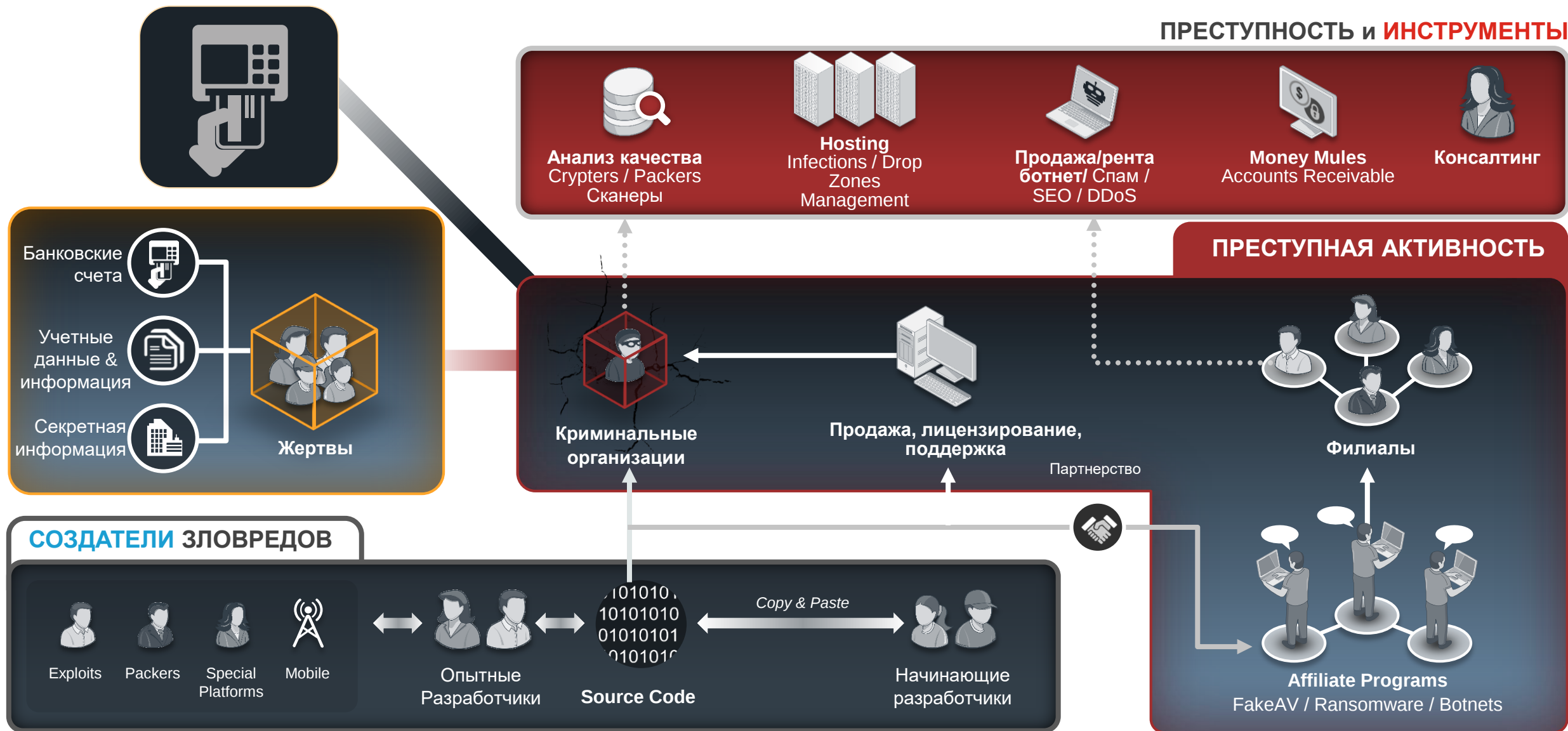




Лабораторія FortiGuard. Технології штучного інтелекту у вивченні та аналізі загроз

Олексій Андріяшин

Организованная киберпреступность



РЫНОК ЭКСПЛОЙТОВ

TheRealDeal

All

I want to order ...

Q Go

[Home](#) / [Exploit Code](#)

Categories

Counterfeits 2

Drugs 1708

Exploit Code 19

FUD Exploits 2

1Day Private Exploits 5

0-Day exploits 12

Government Data 2

Information and Fraud 1043

Other Tools 53

Services 15

Weapons 5

Exchange Rates

Exploit Code

+ Filter

Popularity - This week

Sort



Android WebView 0day RCE

Logger (99.9%) Level 1 (1)

0 37.6896

BTC 37.6896

Buy It Now

FAVORITE



AppleID Password Reset Exploit - Update: *SOLD*

Logger (99.9%) Level 1 (1)

0 37.6896

BTC 37.6896

FAVORITE



ExploitHub

NoobCrypt v2 THE MOST POWERFUL RANSOMWARE ON MARKETS.

