TI-платформа «Перспективного мониторинга» - источник информации об актуальных киберугрозах

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

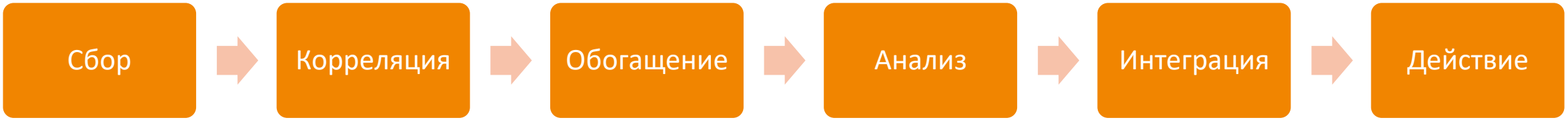
Георгий Караев

Поговорим

- Что это?
- Общая архитектура и технологии
- Применение

Что это такое?

Система для сбора анализ данных об актуальных угрозах из различных источников с целью прогнозирования возможных компьютерных атак

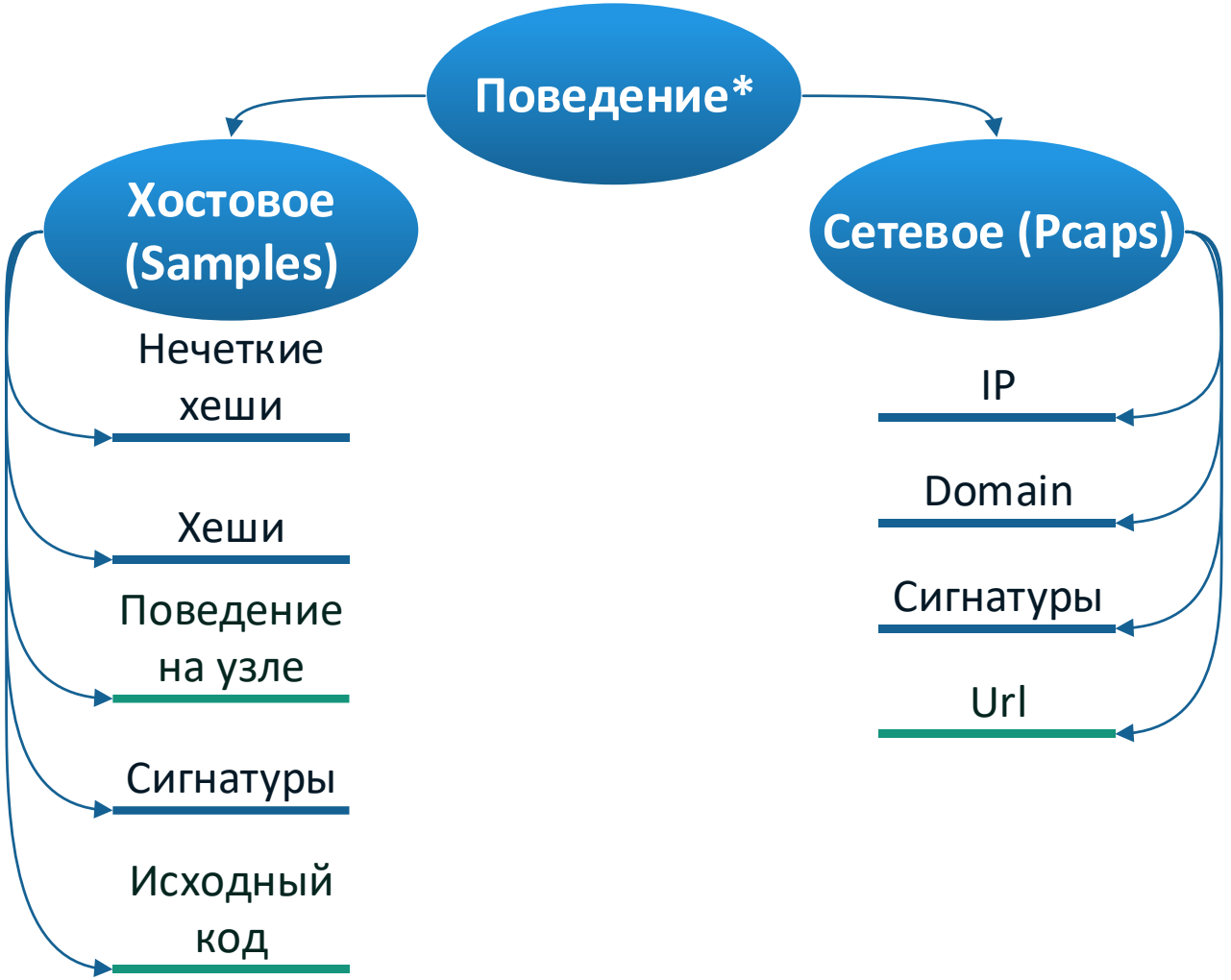


Зачем это все?

- пишем качественные сигнатуры (сетевые, хостовые)
- анализируем актуальные угрозы
- строим и используем(!) модели MO
- интеграция с инструментами SOC

Анализ артефактов (IP, hash, domain, pcap, URL*, sample*)

С чем работаем?



