки для атакующего
- Увеличение цены и времени атаки
- Проактивно обнаружение разведки и попыток проникновения
- Подробный отчет об атаке
- Уменьшение времени обнаружения атаки

Изучение тактик, техник и процедур

Обнаружение атакующего во время атаки

Доставка и эксплуатация **Приманки**

- Раскрытие атак на приманки
- Проведение атак на и с приманок
- ВПО загружаемое на приманки
- Посещенное веб сайты

- Обычные пользователи не должны знать о существовании приманок
- Движок анти-эксплоит: отслеживание активности в реальном времени
- Группировка по различным признакам

Выявление целей атакующего

Выполнение действий: эксфильтрация

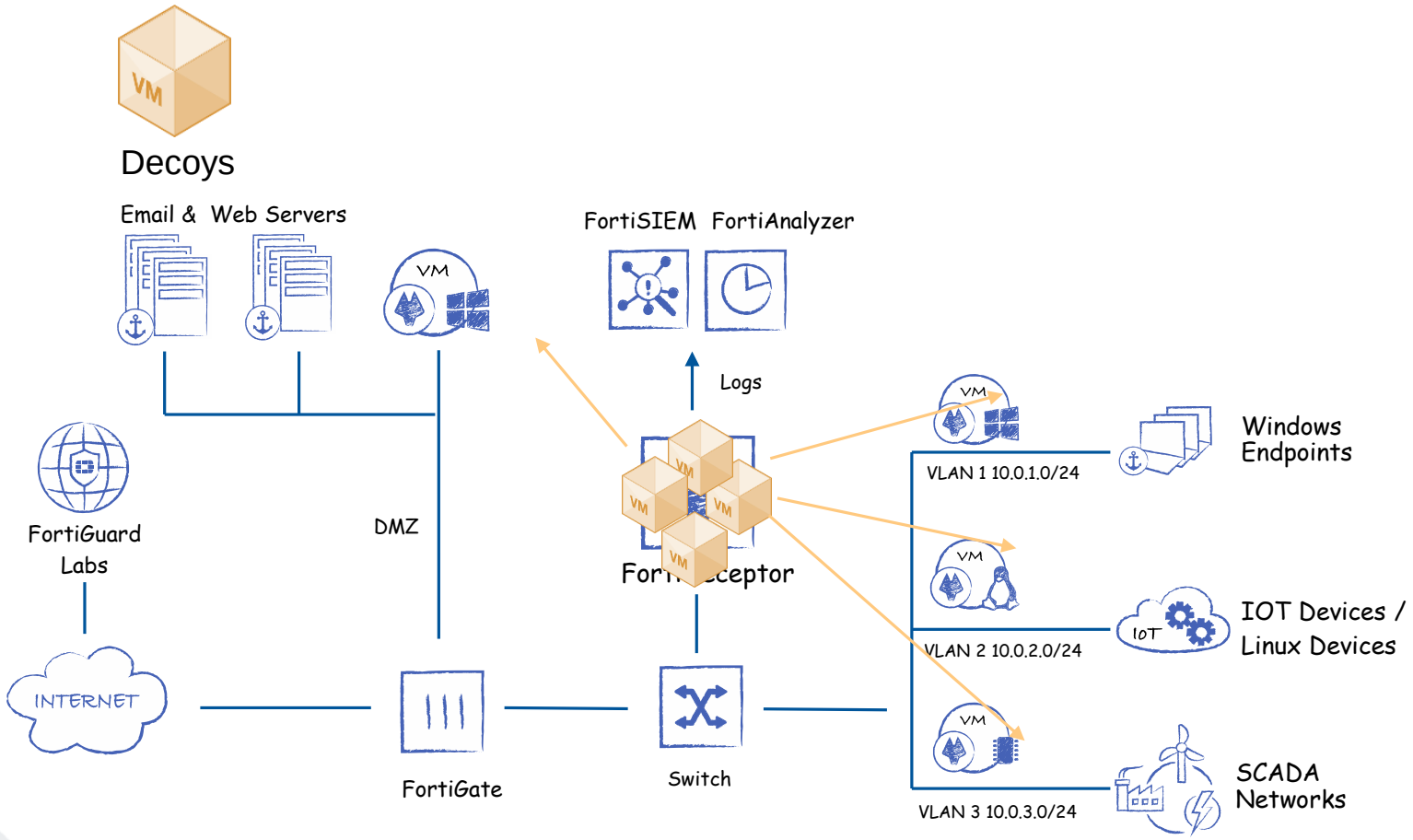
- Различный контент на приманках (файловый или sql серверы)
- Понимание цели атакующего (напр. эксфильтрация данных, сканирование сети)
- Автоматический карантин атакующего (FortiGate)
- Создание нотификации

FortiDeceptor

Архитектура, развертывание, сервисы

FortiDeceptor: развертывание

Ввод в заблуждение | выявление | устранение



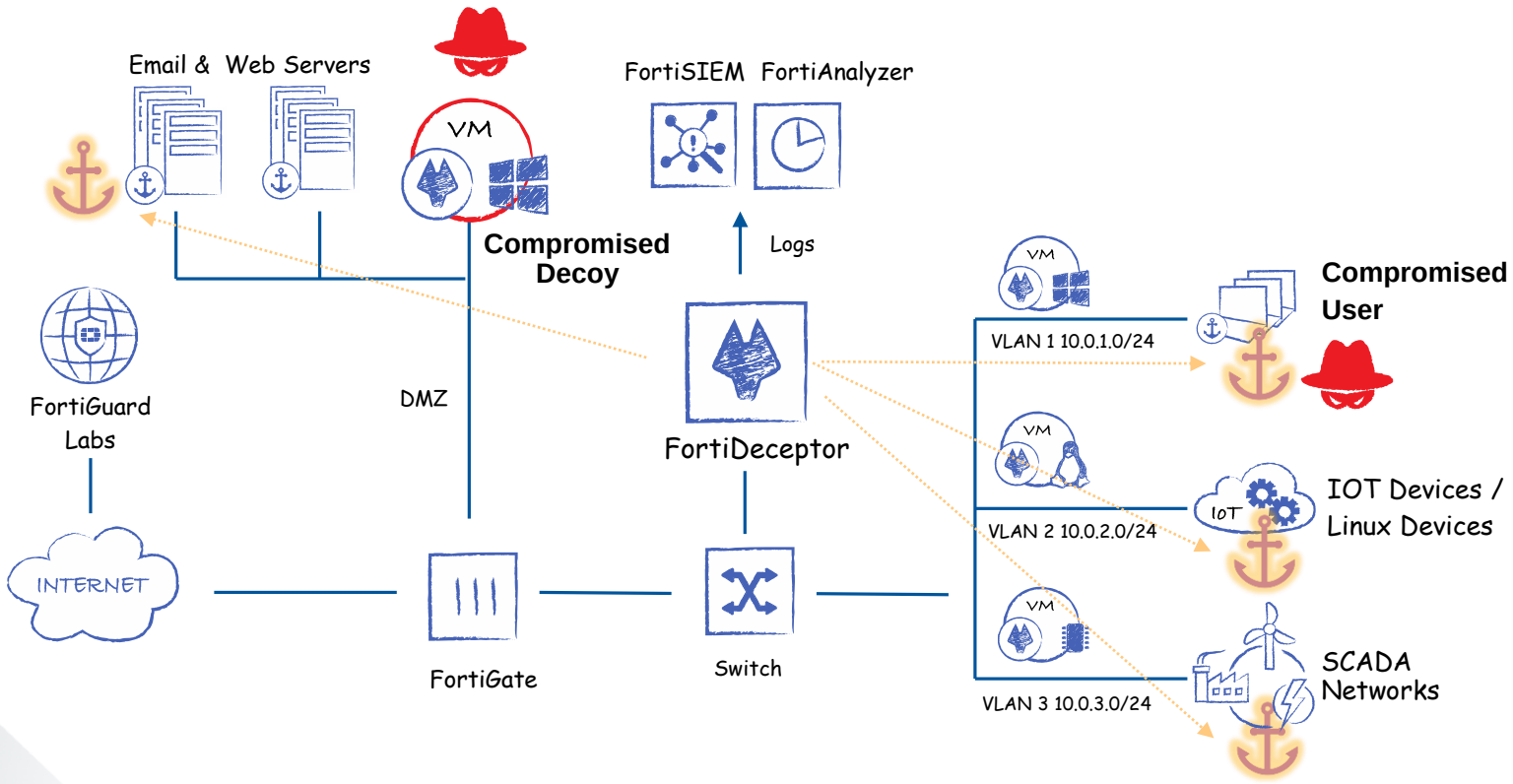
Decoys

Ввести в заблуждение развернув приманки (decoys):