USD 310.00

฿ 0.4339

In stock

Vendor Medon [+10] [-3] Level 1 (294)

Class Digital

Delivery Instant Delivery

Quantity: 1

Buy Now

? Question

Report



FortiGuard Labs

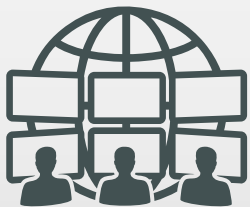
FortiGuard Labs предоставляет сервисы и сведения для защиты в условиях быстро развивающегося ландшафта угроз



- ✓ Актуальные обновления & Проактивная защита
- ✓ Оперативность, масштабируемость и высокая точность
- ✓ Высокие оценки в независимых тестирования и сертификациях



FortiGuard Labs – обзор



215

исследователей
& аналитиков



480,000

часов исследований
за год



Присутствие в



31

стране



Исследования



Разработка



Инновации



**Ответные
меры**



**Распростра-
нение**



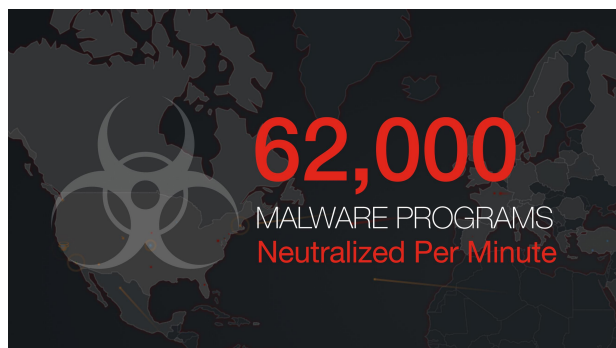
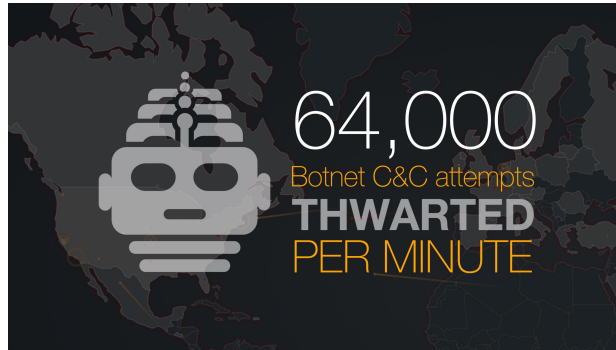
Обучение



100 млрд.