Как устроено

Сбор

- Sandbox
- OSINT
- Объекты пользователей
- HoneyPots
- Ручное добавление

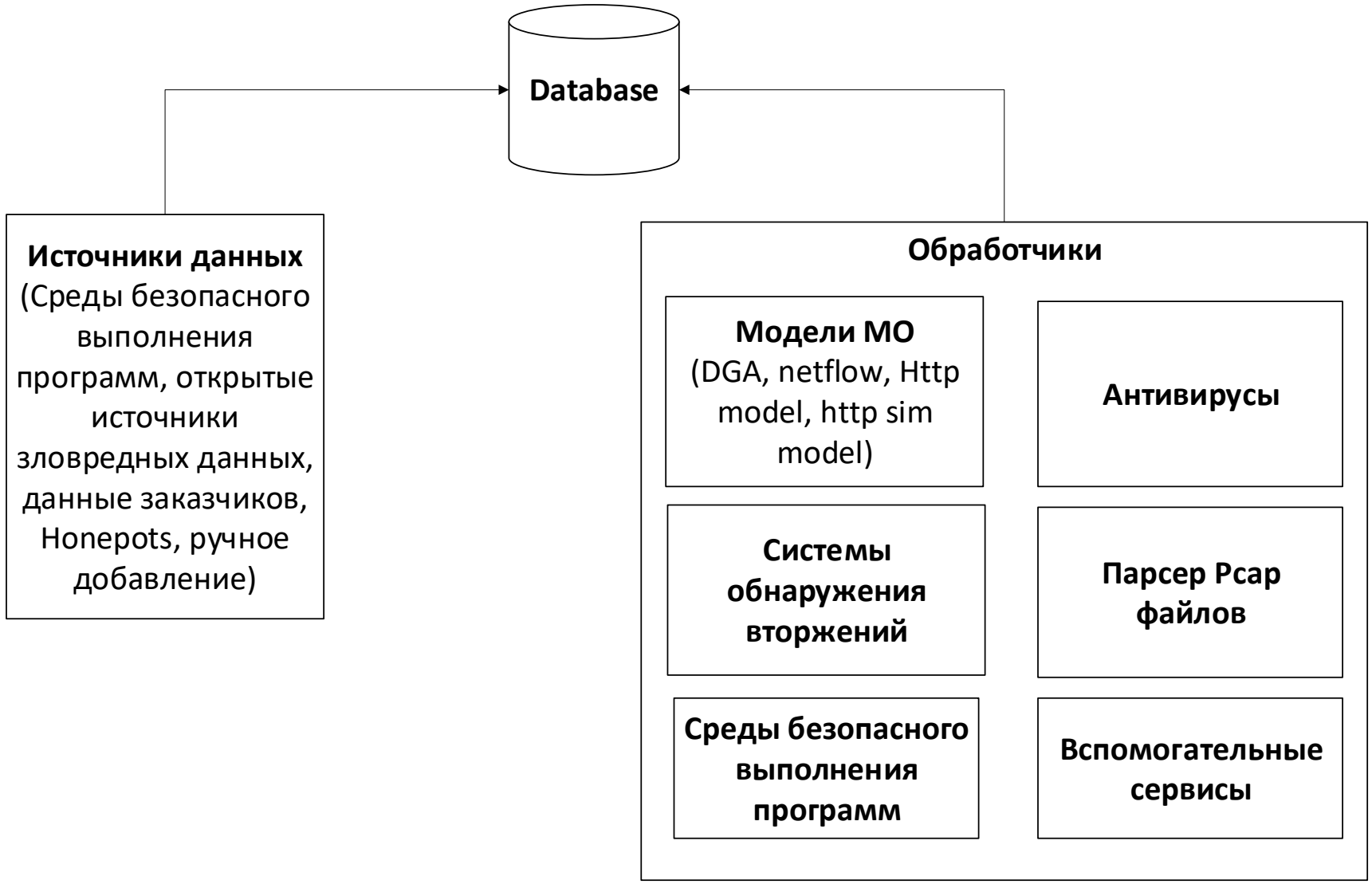
Обработка

- Модели МО
- IDS
- Sandbox
- АВЗ
- Парсеры
- Вспомогательные сервисы

Поставка

- Feeds
- Данные для создания сигнатур

Как устроено



Технологии


python


Celery


scikit
learn


TensorFlow


jupyter


RabbitMQ

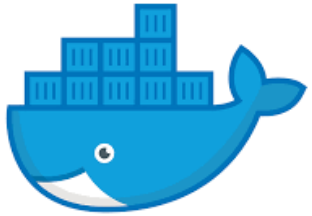

redis


mongoDB


hug
Embrace the APIs of the future


Bottle


SNORT®




docker


cuckoo


VirusTotal
React

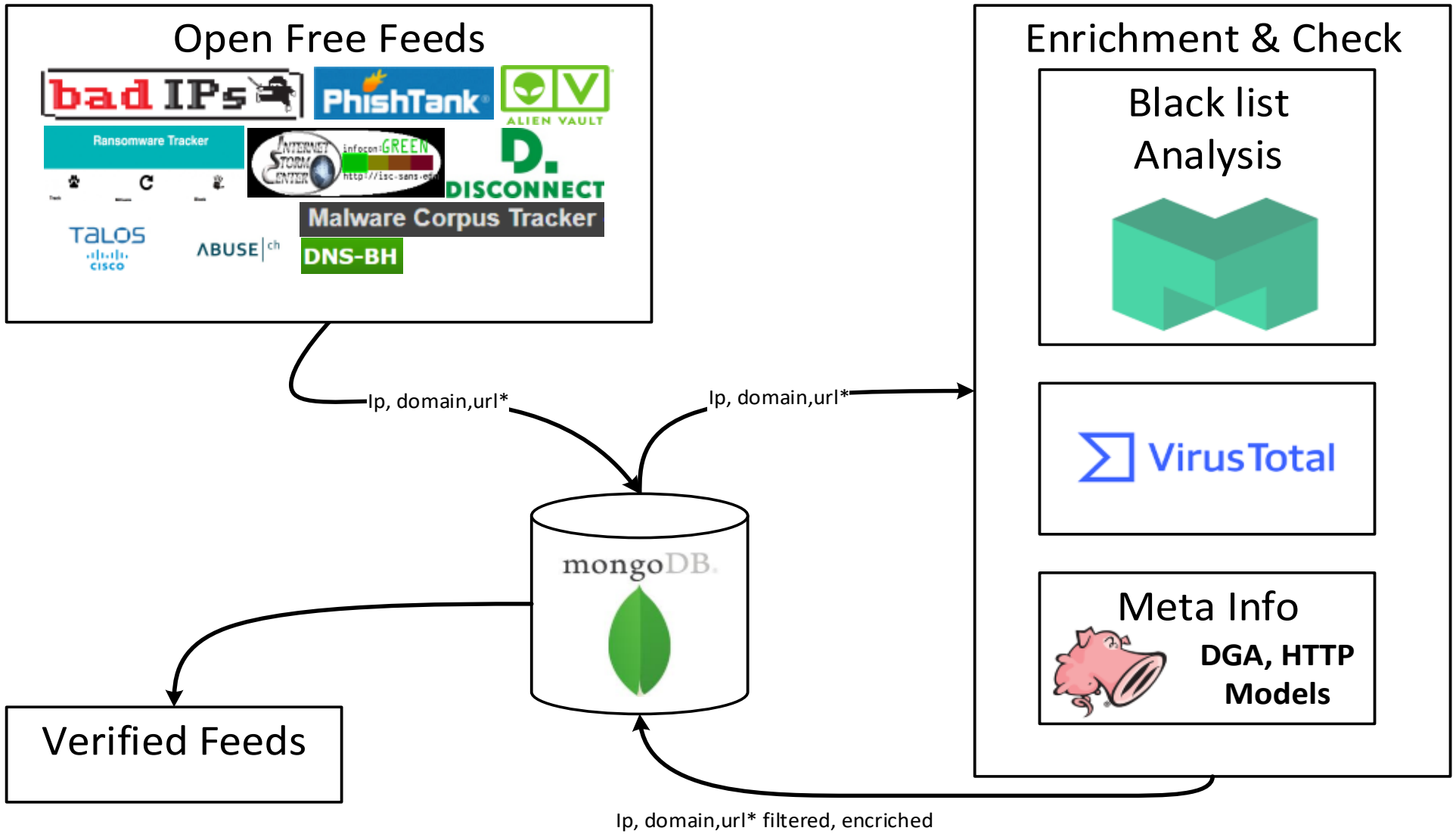
Функции TI платформы

- ✓ Разбор PCAP файлов
- ✓ Получение информацию о факте наличия в «черных списках» (ip, domain)
- ✓ Анализ образцов в песочнице
- ✓ Получение результата сработки IDS для PCAP
- ✓ Предоставление отчетов по ip, domain, url, hash
- ✓ Проверка IP, Domain, Hash, url на VT
- ✓ Интерфейс для сигнатурного аналитика

Функции TI платформы

- ✓ Вычисление интегральной оценки для: ip, sample, pcap, domain
- ✓ Проверка домена на предмет его генерации с помощью алгоритмов автоматического создания (DGA)
- ✓ Поиск похожих образцов по значению нечеткого хеша
- ✓ Проверка HTTP сессии pcap’а и сам pcap на «зловредность»