- Windows 7 /10 (Standard / Custom BYOL)
- Windows Server 2016/2019
- Linux
- SCADA
- SSLVPN

FortiDeceptor: развертывание

Ввод в заблуждение | выявление | устранение



Выявить атакующего:

- Развернув сервисы (lure) на приманке
  - RDP/SMB/SQL* (Windows)
  - SSH/SAMBA* (Linux)
  - MODBUS / S7-200 / IPMI etc
  - SSLVPN bookmarks

- Разместив токены на:
  - PC / серверах
  - Работают как ‘закладки’, ведущие на приманку
  - Обнаружение компрометации рабочих станций и серверов

* Available v3.2 GA May 20

FortiDeceptor: приманки

Windows Decoy

- Windows 7
- Windows 10
- Windows Server 2016
- Windows Server 2019

Lures Available

- SMB
- RDP
- TCP Port Listener
- SQL (server)

VPN Decoy

- FortiOS

Lures Available

- SSLVPN

Linux Decoy

- Ubuntu

Lures Available

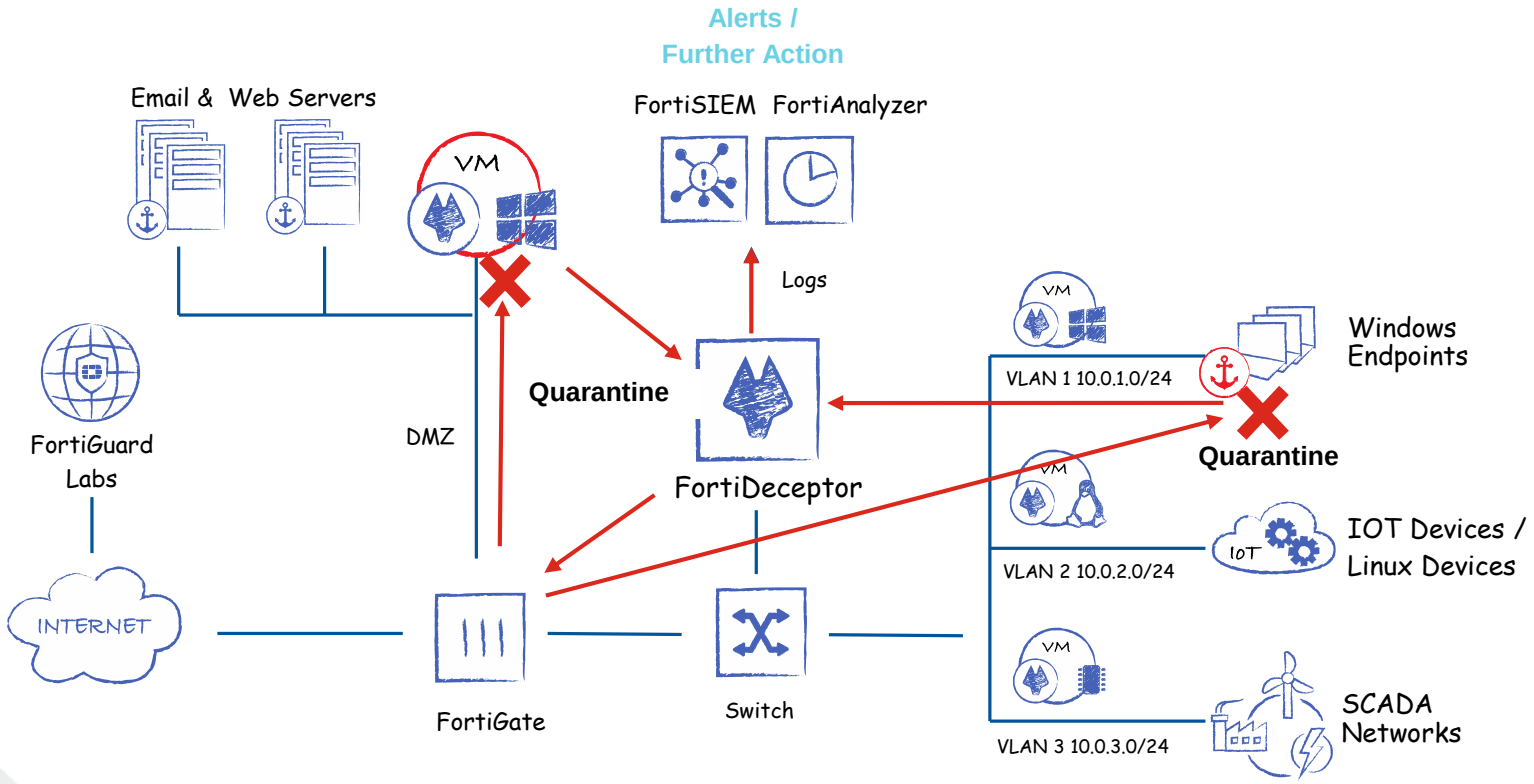
- SSH
- SAMBA

SCADA Decoy & Lures

- HTTP
- FTP
- TFTP
- MODBUS
- S7COMM
- BACNET
- IPMI
- TRIXONEX
- GUARDIAN-AST
- IEC 60870-5-104

FortiDeceptor: развертывание

Ввод в заблуждение | выявление | устранение



Устранение атакующего:

- Автоматический/ручной карантин(средствами FortiGates)
- Отправка событий в FortiAnalyzer / FortiSIEM
- Поддержка syslog и cef
- Расследование!

Обнаружение атакующего

В реальном времени: сервисы FortiDeceptor

IDS 

- Создан на основе сервиса FortiGuard IPS
- Обнаруживает атаки HA и OT приманки

Антивирус 

- Сканирование загруженных файлов
- PCAP

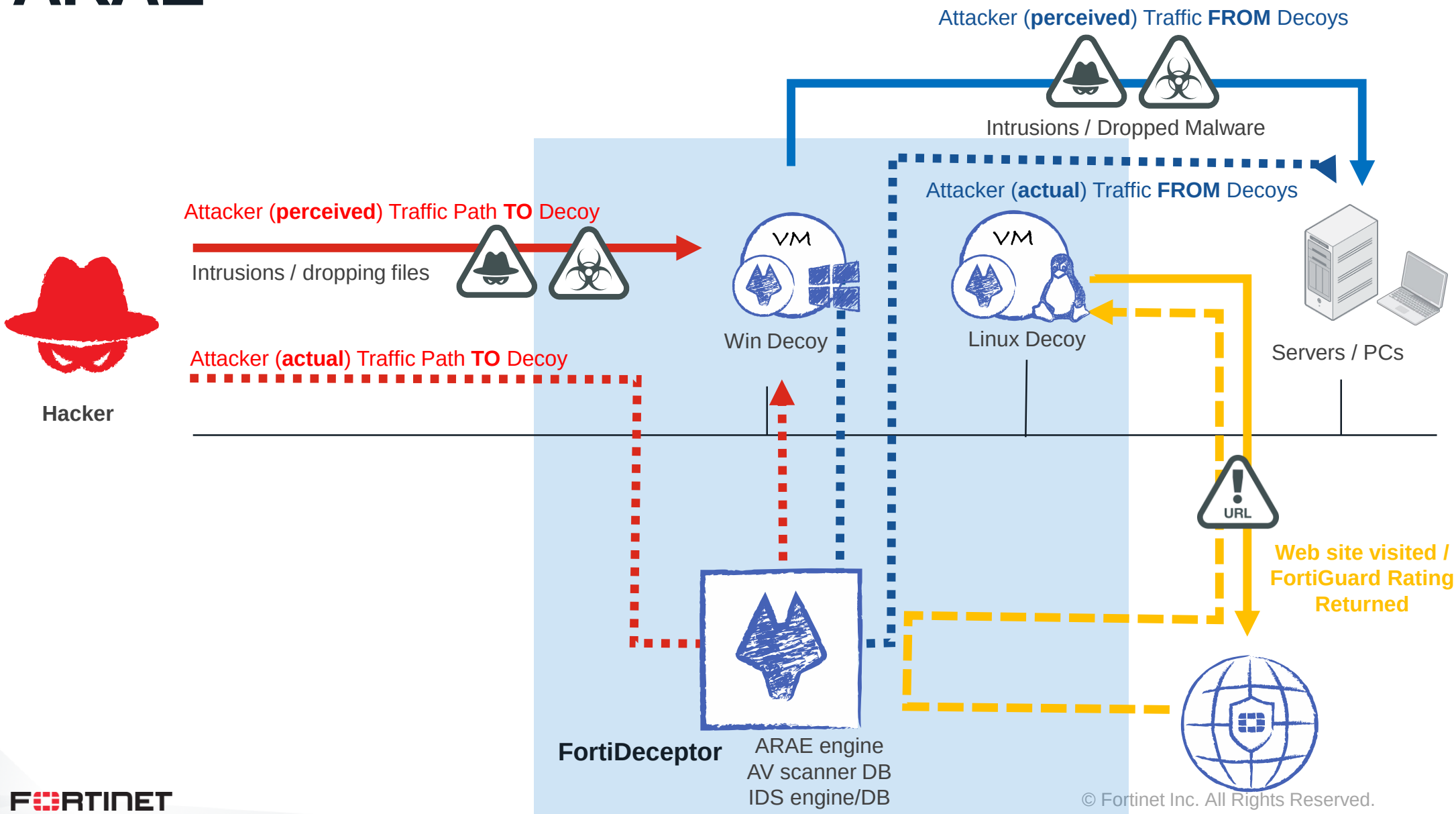
Веб-фильтр 

- Создан на основе движка FortiGuard Web Filtering
- Оценивает сайты, посещенные атакующим с приманок

