Threat Intelligence Portal

Артём Савчук,
Технический директор,
«Перспективный мониторинг»

Регионы присутствия АО «ПМ»

АО «ПМ» сегодня

13

лет на рынке услуг SOC и исследования защищённости

7

лет центр ГосСОПКА (А)

>1600

выполненных ИБ проектов

19

действующих киберполигонов Ampire

300+

проведенных киберучений

3000+

ИБ специалистов прошли обучение на Ampire

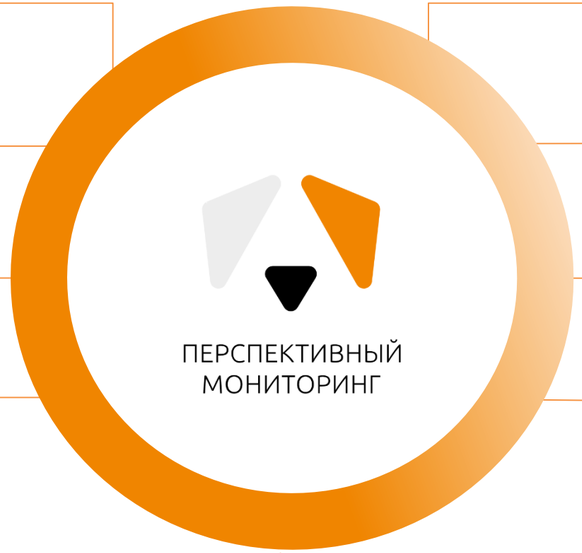
Направления деятельности

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



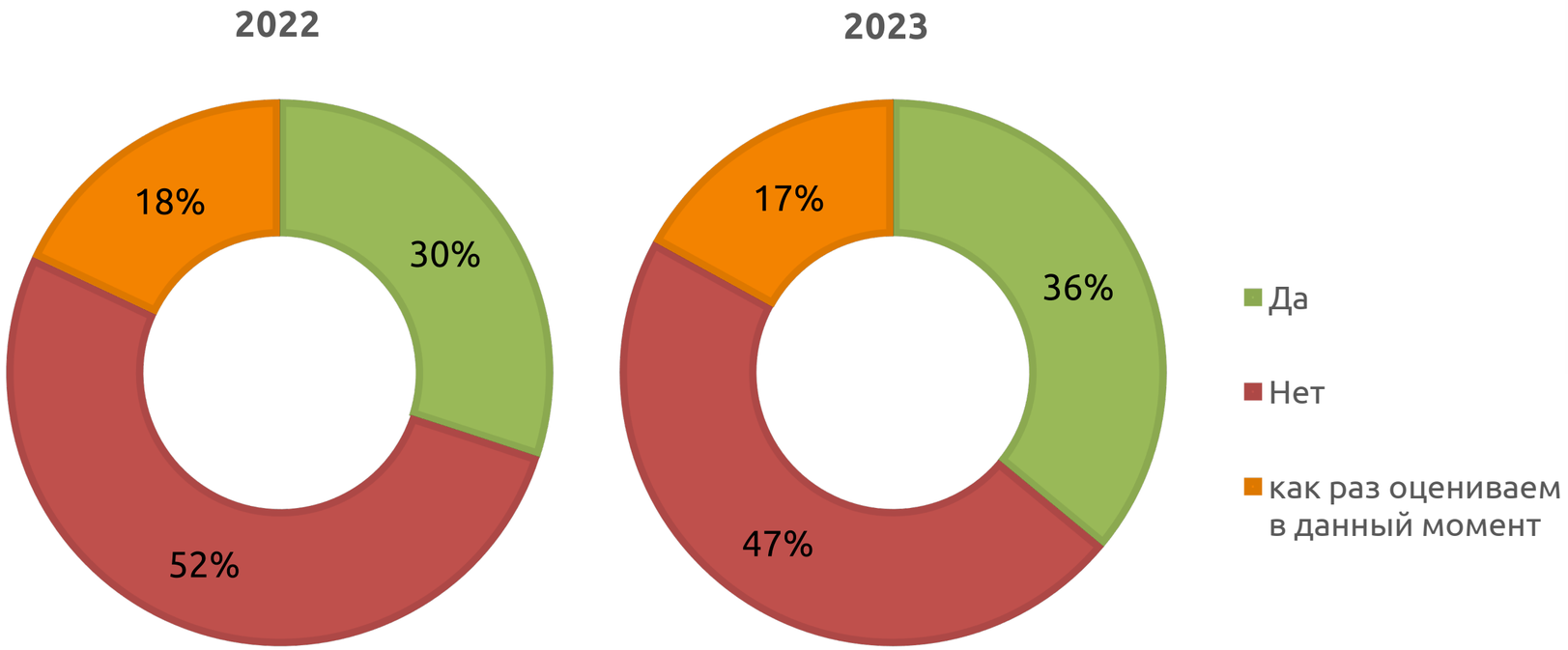
Продукты

- Экспертные данные
- БРП (AM Rules)
- AM TI Portal
- Киберполигон Ampire

Сквозная экспертиза по всем направлениям деятельности

«Мастхев» ли киберразведка (TI)?

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



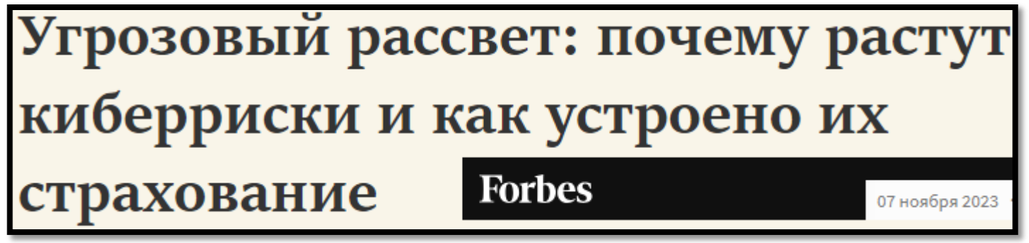
Бизнес пошел в контрразведку

Спрос на услуги предотвращения киберинцидентов растет

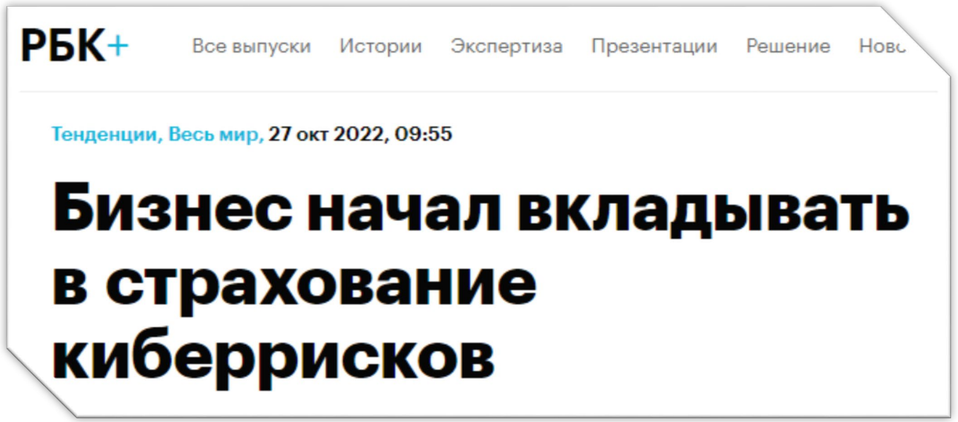
Рост числа киберинцидентов подтолкнул организации чаще обращаться за услугами специалистов по расследованию и предотвращению таких событий: мониторингу теневых форумов, анализу объявлений о продаже данных организации и составах группировок. Участники рынка наблюдают увеличение спроса на подобные услуги 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 посвящённой Threat Intelligence