- ✓ Поиск семантически близких HTTP сессии/pcap’ы

«Черные списки»



Рейтинг IP, domain, pcap, sample

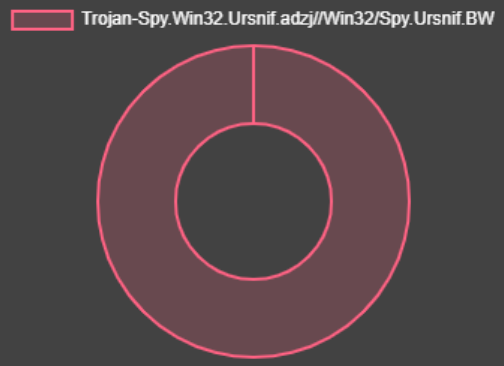
- Нужен для фильтрации/оценки
- Вычисляем используя следующие признаки:
  - Факт того, что домен был создан автоматически (модель DGA)
  - Рейтинг антивирусов
  - Взвешенное количество источников feed’ов,
  - Мета (косвенная) информация (срабатывания правил, результаты моделей МО, «негативный контекст»*)

Информация по домену

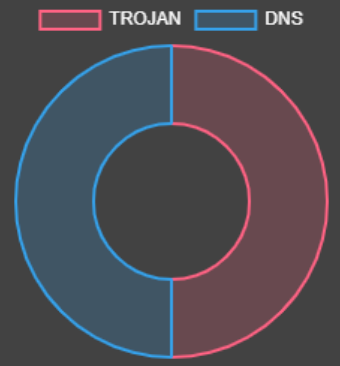
dhsiwyqdlskwsqo.com (2019-08-12) **AM SCORE:0.66**

DGA	true
IDS_SIG	true
AV_RATE	10/67
CATEGORIES	known infection source, bot networks

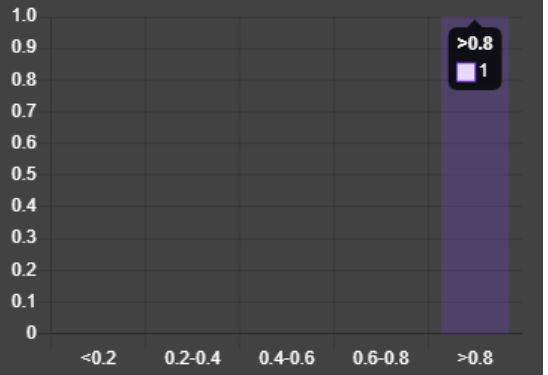
Sample lables



Signatures



Sample scores



Malicious Samples	1
URLs	25
Communicating files	5
Downloaded files	0
Files referring	0
Signatures	2

Malicious Samples

md5	AM Score ↑	AV Rate	Verdict	Submit Name
0435a386b9aabddfea6beb40621711f7	0.82	55/67		no data

Rows per page: 5 1-1 of 1

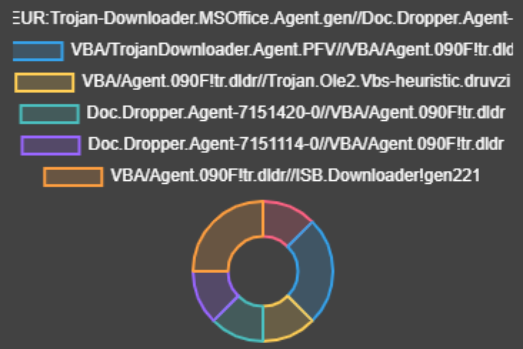
Информация по IP

+ PIPELINE CHARTS PCAPS UPLOAD SAMPLES_TABLE(TEST) ETPRO_FEEDS

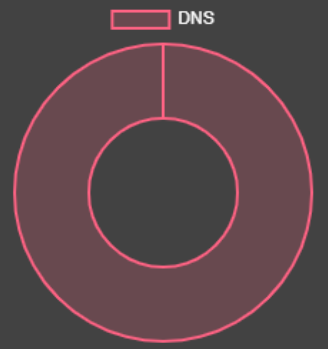
185.189.151.24 (2019-09-10) **AM SCORE:0.77**