событий безопасности
в день

FortiGuard в цифрах





64,000

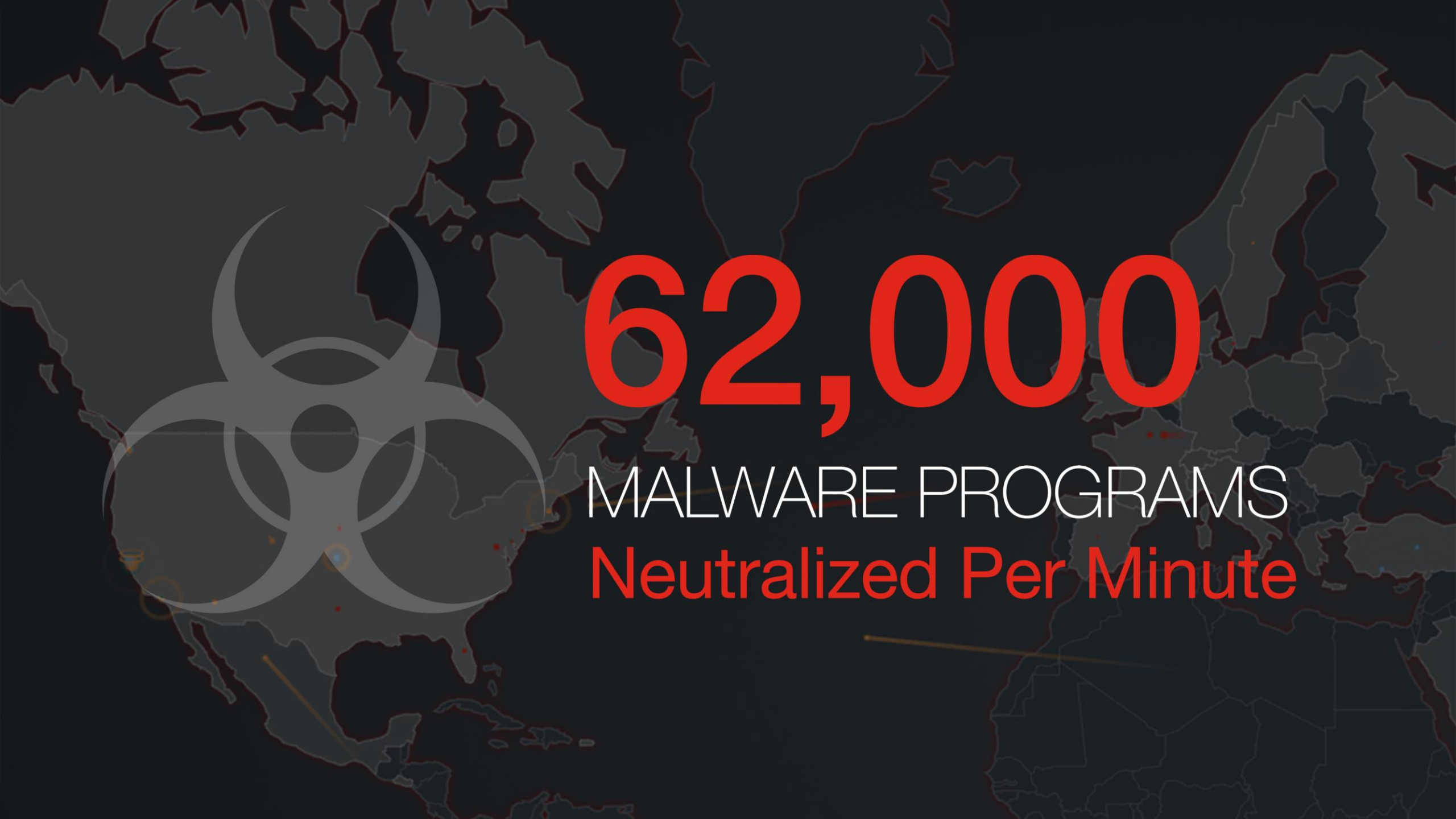
Botnet C&C attempts

THWARTED
PER MINUTE

58



**INTRUSION
PREVENTION**
RULES PER WEEK



62,000

MALWARE PROGRAMS

Neutralized Per Minute

150,000

Malicious Website

ACCESSES

Blocked Per Minute





8,000,000

NETWORK INTRUSION
ATTEMPTS

resisted per minute

490,000 of Threat
HOURS Research
GLOBALLY PER YEAR

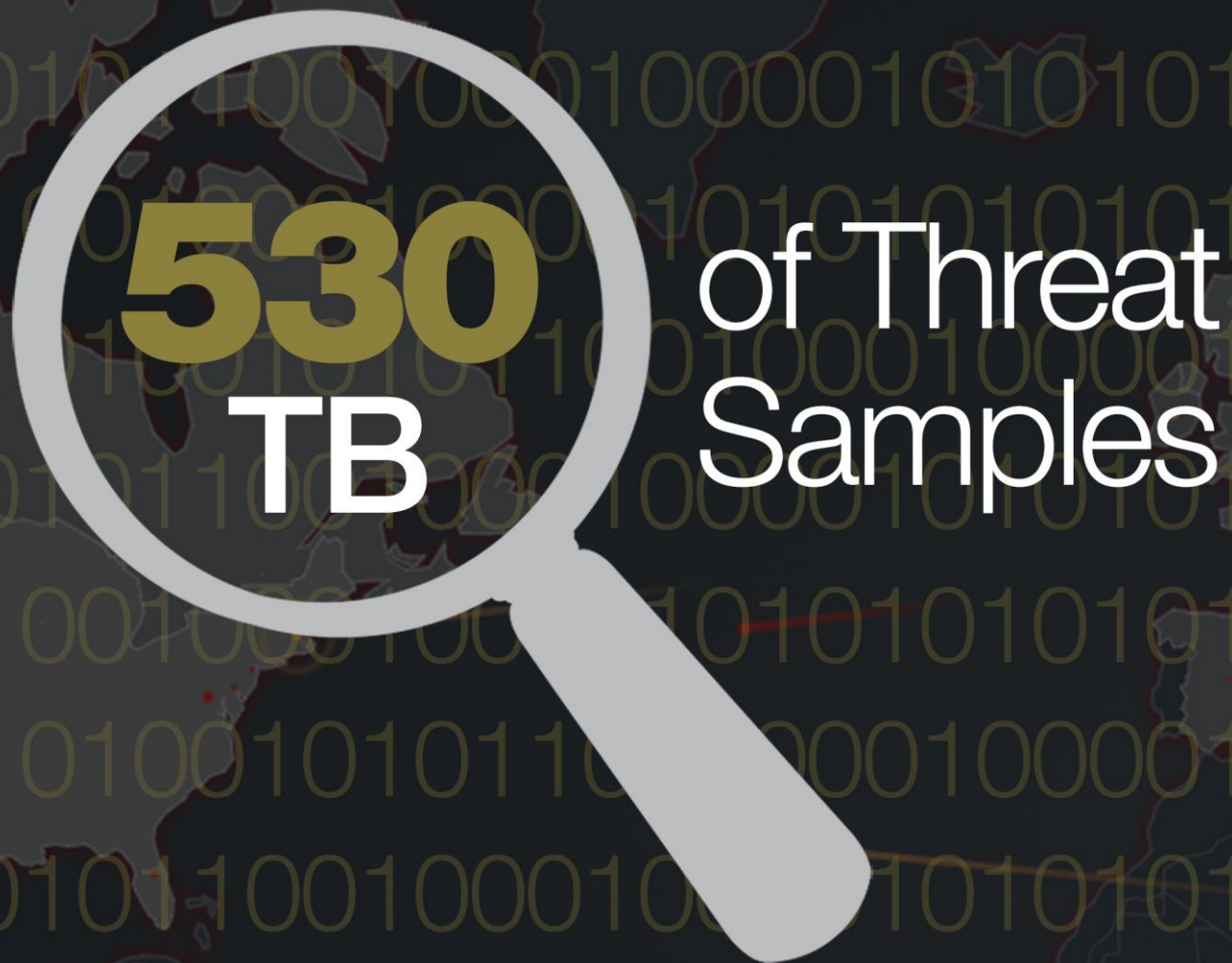


A dark grey world map serves as the background. It features several small, semi-transparent markers: orange circles with dots inside, blue dots, and red dots. Some orange circles have thin lines radiating from them, suggesting a signal or threat. The map is centered on the Atlantic Ocean, showing the Americas to the left and Europe/Africa to the right.

