



# Как оценить угрозы кибербезопасности и при помощи экспертных данных

Артём Савчук,  
Технический директор,  
«Перспективный мониторинг»

# АО «ПМ» сегодня



**13**

лет на рынке услуг  
SOC и исследования  
защищённости

**7**

лет центр  
ГосСОПКА (А)

**>1600**

выполненных ИБ  
проектов

**20**

действующих  
киберполигонов  
Ampire

**300+**

проведенных  
киберучений

**>3500**

КИ/КА в год

# Направления деятельности



## Исследование защищённости

Пентест

Аудит ИБ

Оценка соответствия требованиям Банка России

Категорирование объектов КИИ

## SOC

Коммерческий SOC

Подключение к ГосСОПКА

Расследование инцидентов ИБ

Группа быстрого реагирования

## Продукты

AM Rules (БРП)

AM TI Portal

Киберполигон Ampire

AM Incident Management System

**Сквозная экспертиза** по всем направлениям деятельности

# Что такое TI?



**TI: Threat Information** that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes\*.

Информация об угрозах, которая была собрана, преобразована, проанализирована, интерпретирована или обогащена для обеспечения необходимого контекста для процессов принятия решений.



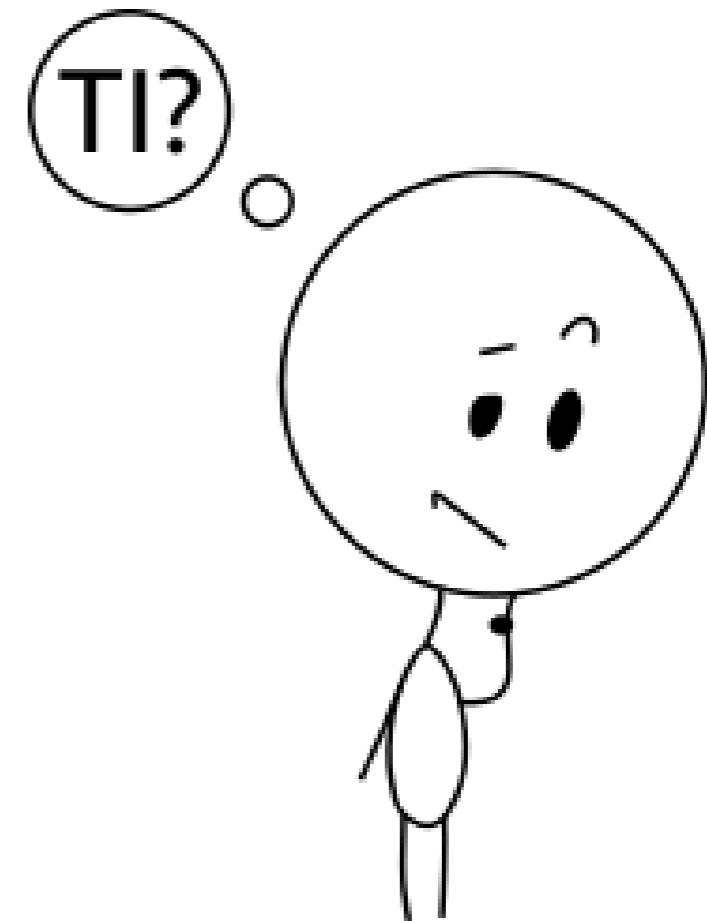
\* [https://csrc.nist.gov/glossary/term/threat\\_intelligence](https://csrc.nist.gov/glossary/term/threat_intelligence)

# Что такое TI?



**TI:** The "cyclical practice" of planning, collecting, processing, analyzing and disseminating information that poses a threat to applications and systems\*\*.

"Циклическая практика" планирования, сбора, обработки, анализа и распространения информации, содержащей сведения об угрозах для приложений и систем.



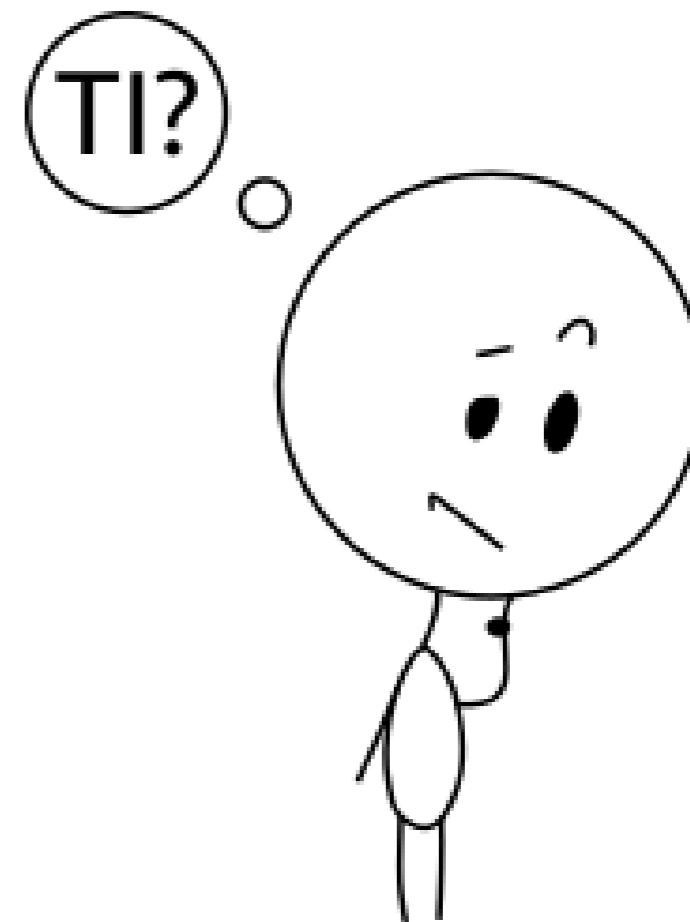
\*\* [https://en.wikipedia.org/wiki/Threat\\_intelligence](https://en.wikipedia.org/wiki/Threat_intelligence)

# TI vs Угрозы



Угроза (безопасности информации) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [ГОСТ Р 50922-2006].

Угроза информационной безопасности организации (угроза ИБ организации) – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способность вызвать негативные последствия (ущерб/вред) для организации [ГОСТ Р 53114-2008].

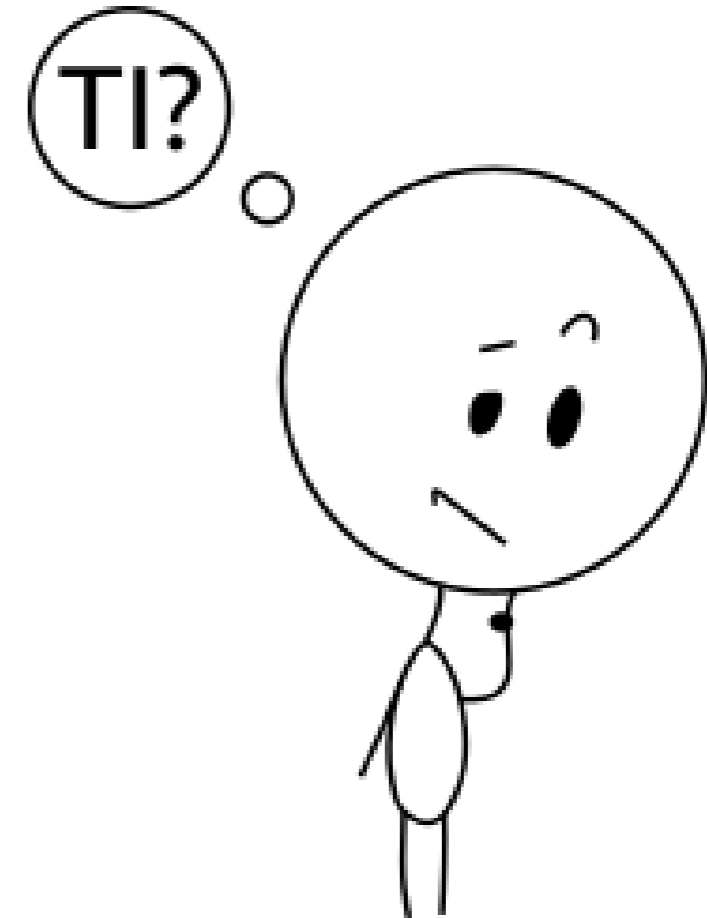


# Угрозы vs Законодательство РФ



- Федеральный закон от 26 июля 2017 г. N 187 -ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации»
- Приказ ФСТЭК России от 21.12.2017 № 235
- Приказ ФСТЭК России от 25.12.2017 № 239
- Методический документ ФСТЭК России «Методика оценки угроз безопасности информации»
- и другие нормативные документы РФ оперируют термином:

«угрозы безопасности информации»



# Угрозы vs Риски



**Угрозный рассвет: почему растут киберриски и как устроено их страхование**

Forbes

07 ноября 2023

РБК+ Все выпуски Истории Экспертиза Презентации Решение Новс

Тенденции, Весь мир, 27 окт 2022, 09:55

**Бизнес начал вкладывать в страхование киберрисков**

интерфакс

ЭКОНОМИКА 12:23, 15 июня 2023

**ЦБ планирует сформировать условия для создания института страхования киберрисков**

Москва. 15 июня. INTERFAX.RU - Банк России планирует сформировать условия для создания института страхования киберрисков и предоставить расширенный перечень данных внешним пользователям для формирования моделей страхования, говорится в материале ЦБ "Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023-2025 годов", опубликованном на сайте регулятора.

"Задача страхования киберрисков состоит в покрытии убытков, возникших в результате успешно реализованных кибератак", - отмечает ЦБ.

Также Банк России отмечает, что рынок страхования киберрисков развивается от года к году. "По данным международных экспертов, по состоянию на 2022 год глобальный рынок страхования киберрисков достигнет \$14 млрд, а к 2025 году он будет составлять уже \$20 млрд", - говорится в материале.

ВЕДОМОСТИ

📍 🔍 👤 Вой

Финансы Инвестиции Технологии Медиа Политика Общество Менеджмент ...