Anti-Reconnaissance Anti-Exploit Engine (ARAE)

- Отслеживание действий атакующего в реальном времени

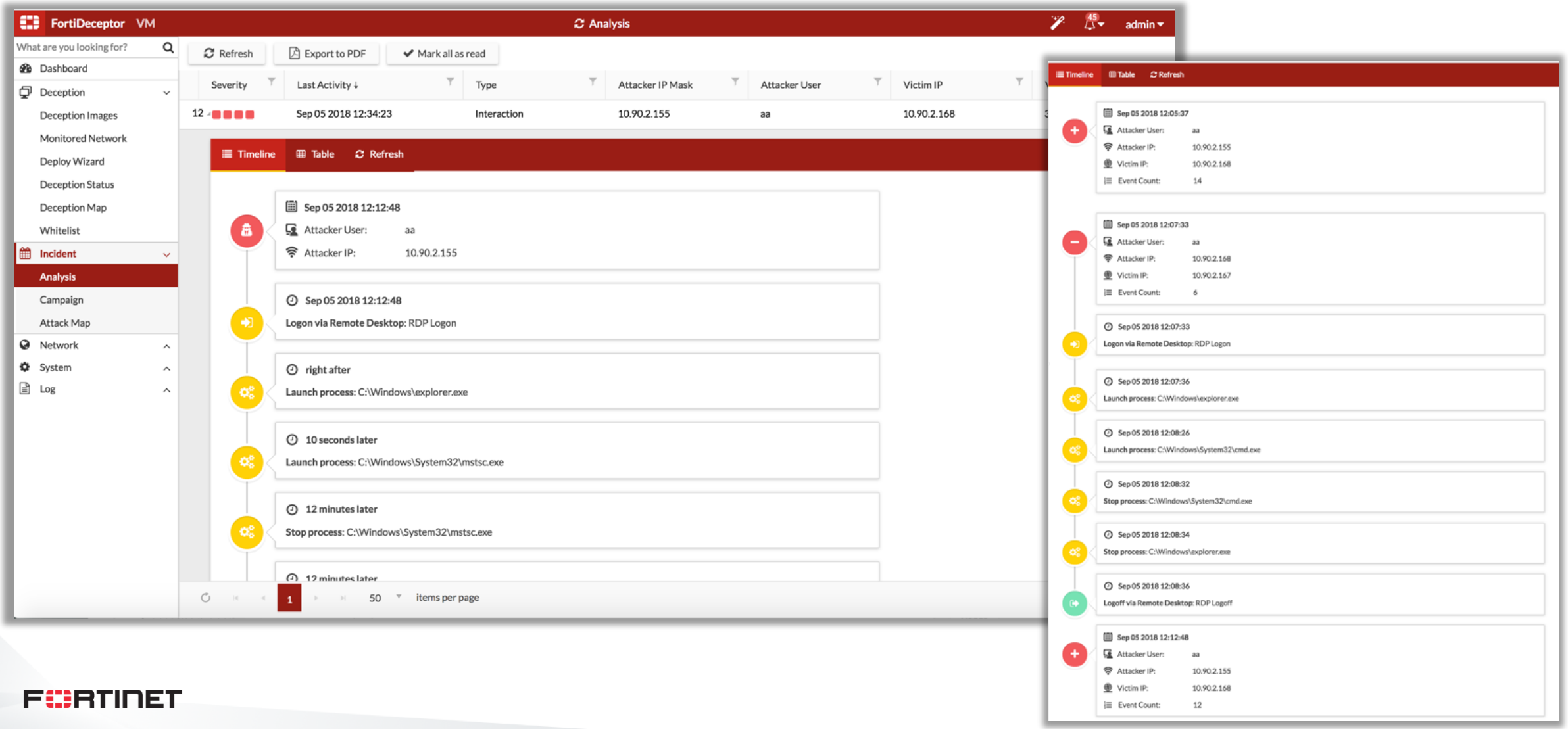
ARAE



FortiDeceptor

Интерфейс

Incident Analysis & Campaign

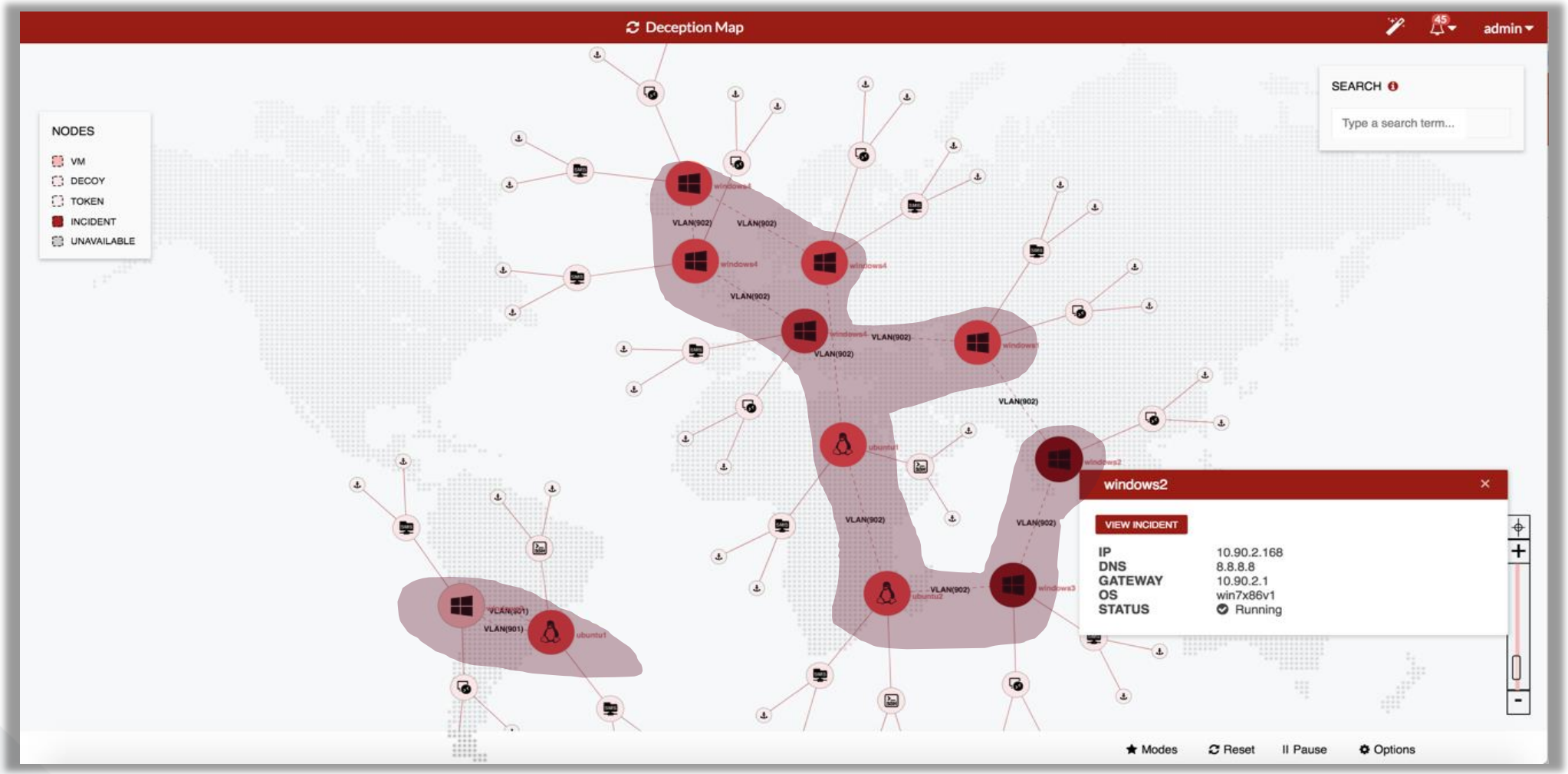