570



ZERO DAY
THREATS DISCOVERED



21,000

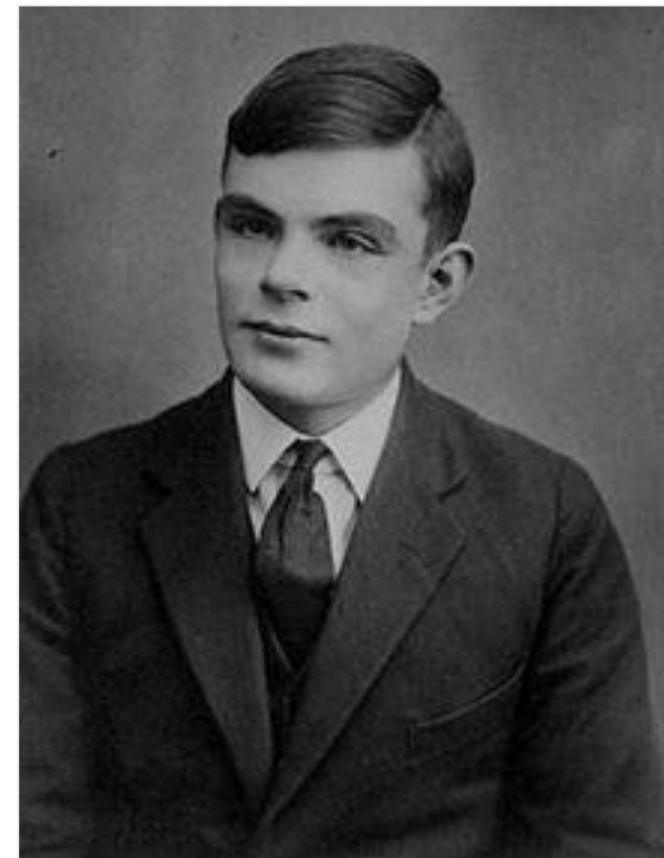
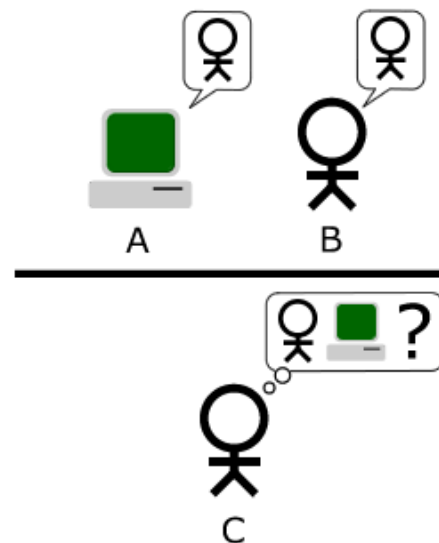


INTRUSION
PREVENTION
RULES

Machine Learning (ML) & Artificial Intelligence (AI)

Могут ли машины мыслить?

- Алан Тьюринг в 1940х годах сравнил принцип обучения машины с развитием младенца
- Описаны первые принципы машинного обучения
- Тест Тьюринга

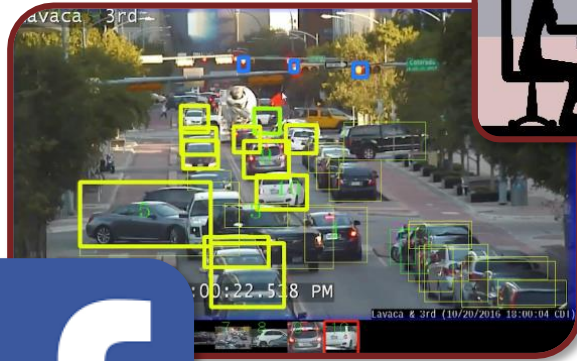
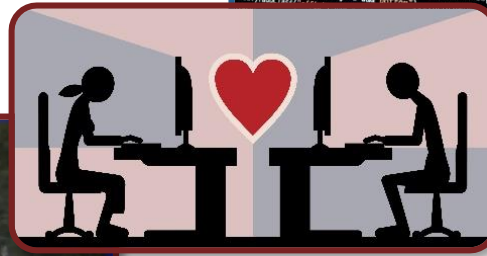


AI & ML – везде и каждый день

Google



NETFLIX



amazon

Типы машинного обучения

Обучение с “учителем”

Обучение по известным шаблонам
Пример: оптическое распознавание
символов

Обучение без “учителя”

Поиск закономерностей, существующих
между объектами.
Пример: обнаружение подозрительного
поведения (аномалий)

Обучение с подкреплением

Взаимодействие со некоторой средой (цепи
Маркова)
Пример: шахматы

Обучение с “учителем”



Обучение без “учителя”



- Определение базовой модели
 - » Типы операций
 - » Суммы операций
 - » Географическое распределение
- Срабатывание, когда транзакции не соответствуют базовой (разрешенной модели)

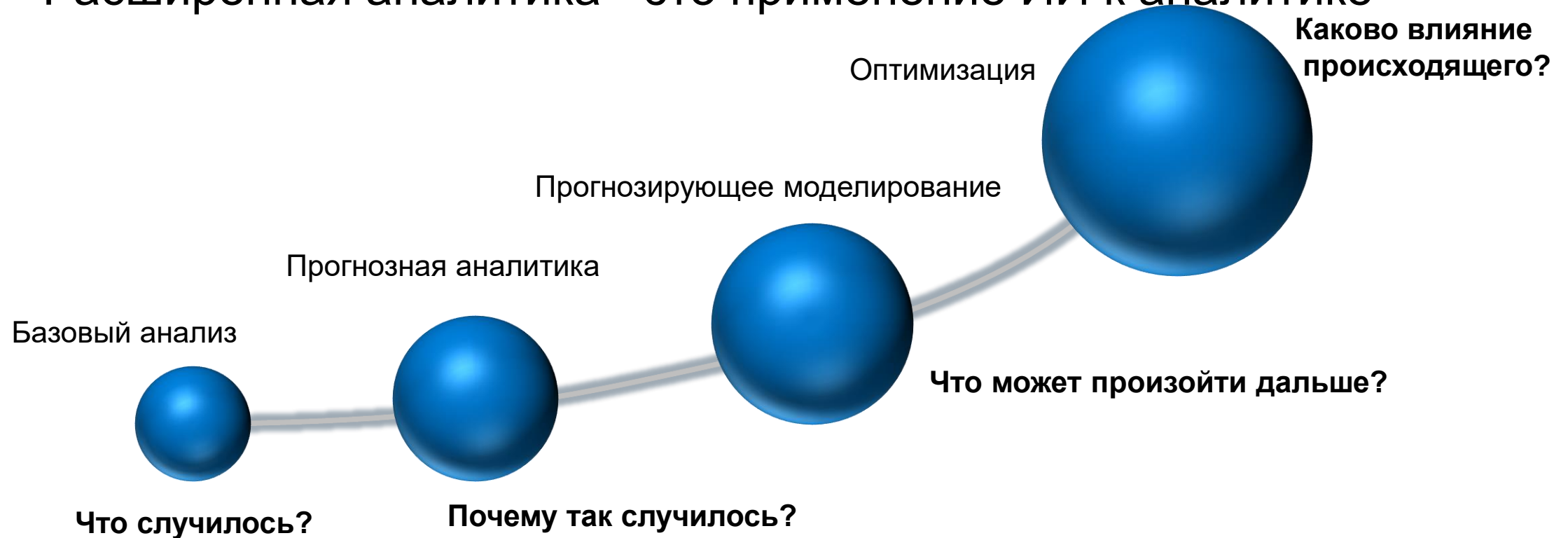
Обучение с подкреплением (вознаграждением)