AS OWNER	SOFTplus Entwicklungen GmbH
COUNTRY	CH
ASN	51395

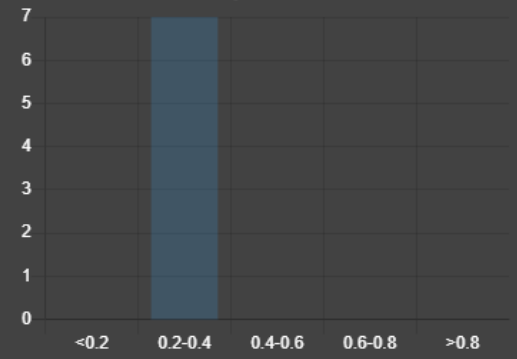
Sample lables



Signatures



Sample scores



Malicious Samples	8
URLs	25
Communicating files	25
Downloaded files	1
Files referring	0
Resolutions	6
Signatures	2

Malicious Samples

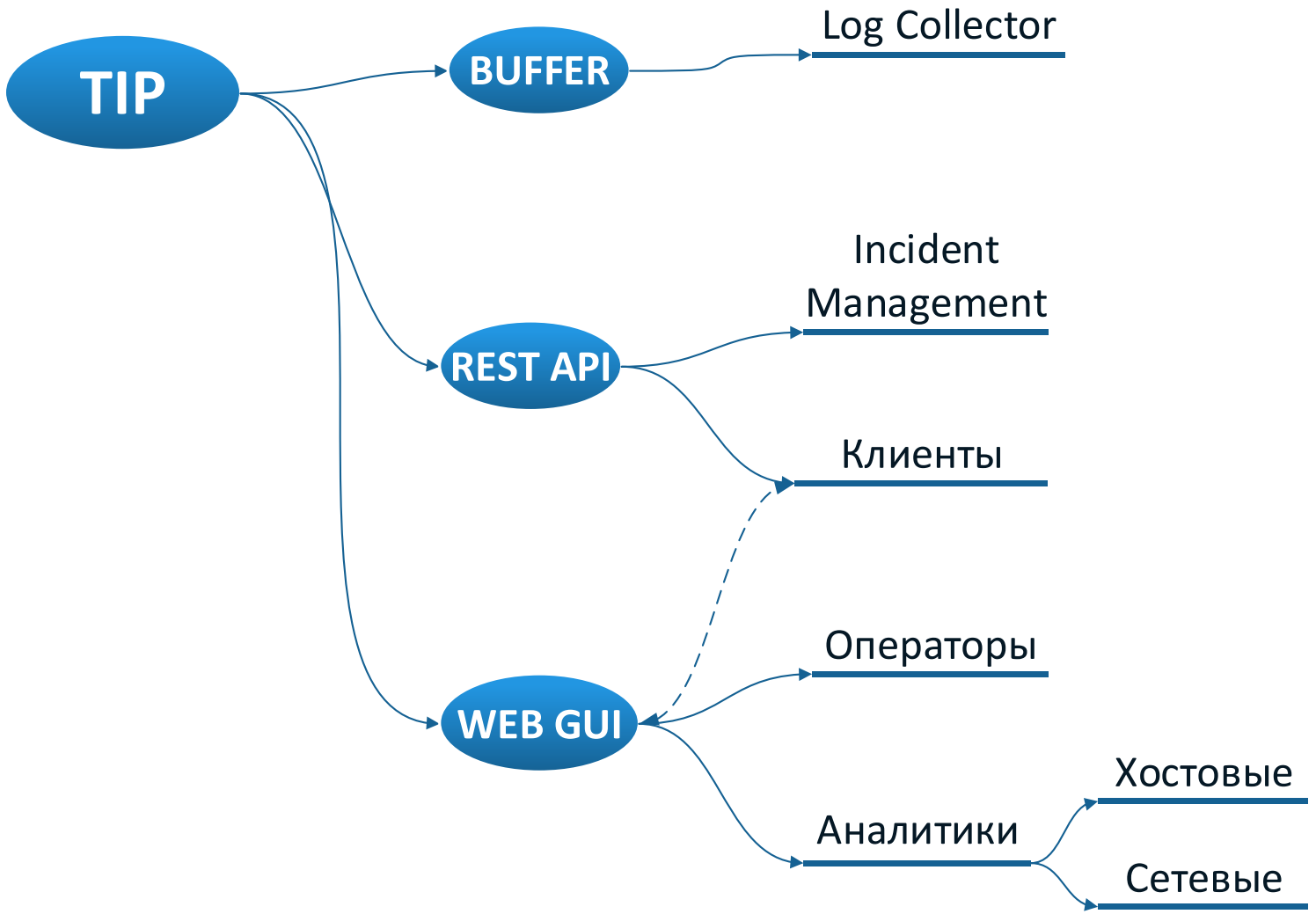
md5	AM Score	AV Rate	Verdict	Submit Name
40be01d925e93b51573b0f3a74e8e6f7		11/60	Malicious activity	no data
0e3dc4df47e8e5b4cf9d3134b4bda9e3	0.24	14/58	Malicious activity	no data
3a1dc4fbe71884560a1a04c0dd6ce25e	0.24	14/58	Malicious activity	no data
3233f90f96e947d3db909f12ddceb920	0.25	39/59	Malicious activity	no data
27a78066bb8f554b7aab91b2d57c1297	0.25	36/60	Malicious activity	no data

Rows per page: 5 1-5 of 8

Что у нас есть?

