ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Использование данных об угрозах (TI) при мониторинге ИБ и обнаружении кибератак

Основные правила вебинара

Обменивайтесь
сообщениями
во вкладке «Чат»

Запись вебинара
будет направлена всем
участникам на указанный
при регистрации e-mail

Задавайте
вопросы во вкладке
«Вопросы»

ПМ сегодня

12

Лет на рынке услуг SOC и исследования защищённости

5

Лет центр ГосСОПКА

>1600

Выполненных ИБ проектов

12

Действующих киберполигонов Ampire

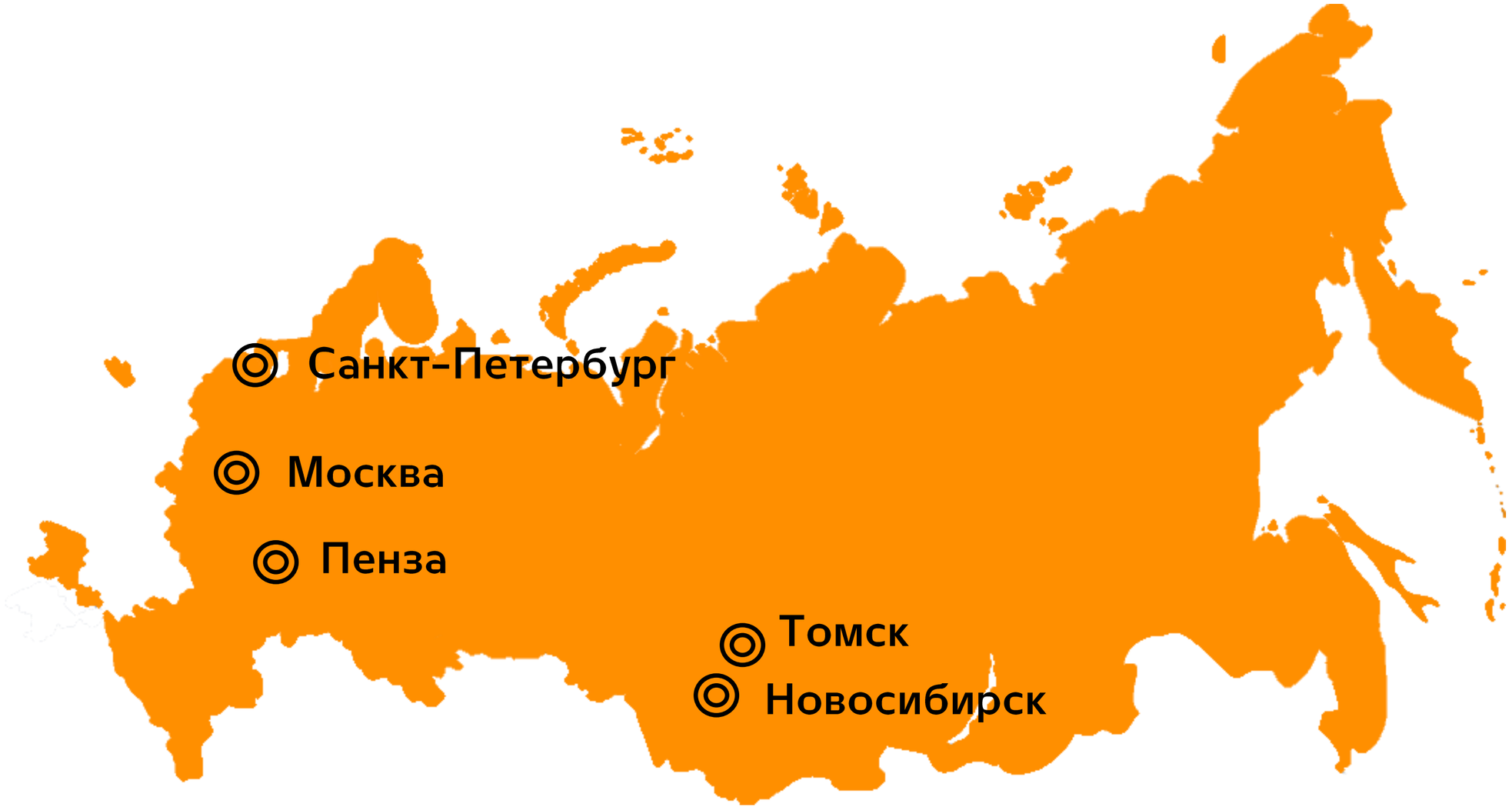
300+

Проведенных киберучений

3000+

ИБ специалистов прошли обучение на Ampire

Регионы присутствия



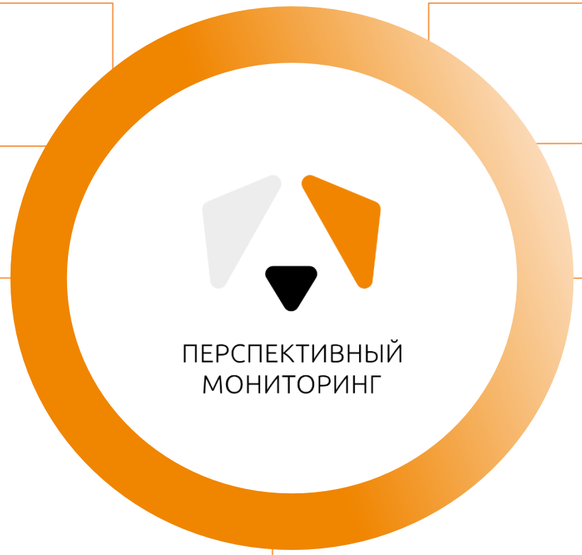
Направления деятельности

Исследование защищённости

- Пентест
- Аудит ИБ
- Оценка соответствия требованиям Банка России

SOC

- Коммерческий SOC
- Подключение к ГосСОПКА
- Расследование инцидентов ИБ



Продукты

- Экспертные данные AMRules
- Киберполигон Ampire

Сквозная экспертиза по всем направлениям деятельности ПМ

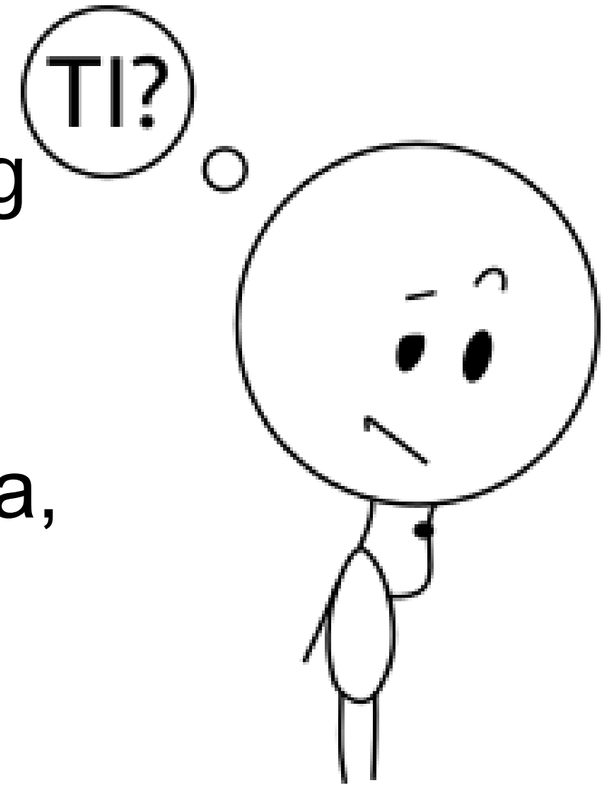
Как кибербразведка (TI) помогает в условиях целевых атак ?

Запись прямого эфира онлайн-конференции AM Live, проходившей 07 сентября 2022 года и посвящённой Threat Intelligence

Что такое и зачем нужен 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.