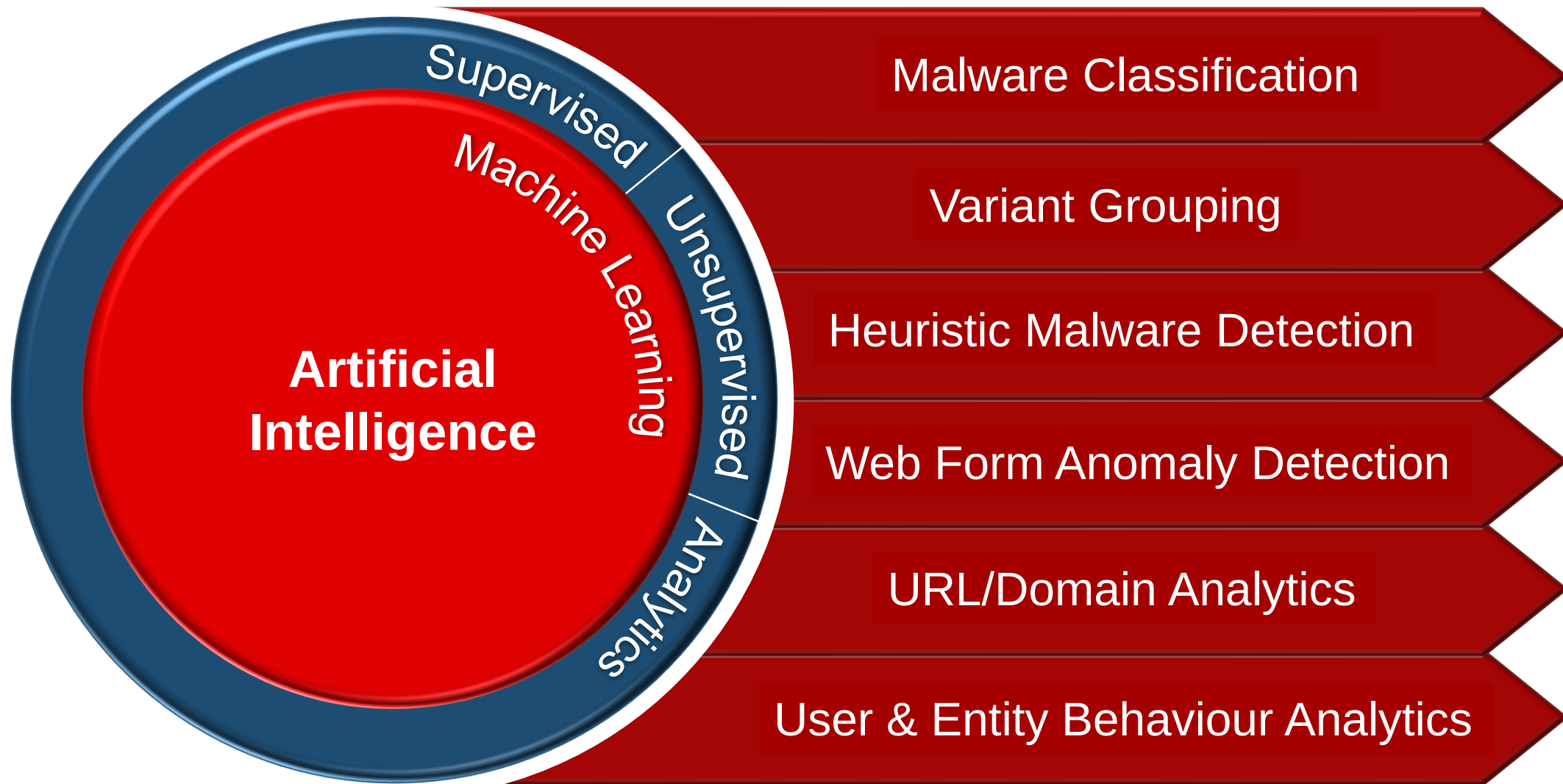
- Из данной позиции, попробуйте действовать на основе текущих (или отсутствующих) знаний
- Если полученная игра выиграна, увеличьте вес для всех ходов в игре
- Если игра проиграна, уменьшите вес