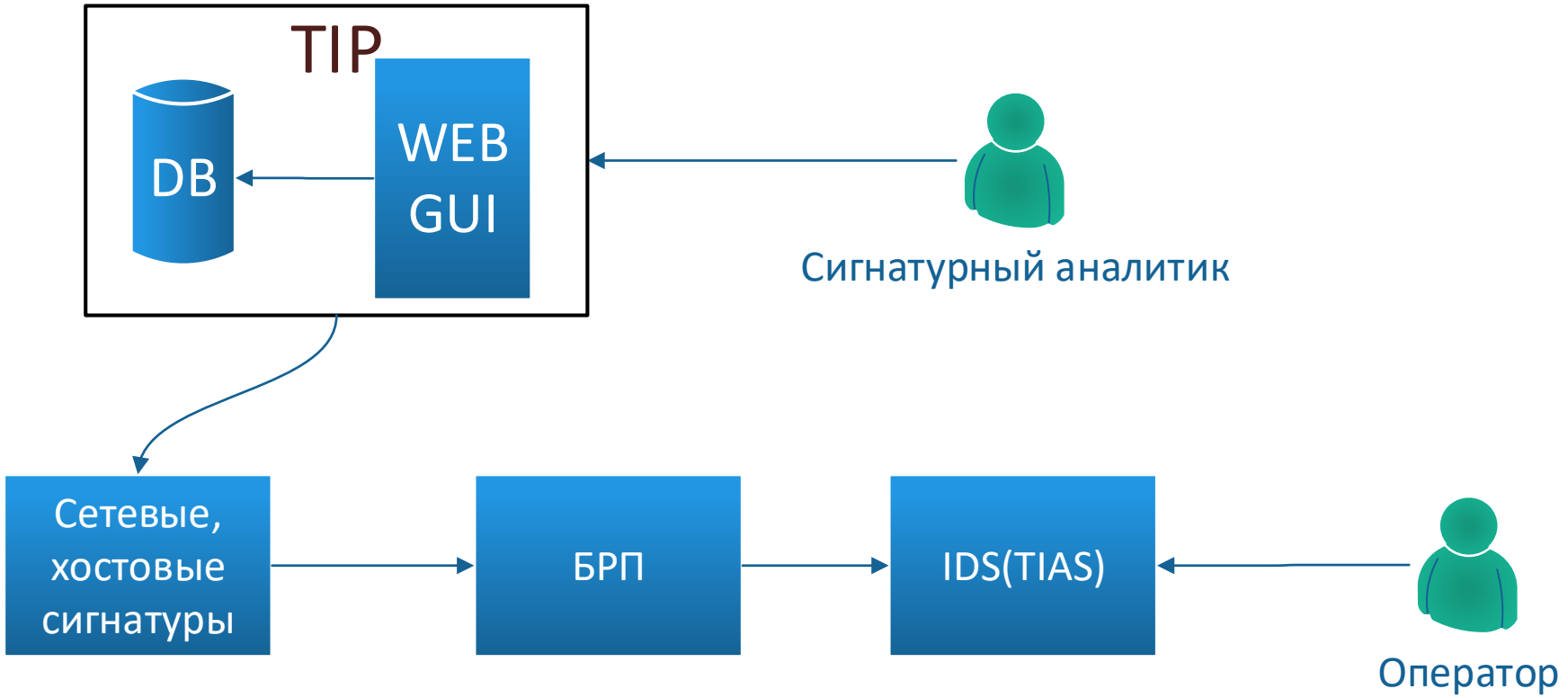
- Более 460к сэмплов
- Более 630к примеров трафика
- Более 900к IP и доменных имен
- Более 700к хешей