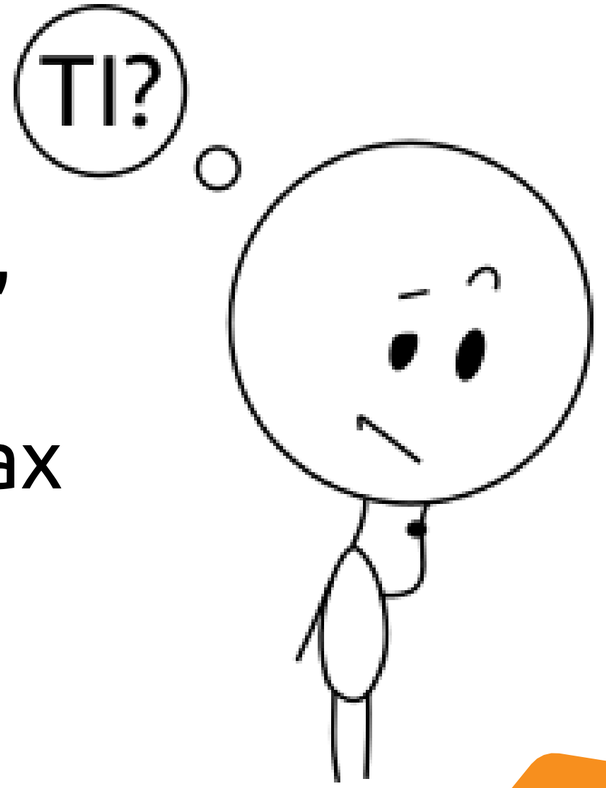


* https://csrc.nist.gov/glossary/term/threat_intelligence

Что такое и зачем нужен 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.



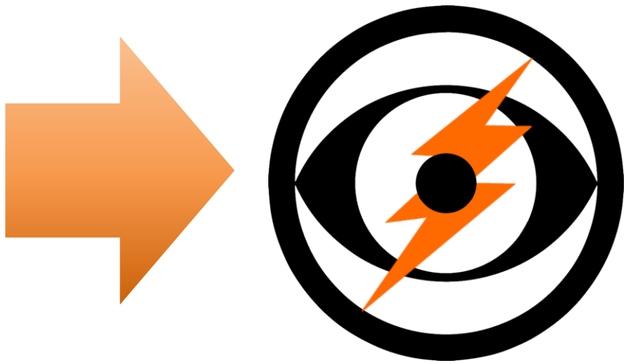
** https://en.wikipedia.org/wiki/Threat_intelligence

Экспертные данные
TI АО «ПМ»

1. т.н. «Базы решающих правил» (БРП, включают наборы snort, yara, ossec, suricata правила)
2. TI feeds (IoC в STIX или любом другом пользовательском формате)
3. AM Rules (Свидетельство Роспатента №2016620316 от 03.03.2016 г.)
4. Бюллетени ИБ

Направление исследования
киберугроз

- Эксплоиты
- ВПО
- Хакерские инструменты
- Целевые атаки
- Threat Intelligence
- […]



ЭД

- БРП для продуктовой линейки ViPNet ИнфоТеКС
- AM_Rules (snort, yara, ossec, suricata rules)
- IOC
- Бюллетени

Как устроен процесс

Сбор

- Открытые источники
- Sandbox
- Объекты пользователей
- Ручное добавление
- Хакерские инс-ты

Обработка

- Модели ML
- IDS/IPS (NGFW)
- Sandbox
- AV
- Парсеры
- Вспомогательные сервисы
- Тестирование

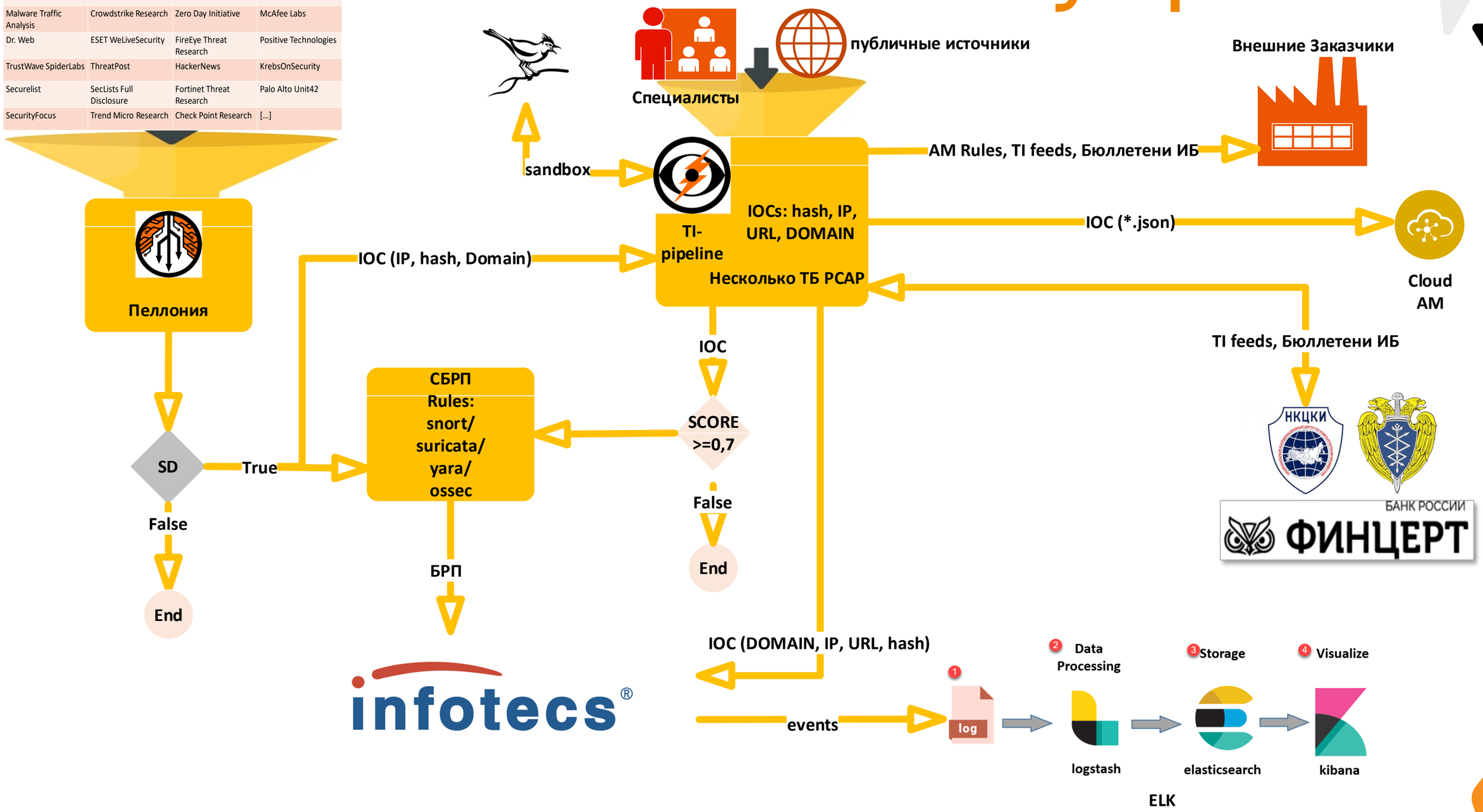
Поставка

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

В основе наших фидов — данные об угрозах, аккумулированные экспертами АО «ПМ» в ходе расследований инцидентов и изучения деятельности хакерских группировок во всем мире, а также данные обезличенной телеметрии, полученные с инсталляций продуктов АО «ИнфоТеКС» в десятках компаний.

Как устроено

НКЦКИ	ФинЦЕРТ	NVD CVE	DHS CISA
Exploit-DB	Packet Storm Security	GitHub	Cisco Talos
Malware Traffic Analysis	Crowdstrike Research	Zero Day Initiative	McAfee Labs
Dr. Web	ESET WeLiveSecurity	FireEye Threat Research	Positive Technologies
TrustWave SpiderLabs	ThreatPost	HackerNews	KrebsOnSecurity
Securelist	SecLists Full Disclosure	Fortinet Threat Research	Palo Alto Unit42
SecurityFocus	Trend Micro Research	Check Point Research	[...]

