Как оценить угрозы кибербезопасности при помощи экспертных данных

Сергей Нейгер
«Перспективный мониторинг»

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

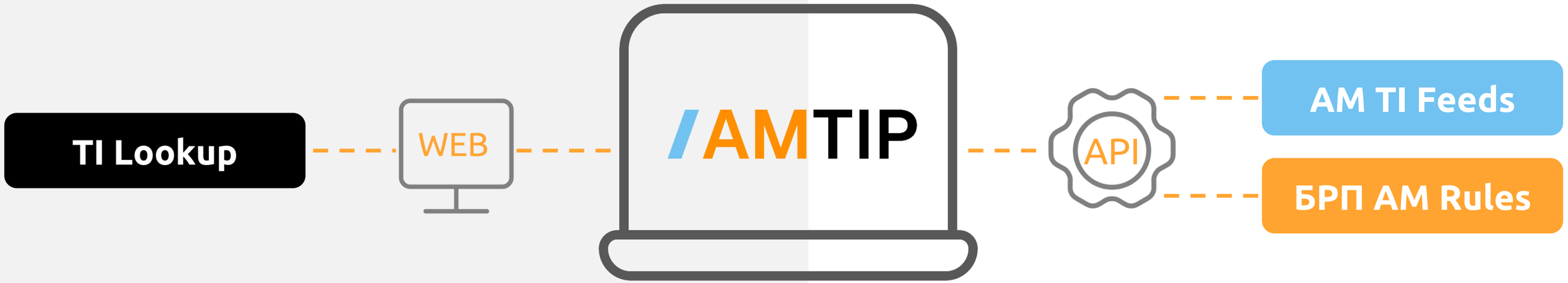
Экспертные данные

Новый источник сведений о киберугрозах

3 Составляющих AM TIP

Для людей

Для машин



- Аналитики SOC
- ТОП Менеджеры
- Физические лица

- Аналитические СЗИ
- Сетевые СЗИ
- Хостовые СЗИ

База решающих правил AM Rules

— собственная база правил обнаружения атак для решений классов IDS/IPS/NGFW. Мы разрабатываем правила, которые выявляют атаки и сопутствующие события на любом этапе вредоносной активности на скомпрометированном узле

50 000

актуальных сигнатур AM Rules

60%

собственных уникальных правил

40%

правил из ET Open, которые дополнительно валидируются и обогащаются аналитиками ПМ

Преимущества БРП AM Rules

35 000 индикаторов компрометации и образцов вредоносного кода анализируются **ежедневно**

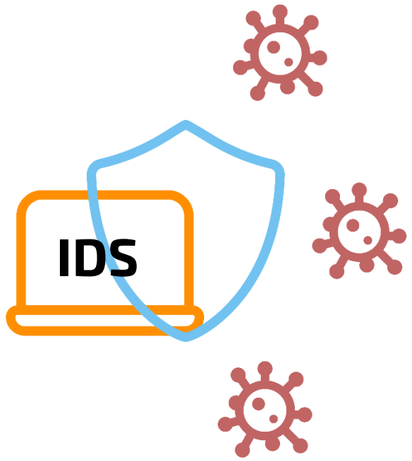
1000 новых сигнатур AM Rules ежемесячно

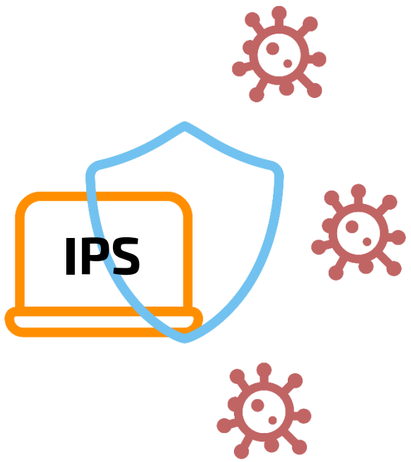
№1 первые на российском рынке, кто начал выпускать собственные сигнатуры с 2016 года

ViPNet БРП AM Rules работают во всей линейки продуктов ViPNet АО «ИнфоТеКС» с 2018 года