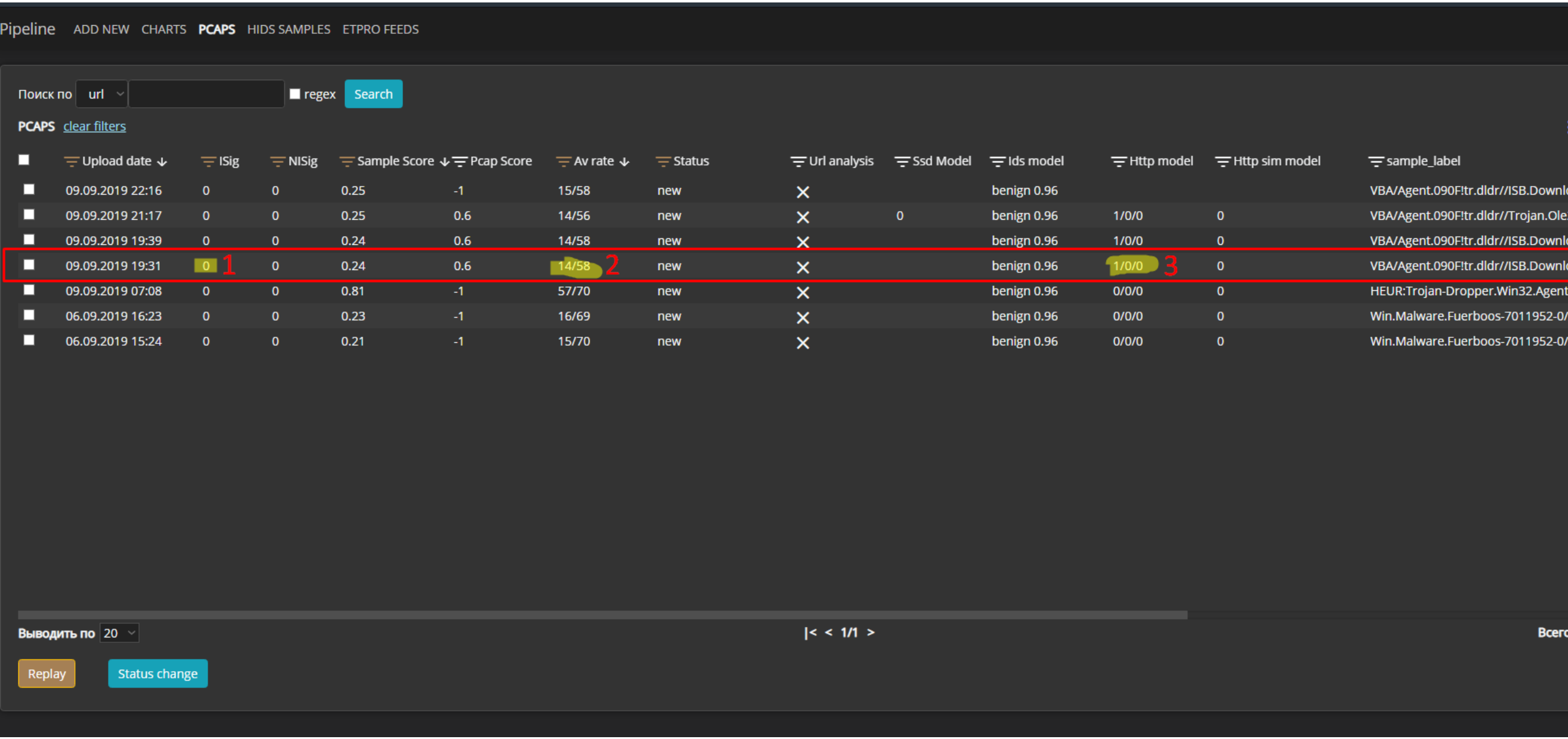
Как использовать



Как использовать

1. Писать сигнатуры:




Pipeline ADD NEW CHARTS PCAPS HIDS SAMPLES ETPRO FEEDS
Поиск по url regex Search
PCAPS clear filters
Upload date ISig NISig Sample Score Pcap Score Av rate Status Url analysis Ssd Model Ids model Http model Http sim model sample_label
09.09.2019 22:16 0 0 0.25 -1 15/58 new benign 0.96 VBA/Agent.090F!tr.dldr//ISB.Downl
09.09.2019 21:17 0 0 0.25 0.6 14/56 new 0 benign 0.96 1/0/0 0 VBA/Agent.090F!tr.dldr//Trojan.Ole
09.09.2019 19:39 0 0 0.24 0.6 14/58 new benign 0.96 1/0/0 0 VBA/Agent.090F!tr.dldr//ISB.Downl
09.09.2019 19:31 0 1 0 0.24 0.6 14/58 2 new benign 0.96 1/0/0 3 0 VBA/Agent.090F!tr.dldr//ISB.Downl
09.09.2019 07:08 0 0 0.81 -1 57/70 new benign 0.96 0/0/0 0 HEUR:Trojan-Dropper.Win32.Agent
06.09.2019 16:23 0 0 0.23 -1 16/69 new benign 0.96 0/0/0 0 Win.Malware.Fuerboos-7011952-0/
06.09.2019 15:24 0 0 0.21 -1 15/70 new benign 0.96 0/0/0 0 Win.Malware.Fuerboos-7011952-0/
Выводить по 20
|< < 1/1 >
Replay
Status change

Sample Info

MD5	0e3dc4df47e8e5b4cf9d3134b4bda9e3
TYPE	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.3, Code page: 1252, Author: Admini...
SHA256	09ca5b58e356bf68f44066aa49668bda625adc5a9655752ac369c813a0a341ea
LINK	https://app.any.run/tasks/e5e14c17-fc22-4a5e-ad30-91f69dab30f7
AM_SAMPLE_SCO...	0.24
SAMPLE_LABEL	VBA/Agent.090F!tr.dldr//ISB.Downloader!gen221
AV_RATE	14/58
UPLOAD_DATE	09.09.2019 19:31
ROOT_ID	5d767e44c146f50009884664
PCAP_ID	5d767e44c146f50009884665

Pcap Raw data Only with content

SOURCE	anyrun
STATUS	new
AM_PCAP_SCORE	0.6
DOMAIN NAMES	COUNT: 1

Sessions

Source -> Dest	Protocol	IPscore	Dscore	DN	Http model
TCP 192.168.100.92:49227 > 185.189.151.24:80	TCP	0.77	0.34	wwd.hollisheal...	0.96

192.168.100.92 -> 185.189.151.24

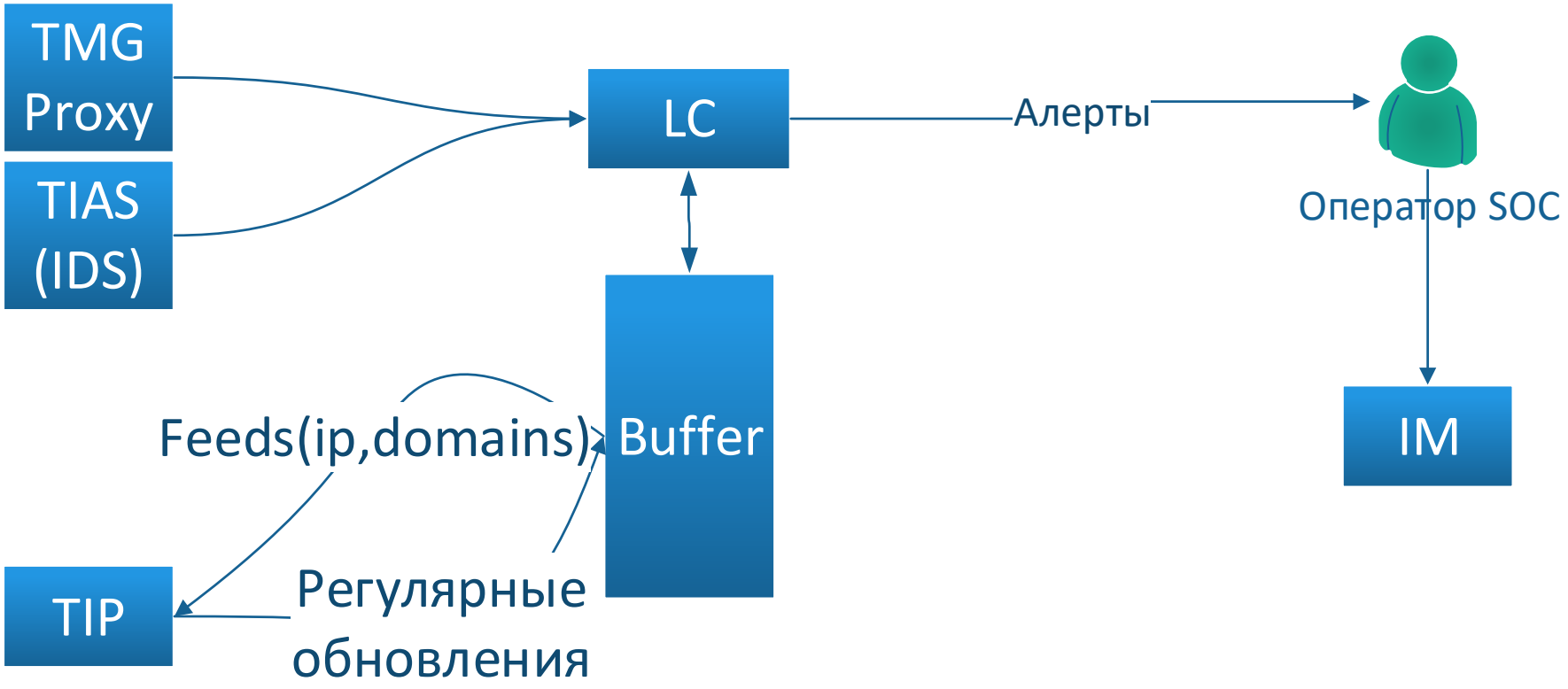
SESSION TAGS	+
STATUS	new
HTTP MODEL	0.96
SESSION DOMAI...	wwd.hollishealth.com 1/71
SESSIONS	GET /lastupdate.zip?bsff HTTP/1.1 Host: wwd.hollishealth.com Connection: Keep-Alive