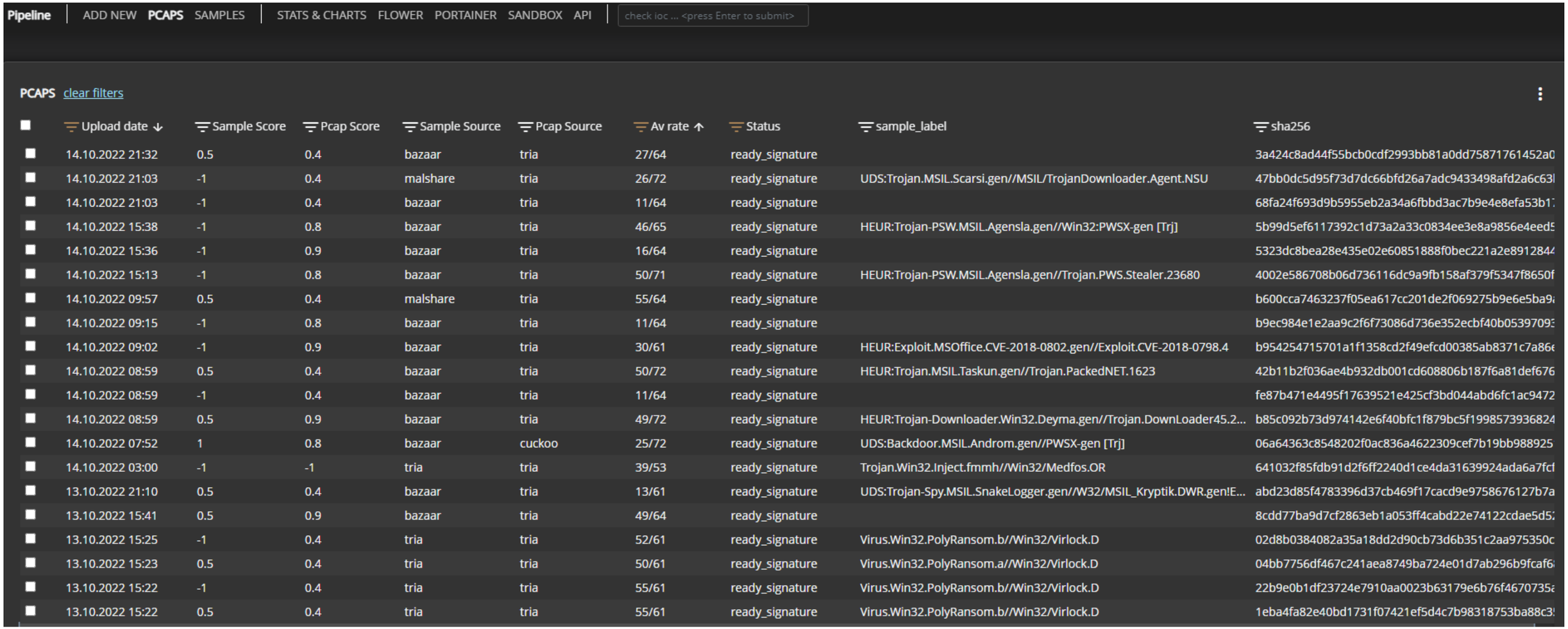


Наши источники

НКЦКИ	ФинЦЕРТ	NVD CVE	DHS CISA
Exploit-DB	Packet Storm Security	GitHub	Cisco Talos
Malware Traffic Analysis	Crowdstrike Research	Zero Day Initiative	McAfee Labs
Dr. Web	ESET WeLiveSecurity	FireEye Threat Research	Positive Technologies
TrustWave SpiderLabs	ThreatPost	HackerNews	KrebsOnSecurity
Securelist	SecLists Full Disclosure	Fortinet Threat Research	Palo Alto Unit42
SecurityFocus	Trend Micro Research	Check Point Research	и другие (>30 шт.)

