

# Обогащение СЗИ и расследования инцидентов с помощью TIR



**Артём Савчук**

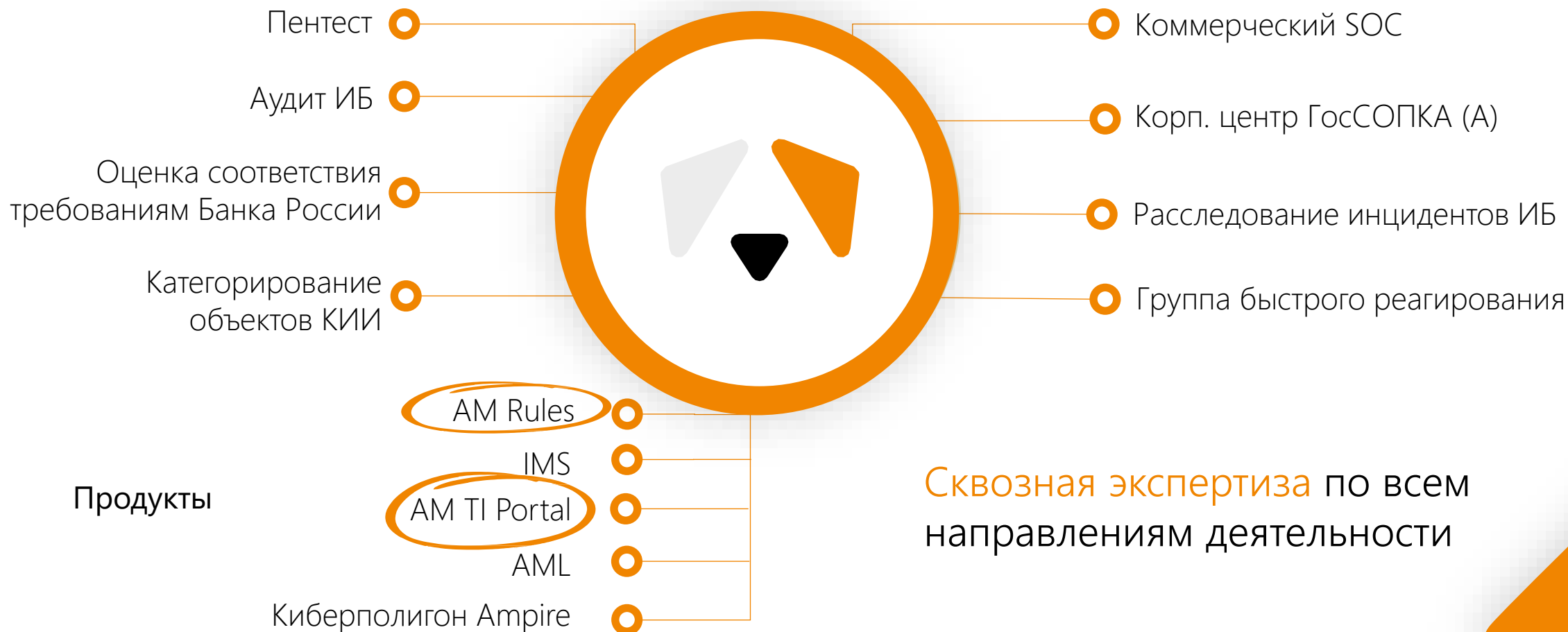
Технический директор компании «Перспективный мониторинг»