Ведомости& Спорт Право Страна Технологии и инновации Капитал Промышленность

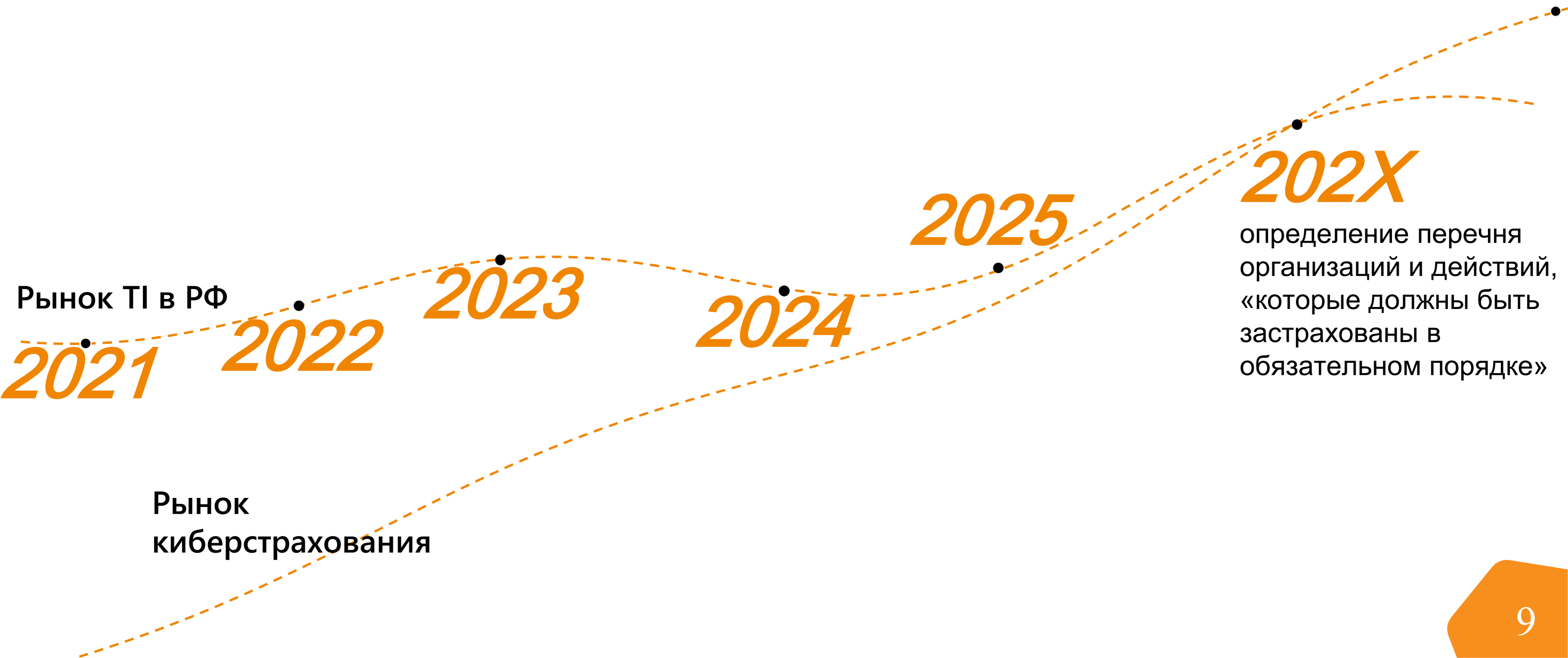
🔒 29 сентября, 00:21 / Технологии

**Для страхования киберрисков может быть создан отдельный фонд**

Он может стать частью новой нацпрограммы «Экономика данных»



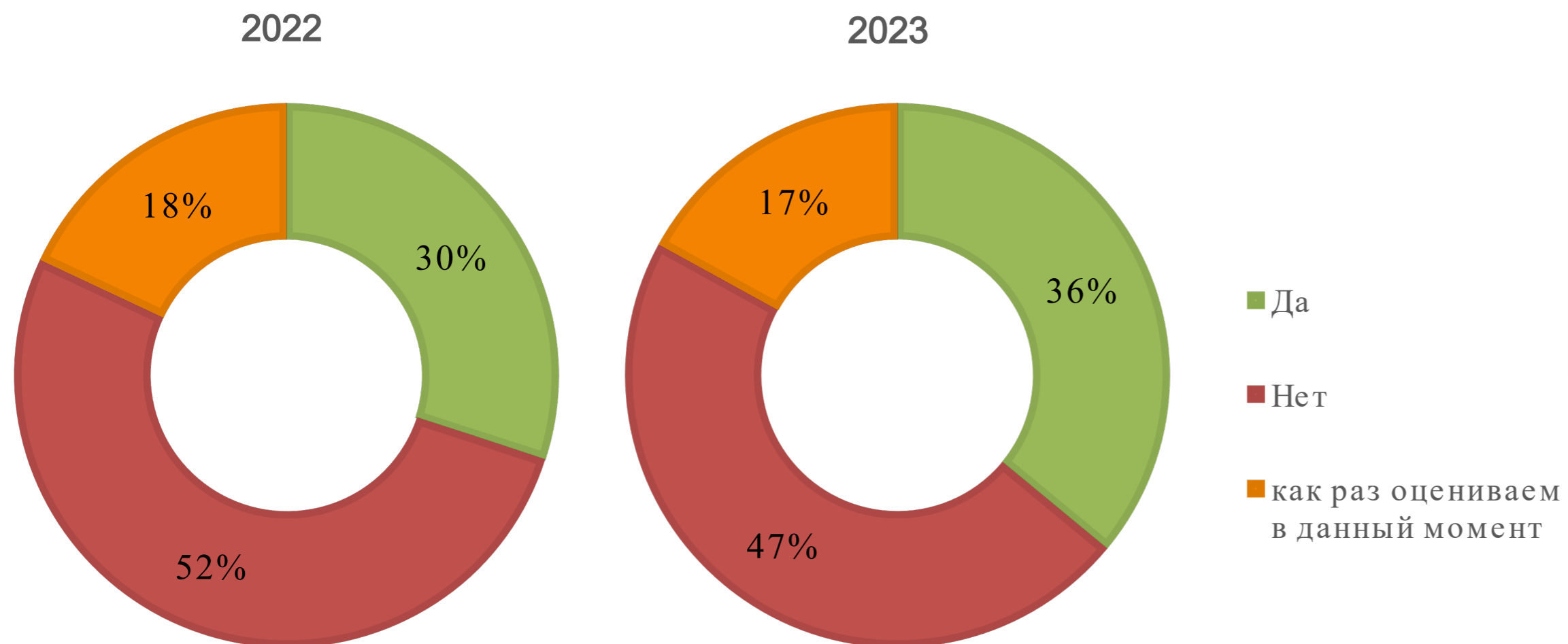
# Предотвратить или компенсировать



# «Мастхев» ли TI?



«Вы используете сервисы Threat Intelligence в данный момент?»\*



## Бизнес пошел в контрразведку

### Спрос на услуги предотвращения киберинцидентов растет

Рост числа киберинцидентов подтолкнул организации чаще обращаться за услугами специалистов по расследованию и предотвращению таких событий: мониторингу теневого форума, анализу объявлений о продаже данных организации и составах группировок. Участники рынка наблюдают увеличение спроса на подобные услуги на 20-40% год к году. Сейчас их объем оценивается на уровне 15 млрд руб.— около 8% от всего рынка информбезопасности. Интерес к сегменту начали проявлять и госзаказчики, но серьезного роста такие клиенты не обеспечат из-за регуляторных барьеров, полагают эксперты.

\*Опрос зрителей онлайн-конференции AM Live, проходившей 18 октября 2023 года и посвященной Threat Intelligence

# Экспертные данные

## АО «ПМ»



1

«Базы решающих правил»  
(БРП, включают наборы  
snort, yara, ossec, suricata  
правил)

2

TI feeds (IoC в STIX или любом  
другом пользовательском  
формате)

3

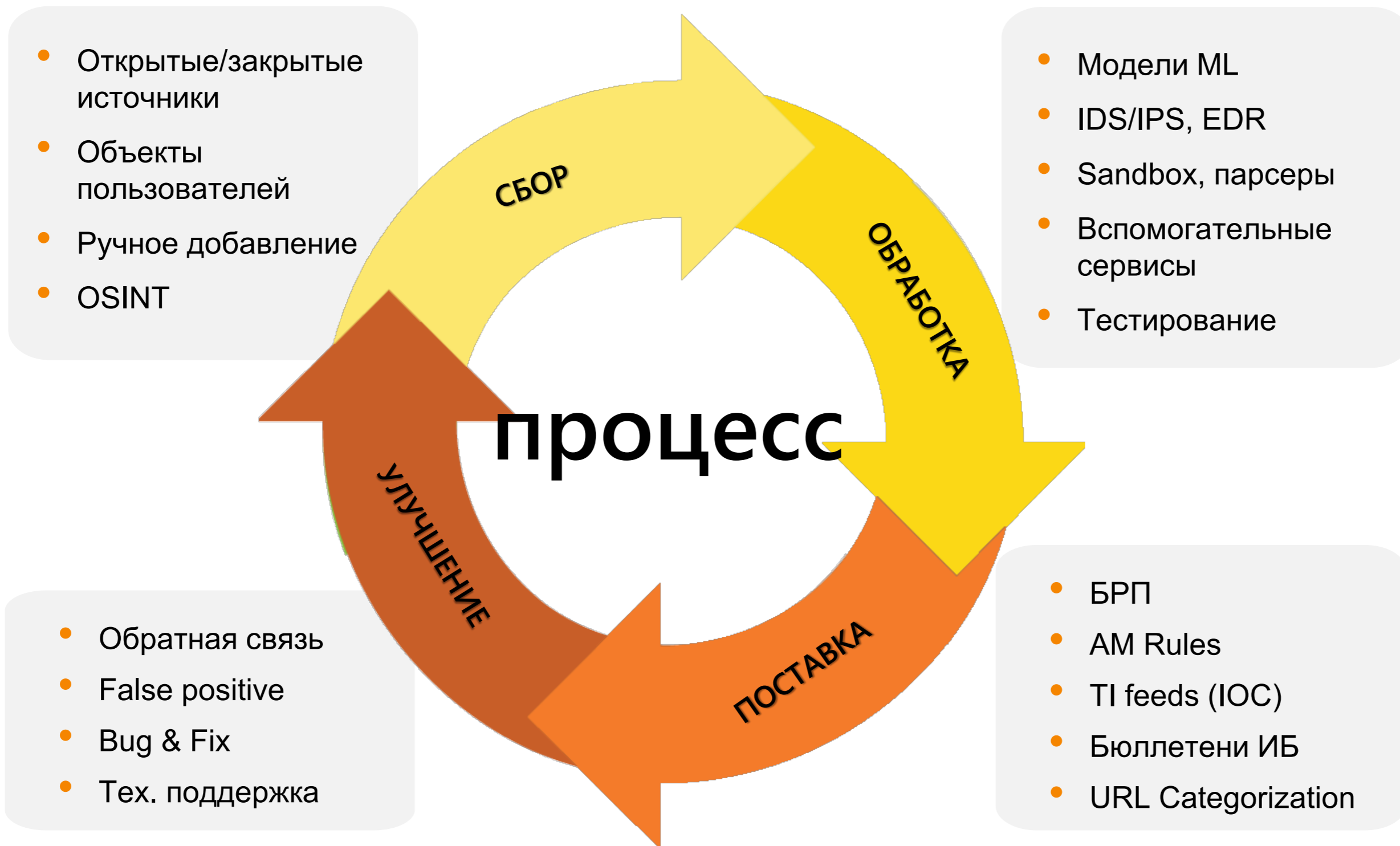
AM Rules (Свидетельство  
Роспатента №2016620316 от  
03.03.2016 г.)