Угрозы vs Риски


Угрозовый 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

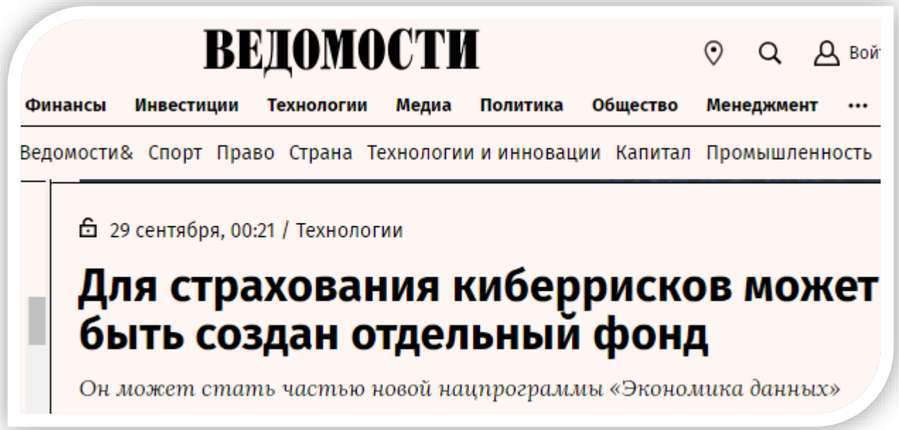
ЭКОНОМИКА 12:23, 15 июня 2023

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

Финансы Инвестиции Технологии Медиа Политика Общество Менеджмент

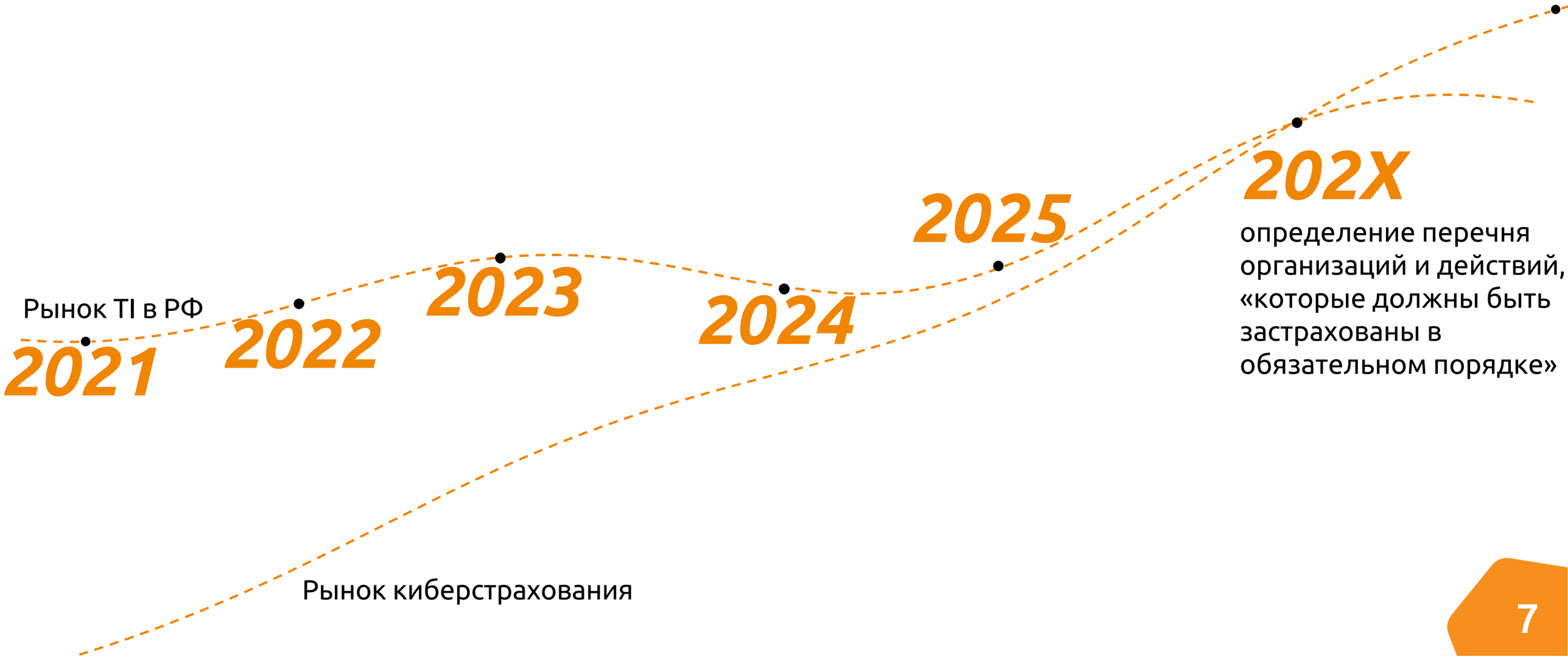
Ведомости& Спорт Право Страна Технологии и инновации Капитал Промышленность

29 сентября, 00:21 / Технологии

Для страхования киберрисков может быть создан отдельный фонд

Он может стать частью новой нацпрограммы «Экономика данных»