Работа с публичными источниками

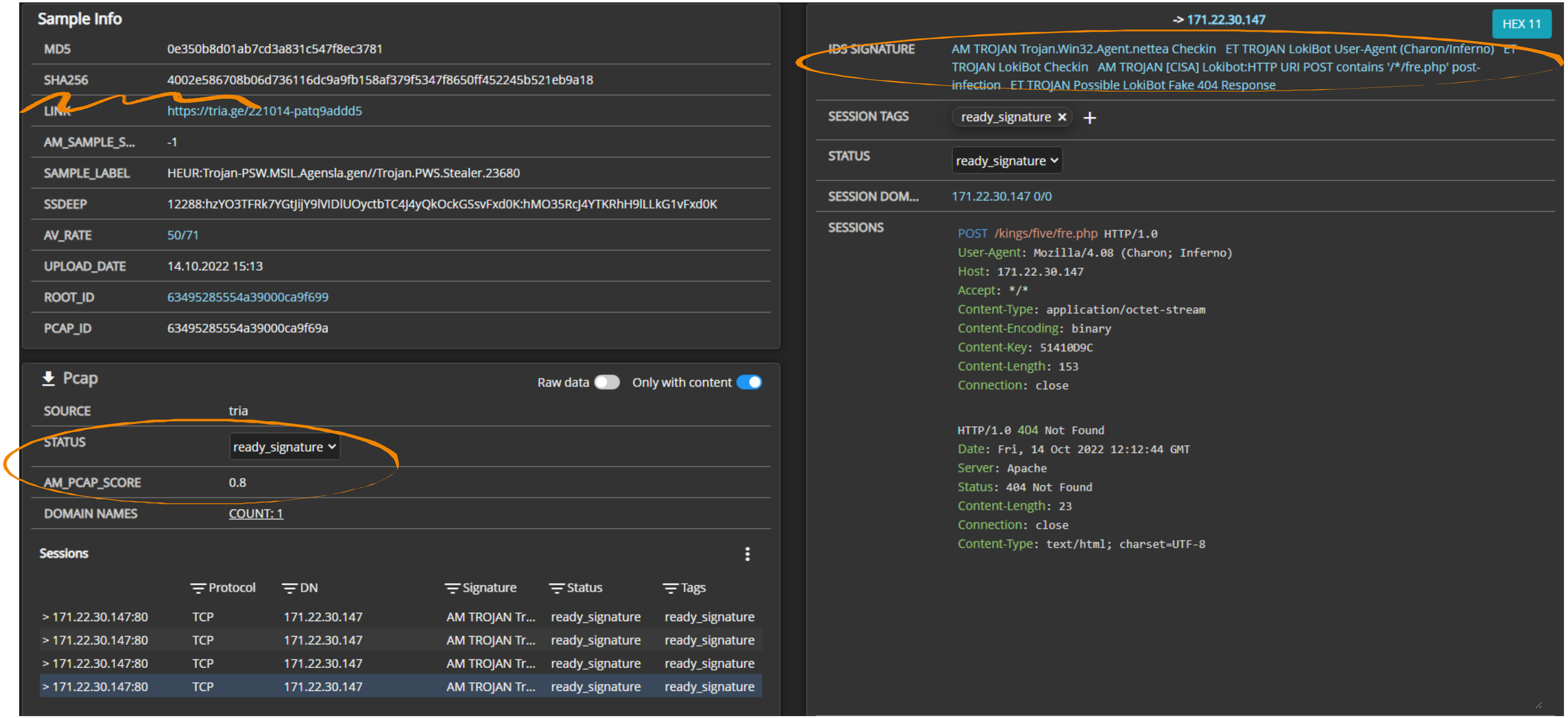
TI-pipeline



Upload date	Sample Score	Pcap Score	Sample Source	Pcap Source	Av rate	Status	sample_label	sha256
14.10.2022 21:32	0.5	0.4	bazaar	tria	27/64	ready_signature		3a424c8ad44f55bcb0cdf2993bb81a0dd75871761452a0
14.10.2022 21:03	-1	0.4	malshare	tria	26/72	ready_signature	UDS:Trojan.MSIL.Scarsi.gen//MSIL/TrojanDownloader.Agent.NSU	47bb0dc5d95f73d7dc66bfd26a7adc9433498afd2a6c63
14.10.2022 21:03	-1	0.4	bazaar	tria	11/64	ready_signature		68fa24f693d9b5955eb2a34a6fbbd3ac7b9e4e8efa53b1
14.10.2022 15:38	-1	0.8	bazaar	tria	46/65	ready_signature	HEUR:Trojan-PSW.MSIL.Agensla.gen//Win32:PWSX-gen [Trj]	5b99d5ef6117392c1d73a2a33c0834ee3e8a9856e4eed5
14.10.2022 15:36	-1	0.9	bazaar	tria	16/64	ready_signature		5323dc8bea28e435e02e60851888f0bec221a2e8912844
14.10.2022 15:13	-1	0.8	bazaar	tria	50/71	ready_signature	HEUR:Trojan-PSW.MSIL.Agensla.gen//Trojan.PWS.Stealer.23680	4002e586708b06d736116dc9a9fb158af379f5347f8650f
14.10.2022 09:57	0.5	0.4	malshare	tria	55/64	ready_signature		b600cca7463237f05ea617cc201de2f069275b9e6e5ba9
14.10.2022 09:15	-1	0.8	bazaar	tria	11/64	ready_signature		b9ec984e1e2aa9c2f6f73086d736e352ecbf40b0539709
14.10.2022 09:02	-1	0.9	bazaar	tria	30/61	ready_signature	HEUR:Exploit.MSOffice.CVE-2018-0802.gen//Exploit.CVE-2018-0798.4	b954254715701a1f1358cd2f49efcd00385ab8371c7a86
14.10.2022 08:59	0.5	0.4	bazaar	tria	50/72	ready_signature	HEUR:Trojan.MSIL.Taskun.gen//Trojan.PackedNET.1623	42b11b2f036ae4b932db001cd608806b187f6a81def676
14.10.2022 08:59	-1	0.4	bazaar	tria	11/64	ready_signature		fe87b471e4495f17639521e425cf3bd044abd6fc1ac9472
14.10.2022 08:59	0.5	0.9	bazaar	tria	49/72	ready_signature	HEUR:Trojan-Downloader.Win32.Deyma.gen//Trojan.DownLoader45.2...	b85c092b73d974142e6f40bfc1f879bc5f1998573936824
14.10.2022 07:52	1	0.8	bazaar	cuckoo	25/72	ready_signature	UDS:Backdoor.MSIL.Androm.gen//PWSX-gen [Trj]	06a64363c8548202f0ac836a4622309cef7b19bb988925
14.10.2022 03:00	-1	-1	tria	tria	39/53	ready_signature	Trojan.Win32.Inject.fmmh//Win32/Medfos.OR	641032f85fdb91d2f6ff2240d1ce4da31639924ada6a7fc
13.10.2022 21:10	0.5	0.4	bazaar	tria	13/61	ready_signature	UDS:Trojan-Spy.MSIL.SnakeLogger.gen//W32/MSIL_Kryptik.DWR.gen!E...	abd23d85f4783396d37cb469f17cacd9e9758676127b7a
13.10.2022 15:41	0.5	0.9	bazaar	tria	49/64	ready_signature		8cdd77ba9d7cf2863eb1a053ff4cabd22e74122cdae5d5
13.10.2022 15:25	-1	0.4	tria	tria	52/61	ready_signature	Virus.Win32.PolyRansom.b//Win32/Virlock.D	02d8b0384082a35a18dd2d90cb73d6b351c2aa975350c
13.10.2022 15:23	0.5	0.4	tria	tria	50/61	ready_signature	Virus.Win32.PolyRansom.a//Win32/Virlock.D	04bb7756df467c241aea8749ba724e01d7ab296b9fcaf6
13.10.2022 15:22	-1	0.4	tria	tria	55/61	ready_signature	Virus.Win32.PolyRansom.b//Win32/Virlock.D	22b9e0b1df23724e7910aa0023b63179e6b76f4670735
13.10.2022 15:22	0.5	0.4	tria	tria	55/61	ready_signature	Virus.Win32.PolyRansom.b//Win32/Virlock.D	1eba4fa82e40bd1731f07421ef5d4c7b98318753ba88c3

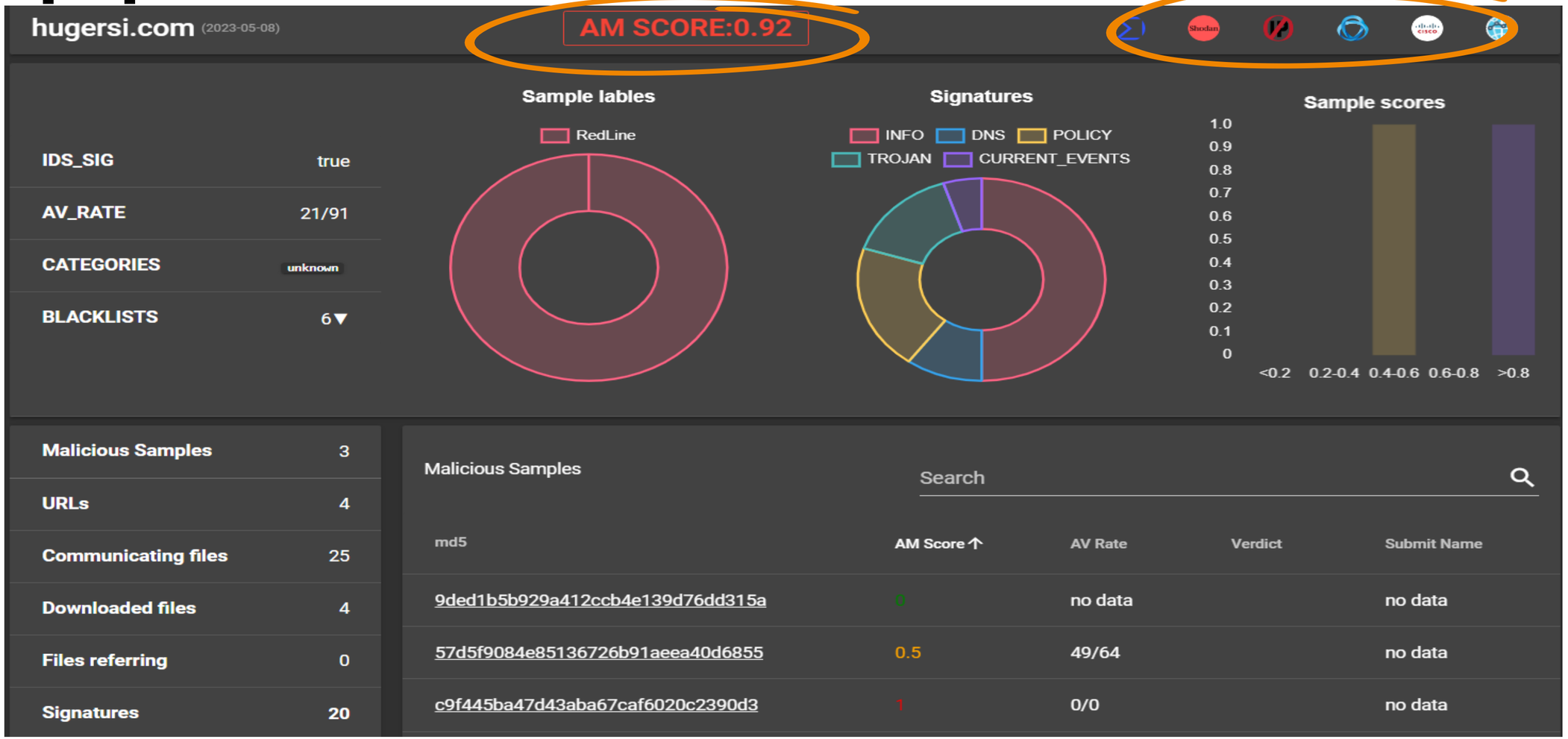
TIP автоматически собирает, обрабатывает и сопоставляет данные об образцах

TI-pipeline



Sample info в TIP с иллюстрацией сигнатур, сессии

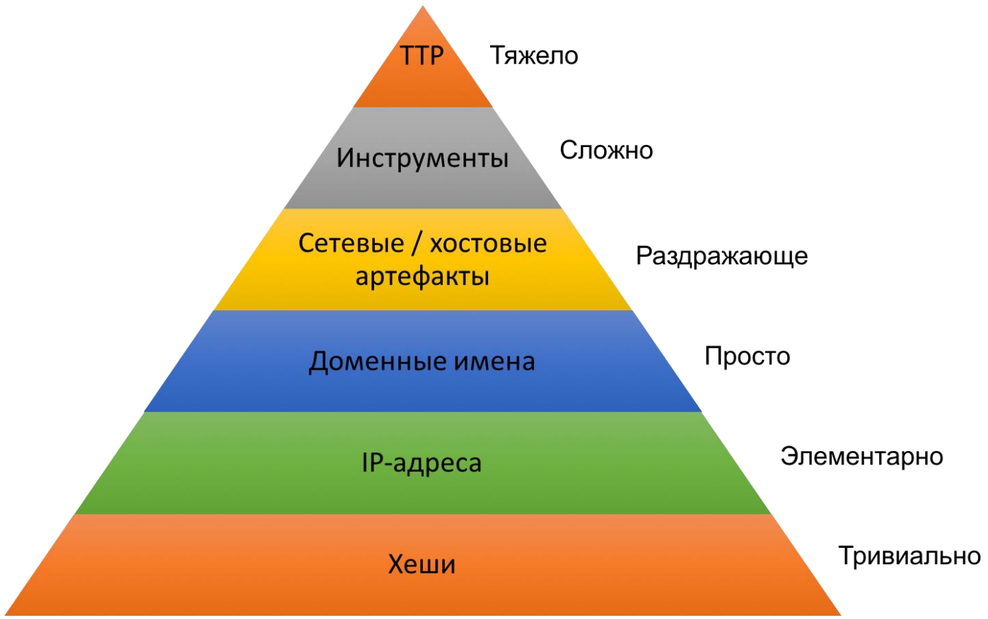
TI-pipeline: AM SCORE



Вычисляем используя следующие признаки:

- Факт того, что домен был создан автоматически (модель DGA)
- Рейтинг AV
- Количество источников feed'ов
- Мета (косвенная) информация (срабатывания правил, результаты моделей МО, «негативный контекст», добавлен аналитиком и др.)