Расширенная аналитика

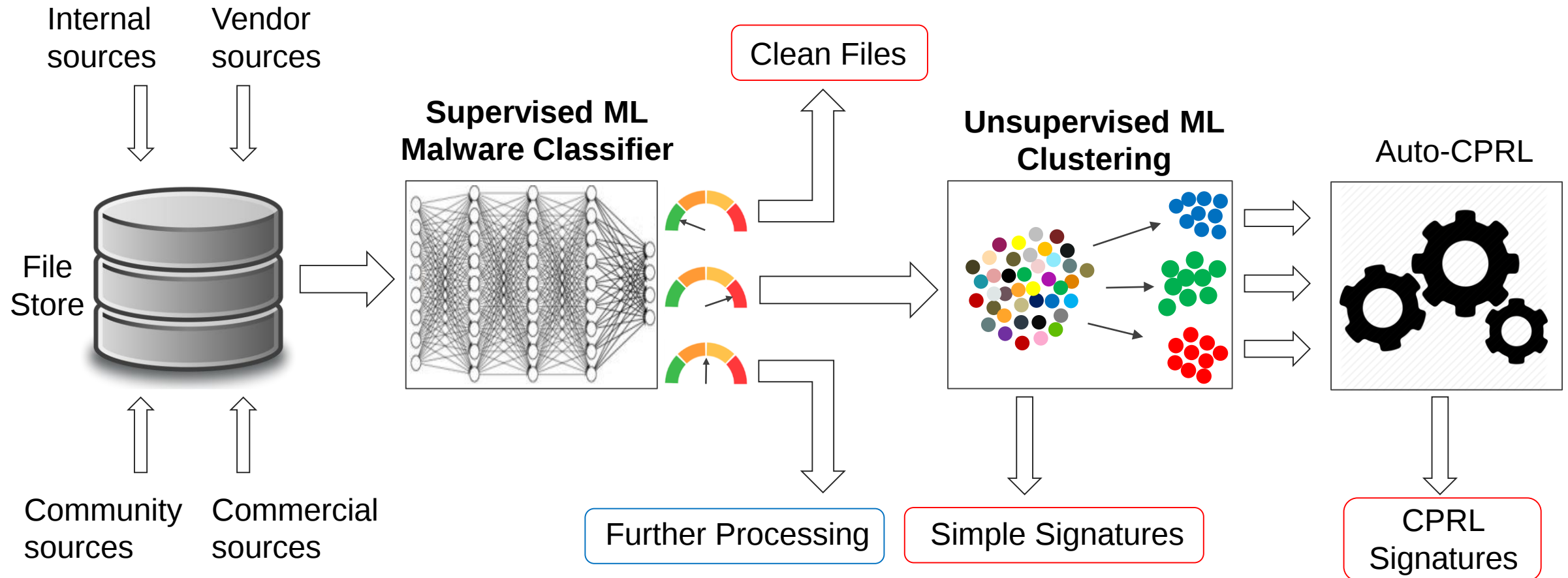
- Аналитика - это извлечение полезной информации из больших объемов данных
- Расширенная аналитика - это применение ИИ к аналитике