4

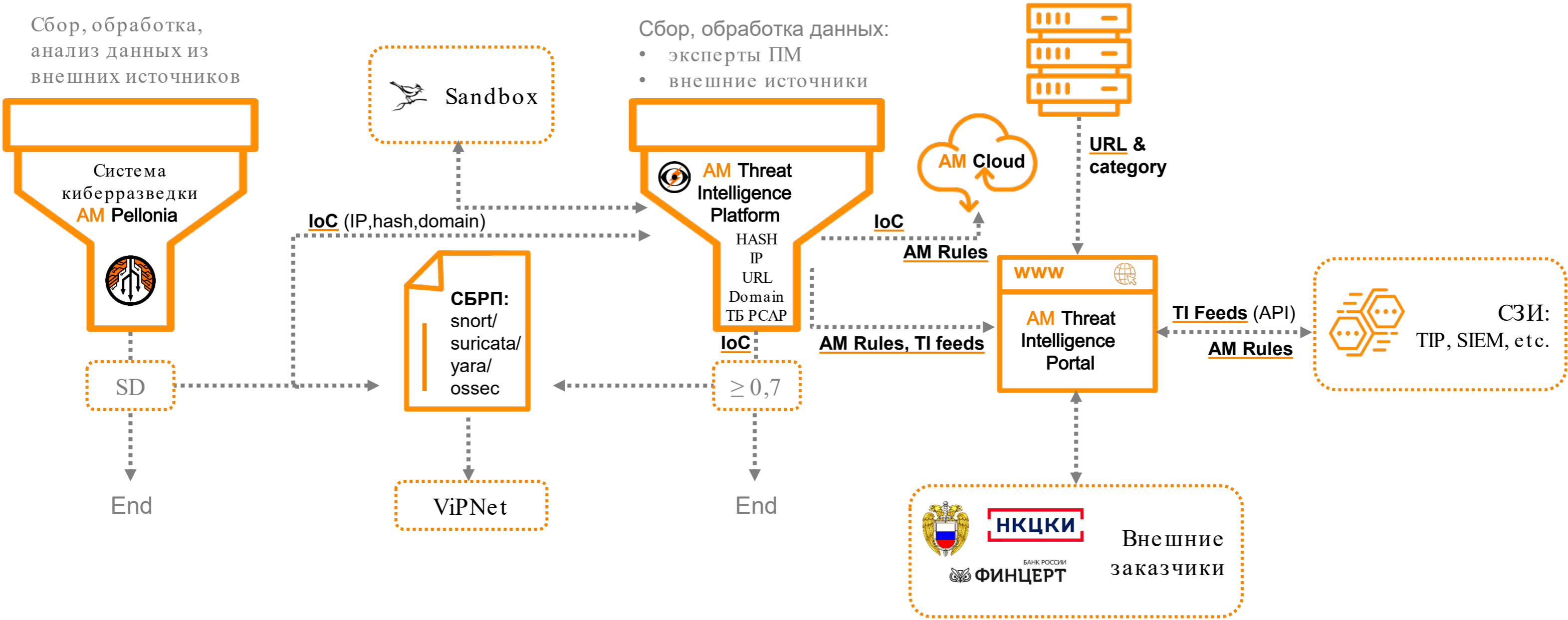
Категорированные веб-ресурсы

5

Бюллетени ИБ



# Как устроено



# Статистика IoC



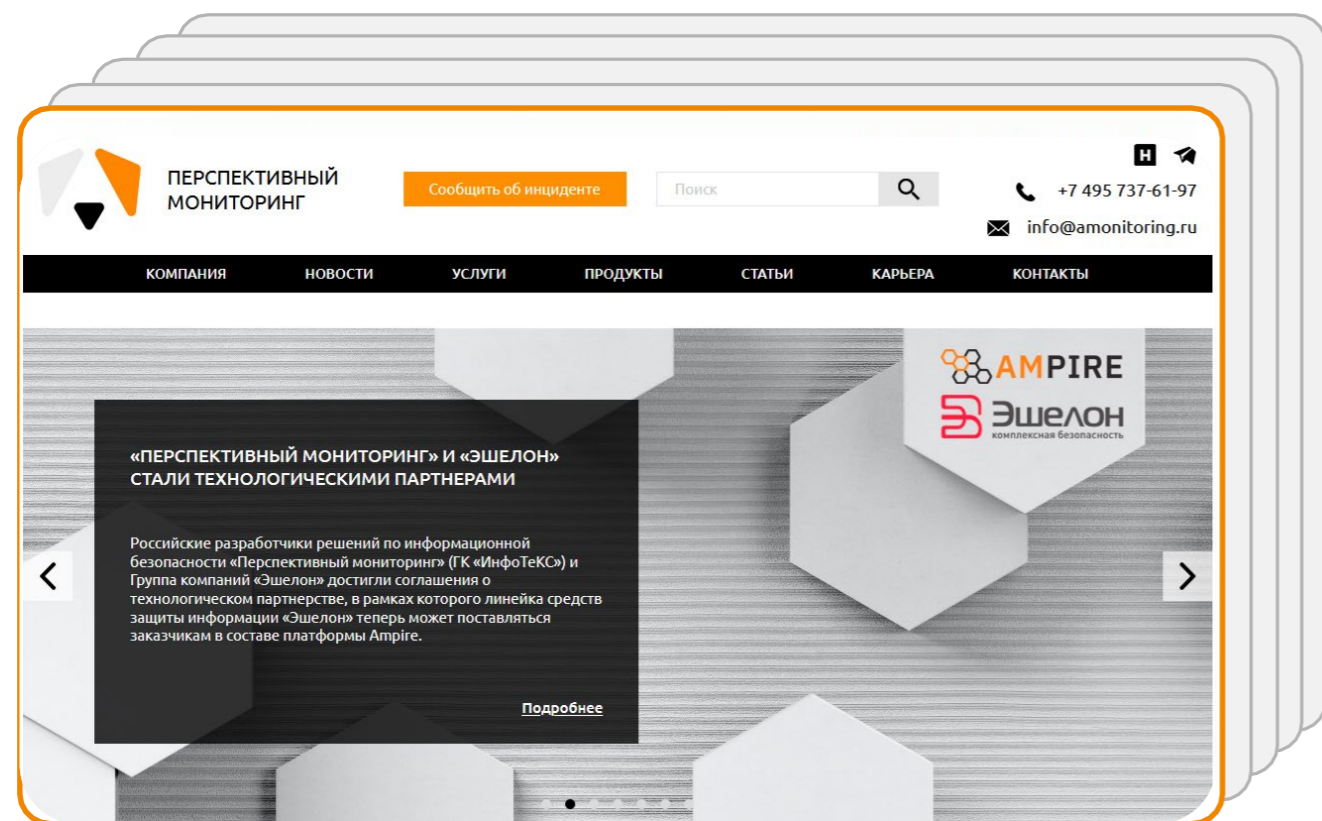
Периодичность	IP	Domain	Hash	URL	Samples
В день ~	3 100	1400	3200	37 400	876
В неделю ~	21 800	10 000	22 700	262 115	6 100
В месяц ~	87 300	40 200	91 100	1 048 400	24 500

> 2 000 000 samples pcap

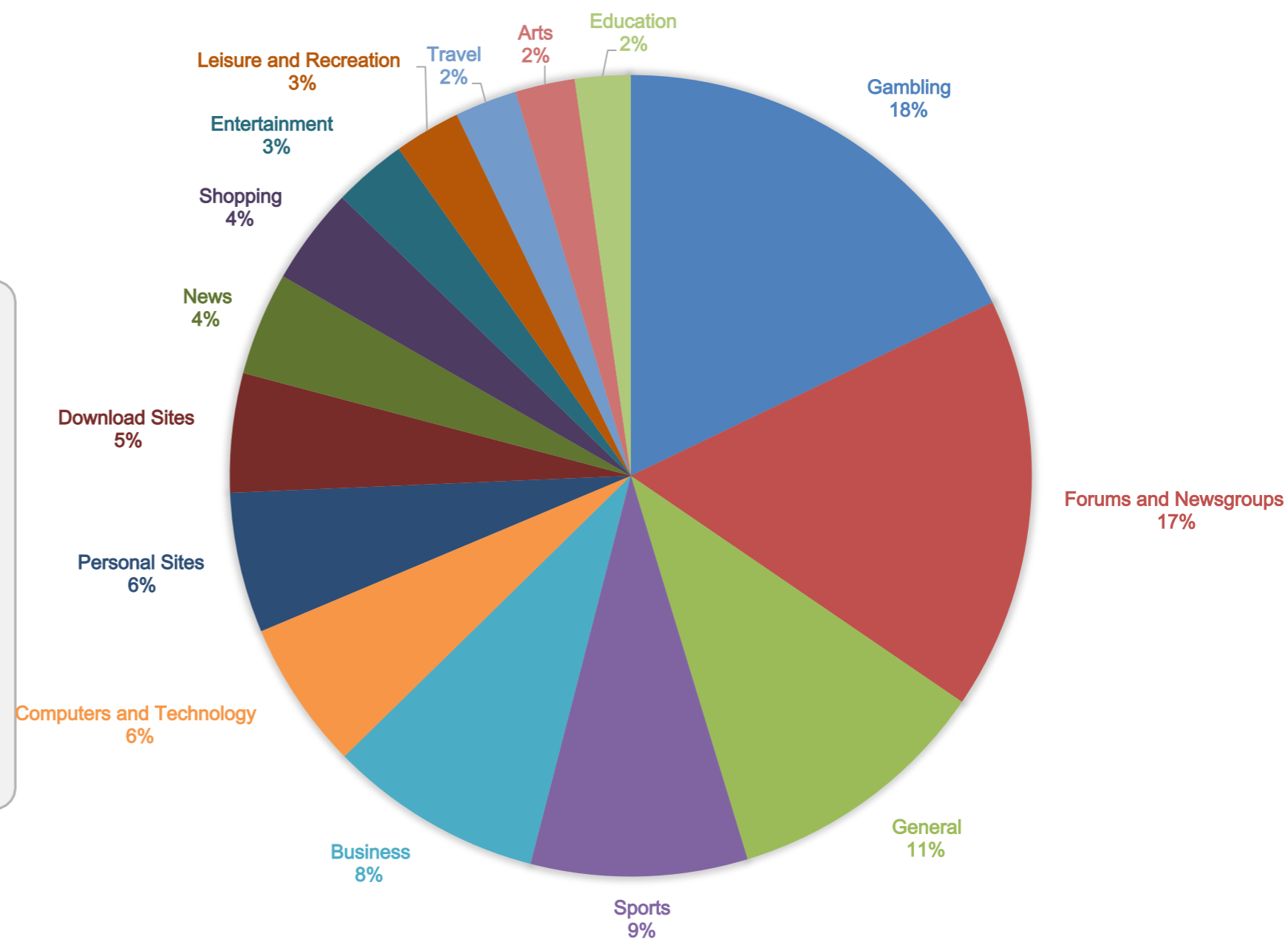
TOTAL	>100 000 000 IP, domain, url, hash, samples				
-------	---	--	--	--	--