# Направления деятельности



## Исследование защищённости

## SOC

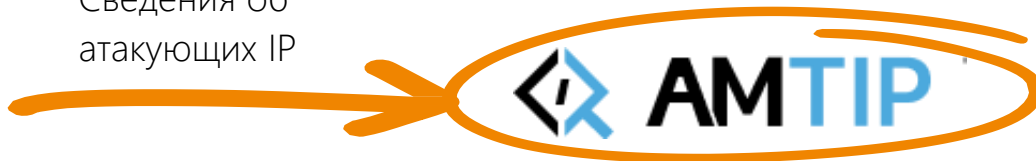


# Экосистема продуктов ПМ



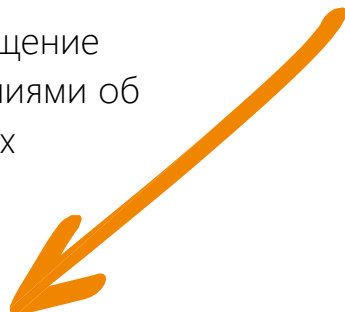
**[ ] AML**

Сведения об атакующих IP



**AMTIP**

Обогащение сведениями об угрозах

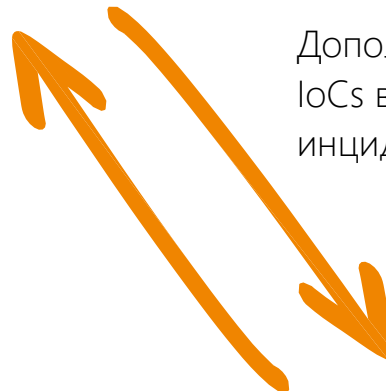


**AMPIRE**

Тренируем пользователей работе с компьютерными инцидентами и карточками в формате НКЦКИ



Дополнительный контекст по IoCs в событиях и карточках инцидентов



**incident management**

# AMTIP Threat Intelligence Portal

– веб-сервис, обеспечивающий доступ к базе экспертных данных АО «ПМ»

Портал интегрирован с внутренними и внешними сервисами экспертных данных ПМ, что позволяет оперировать всегда актуальными данными в режиме реального времени

- 01** Вектор внимания ориентирован на сведения об угрозах, направленных на российское киберпространство
- 02** Оценка вредоносности ресурсов AM SCORE на основе собственной экспертизы ПМ
- 03** Включает экспертные данные ПМ и базу решающих правил AM Rules

Включен в реестр отечественного ПО,  
реестровая запись №22808 от 06.06.2024



amtip.ru

# Свидетельства и лицензии AM Rules



## Сведения, содержащиеся в записи о программном обеспечении, включенном в реестр российского программного обеспечения

Предмет	Значение
Порядковый номер реестровой записи	19400
Дата формирования реестровой записи	04.10.2023 20:22:20
Наименование программного обеспечения	База решающих правил AM Rules
Предшущие и (или) альтернативные наименования	
Правообладатель	
Наименование правообладателя	Акционерное общество «Перспективный мониторинг»
Код страны правообладателя в соответствии с Общероссийским классификатором стран мира	643, Россия
ИНН (идентификационный номер налогоплательщика)	7714706154
Сведения об основаниях возникновения у правообладателя (правообладателей) исключительного права на программное обеспечение на территории всего мира и на весь срок действия исключительного права	собственная разработка
Адрес страницы сайта правообладателя в информационно-телекоммуникационной сети «Интернет», на которой размещена документация, содержащая описание функциональных характеристик программного обеспечения и информацию, необходимую для установки и эксплуатации программного обеспечения	<a href="https://amonitoring.ru/product/amrules/">https://amonitoring.ru/product/amrules/</a>
Адрес страницы сайта правообладателя в сети «Интернет», на которой размещены информация о стоимости программного обеспечения или порядке ее определения либо сведения о возможности использования программного обеспечения на условиях открытой лицензии или иного безвозмездного лицензионного договора	<a href="https://amonitoring.ru/product/amrules/">https://amonitoring.ru/product/amrules/</a>
Код (коды) продукции в соответствии с Общероссийским классификатором продукции по видам экономической деятельности	62 Продукты программные и услуги по разработке программного обеспечения; консультационные и аналогичные услуги в области информационных технологий

Продукт зарегистрирован в Роспатенте и [Реестре отечественного ПО](#)