Ежедневно производится обновление базы правил

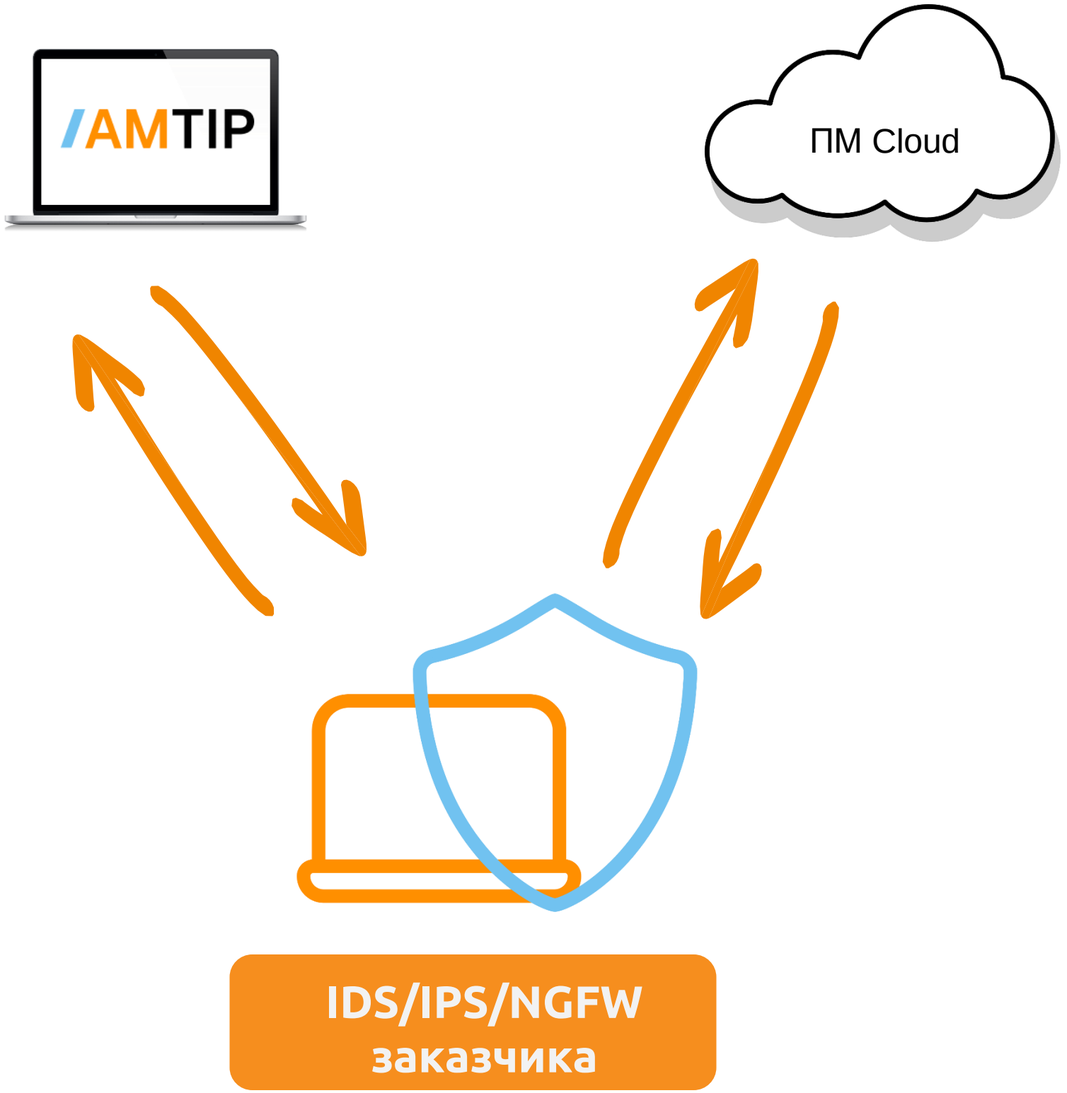
Где применимы БРП AM Rules





Форматы поставки БРП AM Rules

Поставляем БРП через AM Threat Intelligence Portal или облачное хранилище АО «ПМ»



Форматы поставки

Сетевые правила

SURICATA

SNORT

Хостовые правила

OSSEC

YARA

AM URL фильтрация

— присвоение категорий веб-ресурсам в зависимости от контента и связанных атрибутов на основе собственного алгоритма ПМ