# URL-фильтрация

- 80 категорий
- > 90 млн. доменов




TOP 15 КАТЕГОРИЙ



# Бюллетени ИБ



Информационный бюллетень Центра мониторинга АО «ПМ»

Название документа	<b>Уязвимость “MonikerLink” в Microsoft Outlook</b>
Разослан	2024-03-05
Идентификатор	AM-2024-ALE-0305-01
 Описание угрозы	<b>CVE-2024-21413</b> <b>CVSSv3.1: 9.8, AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</b> <b>Объект уязвимости:</b> Компонент библиотеки ole32.dll в Microsoft Outlook <b>Требования к атакующему:</b> Удаленный неаутентифицированный <b>Максимальный результат атаки:</b> Удаленное исполнение кода





## Меры противодействия



### Использовать правило ViPNet IDS NS:

- sid 3285268 "AM EXPLOIT Microsoft Windows Outlook NTLM Credentials Leak aka 'MonikerLink' (CVE-2024-21413)"



### Использовать правило ViPNet IDS HS / ViPNet EPP:

- 902486 "Подозрение на эксплуатацию MonikerLink в Microsoft Outlook"



### Использовать метаправило ViPNet TIAS:

- Раскрытие NTLM-хэша аутентификации в Microsoft Outlook (CVE-2024-21413)

## Ссылки на источники

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413>
- <https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture>

# Экспертные данные АО «ПМ»



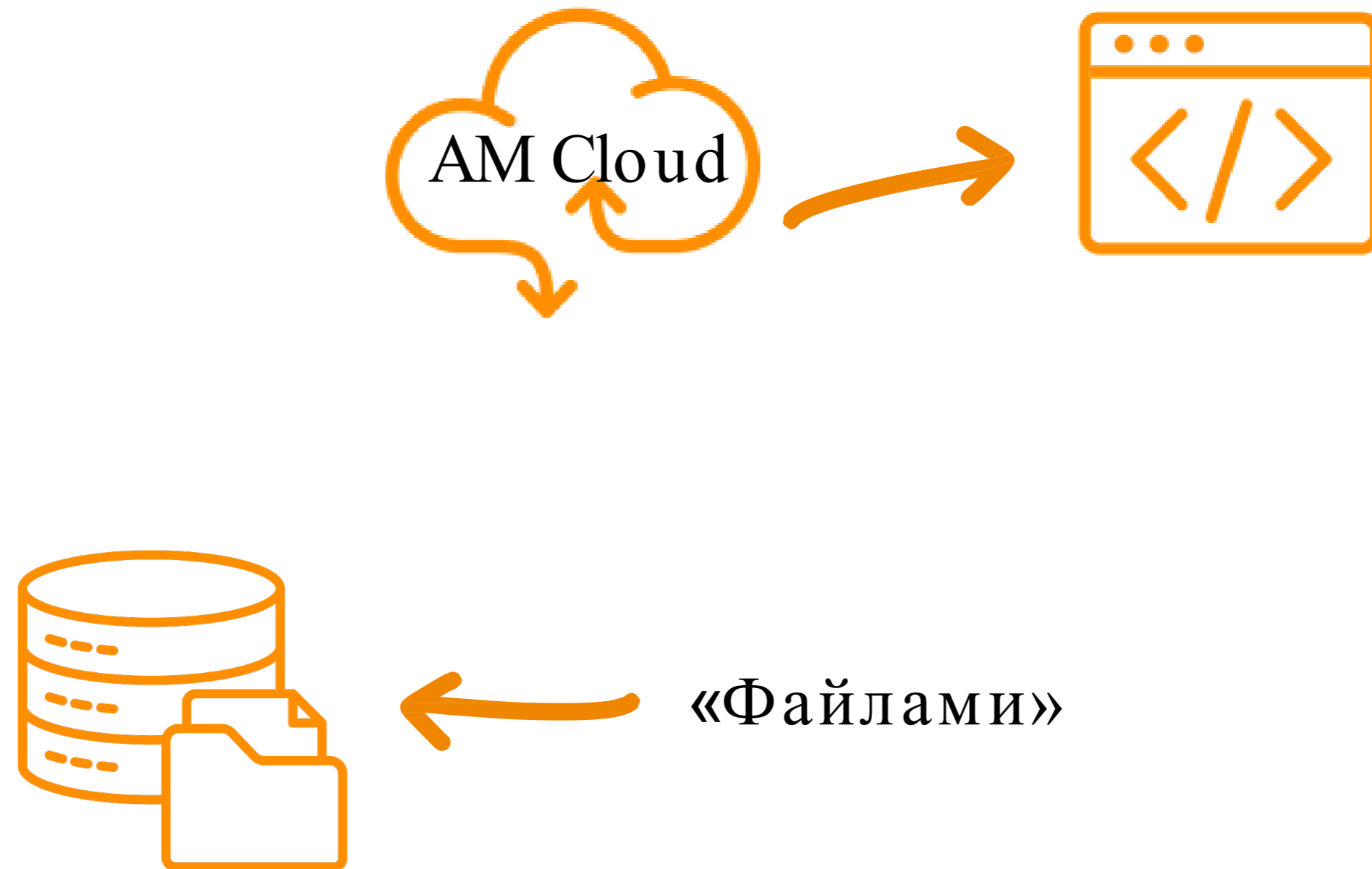
Snort / Suricata / yara / ossec  
> 400 000 правил/сигнатур