Предотвратить или компенсировать



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

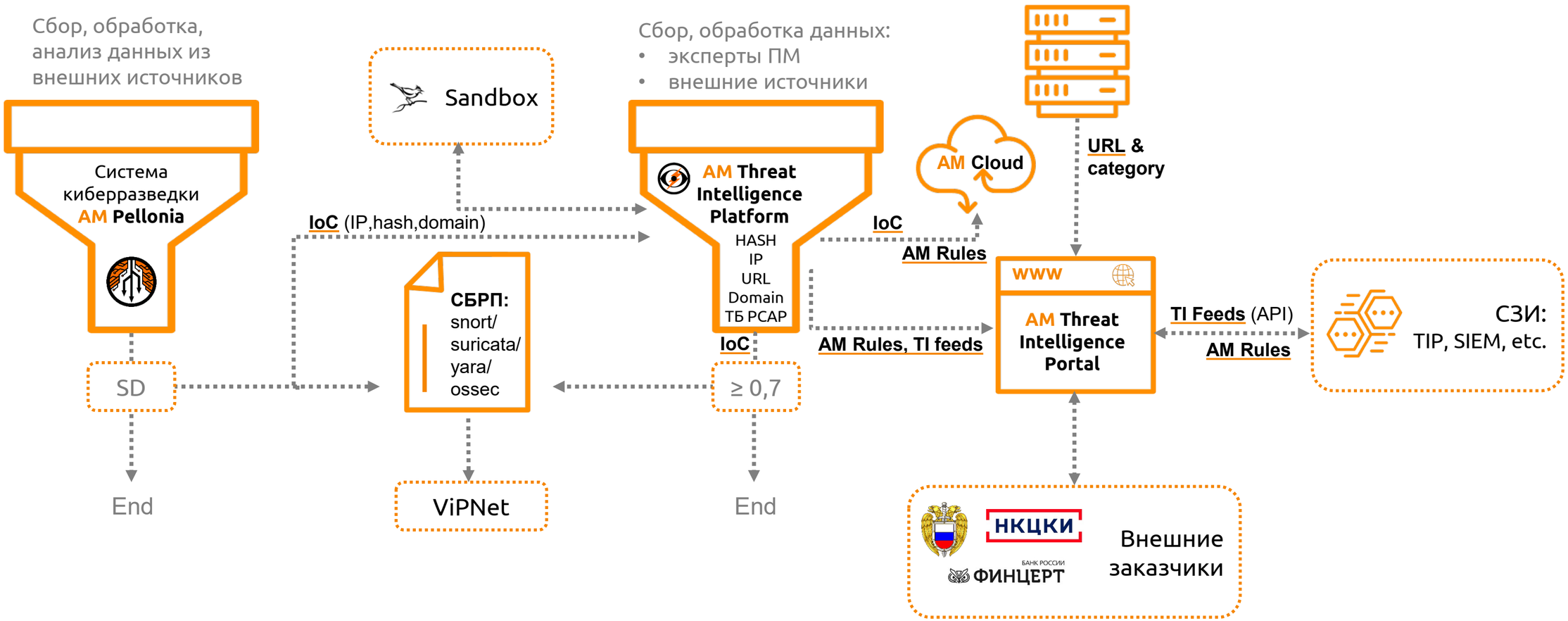
- Открытые/закрытые источники
- Объекты пользователей
- Ручное добавление
- OSINT

- Модели ML
- IDS/IPS, EDR
- Sandbox, Парсеры
- Вспомогательные сервисы
- Тестирование

- Обратная связь
- False positive
- Bug & Fix
- Тех.поддержка

- БРП
- AM Rules
- TI feeds (IOC)
- Бюллетени ИБ
- URL Categorization

Как устроено

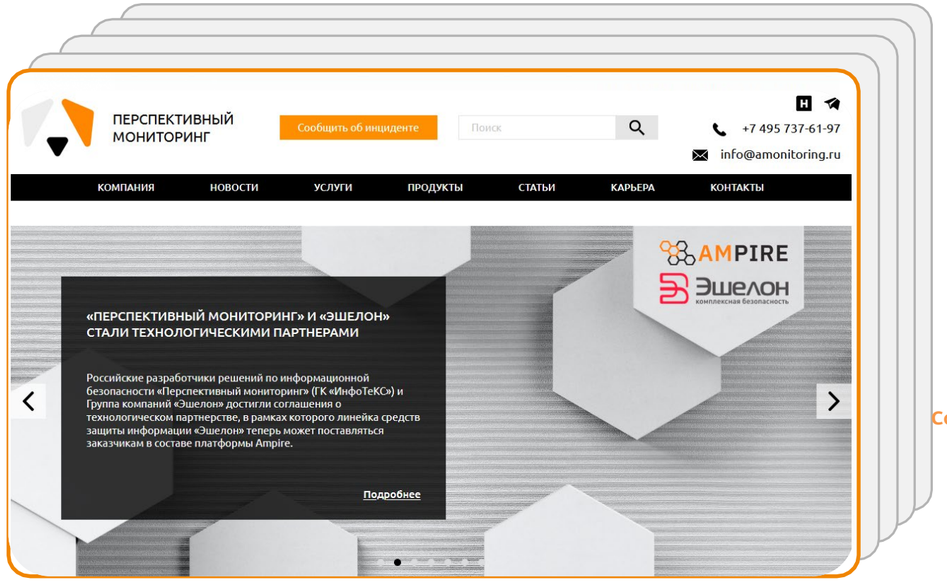


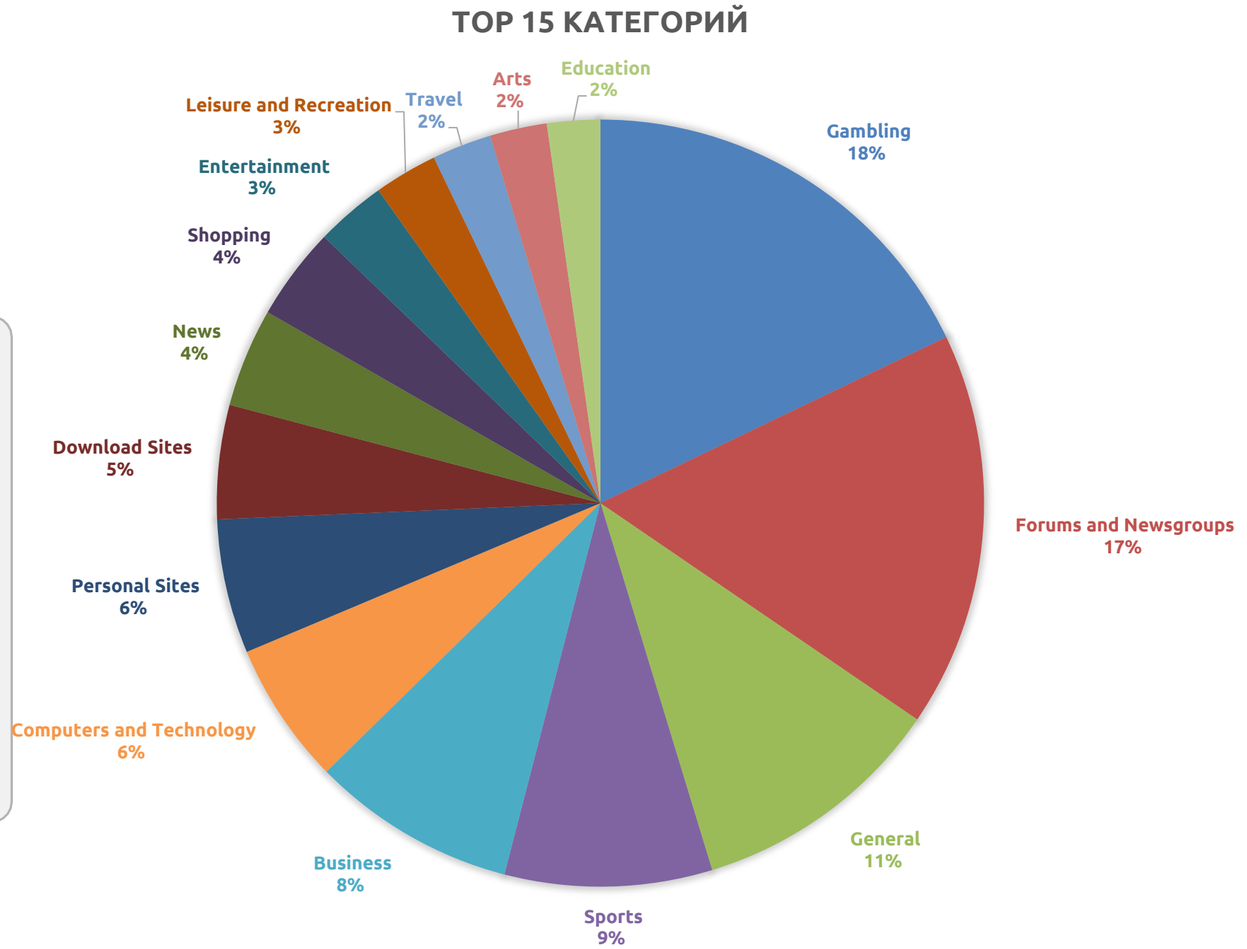
Статистика IoC

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

- 81 категория
- > 75 млн. доменов





Бюллетени ИБ

Информационный бюллетень Центра мониторинга АО «ПМ»