SIMILAR SESSIONS

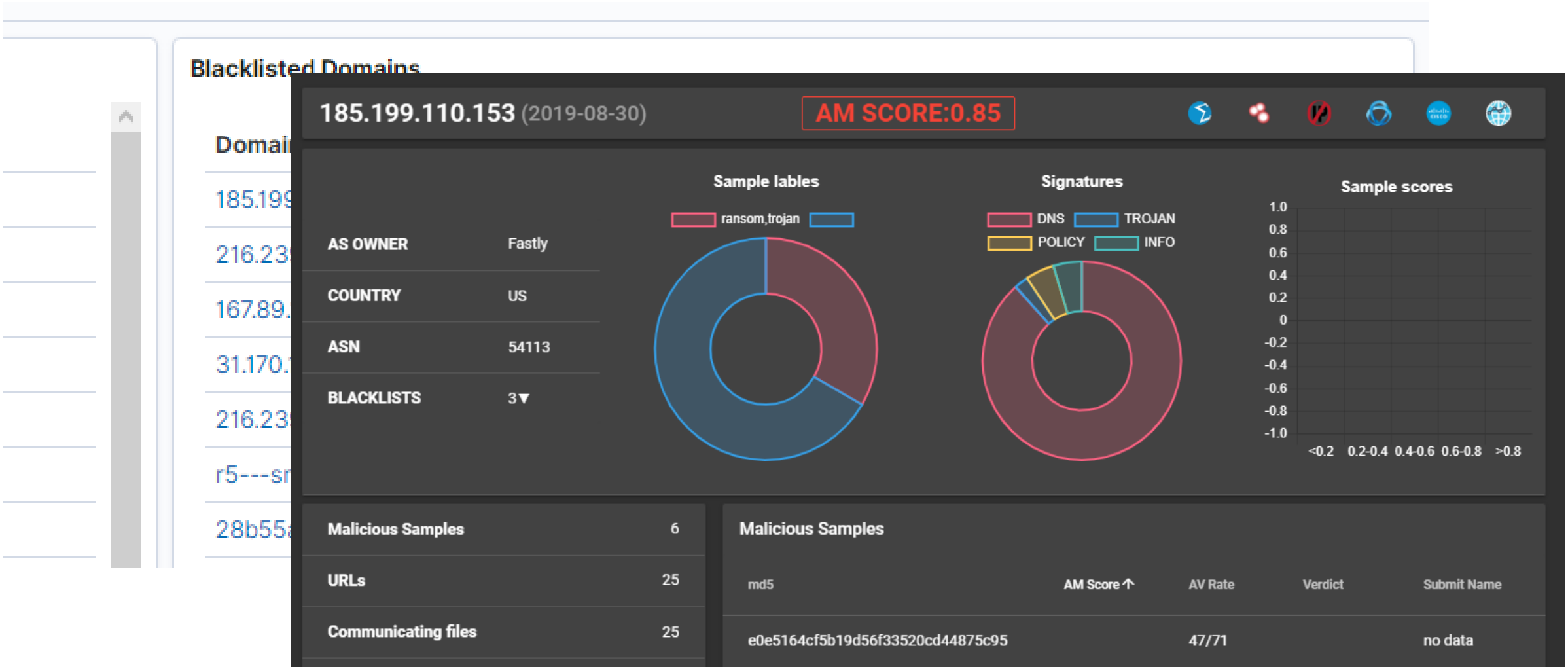
+ session: TCP 192.168.100.130:51127 > 185.189.151.24:80	prob: 0.53	ids: 0
+ session: TCP 192.168.100.93:49290 > 185.189.151.24:80	prob: 0.51	ids: 0
+ session: TCP 192.168.100.188:49325 > 185.189.151.24:80	prob: 0.51	ids: 0
+ session: TCP 192.168.100.13:49368 > 31.214.157.219:80	prob: 0.51	ids: 0
+ session: TCP 192.168.100.209:49236 > 31.214.157.219:80	prob: 0.51	ids: 0