URL-фильтрация  
90 млн. доменов

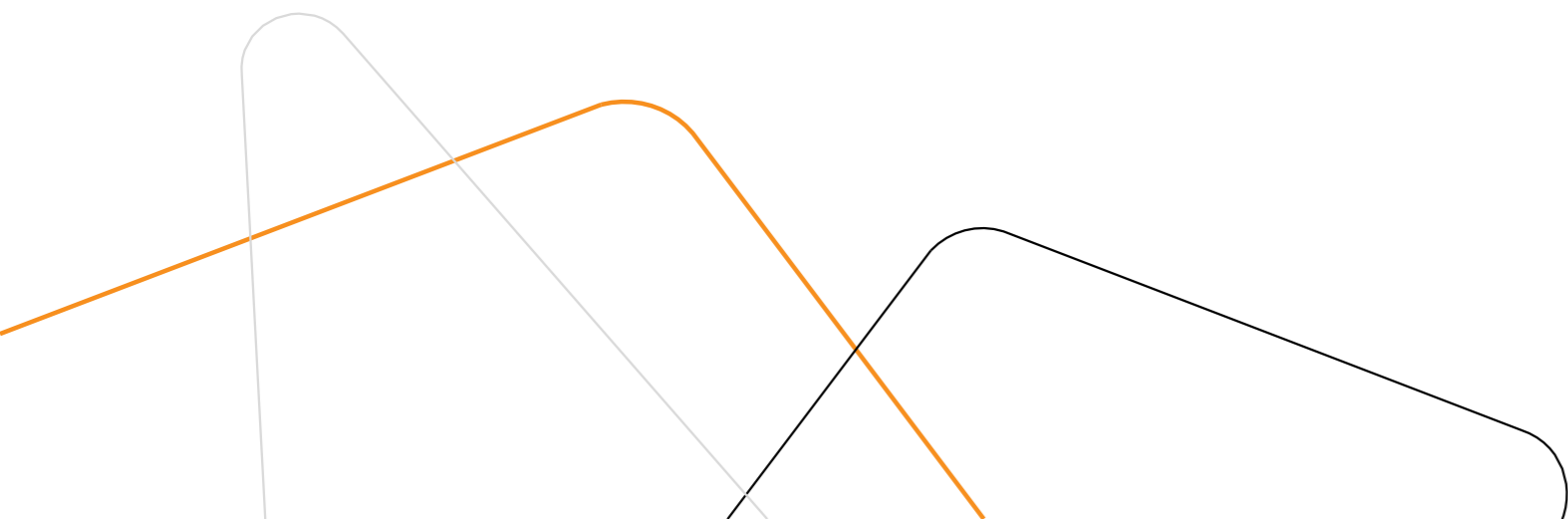


IP, Domain, URL, Hash  
STIX2.1 > 4 млн. IoC

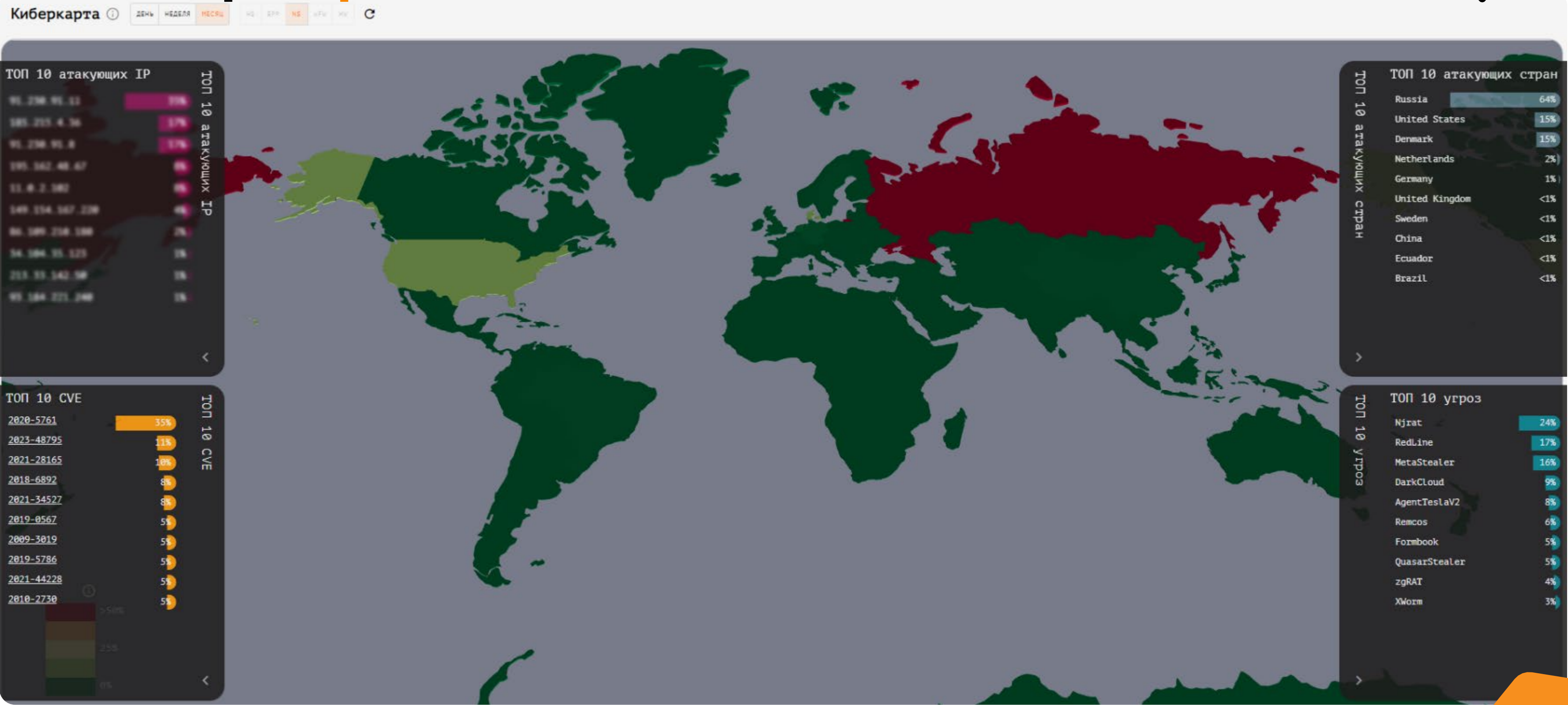
# Способы доставки ЭД



# AM Threat Intelligence Portal



# Киберкарта



# Поиск по domain



ПОИСК

Обнаруженные угрозы

**AM SCORE 0.72**

4/89

Результаты для: mlcrosoft.site

Домен верхнего уровня: -  
Местонахождение: -  
Дата первого появления: 9 окт., 2021 04:00  
Дата последнего обновления: 12 нояб., 2023 07:41  
TTP: T1566

Метки образца: -  
Чёрные списки: -  
Алгоритм генерации доменов (DGA): Нет

Категории: -

Правила/Сигнатуры 1

sid	Время изменения	Название	Группы	TTP
3208272	04.03.24 12:31	AM DNS Query for mlcrosoft.site (Winnti APT41 // Operation Cuckoo bees)	dns	T1608.001 TA0011

Краткое описание

Правило реагирует на запрос к домену mlcrosoft.site, связанному с Winnti APT41 // Operation Cuckoo bees

Полное описание

Правило реагирует на запрос к домену mlcrosoft.site, связанному с Winnti APT41 // Operation Cuckoo bees

Критичность: Низкая  
Типы атаки: Вредоносный ресурс  
Платформы: -

Исходный текст

```
alert udp $HOME_NET any -> any 53 (msg:"AM DNS Query for mlcrosoft.site (Winnti APT41 // Operation Cuckoo bees)"; content:"|01 0000 01 000000000000|"; depth:10; offset:2; content:"|09|mlcrosoft|04|site|00|"; fast_pattern; nocase; distance:0; reference:url,virustotal.com/en/url/546945477931fc298b4cfa8880e5d12697d338d0aa2605aa42210740ca73d97a/analysis; reference:url,ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new; classtype:trojan-activity; sid:3208272; rev:2; metadata: affected_asset src, affected_product n/a, affected_vendor n/a, attack_target Client_Endpoint, tag T1608.001, tag TA0011, tias_category Malware;)
```

SNORT SURICATA

РАЗВЕРНУТЬ

НАЗВАНИЯ ОБЪЕКТОВ

ПО ЦЕНТРУ

- Analysis-tool
- Domain-name
- Indicator
- Malware-analysis
- Url

Обзор

Whois: Create date: 2021-05-27 Domain name: mlcrosoft.site Domain registrar id: 1556 Domain registrar url: http://www.west263.com ...

Связные IP-адреса: -

Поддомены: online.mlcrosoft.site, ns2.mlcrosoft.site, ns1.mlcrosoft.site

# Поиск по URL

http://tuginsaat.com/

ПОИСК



Обнаруженные угрозы

AM SCORE 0.47

Результаты для: http://tuginsaat.com

Домен: tuginsaat.com  
IP-адрес: 93.89.224.19  
Местонахождение: Турция, Стамбул 🇹🇷  
Дата первого появления: 11 июля, 2020 02:23  
Дата последнего обновления: 30 окт., 2023 17:01  
TTP: -

Метки образца: -  
Чёрные списки: -

Категории: uncategorized

Правила/Сигнатуры 1

sid	Время изменения	Название	Группы	TTP
900126	23.12.21 17:33	legion_777		T1587.001

Краткое описание

Полное описание

Критичность: -  
Типы атаки: -  
Платформы: -

Исходный текст

```
rule legion_777
{
  meta:
    sid = "900126"
    description = "Обнаружен шифровальщик Legion_777"

    reference = ""
    techniques = "T1587.001"
    capec = ""
    cwe = ""
    cve = ""

  strings:
    $s1 = "http://tuginsaat.com/wp-content/themes/twentythirteen/stats.php"
    $s2 = "read_this_file.txt" wide
    $s3 = "seven_legion@india.com"
    $s4 = {46 4f 52 20 44 45 43 52 59 50 54 20 46 49 4c 45 53 0d 0a 53 45 4e 44 20
4f      4e 45 20 46 49 4c 45 20 49 4e 20 45 2d 4d 41 49 4c 0d 0a 73 65 76 65 6e
5f      6c 65 67 69 6f 6e 40 69 6e 64 69 61 2e 63 6f 6d }
    $s5 = "%s_%02i-%02i-%02i-%02i-%02i_%$s$.777"

  condition:
    4 of ($s*)
}
```

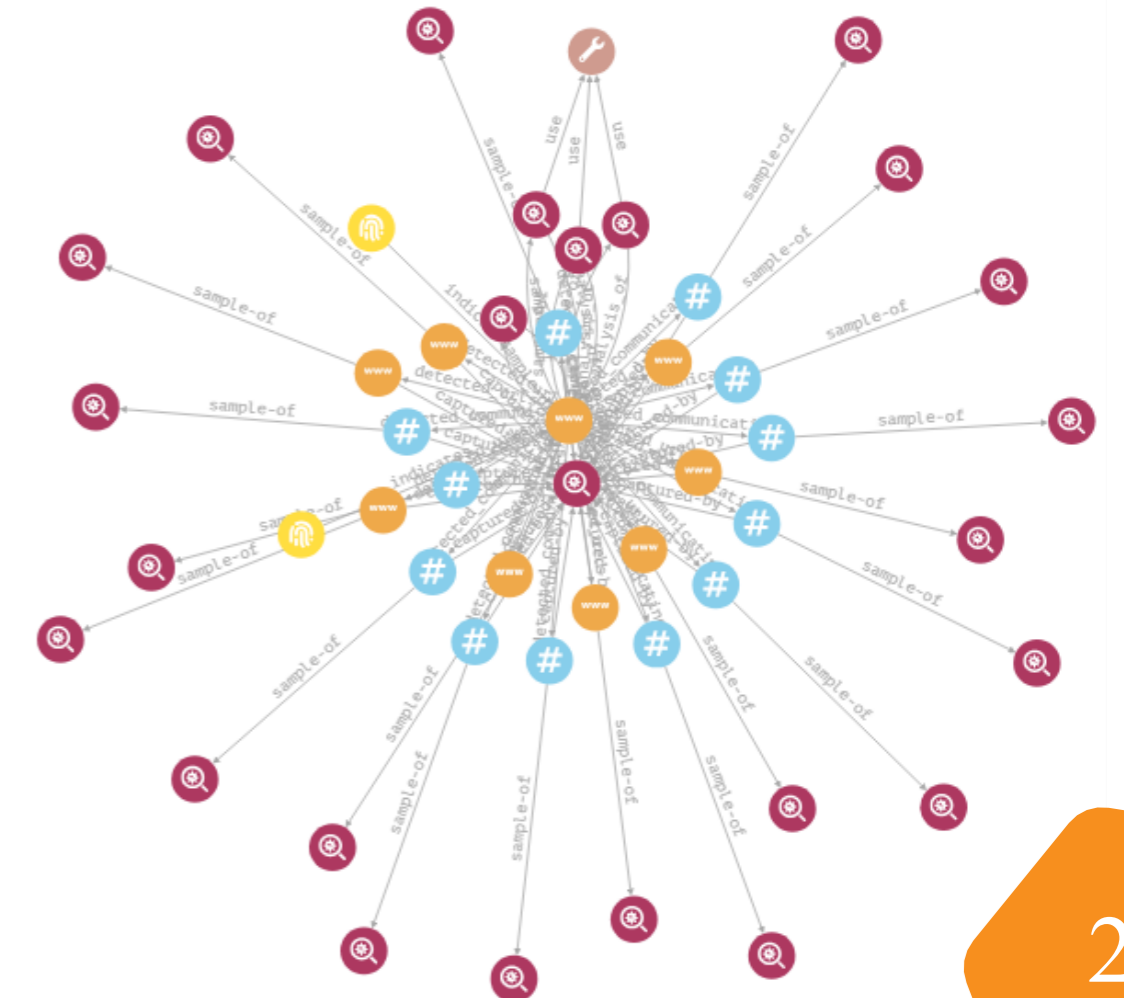
YARA

РАЗВЕРНУТЬ ↗

НАЗВАНИЯ ОБЪЕКТОВ

ПО ЦЕНТРУ

Analysis-tool # File # Indicator # Malware-analysis # Url



# Поиск по IP



185.205.209.166 ПОИСК

Обнаруженные угрозы  
**AM SCORE 0.72**  
2/80

Результаты для: 185.205.209.166  
Сеть: 185.205.208.0/22  
ASN: 44901  
Владелец ASN: BelCloud Hosting Corporation  
Местонахождение: Болгария, София  
Дата первого появления: 24 мая, 2020 07:00  
Дата последнего обновления: 5 янв., 2024 05:44  
ТИП: IP  
Метки образца: -  
Чёрные списки: -  
Категории: malware