SOC Display

Анимированная карта атак

SOC Display

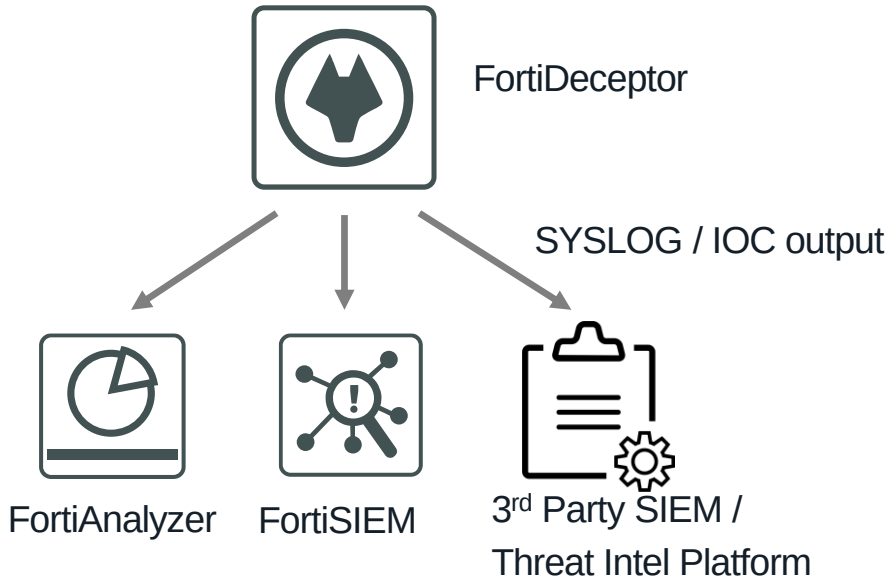
Карта приманок



FortiAnalyzer Integration

Fabric ADOM

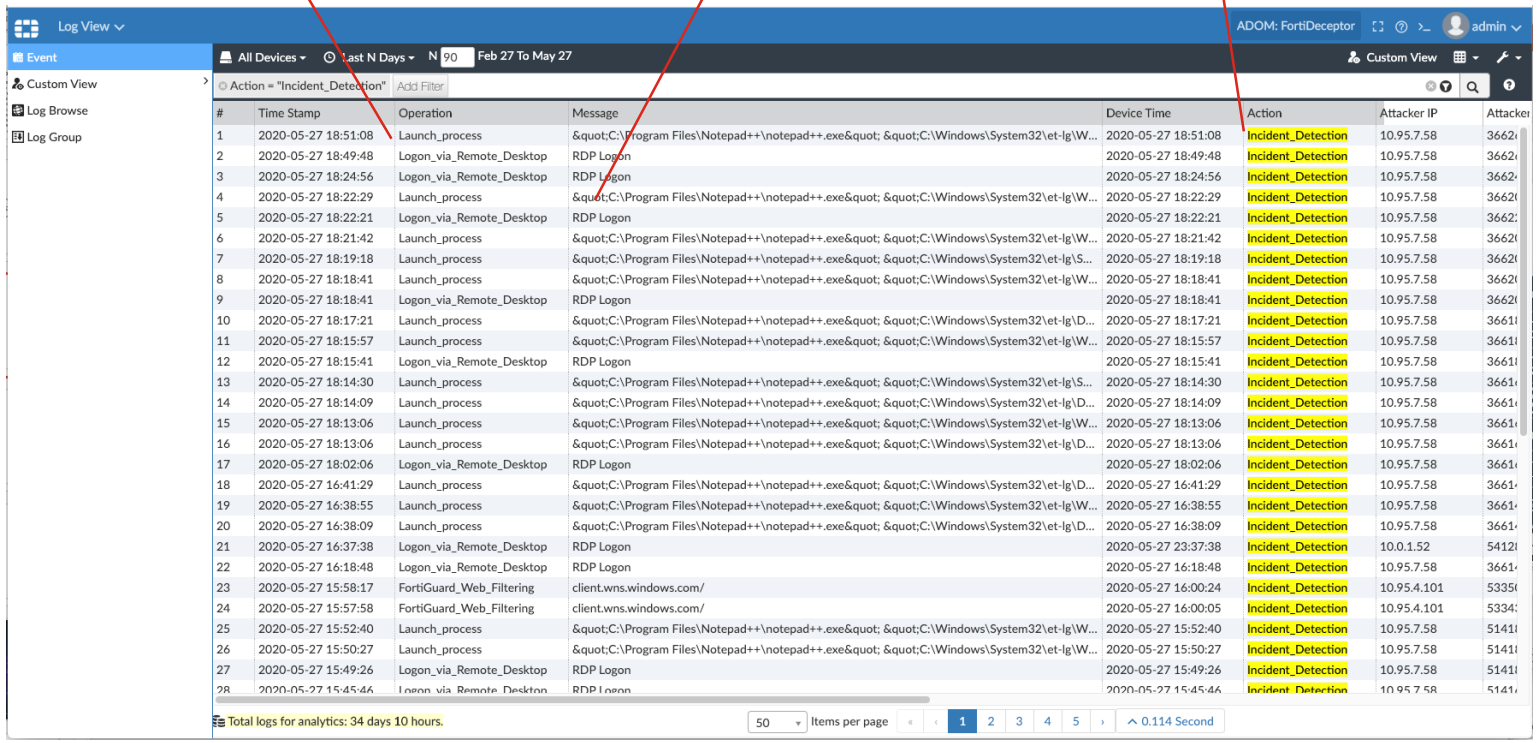
- Интеграция с FortiAnalyzer
- Интеграция с FortiSIEM