Как использовать

2. Выявлять инциденты

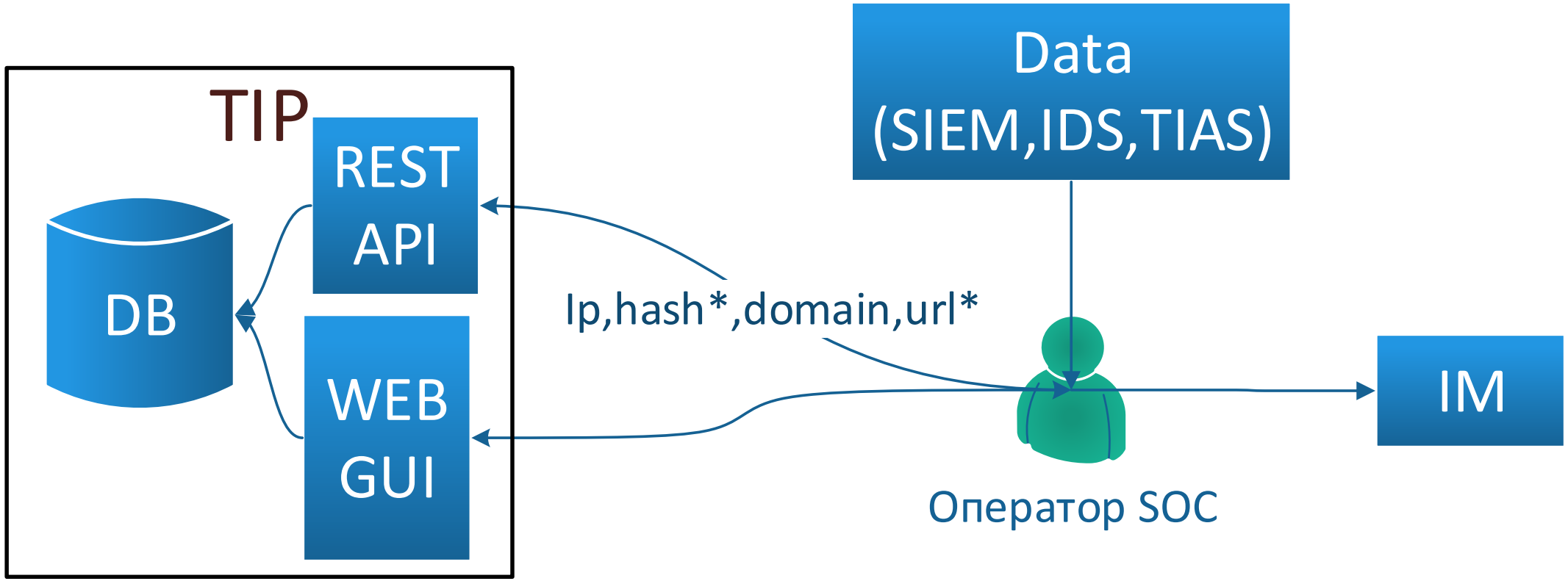


Обращения к «плохим» адресам



Как использовать

3. Проверять гипотезы по IoC



Как использовать

REST API:

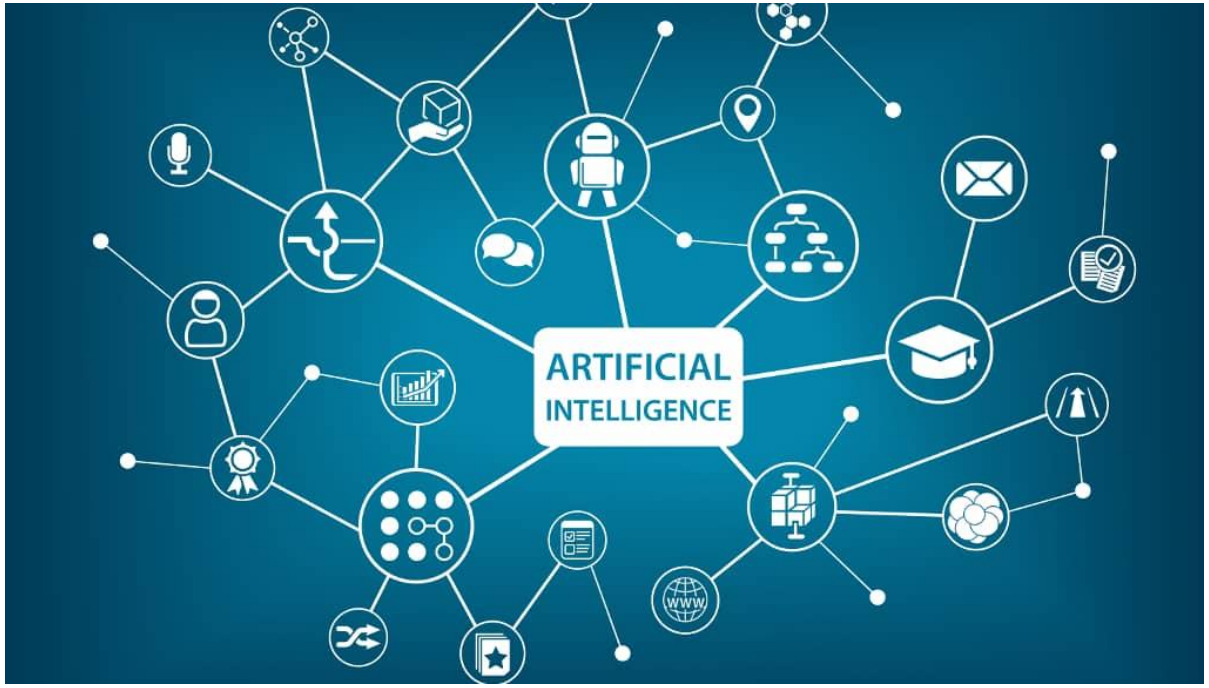
GET report/ip


```
{
    "country": "US",
    "as_owner": "Wikimedia Foundation Inc.",
    "asn": 12345,
    "resolutions": []
    "blacklists": [],
    "signatures": [
        {
            "msg":"ET INFO JAVA - ClassID",
        },
    ],
    "am_ip_score":0.6,
    "malware_samples": []
}
```

```
{
    "malware_samples": [
        {
            "md5": "",
            "ssdeep":"",
            "tags": ["adwind"],
            "type": "exe",
            "verdict": "malicious",
            "sample_label": "trojan",
            "am_sample_score": 0.99
        }
    ]
}
```

Какой интеллект?

- Анализ HTTP сессий
- Анализ событий IDS NS
- DGA
- Модель похожести сессий
- Модель похожести образцов



А дальше что

- Увеличиваем число источников
- Фишинг
- Шифрованный трафик
- Анализ трендов и построение прогнозов
- Обновление REST API 2.0

Спасибо за внимание!

И подключайтесь к ГосСОПКА

Георгий Караев

Руководитель направления

Georgy.Karaev@amonitoring.ru