Правила/Сигнатуры 1

sid	Время изменения	Название	Группы	TTP
3086102	21.04.24 02:03	AM CURRENT_EVENTS HTTP request to malicious IP endpoint in header 185.205.209.166	current_events	

Краткое описание  
Правило реагирует на запрос к IP-адресу 185.205.209.166

Полное описание  
Правило реагирует на запрос к IP-адресу 185.205.209.166 VBA/Agent.Downloader

Критичность: Низкая  
Типы атаки: Вредоносный ресурс  
Платформы: -

Исходный текст

```
alert tcp $HOME_NET any -> any any (msg:"AM CURRENT_EVENTS HTTP request to malicious IP endpoint in header 185.205.209.166"; threshold:type limit, track by_src, count 1, seconds 120; content:"|0d0a|Host: 185.205.209.166|0d0a|"; reference:url,virustotal.com/gui/url/dc8259045d603f6006037218a8a70eef11810d82b7920e2d36d0661fcac64d0b/detection; classtype:trojan-activity; sid:3086102; rev:4; metadata: affected_asset src, affected_product microsoft:visual_basic, affected_product microsoft:windows, affected_product vba, affected_vendor microsoft, attack_target Client_Endpoint, tag AM.ARMA, tias_category Malware;)
```

SNORT SURICATA

РАЗВЕРНУТЬ НАЗВАНИЯ ОБЪЕКТОВ ПО ЦЕНТРУ

Analysis-tool Domain-name File Indicator Ipv4-addr  
Malware-analysis Url



# Поиск по hash



0077d8598d334bc73a2d3542407db8c17a465c8c6921599b9bec41a96684a4b9

ПОИСК

Обнаруженные угрозы

AM SCORE 0.5

31/73

Результаты для: 0077d8598d334bc73a2d3542407db8c17a465c8c6921599b9bec41a96684a4b9

Размер: 908.0 КБ  
Дата первого появления: 3 авг., 2020 01:27  
Дата последнего обновления: 31 авг., 2023 14:51  
Тип файла: PE32 executable  
TTP: [IA0011](#)  
Тактики: -  
Техники: -  
Категории: -

Метки образца: Win32/Emotet.CO//Trojan.Downloader34.10773  
Потенциально нежелательное приложение (PUA): Нет



Правила/Сигнатуры 0

sid	Время изменения	Название	Группы	TTP
Отсутствуют данные				

Обзор

MD5: ef83298484ce05152ac1d6bb06dbaaa9  
SHA-1: b2c829299a9b6b103587b052361313cc5f1d5cc0  
SHA-256: 0077d8598d334bc73a2d3542407db8c17a465c8c6921599b9bec41a96684a4b9  
SSDEEP: 12288:W/J+NC0xu2rPcHKeNmcZvF/SZGYzZ5Q/zN:sJ8...mcVF/mGY4LN  
TLSH: -  
Размер: 908.0 КБ  
Тип файла: PE32 executable  
TrID: (.EXE) Win32 Executable MS Visual C++ (generic) (31206/45/13)(47.3%), (.EXE) Win64 Executable (generic) (10523/12/4)(15.9%), (.DLL) Win32 Dynamic Link Library (g...

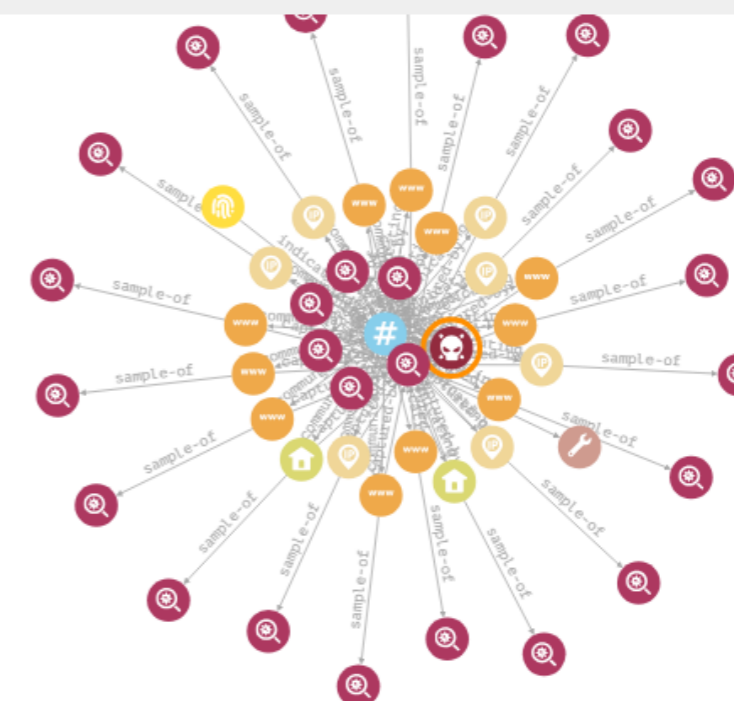
Связи

Связанные URL-адреса

Дата последнего обновления	Ссылка	Обнаружения
5 дек., 2020 07:02	<a href="http://185.94.252.13/iazGFCroyA/iUZk78/GLGoSCTAYpDPmBE1gg">http://185.94.252.13/iazGFCroyA/iUZk78/GLGoSCTAYpDPmBE1gg</a>	0 / 0
5 дек., 2020 07:01	<a href="http://185.94.252.13/w0kIcBt1z958Eu0g9gG/@p2GF22wyFaPHHU/sknqpJ4C25T/YSSoHqwtPZtFDwL">http://185.94.252.13/w0kIcBt1z958Eu0g9gG/@p2GF22wyFaPHHU/sknqpJ4C25T/YSSoHqwtPZtFDwL</a>	0 / 0

РАЗВЕРНУТЬ НАЗВАНИЯ ОБЪЕКТОВ ПО ЦЕНТРУ

Analysis-tool Domain-name File Indicator Ipv4-addr Malware  
Malware-analysis Url



id: "malware--3e5018e8-2b17-43ec-b38f-b64262d0397d",  
spec\_version: "2.1",  
type: "malware",

# Поиск по CVE

2023-23397

ПОИСК

## Правила/Сигнатуры

sid	Время изменения	Название	Группы	TTP
3220816	20.04.24 23:53	AM EXPLOIT Possible Microsoft Outlook NTLM-relay Attack via phishing e-mail (CVE-2023-23397)	exploit	T1566

### Краткое описание

Правило реагирует на возможную попытку атаки NTLM Relay посредством фишингового письма, содержащего эксплуатацию уязвимости повышения привилегий в Microsoft Outlook

### Полное описание

Данная уязвимость в компоненте MS Outlook, отвечающем за календарь событий, затрагивает все версии продукта для операционной системы Windows и представляет собой повышение привилегий посредством кражи NTLM-хэша аутентификации жертвы. Уязвимые параметры - "PidLidReminderFileParameter", значение которого указывает на путь до файла - звукового оповещения календаря, и "PidLidReminderOverride". Злоумышленник должен отправить специально сформированное письмо, содержащее путь до пользовательского звука оповещения, значением которого является SMB-адрес, что при открытии письма жертвой приведет к отправке Net-NTLMv2 хэша аутентификации на этот адрес и последующей краже конфиденциальных данных. Отличительная особенность данной уязвимости в том, что для эксплуатации не требуется действий от пользователя, кроме как открыть фишинговое письмо (0-click уязвимость). Правило реагирует на следующие фрагменты письма: \* |1f 85 00 00| - идентификатор параметра "PidLidReminderFileParameter" \* |1c 85 00 00| - идентификатор параметра "PidLidReminderOverride" \* |5c 00 5c 00| - "\\", указывающее на наличие UNC-пути до сетевого ресурса \* |08 20 06 00 00 00 00 00 c0 00 00 00 00 00 46| - GUID множества параметров, к которому принадлежит "PidLidReminderFileParameter" \* |02 20 06 00 00 00 00 00 c0 00 00 00 00 00 46| - GUID множества параметров, к которому принадлежит "PidLidReminderOverride"

Критичность: Высокая

Типы атаки: Эксплуатация уязвимостей

Платформы: windows

### Исходный текст

```
alert tcp $EXTERNAL_NET any -> $HOME_NET [25,110,143,193,587,995] (msg:"AM EXPLOIT Possible Microsoft Outlook NTLM-relay Attack via phishing e-mail (CVE-2023-23397)"; flow:established,to_server; content:"|1f 85 00 00|"; fast_pattern; content:"|08 20 06 00 00 00 00 00 c0 00 00 00 00 00 46|"; distance:0; content:"|1c 85 00 00|"; content:"|02 20 06 00 00 00 00 00 c0 00 00 00 00 00 46|"; distance:0; content:"|5c 00 5c 00|"; reference:cve,2023-23397; reference:url,mdsec.co.uk/2023/03/exploiting-cve-2023-23397-microsoft-outlook-elevation-of-privilege-vulnerability; reference:url,msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397; reference:url,github.com/sqrtZeroKnowledge/CVE-2023-23397_EXPLOIT_0DAY/blob/main/MsgKitTestTool/AppointmentTest.cs; classtype:file-format; sid:3220816; rev:2; metadata: affected_asset dst, affected_os Windows, affected_product 1c, affected_product microsoft:365_apps, affected_product microsoft:office, affected_product microsoft:outlook, affected_product microsoft:windows, affected_vendor 1c, affected_vendor microsoft, attack_target Client_Endpoint, attack_target Mail_Server, tag T1566, tias_category Exploitation, tias_category Phish;)
```