Индикаторы компрометации (IoC)



Пирамида индикаторов компрометации в зависимости от сложности получения данных (т.н. «Пирамида боли» David J Bianco)

IPv4 Domain Хэши (MD5, SHA1)

URL Транзакционные (MTA, User-agent) Имена файлов/путь

mutex Значения реестра e-mails

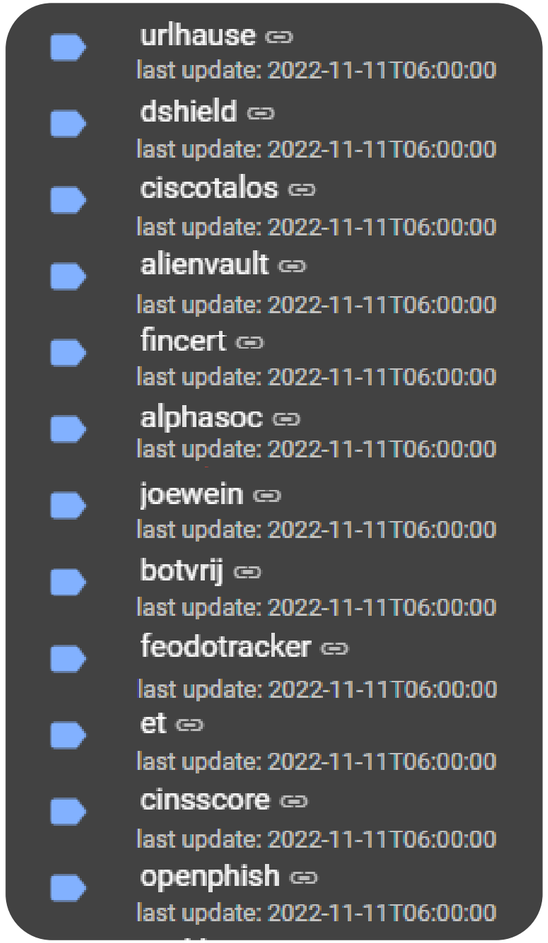
Наиболее популярные типы индикаторов компрометации

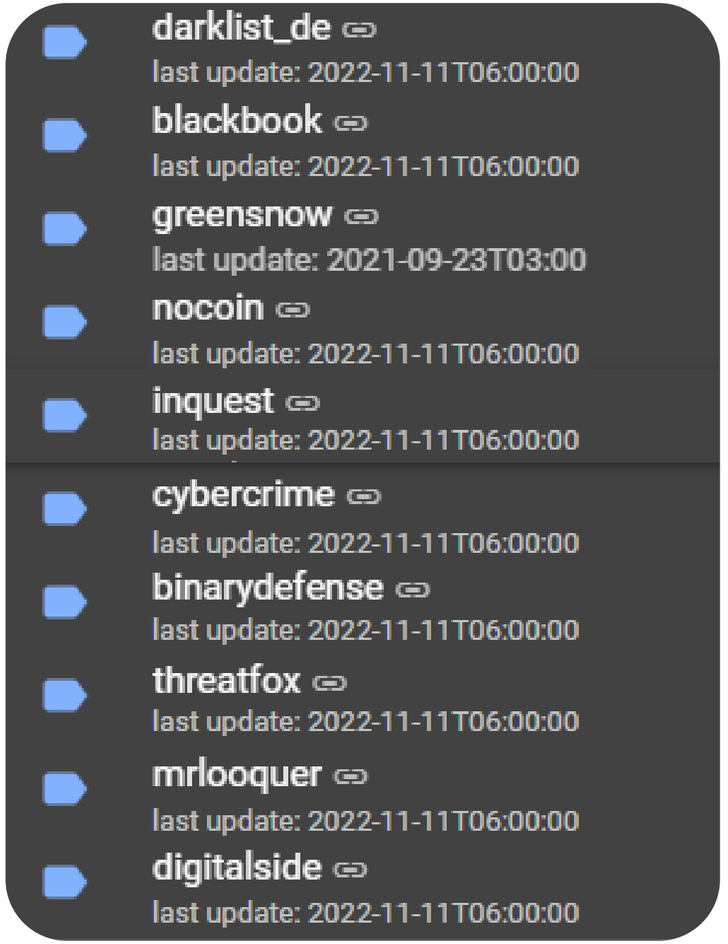
Разведка	Оснащение	Доставка	Заражение	Инсталляция	Получение управления	Выполнение действий
Файл – имя Файл URI – URL HTTP - GET HTTP – User Agent URI – имя домена Адрес – e-mail Адрес – IPv4	Файл – путь Файл URI – URL	Поведение Файл – имя Файл – путь Файл URI – URL HTTP – POST Заголовок e-mail – Тема Заголовок e-mail – X-Mailer URI – имя домена Хеш – MD5 Хеш – SHA1 Адрес – e-mail Адрес – IPv4	Поведение Ключ реестра Win Файл – имя Файл URI – URL URI – имя домена Хеш – MD5 Хеш – SHA1 Адрес – CIDR Адрес – IPv4	Код – Бинарный код Процессы Win Ключ реестра Win Файл – имя Файл – путь Файл URI – URL HTTP – GET HTTP – User Agent URI – имя домена Хеш – MD5 Хеш – SHA1 Адрес – e-mail Адрес – IPv4	Поведение Процессы Win Ключ реестра Win Файл URI – URL HTTP – GET HTTP – POST HTTP – User Agent URI – имя домена Хеш – MD5 Адрес – e-mail Адрес – IPv4	Поведение Процессы Win Сервисы Win Файл – Путь Файл – Имя Файл URI – URL URI – имя домена Хеш – MD5 Хеш – SHA1 Адрес – IPv4

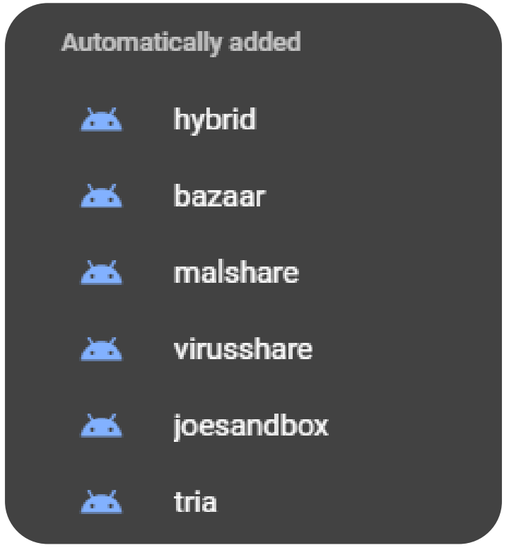
Наложение известных индикаторов компрометации на этапы Kill Chain