Название документа	**Уязвимость удаленного исполнения кода в Apache ActiveMQ**
Разослан	2023-11-27
Идентификатор	AM-2023-ALE-1127-02
Описание угрозы	**CVE-2023-46604**

CVSSv3.1: 10.0, AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H

Объект уязвимости: Класс Marshaller протокола OpenWire в Apache ActiveMQ

Требования к атакующему: Удаленный неаутентифицированный

Максимальный результат атаки: Удаленное исполнение кода

Бюллетени ИБ

Меры противодействия

Обновить ПО до актуальной версии, следовать указаниям из бюллетеня безопасности Apache:

- https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt

Использовать правила ViPNet IDS NS:

- sid 3252852 "AM EXPLOIT Apache ActiveMQ < v5.18.3 Java Deserialization RCE via 'FileSystemXmlApplicationContext' (CVE-2023-46604)"
- sid 3252842 "AM EXPLOIT [ET] Apache ActiveMQ < v5.18.3 Java Deserialization RCE via 'ClassPathXmlApplicationContext' (CVE-2023-46604)"
- sid 3252853 "AM EXPLOIT [ET] Possible Apache ActiveMQ < v5.18.3 RCE Server Response (CVE-2023-46604)"

Использовать метаправило ViPNet TIAS:

- Удаленное исполнение кода в Apache ActiveMQ (CVE-2023-

Экспертные данные АО «ПМ»

Snort / Suricata / yara / ossec

> 400 000 правил/сигнатур

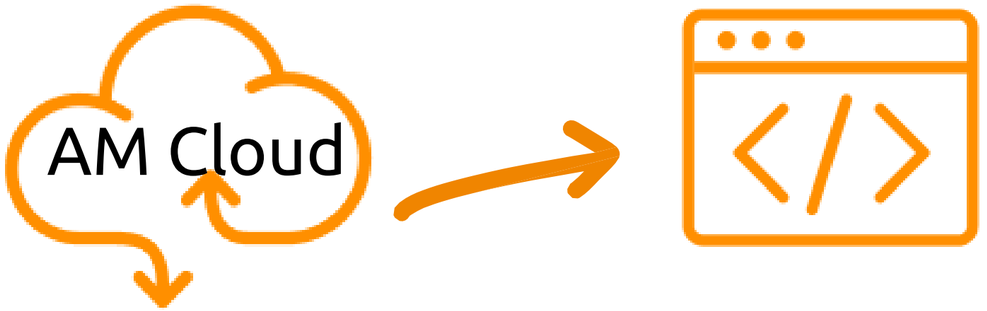
URL-фильтрация

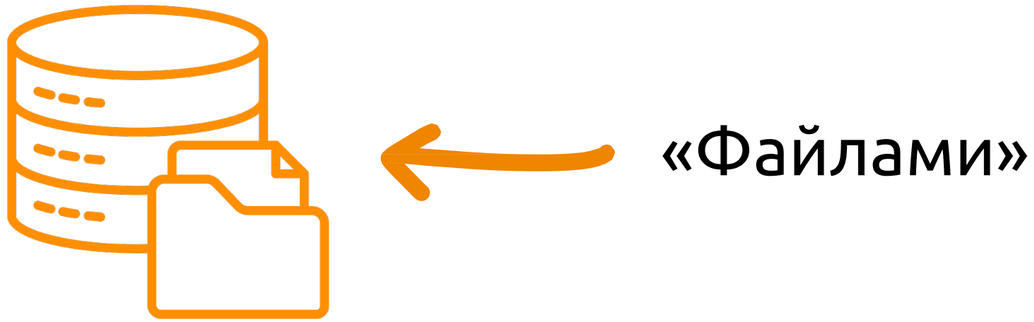
75 млн. доменов

IP, Domain, URL, Hash

STIX2.1 > 4 млн. IoC

Способы доставки ЭД



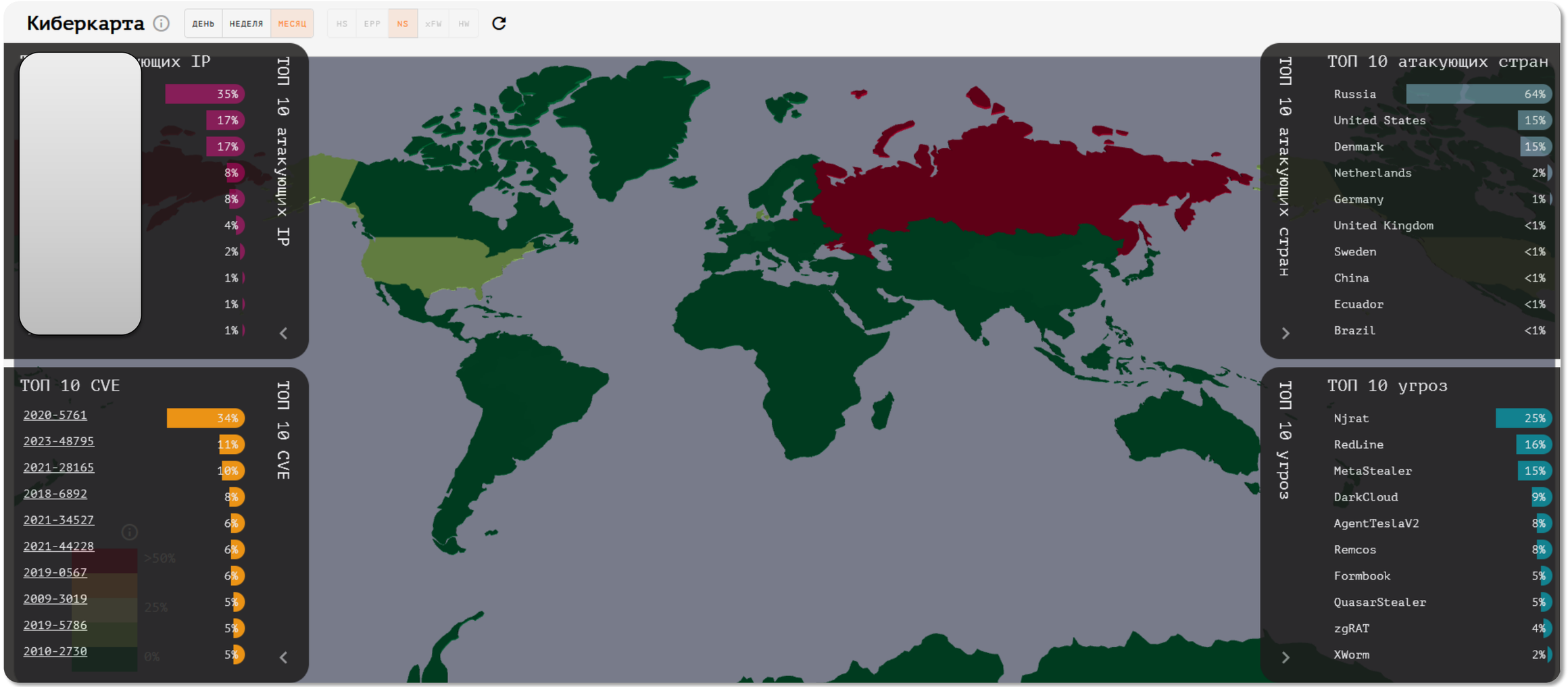


«Файлами»