SNORT SURICATA

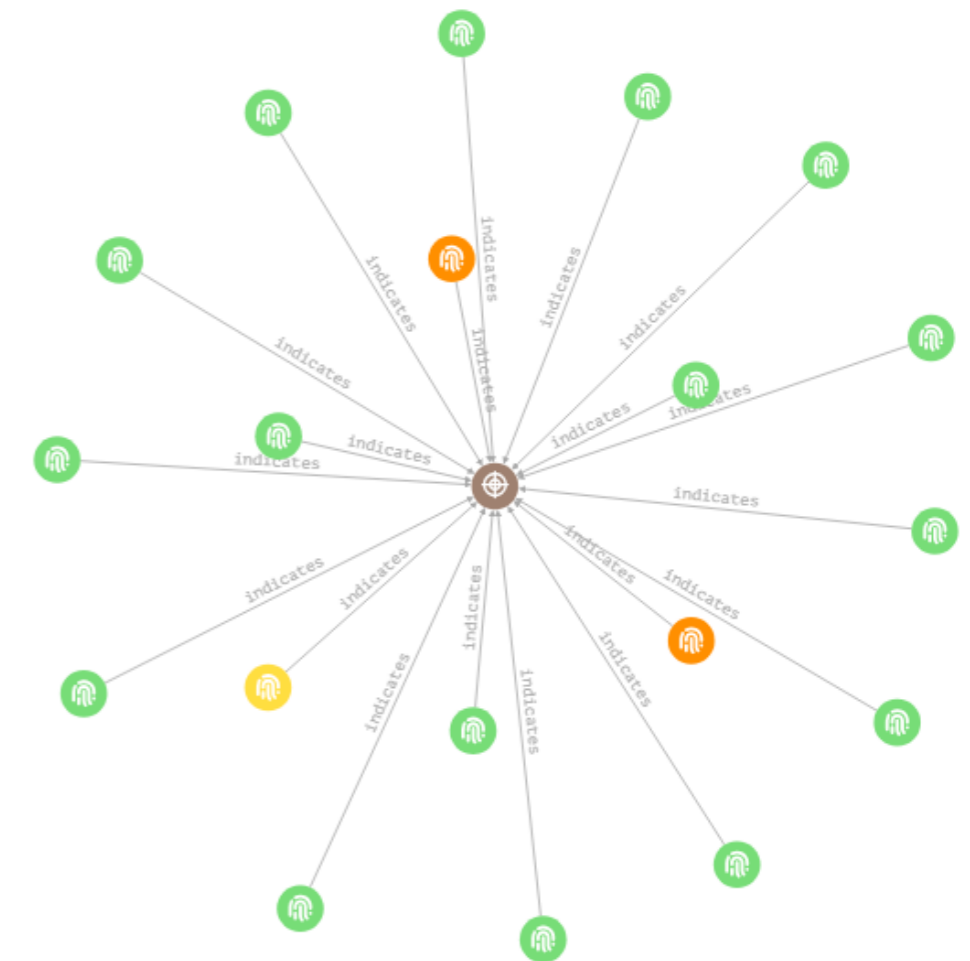
2044687	04.03.24 12:58	ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M8 (CVE-2023-23397)	exploit	-
2044686	04.03.24 12:58	ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M7 (CVE-2023-23397)	exploit	-
2044685	04.03.24 12:58	ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M6 (CVE-2023-23397)	exploit	-
2044684	04.03.24 12:58	ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M5 (CVE-2023-23397)	exploit	-

РАЗВЕРНУТЬ

НАЗВАНИЯ ОБЪЕКТОВ

ПО ЦЕНТРУ

Indicator Vulnerability



# Доп. функционал



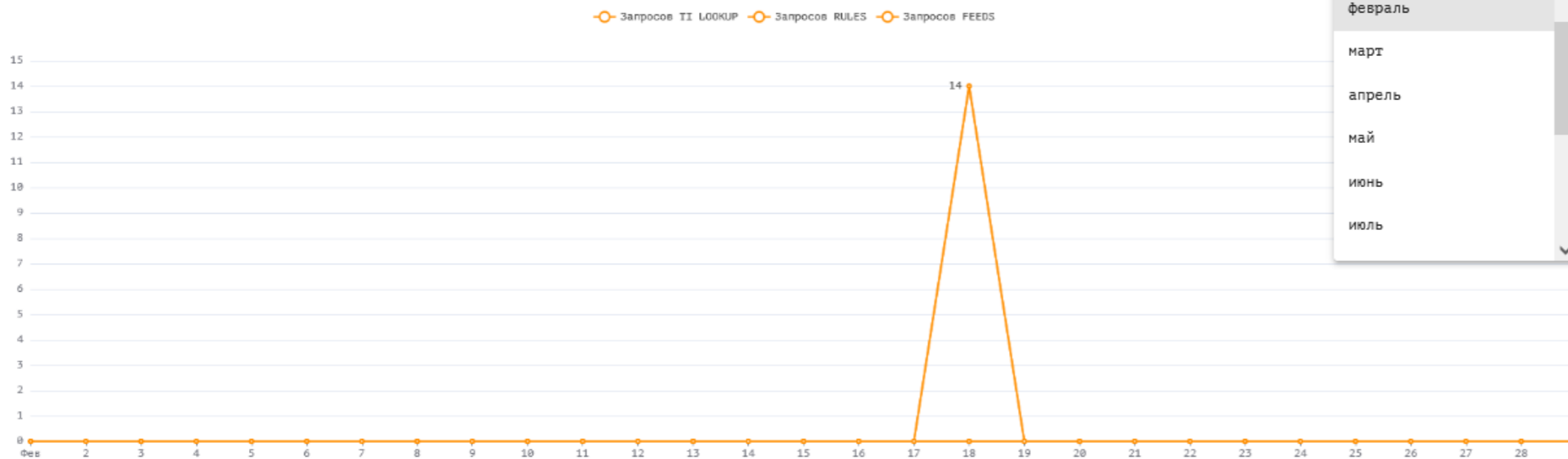
API key

API key: \*\*\*\*\*

Квоты на запросы

Запросов TI LOOKUP в минуту: 0/6  
Запросов TI LOOKUP в день: 14/3000  
Запросов RULES в минуту: 0/6  
Запросов RULES в день: 0/10000  
Запросов FEEDS в минуту: 0/6  
Запросов FEEDS в день: 0/10000