*https://www.securitylab.ru/blog/personal/Business_without_danger/320988.php

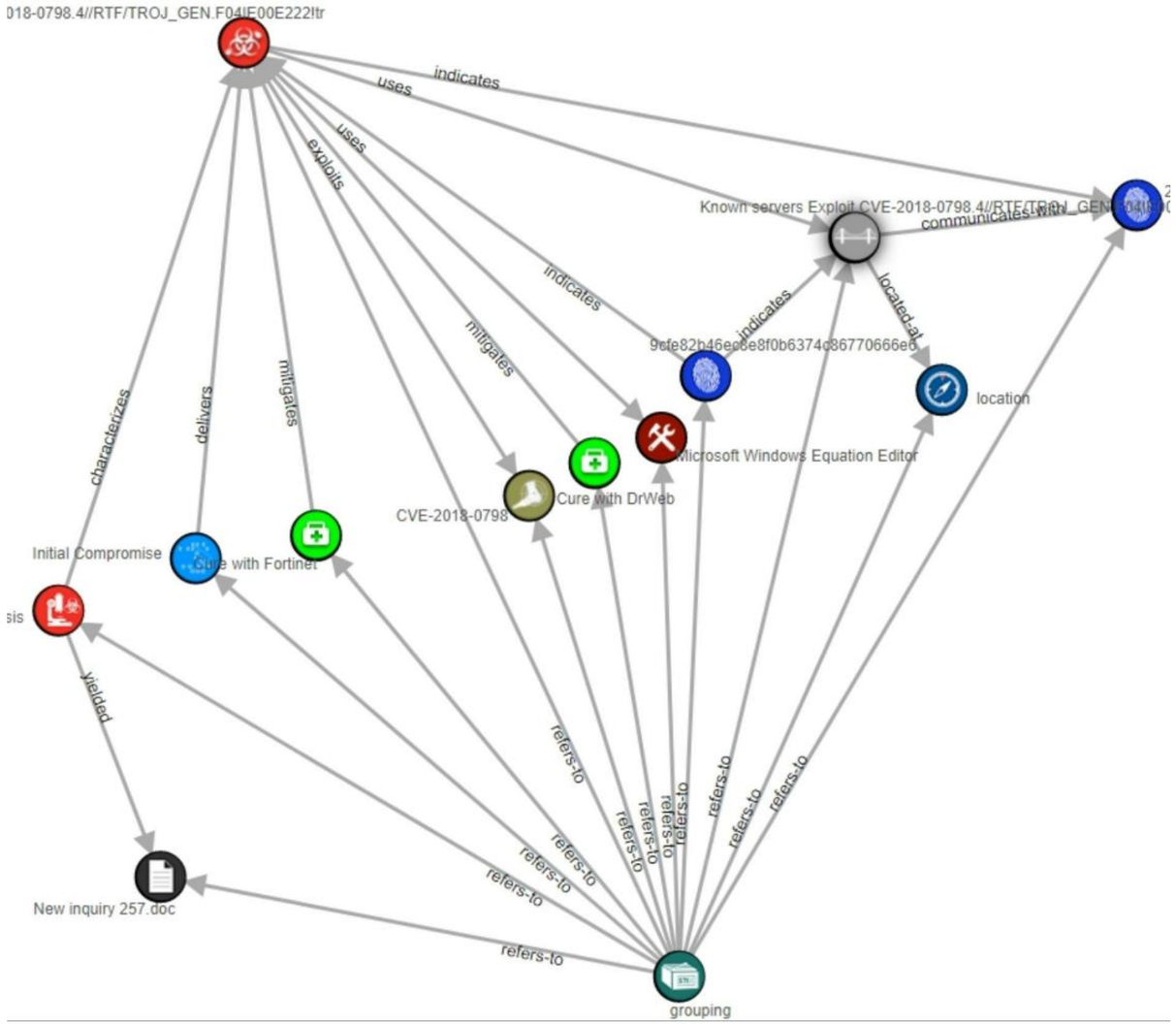
Источники данных об IoC







IoC в STIX 2.1




```
{
  "type": "bundle",
  "id": "bundle--a379c084-b08b-49a8-bfae-e8f4c1d2b876",
  "objects": [
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware--08f61c11-0100-4b44-8974-fdd5f4d2c72d",
      "created": "2022-09-07T14:14:15.735995Z",
      "modified": "2022-09-07T14:14:15.735995Z",
      "name": "Exploit.CVE-2018-0798.4//RTF/TROJ_GEN.F04IE00E222!tr",
      "is_family": false
    },
    {
      "type": "vulnerability",
      "spec_version": "2.1",
      "id": "vulnerability--5167c739-de46-4119-b8e6-27580435c1a4",
      "created": "2022-09-07T14:14:15.735995Z",
      "modified": "2022-09-07T14:14:15.735995Z",
      "name": "CVE-2018-0798",
      "external_references": [
        {
          "source_name": "cve",
          "external_id": "CVE-2018-0798"
        }
      ]
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--1905bb7b-6c4c-4ec5-9f6b-5a9ea54175a2",
      "created": "2022-09-07T14:14:15.735995Z",
      "modified": "2022-09-07T14:14:15.735995Z",
      "relationship_type": "exploits",
      "source_ref": "malware--08f61c11-0100-4b44-8974-fdd5f4d2c72d",
      "target_ref": "vulnerability--5167c739-de46-4119-b8e6-27580435c1a4"
    },
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--c5ce2ce4-8676-4818-be30-b2f03d0f8ee4",
      "created": "2022-08-29T14:35:58.688584Z",
      "modified": "2022-08-29T14:35:58.688584Z",
      "name": "9cfe82b46ec8e8f0b6374c86770666e6",
      "description": "Malicious hash 9cfe82b46ec8e8f0b6374c86770666e6",
      "indicator_types": [
        "malicious-activity"
      ],
      "pattern": "[file:hashes.MD5 = '9cfe82b46ec8e8f0b6374c86770666e6']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "valid_from": "2022-08-29T14:35:58.688584Z",
      "labels": [
        "Exploit.CVE-2018-0798.4//RTF/TROJ_GEN.F04IE00E222!tr"
```

Статистика IoC

Периодичность	IP	Domain	URL	Samples
В день ~	2050	2100	1200	2500
В неделю ~	15000	18500	8000	11000
В месяц ~	64000	95000	37000	40000
		> 1 500 000 samples pcap		
TOTAL		> 3 000 000 IP, domain, url		> 2 300 000 samples files

Система БРП

Не задано | AM | Исходный текст | Свои | С неизвестными метаданными | Без "Pipeline"

Включено	Статус	Дата изменения	Группа	SID	Сообщение	Автор правила
✓	✔	30.09.22 13:02	emerging-exploit	3204869	AM EXPLOIT Possible Apache Log4j2 JNDI RCE with unicode characters var 2 (CVE-2021-44228)	Nikolay.Galkin
✓	✔	30.09.22 13:02	emerging-exploit	3204868	AM EXPLOIT Possible Apache Log4j2 JNDI RCE with unicode characters var 1 (CVE-2021-44228)	Nikolay.Galkin
✓	✔	28.09.22 15:53	emerging-exploit	3204835	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style) (CVE-2017-0144)	ET
✓	✔	10.10.22 13:37	emerging-exploit	3204834	AM EXPLOIT Zoho Password Manager Pro below v12.1 XML-RPC Java Deserialization (CVE-2022-35405)	Solovyev.Artem
✓	✔	29.09.22 14:41	emerging-scan	3204833	AM SCAN [ET] Possible Nmap User-Agent Observed	ET
✓	✱	27.09.22 14:49	emerging-exploit	3204804	AM EXPLOIT Alt-N MDaeamon Buffer Overflow Vulnerability	Galants.Yury
✓	✔	10.10.22 14:16	emerging-exploit	3204788	AM EXPLOIT Novell NetWare Portmapper Callit Stack Buffer Overflow (CVE-2009-5153)	Galants.Yury
✓	✔	18.10.22 17:10	emerging-exploit	3204779	AM EXPLOIT Generic Possible HeapGrooming for HeapOverflows: HeapDefragmentation Allocs var 2	Galants.Yury
✓	✔	10.10.22 13:41	emerging-exploit	3204778	AM EXPLOIT ZLib <= v1.2.12 Buffer Overflow via large 'extra' file header field (CVE-2022-37434)	Solovyev.Artem
✓	✔	14.10.22 17:29	emerging-exploit	3204777	AM EXPLOIT D-Link DIR-880L/868L/865L/860L RCE via Service parameter in /soap.cgi (CVE-2018-6530)	Kartunchikov.Artem
✓	✔	17.10.22 16:51	emerging-exploit	3204776	AM EXPLOIT [ET] Possible D-Link DIR-820L RCE via Value parameter in /getcfg.php (CVE-2022-28958)	ET
✓	✔	17.10.22 16:51	emerging-exploit	3204775	AM EXPLOIT [ET] D-Link DIR-820L RCE via DeviceName in /lan.asp (CVE-2022-26258)	ET
✓	✔	05.10.22 16:15	emerging-exploit	3204689	AM EXPLOIT Possible WordPress WPGateway <= v3.5 Privilege Escalation (CVE-2022-3180)	Solovyev.Artem
✓	✔	03.10.22 16:43	emerging-exploit	3204684	AM EXPLOIT Google Chrome prior to 101.0.4951.41 Type Confusion in V8 via tag_constructor (CVE-2022-1486)	Kartunchikov.Artem
✓	✔	17.10.22 16:36	emerging-malware	3204683	AM TROJAN DownLoader45.7073 HTTP Request to 'hamsterarc_v.4.0.0.75_soax23.exe'	Galants.Yury
✓	✔	17.10.22 16:36	emerging-malware	3204682	AM TROJAN DownLoader45.7073 HTTP Request to 'sxcon64.exe'	Galants.Yury
✓	✔	07.10.22 15:57	emerging-exploit	3204674	AM EXPLOIT Microsoft Windows IKE Protocol Buffer Overflow (CVE-2022-34721)	Nikolay.Galkin
✓	✔	05.10.22 16:15	emerging-exploit	3204673	AM EXPLOIT Generic Path Traversal in HTTP URI var 19	Nikolay.Galkin
✓	✔	27.09.22 16:26	emerging-exploit	3204672	AM EXPLOIT Microsoft Windows NFSv4 Buffer Overflow (CVE-2022-34715)	Nikolay.Galkin
✓	✔	20.09.22 16:41	emerging-dns	3204671	AM DNS Query for youla.id8374.ru (Phishing Campaign)	Nikolay.Galkin