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

AM Threat Intelligence Portal

Киберкарта


Киберкарта
ДЕНЬ
НЕДЕЛЯ
МЕСЯЦ
HS
EPP
NS
xFW
HW
ТОП 10 атакующих IP
35%
17%
17%
8%
8%
4%
2%
1%
1%
1%
ТОП 10 атакующих стран
Russia 64%
United States 15%
Denmark 15%
Netherlands 2%
Germany 1%
United Kingdom <1%
Sweden <1%
China <1%
Ecuador <1%
Brazil <1%
ТОП 10 CVE
2020-5761 34%
2023-48795 11%
2021-28165 10%
2018-6892 8%
2021-34527 6%
2021-44228 6%
2019-0567 6%
2009-3019 5%
2019-5786 5%
2010-2730 5%
>50%
25%
0%
ТОП 10 угроз
Njrat 25%
RedLine 16%
MetaStealer 15%
DarkCloud 9%
AgentTeslaV2 8%
Remcos 8%
Formbook 5%
QuasarStealer 5%
zgRAT 4%
XWorm 2%

Поиск по domain

mlcrosoft.site

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

Категории: -

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

Правила/Сигнатуры 1

sid	Время изменения	Название	Группы	TTP
3208272	02.05.23 15:05	AM DNS Query for mlcrosoft.site (Winnti APT41 // Operation Cuckoobees)	dns	TA0011 T1608.001

Краткое описание

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

Полное описание

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

Критичность: Низкая
Типы атаки: Вредоносный ресурс
Платформы: -

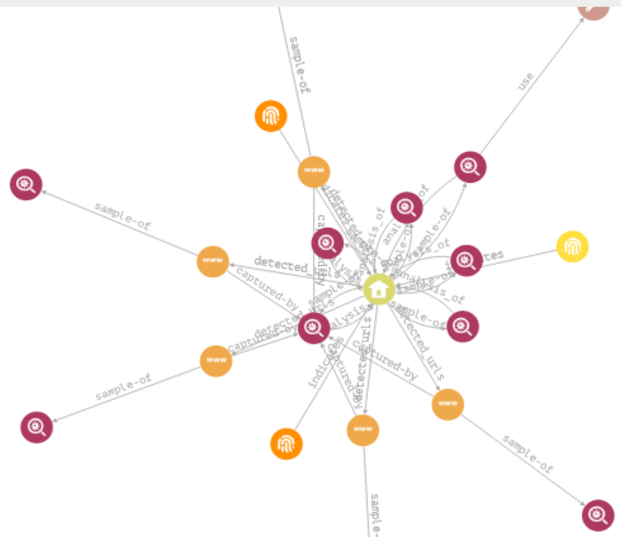
Исходный текст

```
alert udp $HOME_NET any -> any 53 (msg:"AM DNS Query for mlcrosoft.site (Winnti APT41
// Operation Cuckoobees)"; content:"|01 0000 01 00000000000|"; depth:10; offset:2;
content:"|09|mlcrosoft|04|site|00|"; fast_pattern; nocase; distance:0;
reference:url,virustotal.com/en/url/
546945477931fc298b4cfa8880e5d12697d338d0aa2605aa4221074 0ca73d97a/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:1;
metadata: affected_asset src, 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 Expiry date: 2022-05-27 Name server 1: ns3…

Поиск по IP

TI LOOKUP

ПОМОЩЬ

185.205.209.166

ПОИСК

Обнаруженные угрозы

AM SCORE 0.72

Результаты для: 185.205.209.166

Сеть: 185.205.208.0/22
ASN: 44901
Местонахождение: Болгария, София
Дата первого появления: 24 мая, 2020 07:00
Дата последнего обновления: 5 янв., 2024 05:44
TTP: TA0011

Метки образца: -
Чёрные списки: -

Категории: malware

Правила/Сигнатуры 1

sid	Время изменения	Название	Группы	TTP
3086102	17.02.24 20:32	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: -

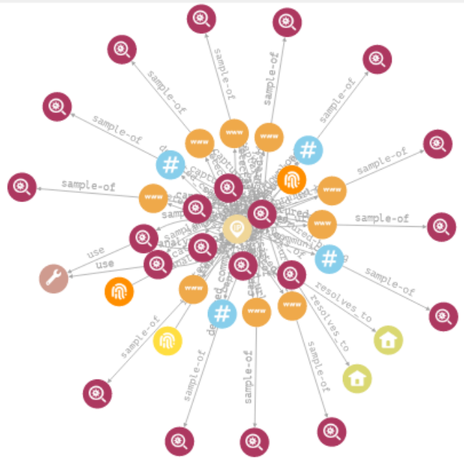
Исходный текст

```
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



Обзор

Whois: NetRange: 185.0.0.0 - 185.255.255.255 CIDR: 185.0.0.0/8 NetName: RIPE-185 NetHandle: NET-185-0-0-0-1 Parent: () NetType: Allocated to RIPE NCC OriginAS: Organization…
Доменное имя: nathost834431.xyz
Выходной Tor-узел: Нет
Связанные домены: nathost834431.xyz, lirtis.botcphp.xyz

Связи

Поиск по hash

81d1e936a8f817e01344049ce63b41e968fec7b265c9d2ab6678412904f15178

ПОИСК

Обнаруженные угрозы

AM SCORE 0.65

47/72

Результаты для: 81d1e936a8f817e01344049ce63b41e968fec7b265c9d2ab6678412904f15178

Размер: 219.1 КБ
Дата первого появления: 27 мар., 2020 08:27
Дата последнего обновления: 2 окт., 2023 14:30
Тип файла: PE32 executable
TTP: TA0043, TA0007, TA0002, TA0011

Метки образца: Trojan-Proxy.Win32.Sybici.lg//Trojan.MulDrop11.47334
Чёрные списки: -
Потенциально нежелательное приложение (PUA): Нет

Категории: peexe | overlay | revoked-cert | runtime-modules | signed | spreader | direct-cpu-clock-access

Правила/Сигнатуры 0

sid	Время изменения	Название	Группы	TTP
		Отсутствуют данные		

Обзор

MD5: dceece60dcee5fd4d47755d6b3a85a75
SHA-1: 6969cc2f1939fd4373a83a2e607318e2cf7d78aa
SHA-256: 81d1e936a8f817e01344049ce63b41e968fec7b265c9d2ab6678412904f15178
SSDEEP: 3072:/kHyNZCT7RbVv513b2cLrEJeGUDL61UNmUCFh9W8Nf3IAK9EjCcak+OWgY5:VCTh/V3DeewB93I/+UOXC
TLSH: T12224481276D44AB7C63B02F1D8AD66B71EB5EC804F2889CF4769DE5F66302C19C3316A
Размер: 219.1 КБ
Magic: PE32 executable

TrID: Win32 Executable MS Visual C++ (generic)(37.8%), Microsoft Visual C++ compiled executable (generic)(20%), Win64 Executable (generic)(12.7%), Win32 Dynamic Link Library...