5 000 000

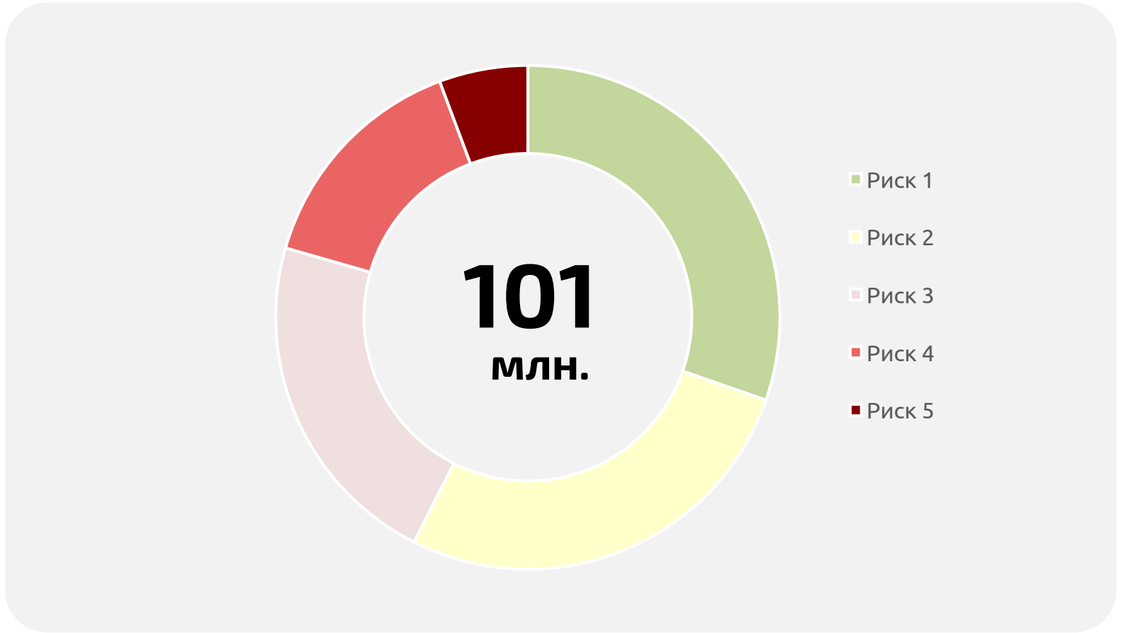
Категорированных ресурсов в 2021 году

100 000 000

Категорированных ресурсов в 2024 году

Категорирование ресурсов

Каждой категории присвоен риск от 1 до 5



81
категория

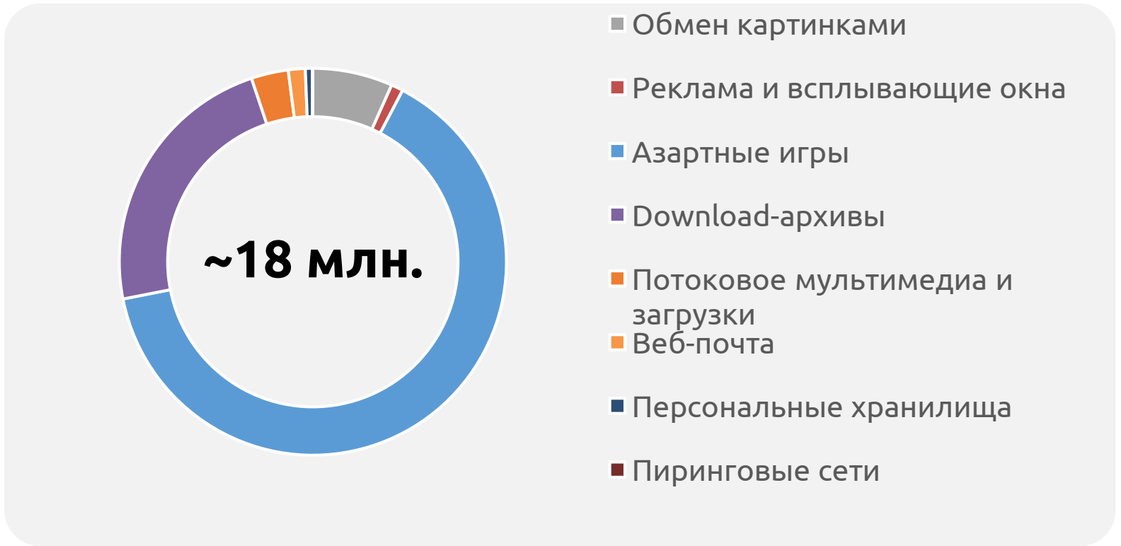
100+ млн.
категорированных ресурсов

15%
ежемесячный
при рост

24/7/365
обновление категоризатора

Категорирование ресурсов

Категорированных ресурсов с риском 4



Категорированных ресурсов с риском 5

Применимость

Управление сетевой безопасностью

Дополнительный способ защиты от фишинговых и других типов хакерских атак, в том числе социальной инженерии