Система БРП («Баз решающих правил») автоматизирует выпуск сборок БРП для различных продуктов АО «ИнфоТеКС»

Система БРП

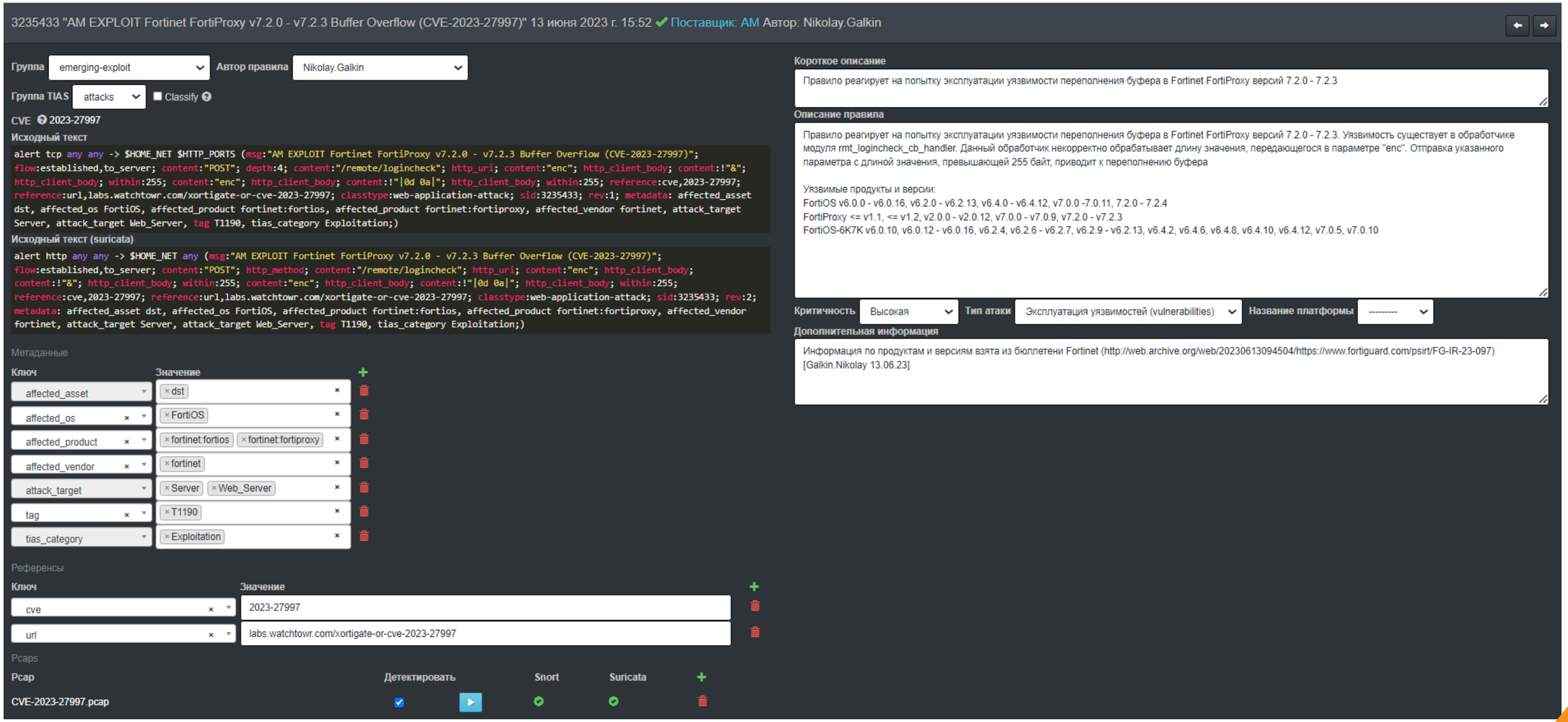


Иллюстрация сигнатуры к уязвимости **CVE-2023-27997**

Бюллетени ИБ

Информационный бюллетень Центра мониторинга АО «ПМ»

Название документа	**Уязвимости в Google Chrome**
Разослан	2022-10-13
Идентификатор	AM-2022-ALE-1013-02
Описание угроз	**CVE-2022-1309**

CVSSv3: 9.6, CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Объект уязвимости: Реализация DevTools API для Google Chrome

Требования к атакующему: Удаленный неаутентифицированный

Максимальный результат атаки: Исполнение произвольного кода

Бюллетени ИБ

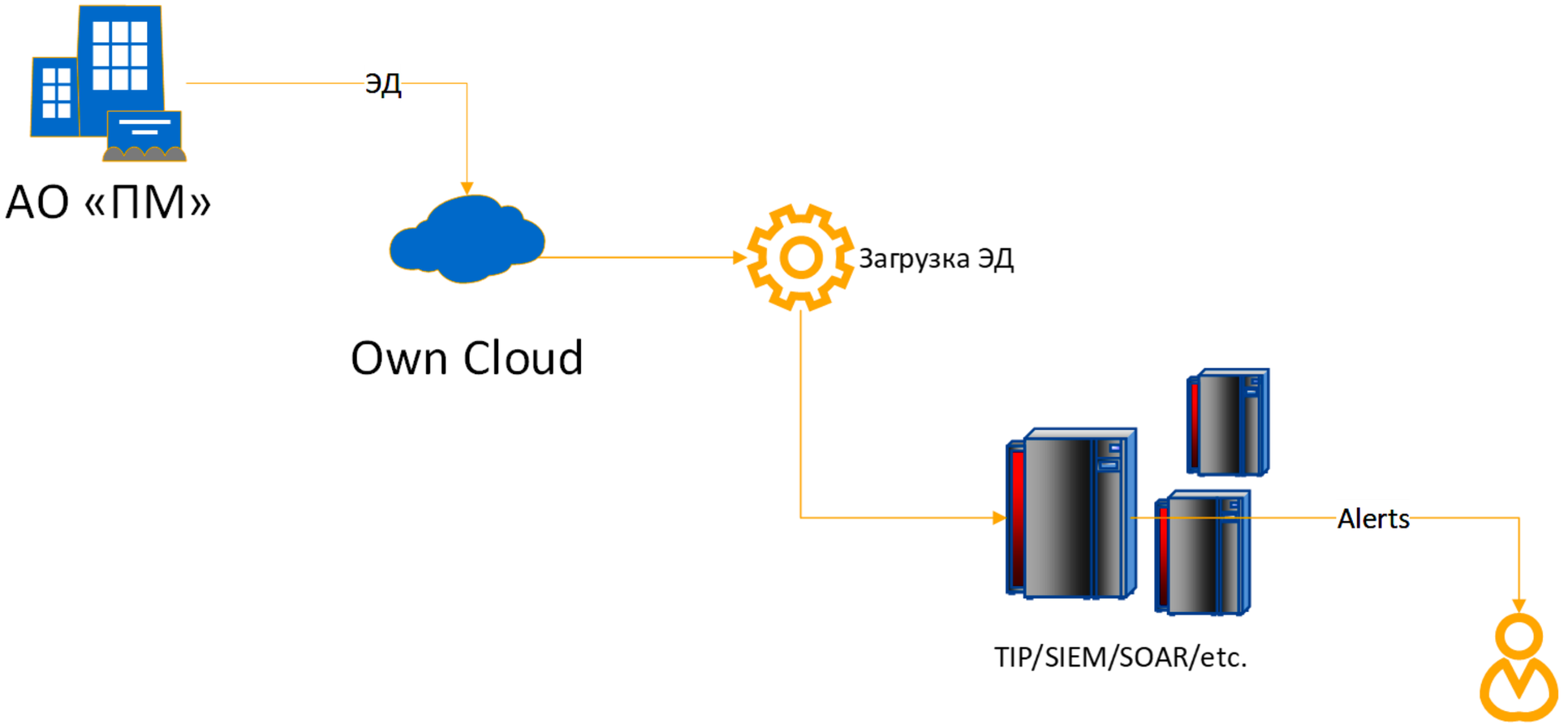
Меры противодействия

Точечно установить новую версию или комплексно обновиться до последних версий, проверив обновления на совместимость