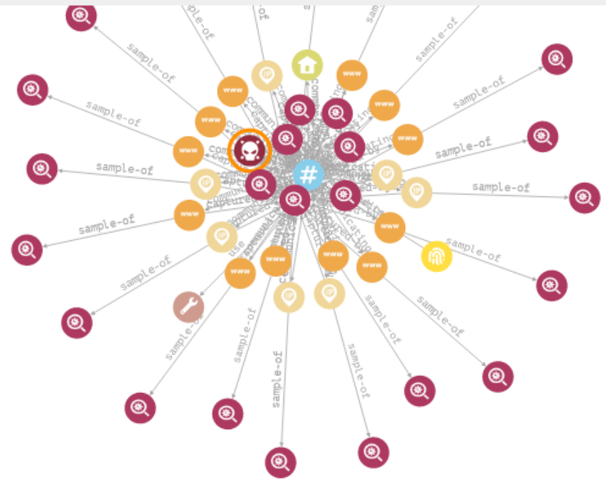
Связи

Связанные URL-адреса

Дата последнего обновления	Ссылка	Обнаружения

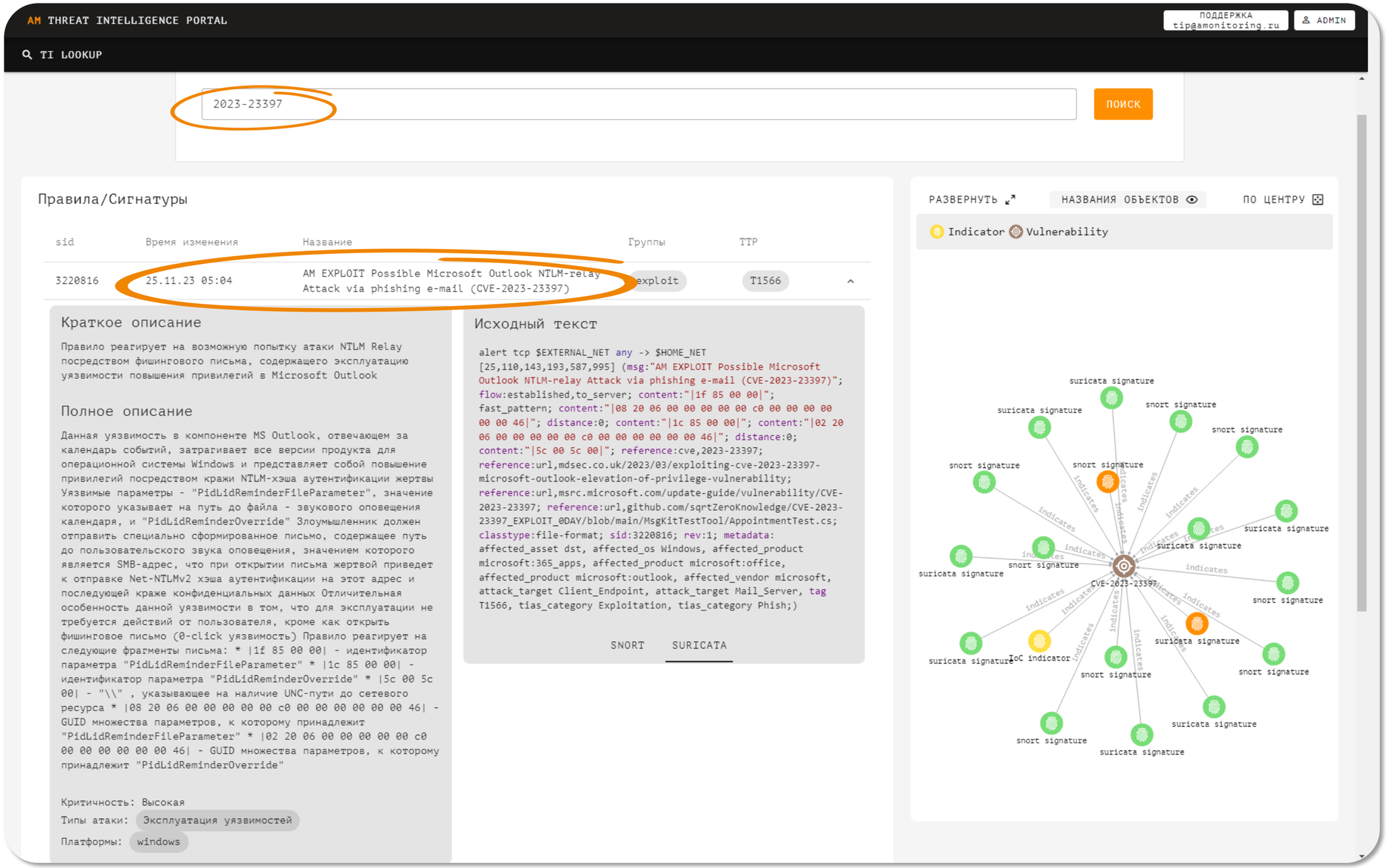
РАЗВЕРНУТЬ НАЗВАНИЯ ОБЪЕКТОВ ПО ЦЕНТРУ

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

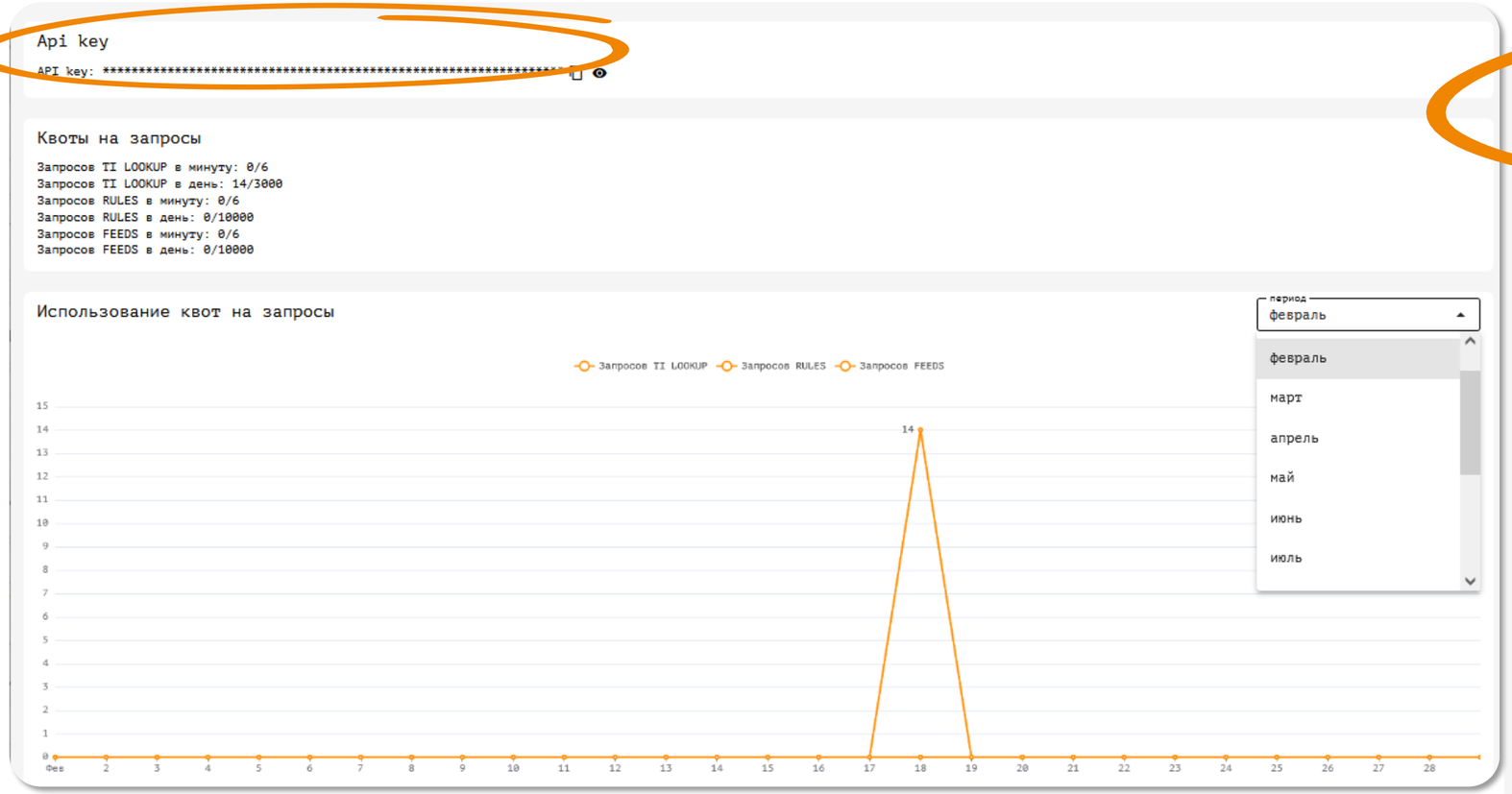


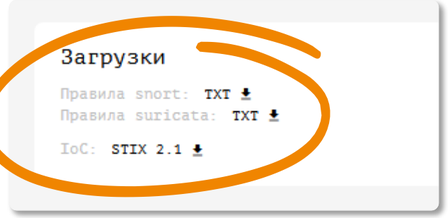
{
id: "malware--30b4429b-6333-4688-

Поиск по CVE


AM THREAT INTELLIGENCE PORTAL
ПОДДЕРЖКА
tip@amonitoring.ru
ADMIN
TI LOOKUP
2023-23397
ПОИСК
Правила/Сигнатуры
sid
Время изменения
Название
Группы
TTP
3220816
25.11.23 05:04
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 00 46| - GUID множества параметров, к которому принадлежит "PidLidReminderFileParameter" * |02 20 06 00 00 00 00 00 c0 00 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 00 46|"; distance:0; content:"|1c 85 00 00|"; content:"|02 20 06 00 00 00 00 00 c0 00 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:1; metadata: affected_asset dst, affected_os Windows, affected_product microsoft:365_apps, affected_product microsoft:office, affected_product microsoft:outlook, affected_vendor microsoft, attack_target Client_Endpoint, attack_target Mail_Server, tag T1566, tias_category Exploitation, tias_category Phish;)
SNORT
SURICATA
РАЗВЕРНУТЬ
НАЗВАНИЯ ОБЪЕКТОВ
ПО ЦЕНТРУ
Indicator
Vulnerability
suricata signature
snort signature
IoC indicator
CVE-2023-23397
indicates