Атакующий запустил процесс

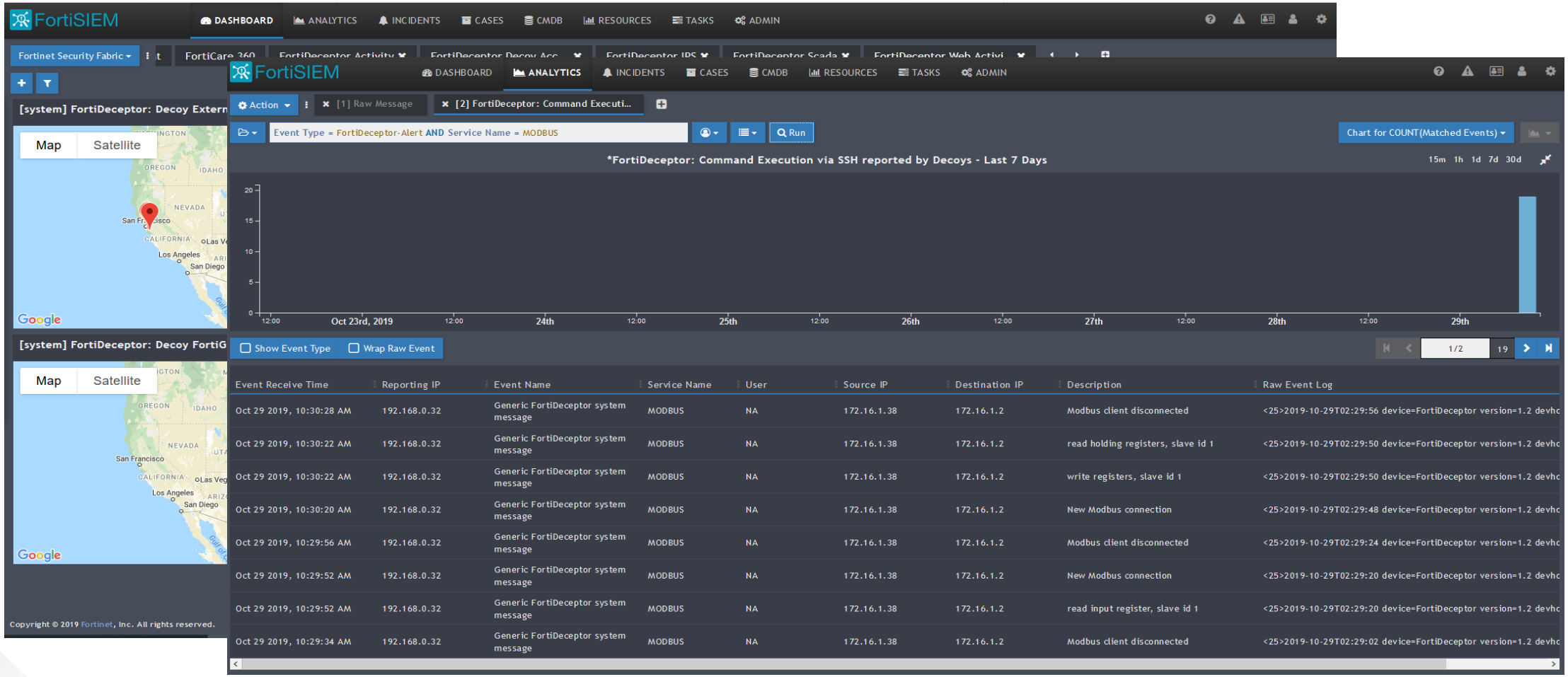
Атакующий подключился по RDP

Обнаружен инцидент



FortiSIEM

FSM v5.2.6+



FORTINET

FortiInsight

Advanced User Entity Behavior Analytics

User Entity Behavior Analytics

Ландшафт угроз

Слепая зона в безопаности

Инсайдер

Подходы к реализации UEBA

На основе сетевых данных

На основе данных систем логирования

На основе событий на рабочих станциях

FortiInsight

Обнаружение и оповещение об инцидентах

Обнаружение

Телеметрия

Реагирование на инциденты

Оповещение

FortiInsight

Компоненты

Архитектура системы

Агент/сервер

Агент для ОС Windows

- Не требует конфигурации
- Шифрованное соединение (TLS 1.2)
- Push развертывание (средствами администрирования ОС)

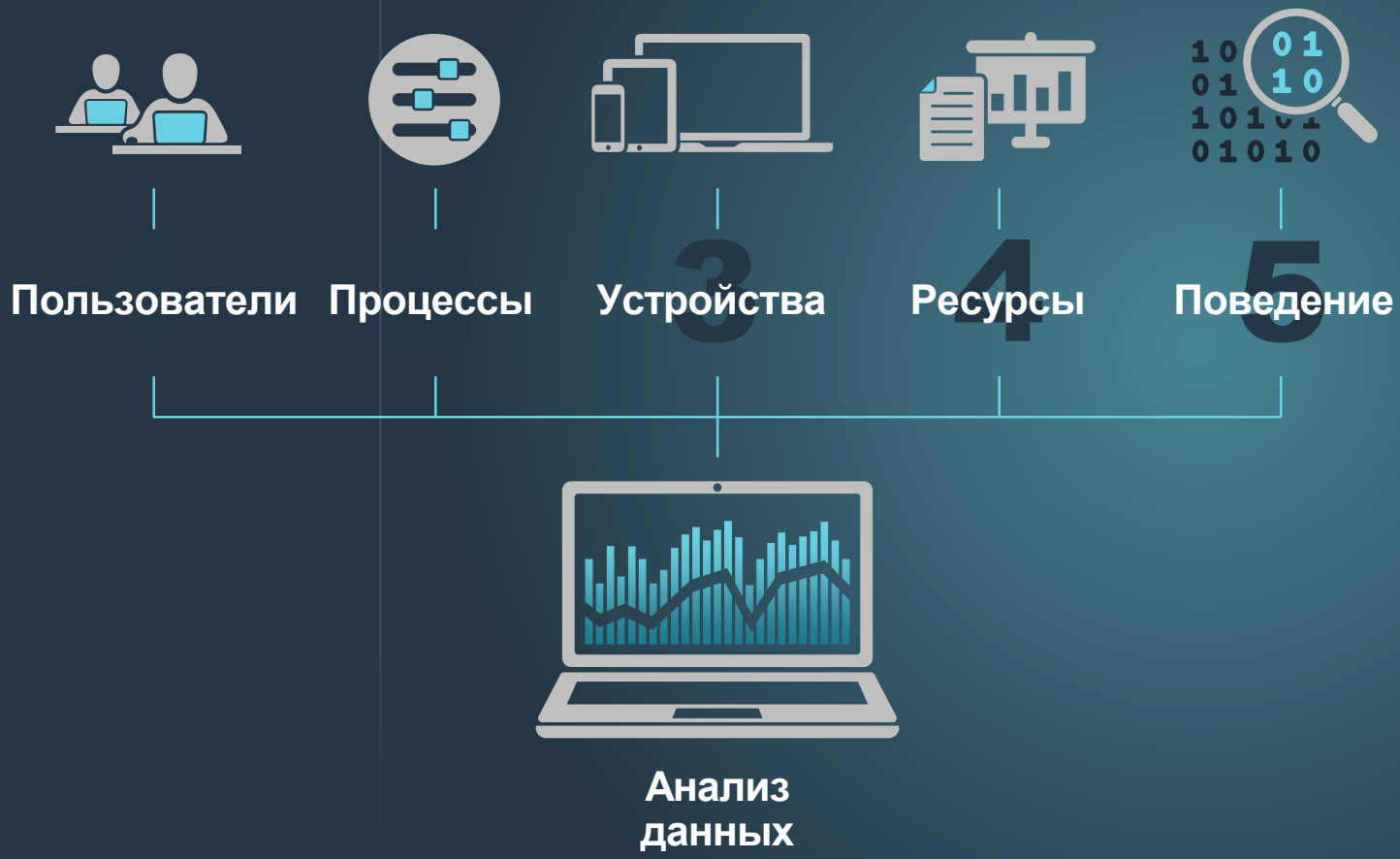
Система развернута в AWS

Хранение, представление, аналитика

- Обнаружение на основе правил
- Обнаружение с помощью машинного обучения
- Поиск угроз