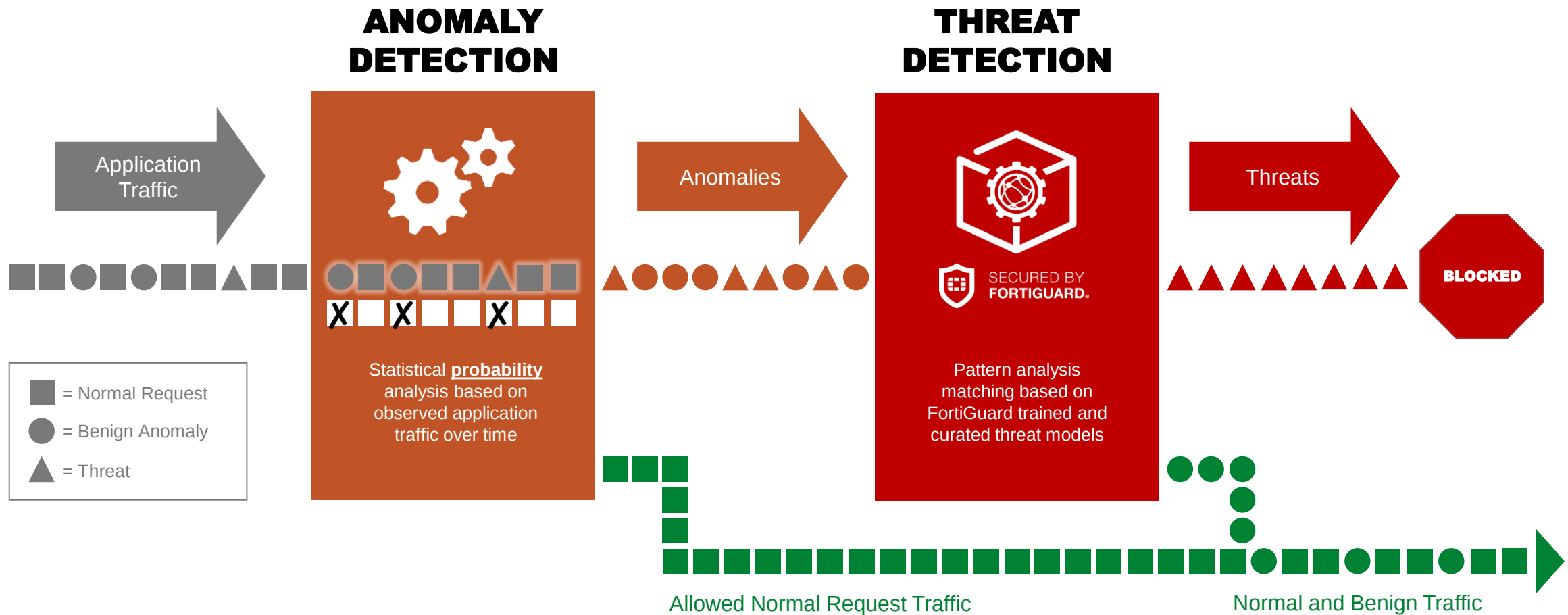
FortiGuard AI



Пример 1. AI-based Malware Processing



Пример 2. FortiWeb Employs 2 Layers of Machine Learning



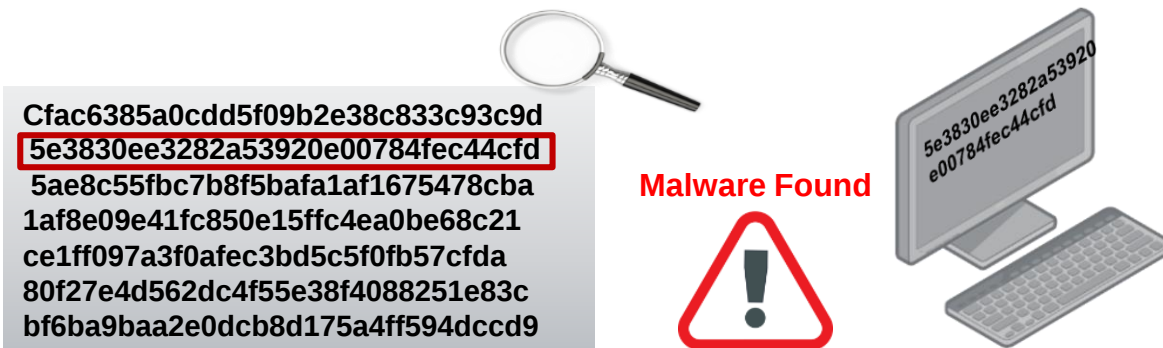
Эволюция технологий **антивирусной защиты**

УРОВЕНЬ I

- Простое MD5 / SHA256 вычисление
- Поддержка больших DB для поиска известных угроз
- Одна сигнатура – один зловред
- Reactive and non-responsive to mutations

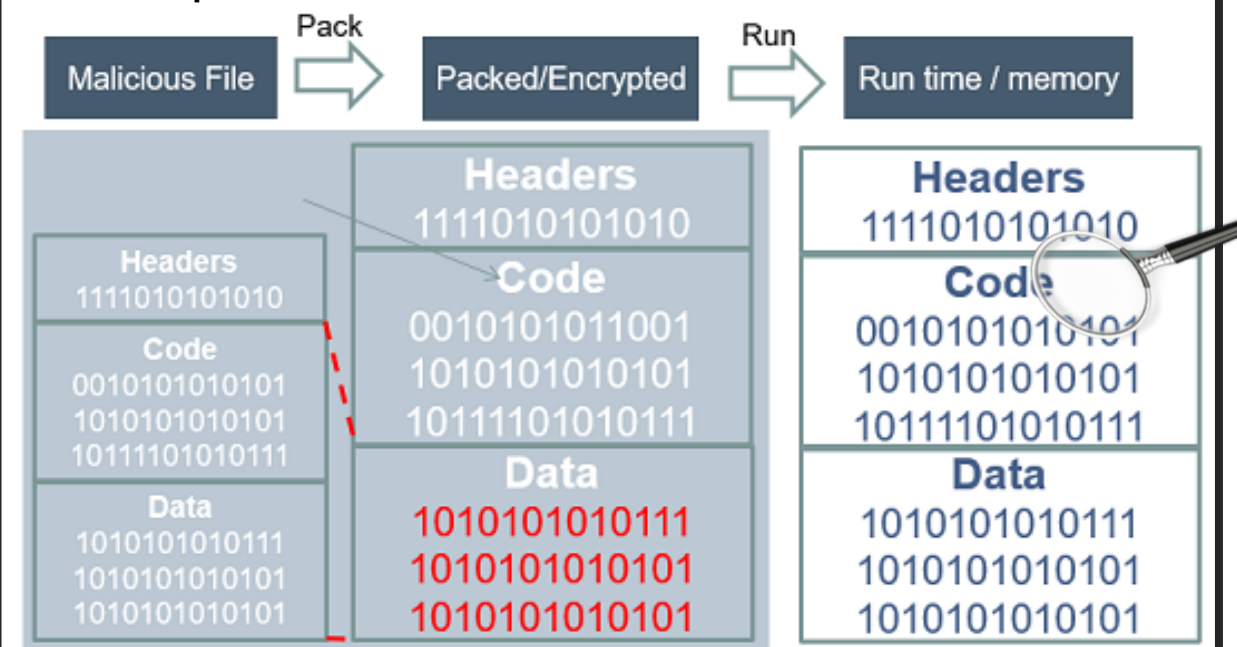
C:\Md5sum malware.exe

5e3830ee3282a53920e00784fec44cfd (malware.exe)



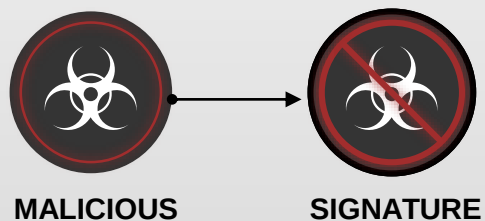
УРОВЕНЬ II

- Content Pattern Recognition Language
- Динамический анализ
- Анализ различных вариантов
- Проактивная защита