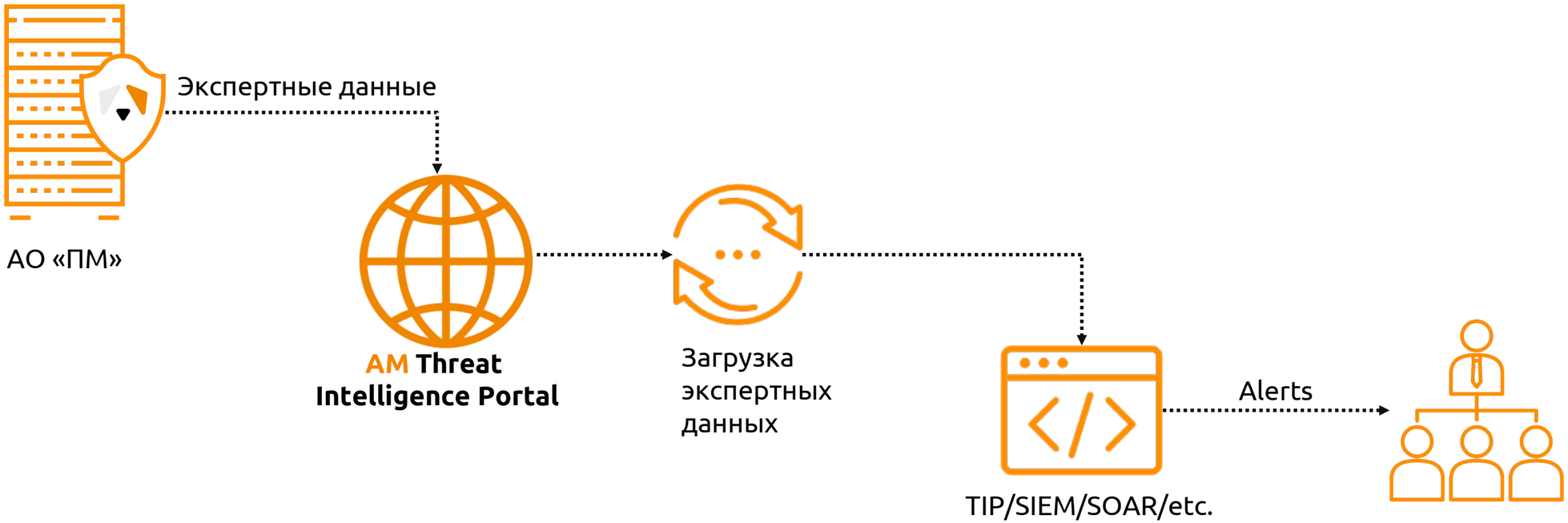
Доп. функционал



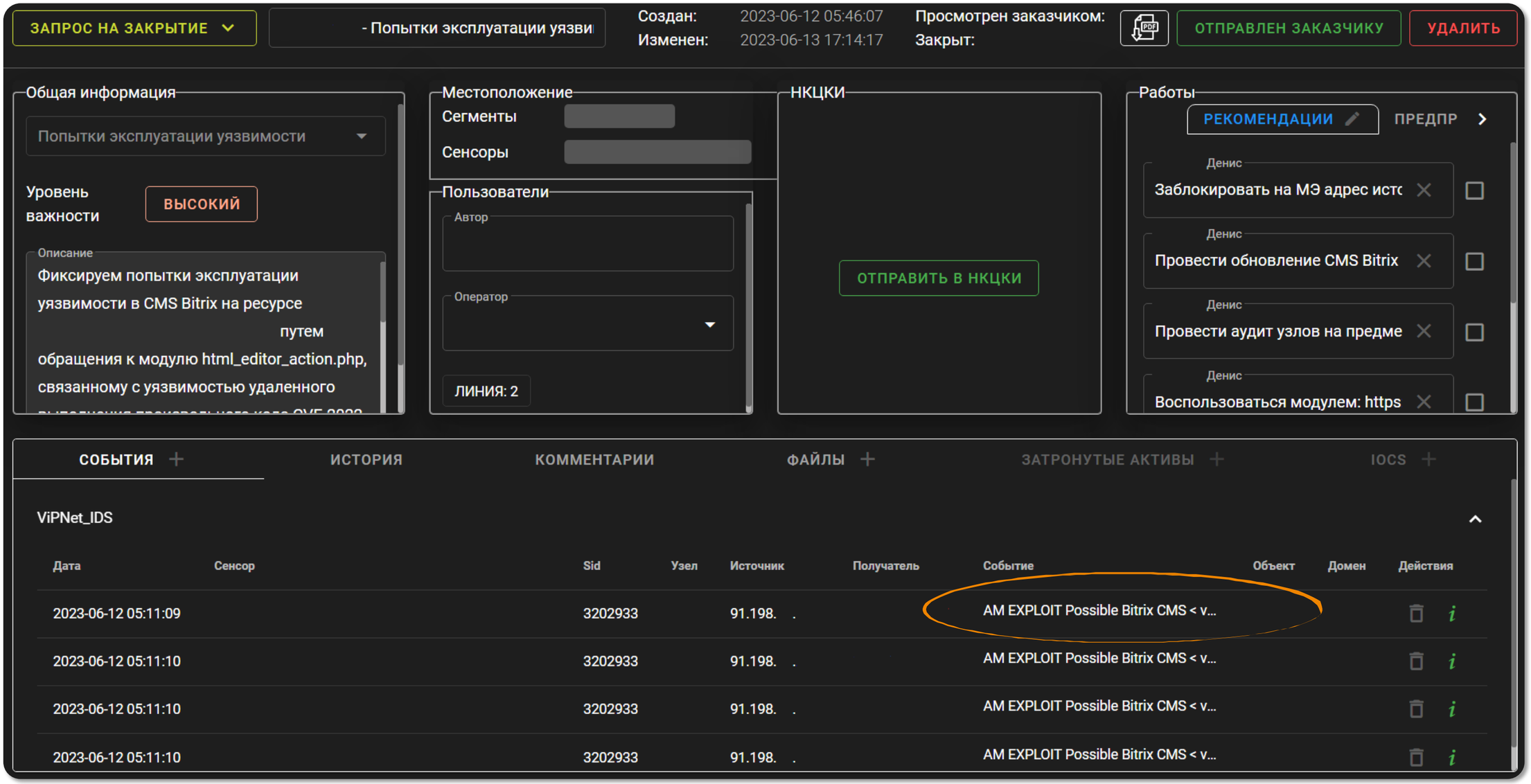


Как использовать ЭД

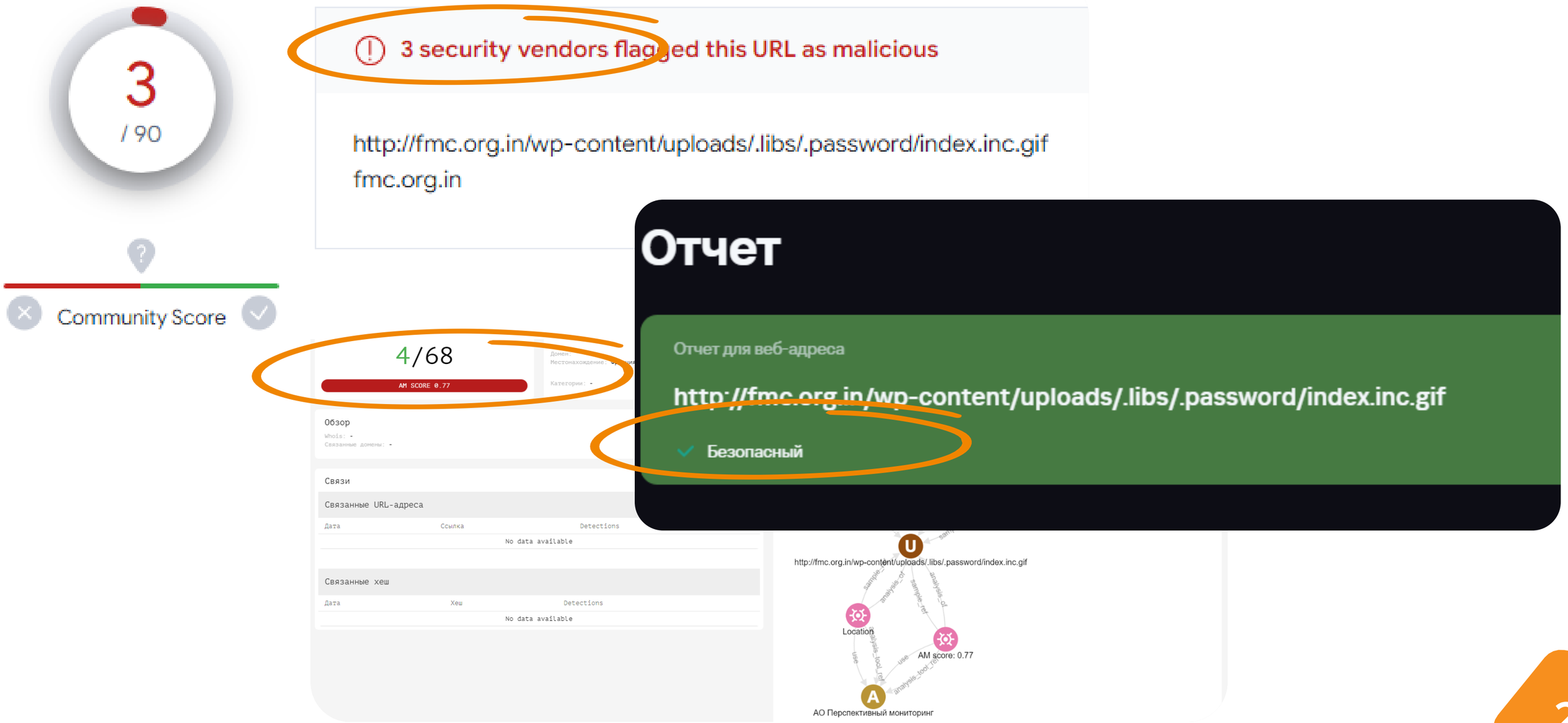
для выявления подозрений на компьютерные инциденты или атаки



Пример использования:



В чём profit?


3
/ 90
Community Score
3 security vendors flagged this URL as malicious
http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif
fmc.org.in
4/68
AM SCORE 0.77
Обзор
Связи
Связанные URL-адреса
Дата
Ссылка
Detections
No data available
Связанные хеш
Дата
Хеш
Detections
No data available
Отчет
Отчет для веб-адреса
http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif
Безопасный
http://fmc.org.in/wp-content/uploads/.libs/.password/index.inc.gif
Location
AM score: 0.77
АО Перспективный мониторинг

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

t.me/pm_public

@AMonitoring

amtip.ru

Артём Савчук

Технический директор

+7 (495) 737-61-97

info@amonitoring.ru