5-факторная модель телеметрии

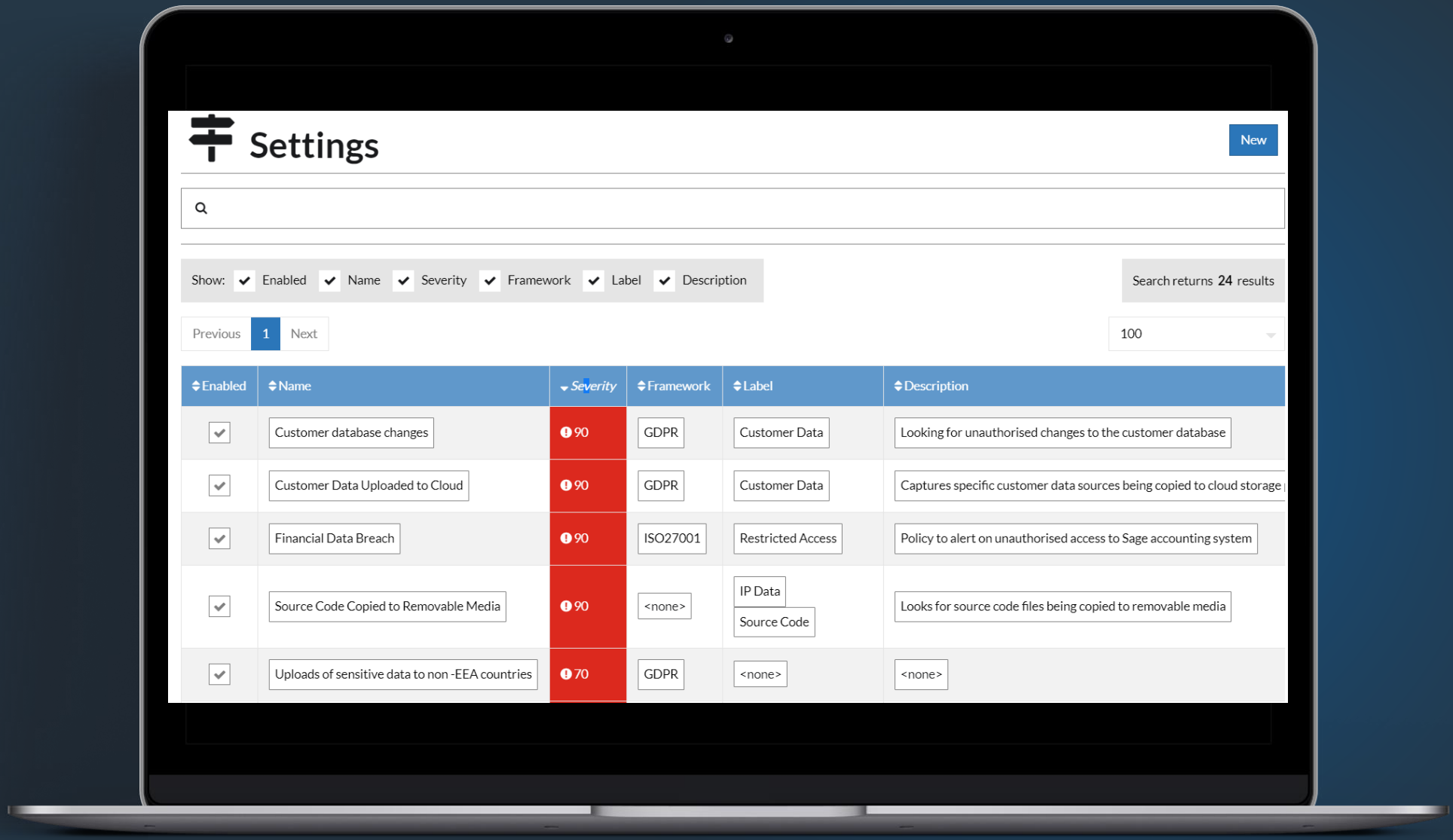
Создана для обнаружения инсайдера



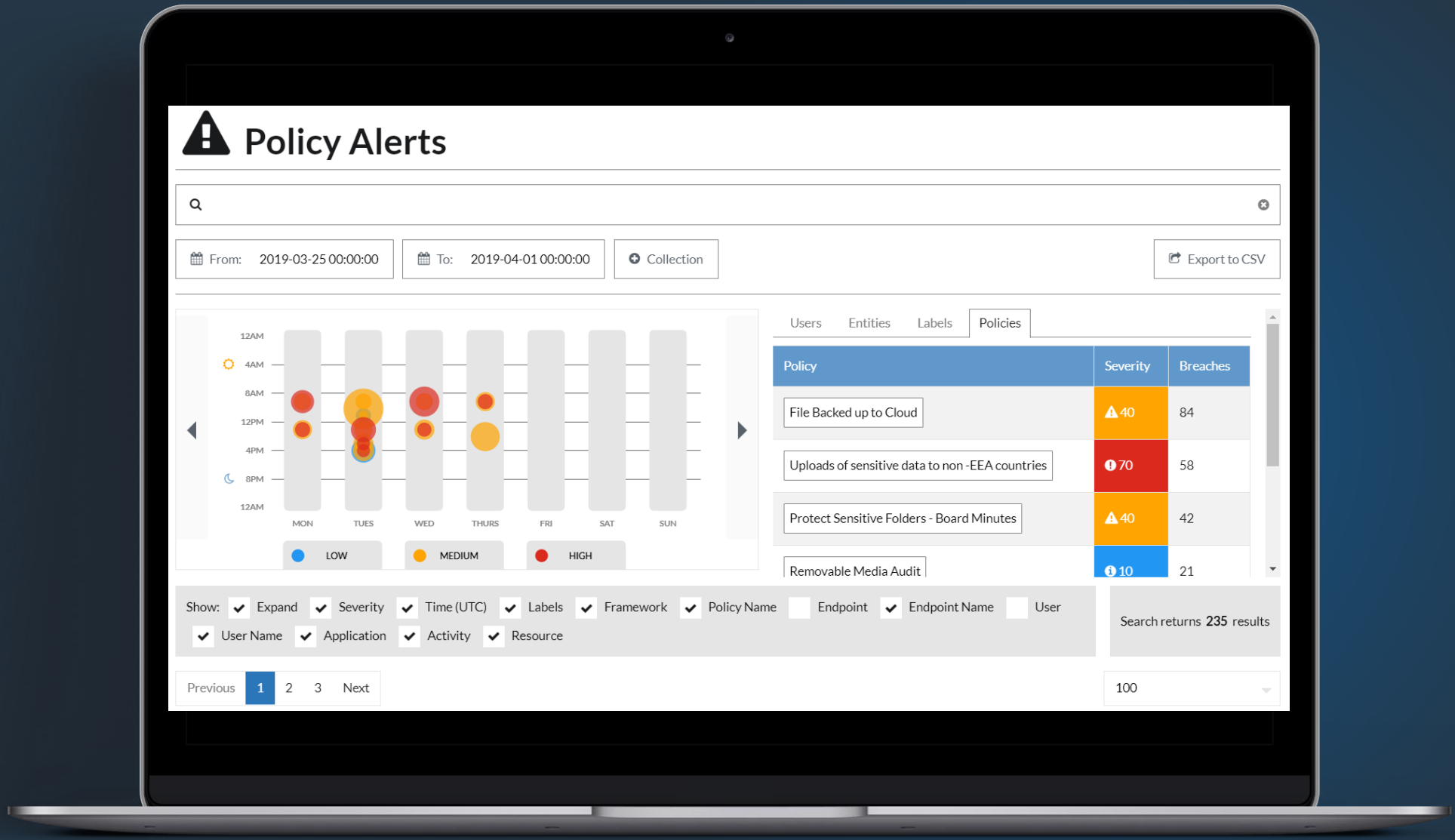
FortiInsight

Аналитика

Политики: обнаружение прогнозируемых угроз



Политики: сработки



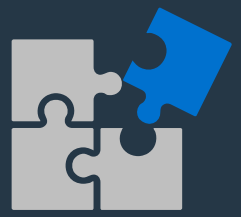
Машинное обучение

Обнаружение аномалий

Машинное обучение

- Движок машинного обучения FortiInsight позволяет обнаруживать аномалии в поведении пользователей

Создание профиля



- Создает профиль «нормального» поведения пользователя

Легкая настройка

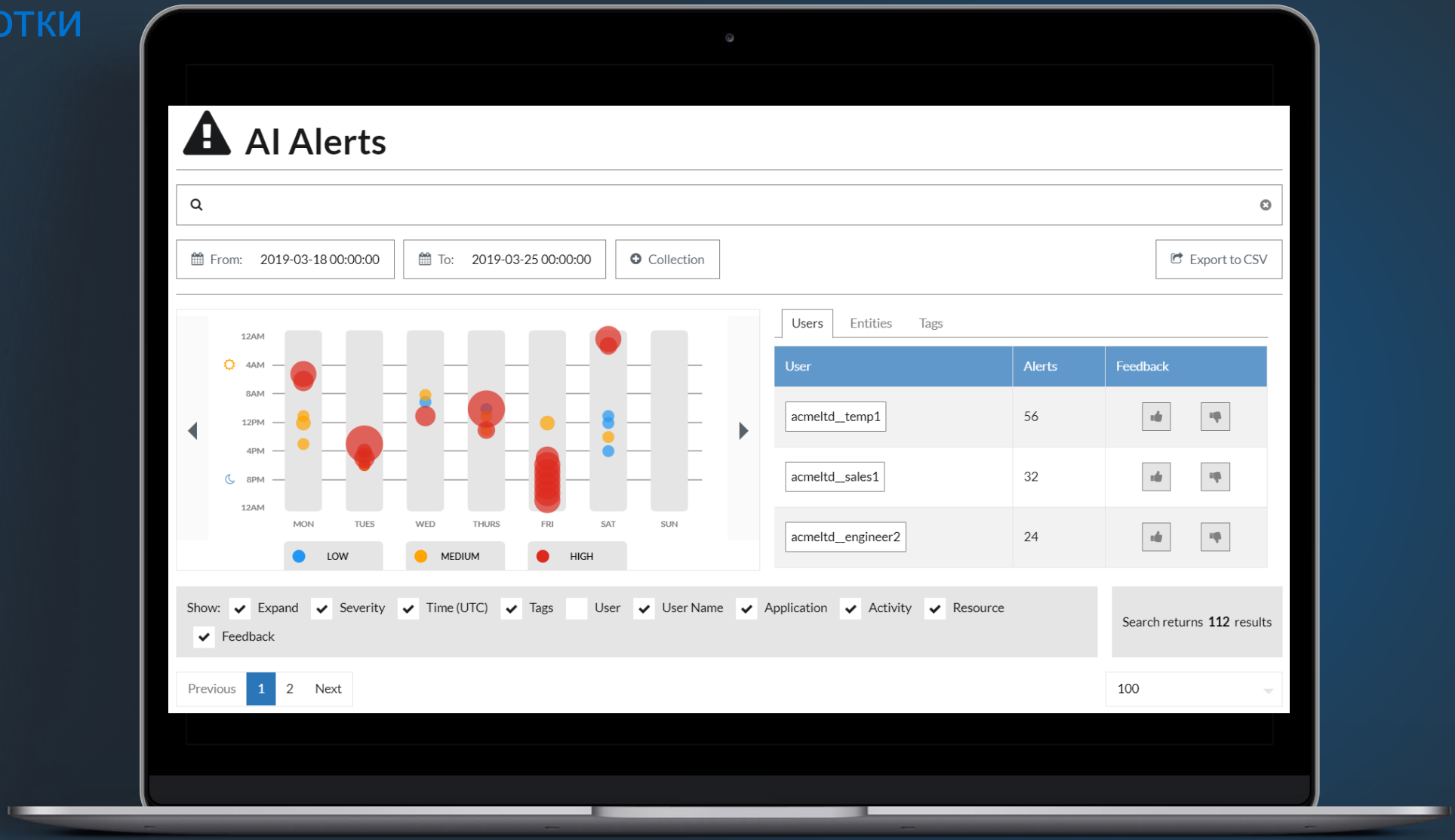
- Формирует профиль пользователя без каких-либо дополнительных настроек