Использовать правила ViPNet

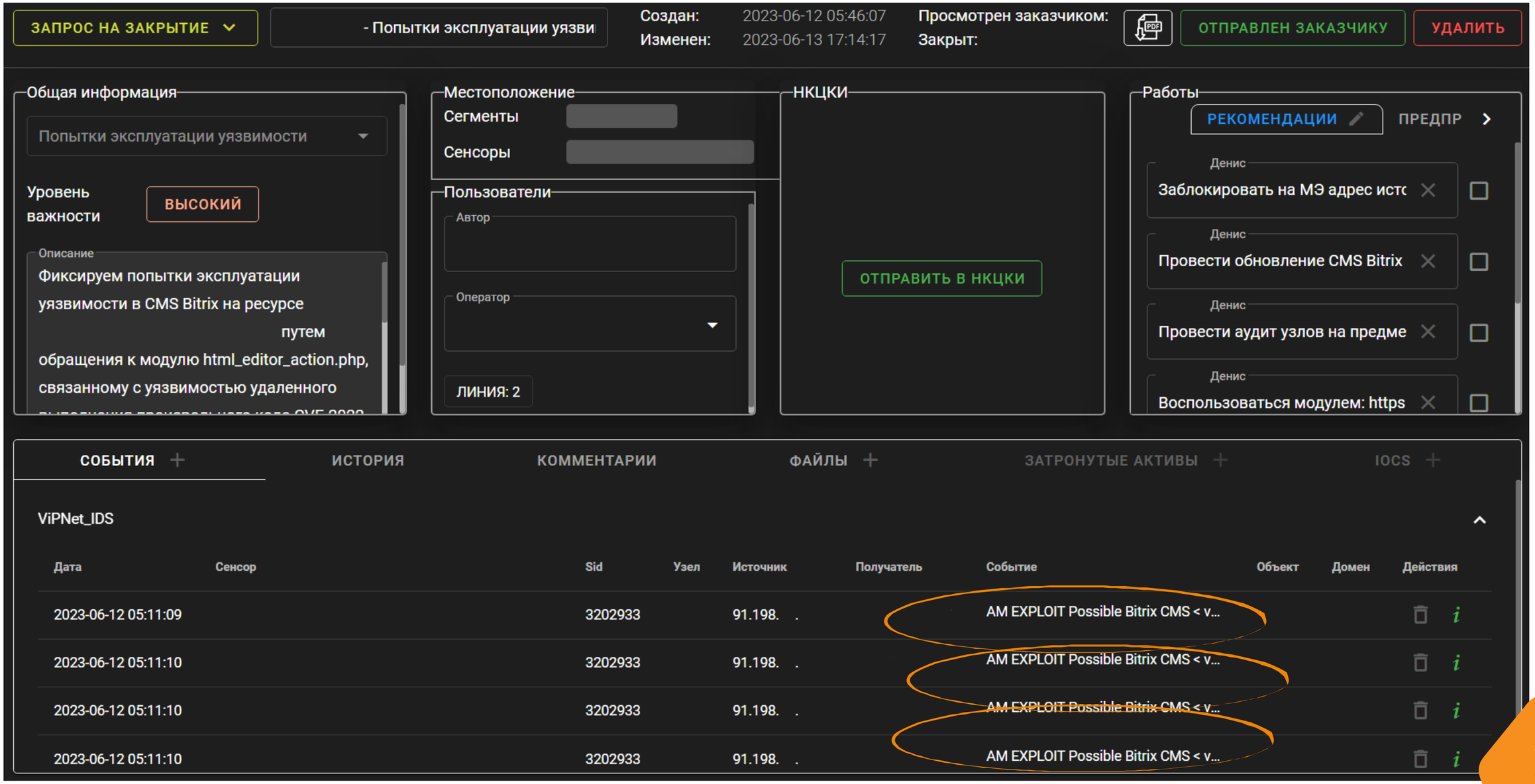
- sid 3204510 "AM EXPLOIT Google Chrome prior to v100.0.4896.88 RCE via devtools.inspectedWindow.eval (CVE-2022-1309)"
- sid 3204621 "AM EXPLOIT Possible Google Chrome prior to v104 UAF via LinkToTextMenuObserver (CVE-2022-2998)"
- sid 3203744 "AM EXPLOIT Possible Google Chrome prior to v103.0.5060.134 UAF via Service Worker API (CVE-2022-2480)"
- sid 3203379 "AM EXPLOIT Possible Google Chrome prior to v102.0.5005.61 Heap Buffer Overflow via uiDevTools (CVE-2022-1876)"
- sid 3204515 "AM EXPLOIT Google Chrome prior to v101.0.4951.41 UAF via BeginTransformFeedback (CVE-2022-1479)"
- sid 3204511 "AM EXPLOIT Google Chrome prior to v100.0.4896.88 RCE via RegExp.replace (CVE-2022-1310)"

Как использовать ЭД



Для выявления подозрений на компьютерные инциденты и атаки

Например:


ЗАПРОС НА ЗАКРЫТИЕ
- Попытки эксплуатации уязви
Создан: 2023-06-12 05:46:07
Изменен: 2023-06-13 17:14:17
Просмотрен заказчиком:
Закрыт:
ОТПРАВЛЕН ЗАКАЗЧИКУ
УДАЛИТЬ
Общая информация
Попытки эксплуатации уязвимости
Уровень важности
ВЫСОКИЙ
Описание
Фиксируем попытки эксплуатации уязвимости в CMS Bitrix на ресурсе путем обращения к модулю html_editor_action.php, связанному с уязвимостью удаленного
Местоположение
Сегменты
Сенсоры
Пользователи
Автор
Оператор
ЛИНИЯ: 2
НКЦКИ
ОТПРАВИТЬ В НКЦКИ
Работы
РЕКОМЕНДАЦИИ
ПРЕДПР
Денис
Заблокировать на МЭ адрес исто
Денис
Провести обновление CMS Bitrix
Денис
Провести аудит узлов на предме
Денис
Воспользоваться модулем: https
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...
2023-06-12 05:11:10
3202933
91.198. .
AM EXPLOIT Possible Bitrix CMS < v...
2023-06-12 05:11:10
3202933
91.198. .
AM EXPLOIT Possible Bitrix CMS < v...
2023-06-12 05:11:10
3202933
91.198. .
AM EXPLOIT Possible Bitrix CMS < v...

Что может предложить ПМ

БРП Snort / Suricata / yara / ossec

> 50 000 правил

URL-фильтрация

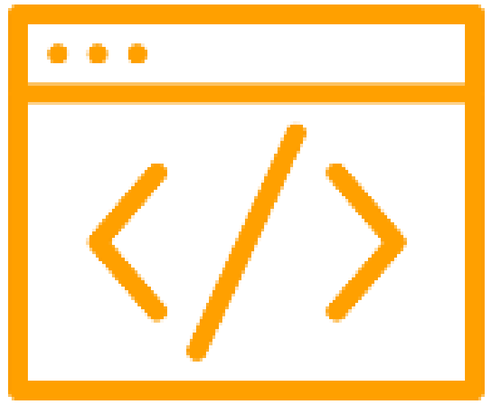
15 млн. доменов

IP, Domain, URL, Hash

STIX2.1, > 1,5 млн. IoC

Способы доставки ЭД

API



«Файлами»

Лицензирование и пилоты

1. Пилот: 1–3 месяца.
2. Лицензирование: по умолчанию 1 год.
3. Интеграция с СЗИ: помогаем и тестируем.
4. Техподдержка: доработка формата, обработка ложных срабатываний.

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Артём Савчук

Заместитель технического директора компании

«Перспективный мониторинг»

Artem.Savchuk@amonitoring.ru

t.me/pm_public

amonitoring.ru