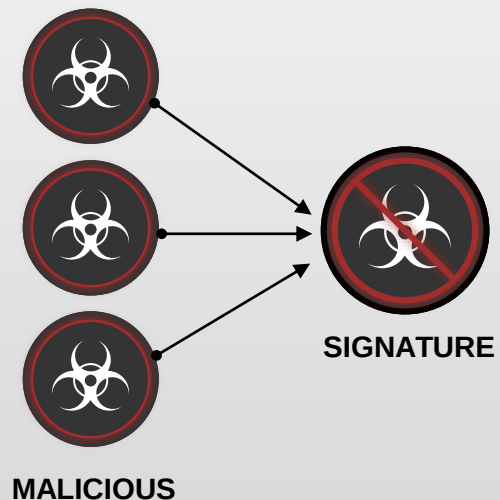


Эволюция технологий **антивирусной защиты**

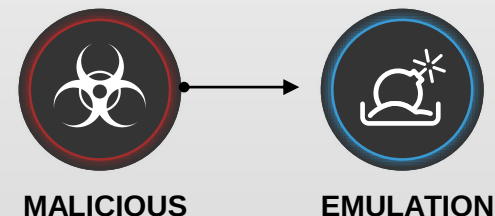
Один зловред –
одна сигнатура



Много зловредов –
одна сигнатура



Поведенческий анализ



Машинное обучение

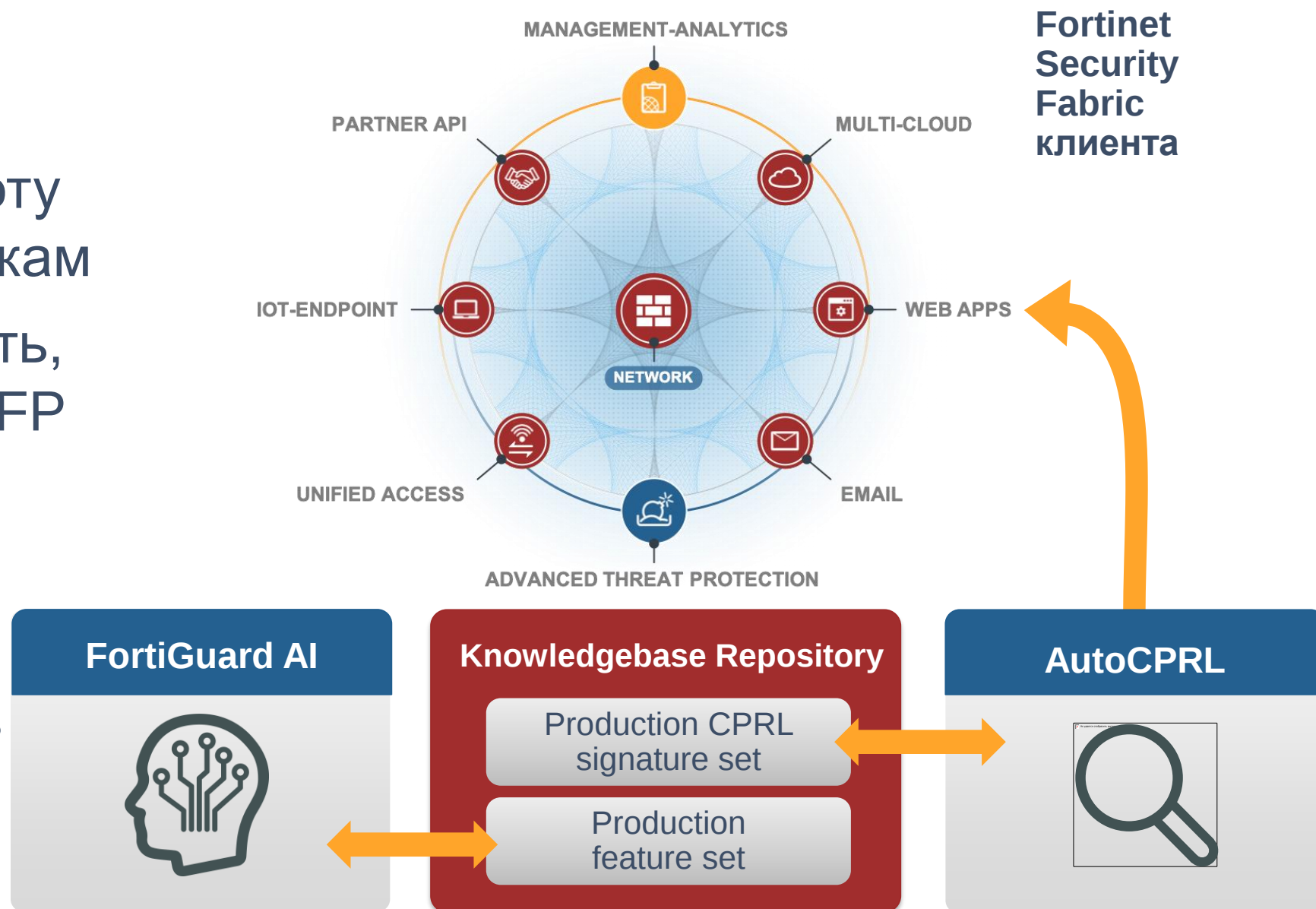


Известная
защита

Неизвестная
защита

FortiGuard

- Значительно затрудняет работу киберпреступникам
- Высокая точность, малый уровень FP
- Проверенная эффективность
- Высокая адаптируемость



FORTINET®