Отслеживание действий пользователей

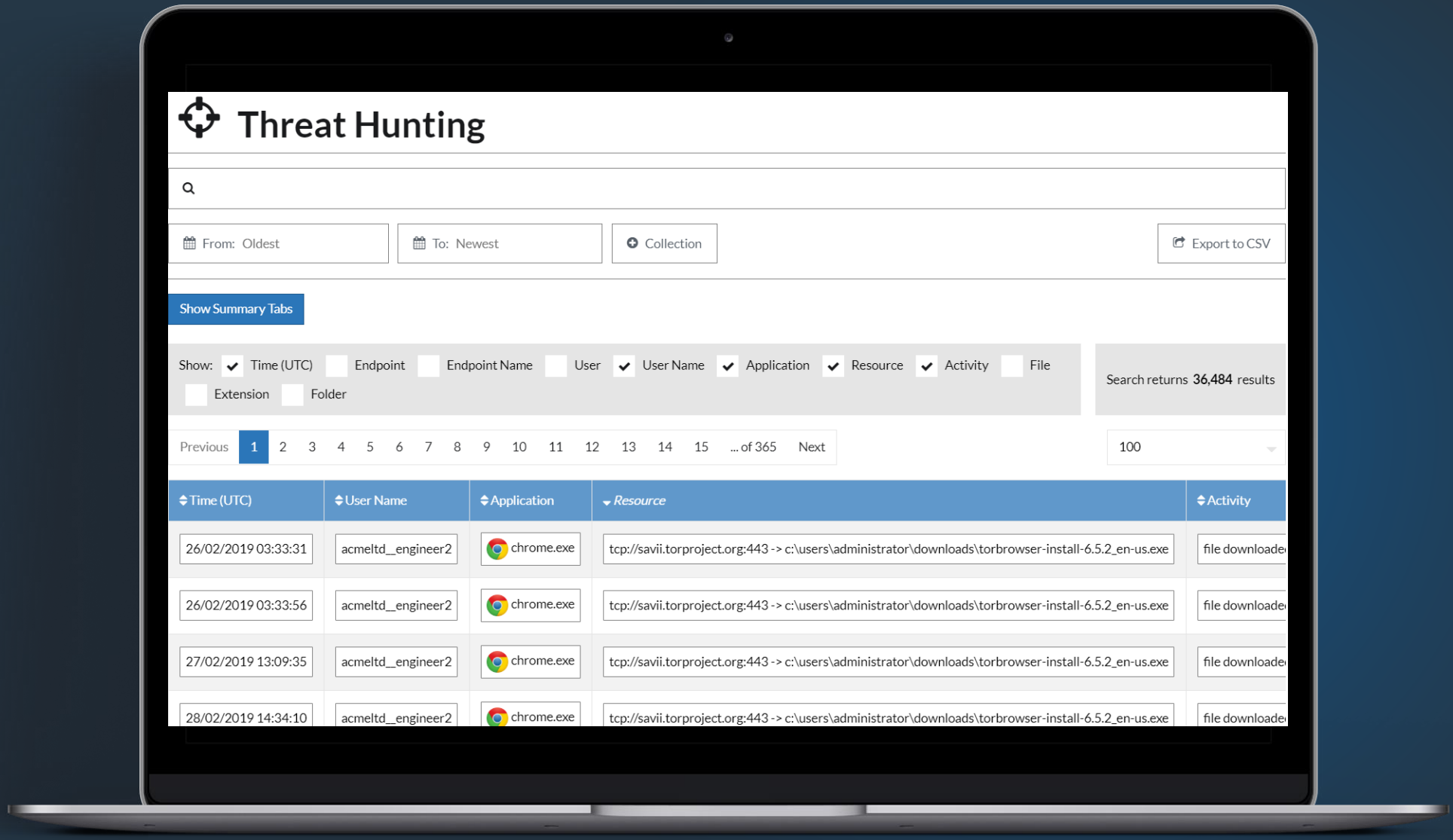
- Использует аналитику поведения пользователей для обнаружения угроз