Использование квот на запросы



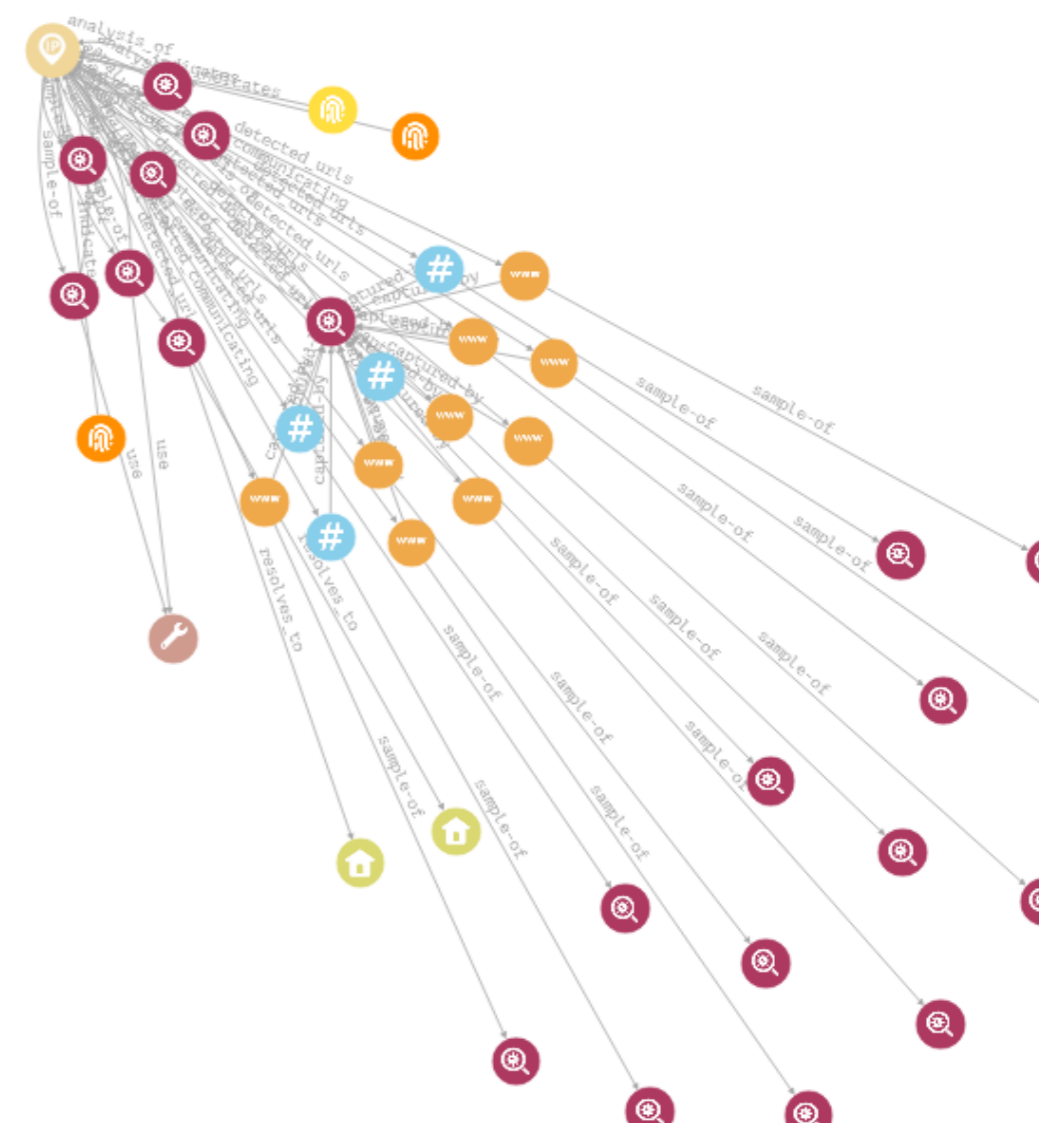
Загрузки

Правила snort: TXT  
Правила suricata: TXT  
IoC: STIX 2.1

РАЗВЕРНУТЬ

НАЗВАНИЯ ОБЪЕКТОВ

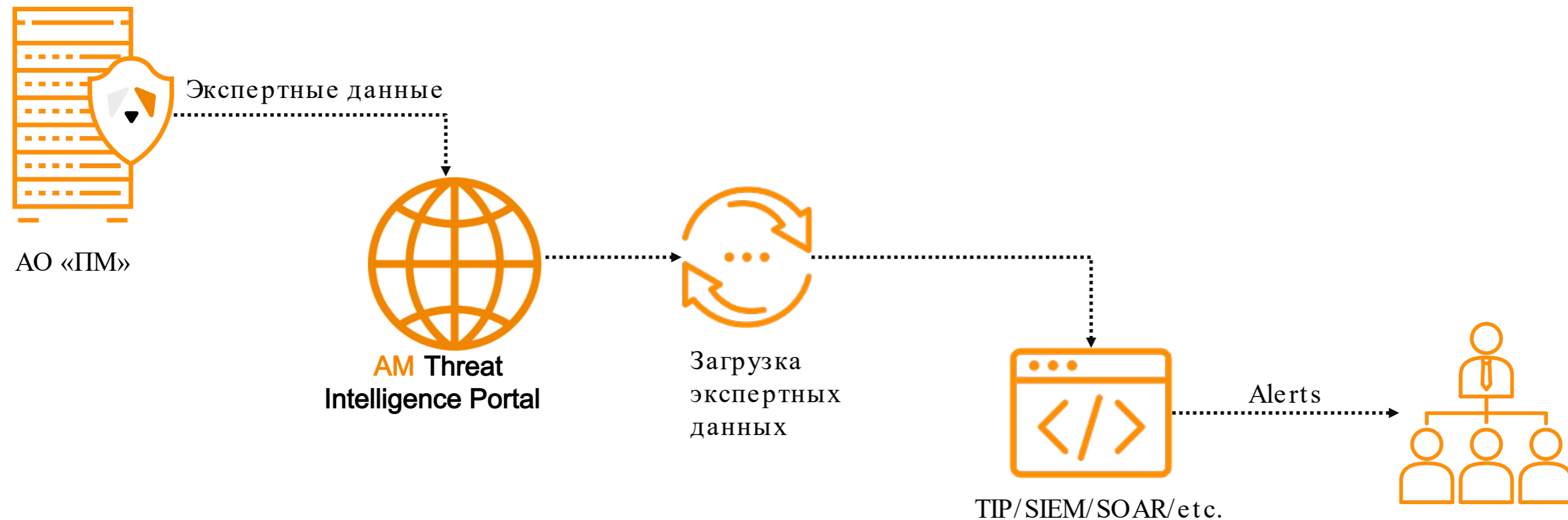
Analysis-tool Domain-name File Indicator Ipv4-addr  
Malware-analysis Url





# Как использовать ЭД

для выявления подозрений на компьютерные инциденты или атаки



# Пример использования:



**ЗАПРОС НА ЗАКРЫТИЕ** - Попытки эксплуатации уязви

Создан: 2023-06-12 05:46:07    Просмотрен заказчиком:  
Изменен: 2023-06-13 17:14:17    Закрыт:

**ОТПРАВЛЕН ЗАКАЗЧИКУ**    **УДАЛИТЬ**

**Общая информация**  
Попытки эксплуатации уязвимости

Уровень важности: **ВЫСОКИЙ**

Описание: Фиксируем попытки эксплуатации уязвимости в CMS Bitrix на ресурсе [redacted] путем обращения к модулю html\_editor\_action.php, связанному с уязвимостью удаленного [redacted]

**Местоположение**  
Сегменты: [redacted]  
Сенсоры: [redacted]

**Пользователи**  
Автор: [redacted]  
Оператор: [redacted]  
ЛИНИЯ: 2

**НКЦКИ**  
**ОТПРАВИТЬ В НКЦКИ**

**Работы**  
**РЕКОМЕНДАЦИИ**    ПРЕДПР >

- Денис: Заблокировать на МЭ адрес истс [redacted]
- Денис: Провести обновление CMS Bitrix [redacted]
- Денис: Провести аудит узлов на предме [redacted]
- Денис: Воспользоваться модулем: https [redacted]

**СОБЫТИЯ** +    **ИСТОРИЯ**    **КОММЕНТАРИИ**    **ФАЙЛЫ** +    **ЗАТРОНУТЫЕ АКТИВЫ** +    **IOCS** +

ViPNet\_IDS

Дата	Сенсор	Sid	Узел	Источник	Получатель	Событие	Объект	Домен	Действия
2023-06-12 05:11:09		3202933		91.198.		AM EXPLOIT Possible Bitrix CMS < v...			<input type="checkbox"/> <i>i</i>
2023-06-12 05:11:10		3202933		91.198.		AM EXPLOIT Possible Bitrix CMS < v...			<input type="checkbox"/> <i>i</i>
2023-06-12 05:11:10		3202933		91.198.		AM EXPLOIT Possible Bitrix CMS < v...			<input type="checkbox"/> <i>i</i>
2023-06-12 05:11:10		3202933		91.198.		AM EXPLOIT Possible Bitrix CMS < v...			<input type="checkbox"/> <i>i</i>

# В чём profit?

Indicator Report

## https://i-trust.dk

Reputation Score



Community Score

⚠ 3 security vendors flagged this URL as ma

http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif  
fmc.org.in

## Отчет

Отчет для веб-адреса

http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif

✓ Безопасный

4/68

AM SCORE 0.77

IBM X-Force Threat Intelligence has introduced exciting changes

Риск  
1

Отчет X-Force об URL

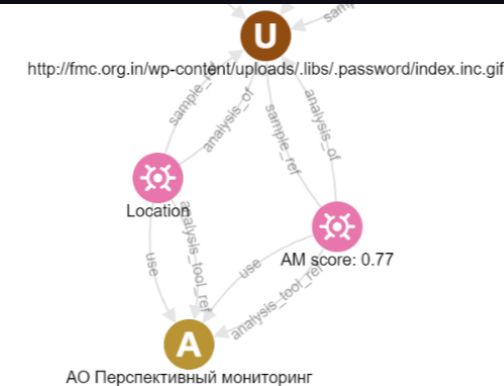
https://i-trust.dk/

Ссылка Detections

No data available

Хеш Detections

No data available



# AM Threat Intelligence Portal

РОССИЙСКАЯ ФЕДЕРАЦИЯ **RU** **2024614349**



ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

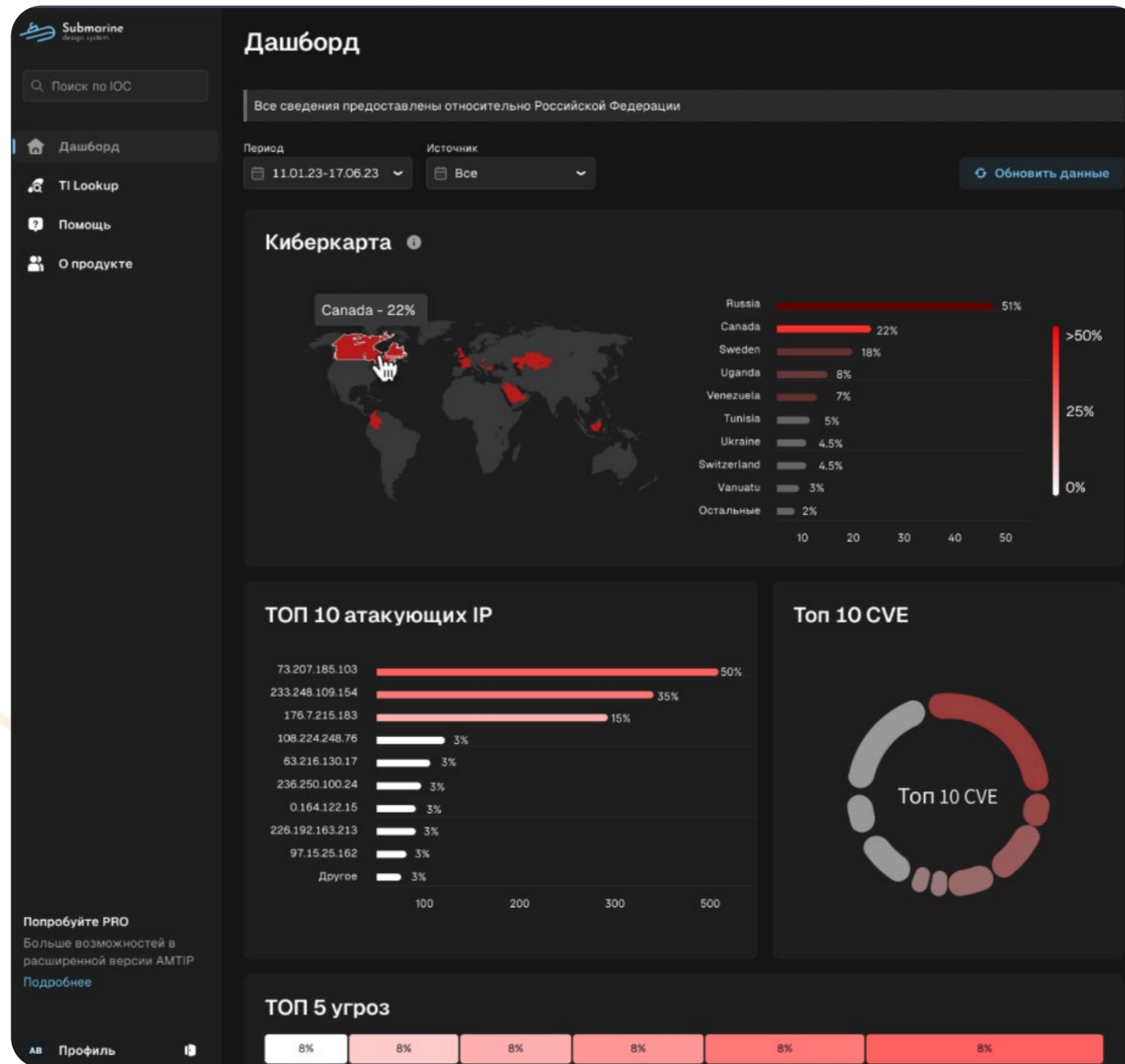
Номер регистрации (свидетельства): <b>2024614349</b>	Правообладатель: <b>АКЦИОНЕРНОЕ ОБЩЕСТВО " ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ" (RU)</b>
Дата регистрации: <b>22.02.2024</b>	
Номер и дата поступления заявки: <b>2024613368 22.02.2024</b>	
Дата публикации: <b>22.02.2024</b>	

Название программы для ЭВМ:  
**AM Threat Intelligence Portal**

Реферат:  
AM Threat Intelligence Portal предназначен для предоставления актуальной информации об угрозах по идентификаторам уязвимостей, IP (интернет протокол)-адресам, хэшам, доменам и адресам ресурса в сети Интернет (URL), что позволяет автоматизировать деятельность и специалистов по информационной безопасности, обеспечить безопасность организации и повысить эффективность реагирования на инциденты. Система предоставляет следующие возможности: Просмотр аналитической информации по угрозам на карте мира; Возможность просмотра комплексных сведений по индикатору компрометации и получения сведений как по интеграции, так и в ручном режиме.



# AM Threat Intelligence Portal 2.0





# Спасибо за внимание!



[t.me/pm\\_public](https://t.me/pm_public)



[@AMonitoring](https://www.youtube.com/@AMonitoring)



[amtip.ru](http://amtip.ru)

Артём Савчук

Технический директор

+7 (495) 737-61-97

[info@amonitoring.ru](mailto:info@amonitoring.ru)