Разграничение прав доступа сотрудникам

Ручное управление политиками доступа на основе категорированных ресурсов

AM Threat Intelligence Feeds

– комплексные сведения об индикаторах компрометации (Indicator of Compromise, IoC), которые помогают выявить угрозы ИБ и своевременно отреагировать на инцидент

Предоставляют важную контекстную информацию о вредоносном ПО и уязвимостях

Включают в себя актуальные сведения техниках и тактиках злоумышленников и прочие атрибуты индикаторов компрометации

Помогают применять своевременные меры для нейтрализации угроз

- Собственная платформа AM **TI Pipeline** для сбора сведений из публичных «песочниц» и антивирусов
- Система киберразведки AM **Pellonia** для сбора сведений из текстовых источников
- **Специалисты** ПМ ежедневно верифицируют и обогащают базу новыми сведениями вручную

51 000 000

индикаторов компрометации

4%

ежемесячный прирост базы

Ключевые преимущества AM TI Feeds

01

Уникальность

Сведения об индикаторах компрометации из SOC’а ПМ

02

«Низкий порог входа»

Низкая стоимость относительно аналогов

03

Мы гибкие

Интегрируемая с продуктами разных вендоров

04

Комплексные сведения об индикаторе

Помимо оценки вредоносности и категории мы предоставляем обширную сведения об индикаторах компрометации: применяемые техники и тактики, взаимосвязи, метки образцов

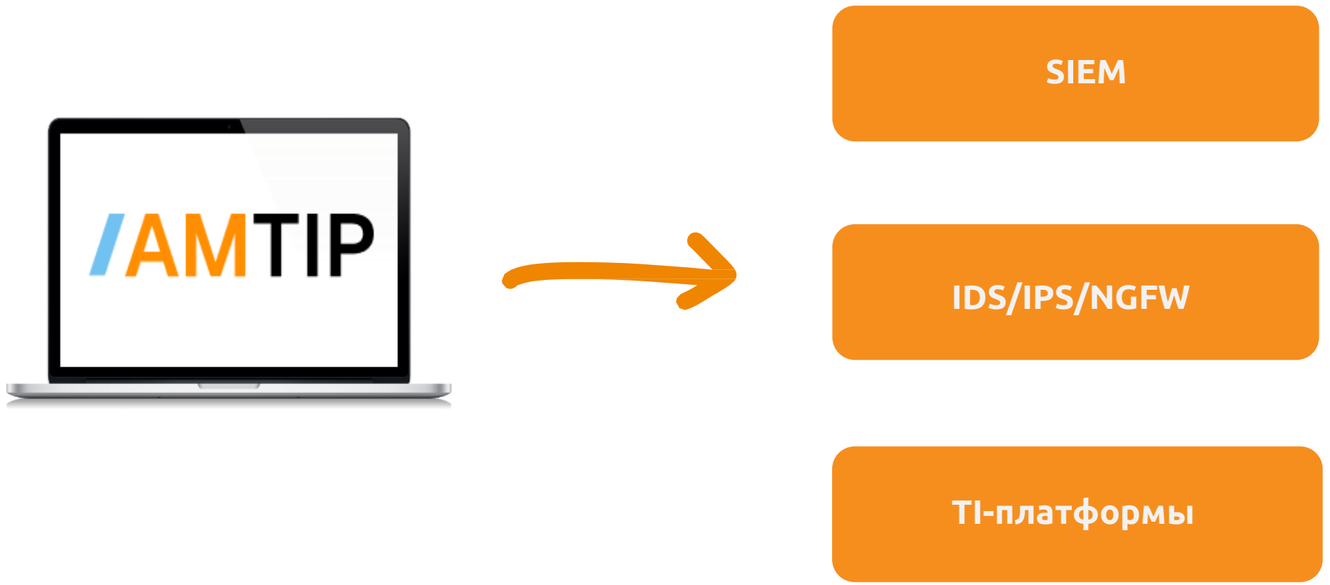
05

Вся линейка ViPNet

Сведения об угрозах используются во всей линейки продуктов ViPNet ОА «ИнфоТеКС»

Поставка AM TI Feeds

Поставляем на языке описания STIX 2.1 формате JSON через AM Threat Intelligence Portal



AM Threat Intelligence Portal

Я

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Сергей Нейгер
«Перспективный мониторинг»

t.me/pm_public amonitoring.ru amtip.ru