Машинное обучение

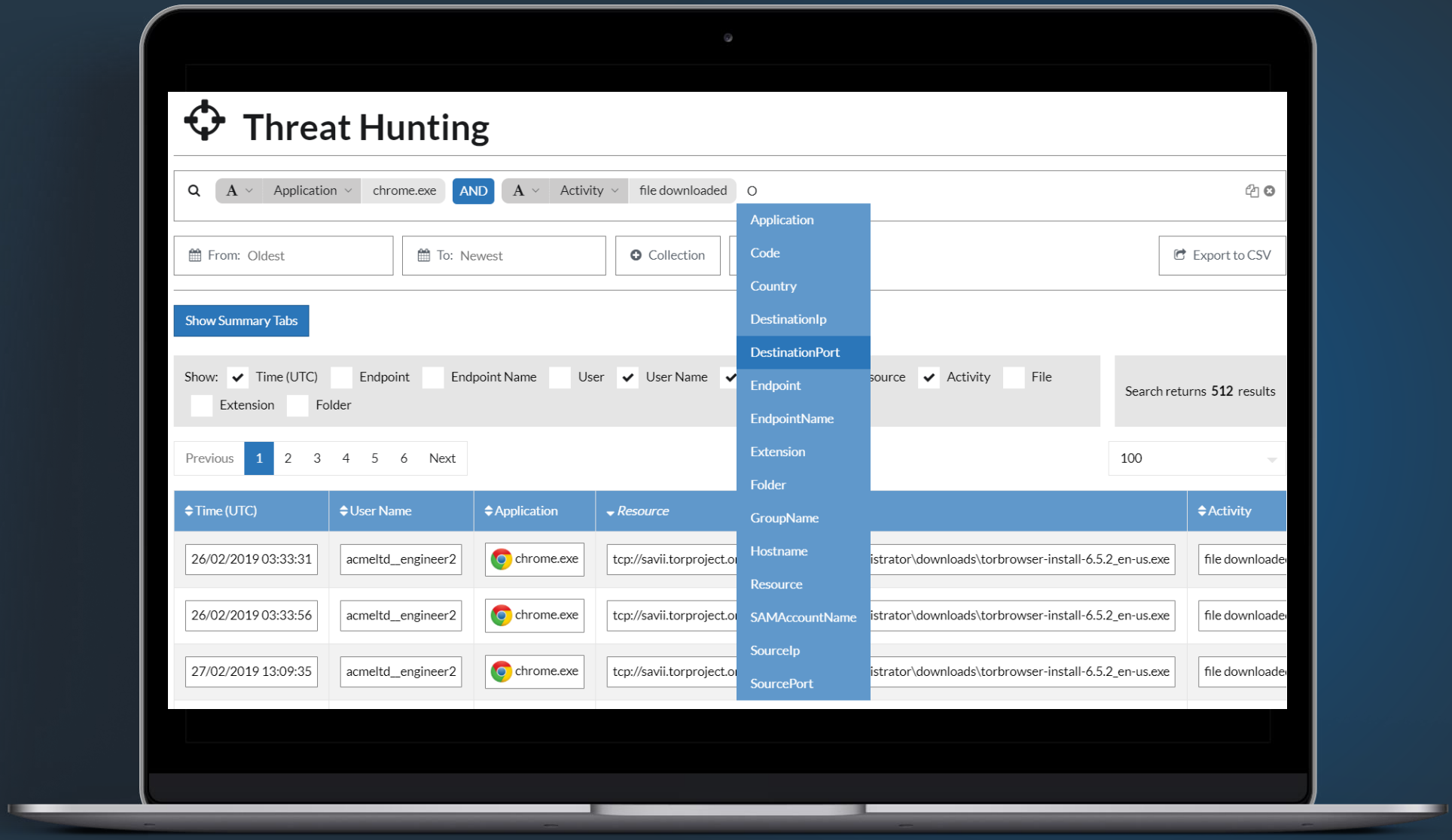
Сработки



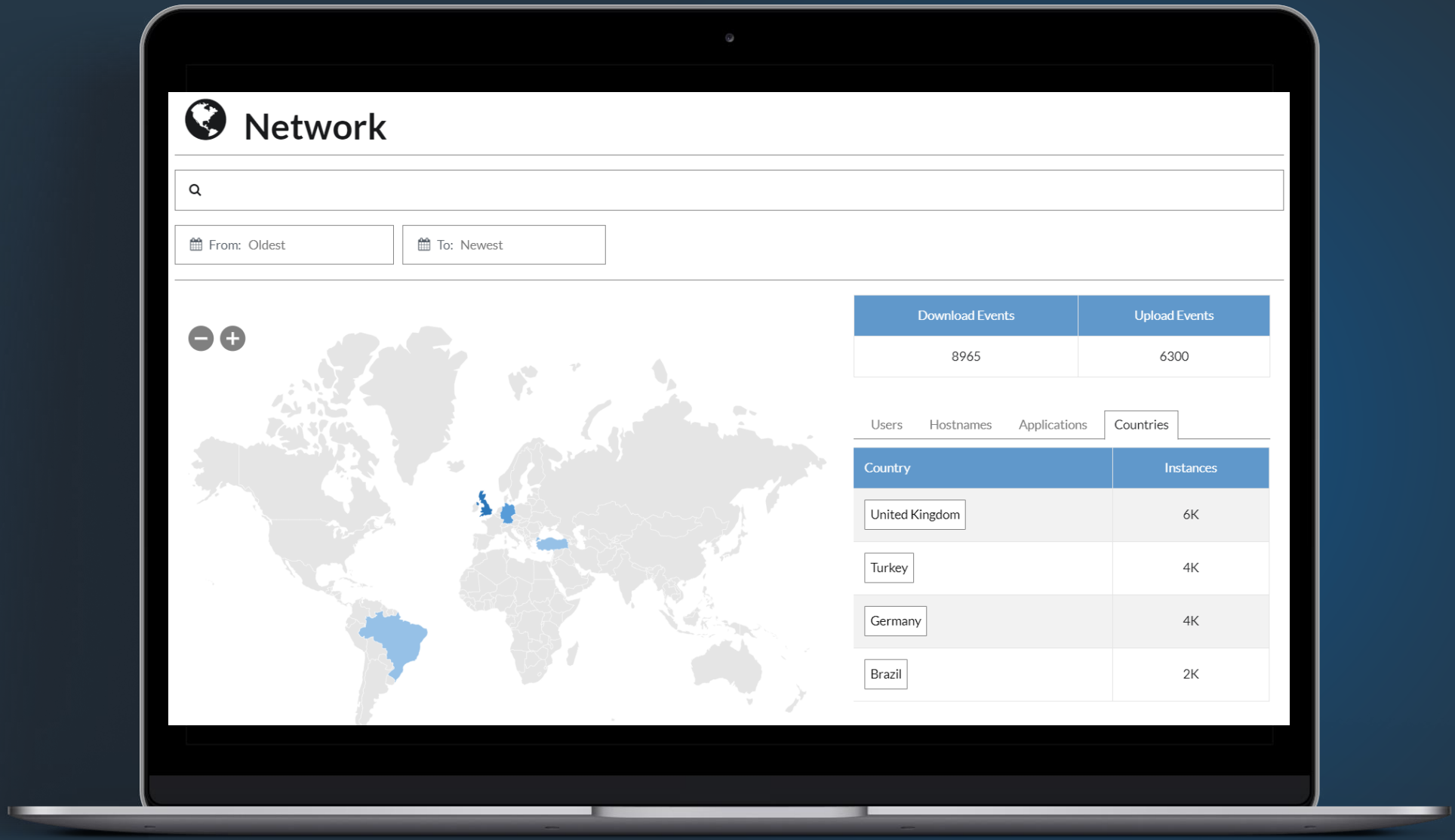
Поиск угроз



Поиск



Анализ передачи данных



Видимость

Интеграция с Fortinet Security Fabric

FortiSIEM

Интеграция с Fortinet Security Fabric

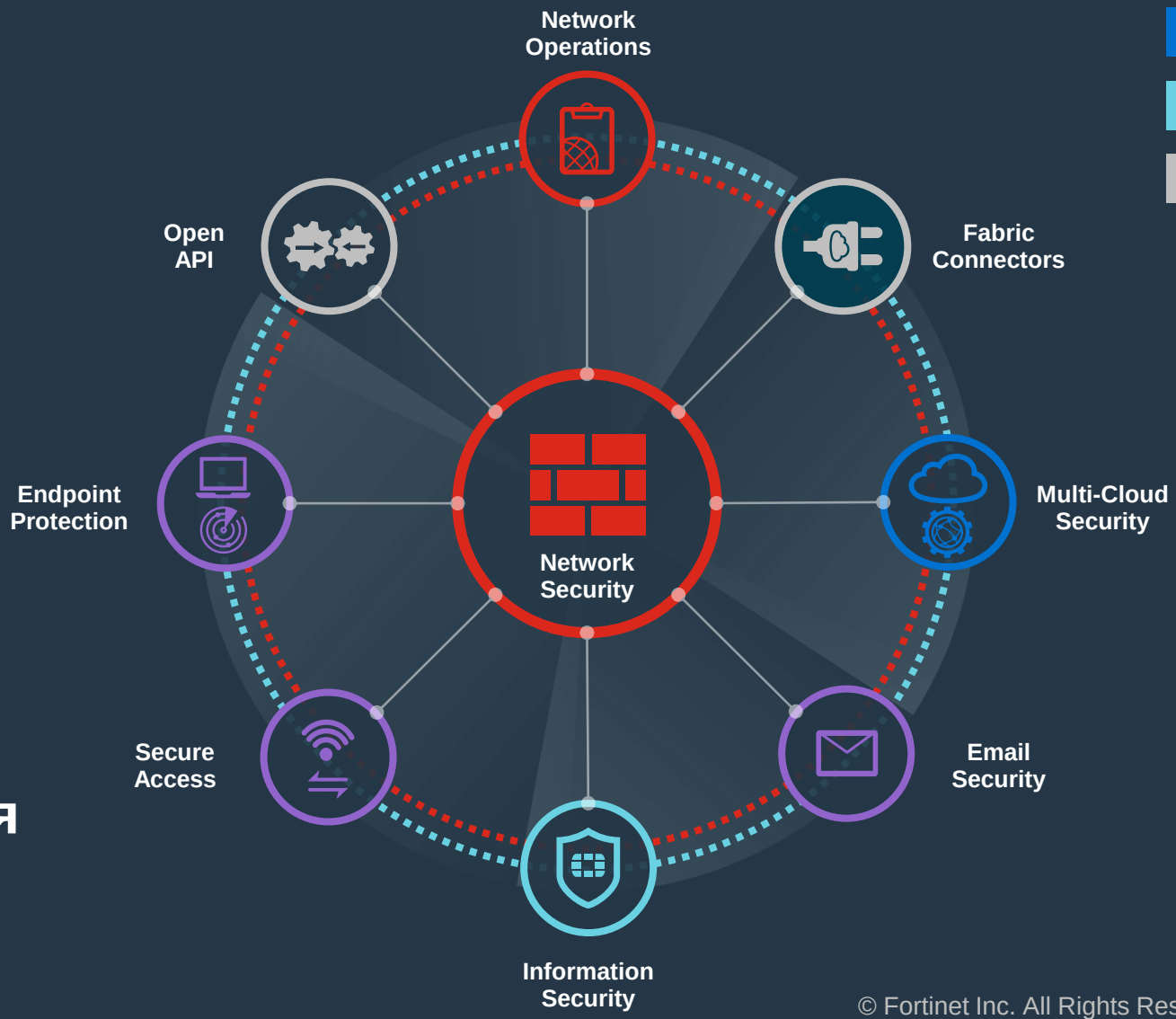
FortiSIEM

- FortiInsight API позволяет передавать в SIEM:
  - Сработки правил
  - Сработки AI

Комлексная
Обеспечение полной видимости поверхности цифровой атаки для лучшего управления рисками ИБ

Интегрированная
Уменьшение сложности сопровождения множества разнородных продуктов

Автоматизированная
Увеличение скорости управления и отклика



cis_se@fortinet.com