# Свидетельства и лицензии АМ ТІР

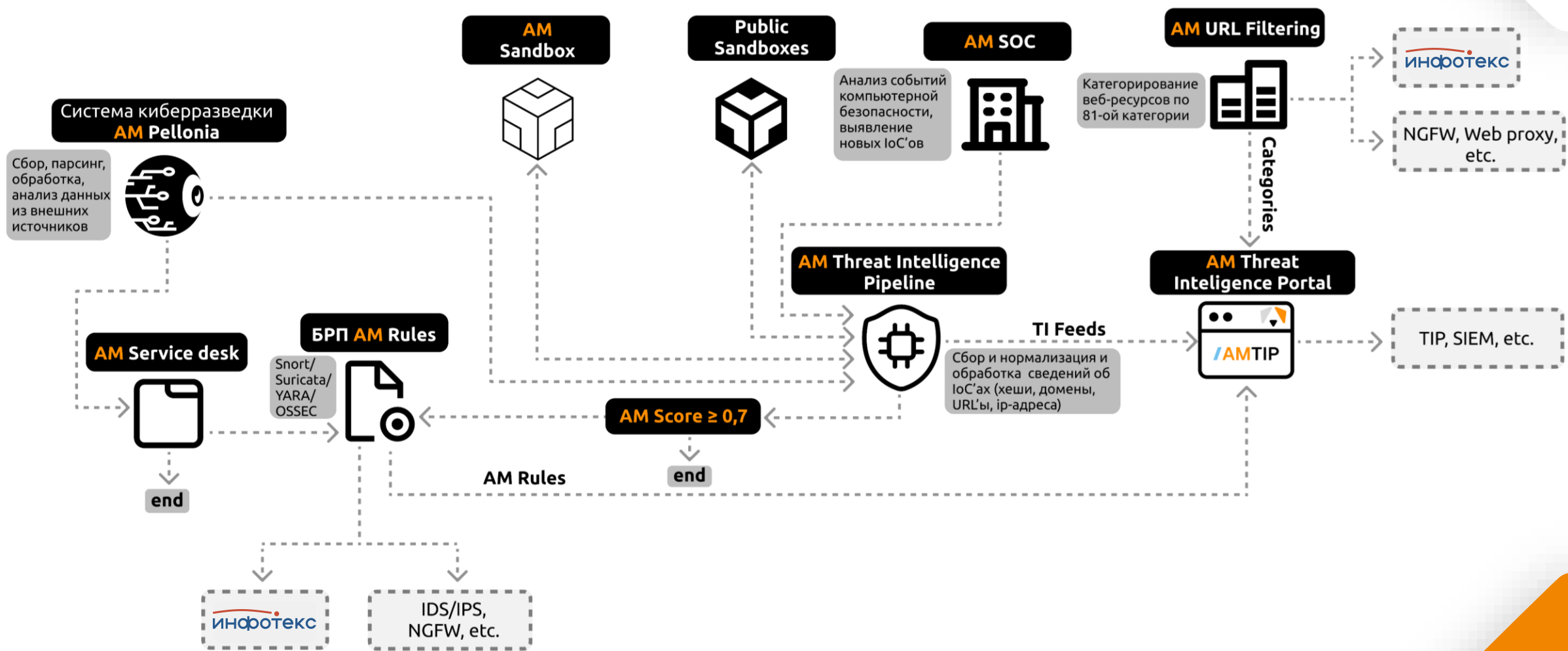
Продукт зарегистрирован в Роспатенте  
и [Реестре отечественного ПО](#)



## Сведения, содержащиеся в записи о программном обеспечении, включенном в реестр российского программного обеспечения

Предмет	Значение
Порядковый номер реестровой записи	22808
Дата формирования реестровой записи	06.06.2024 08:33:44
Наименование программного обеспечения	AM Threat Intelligence Portal
Предыдущие и (или) альтернативные наименования	
Правообладатель	
Наименование правообладателя	Акционерное общество "Перспективный мониторинг"
Код страны правообладателя в соответствии с Общероссийским классификатором стран мира	643, Россия
ИНН (идентификационный номер налогоплательщика)	7714706154
Сведения об основаниях возникновения у правообладателя (правообладателей) исключительного права на программное обеспечение на территории всего мира и на весь срок действия исключительного права	собственная разработка
Адрес страницы сайта правообладателя в информационно-телекоммуникационной сети «Интернет», на которой размещена документация, содержащая описание функциональных характеристик программного обеспечения и информацию, необходимую для установки и эксплуатации программного обеспечения	<a href="https://amonitoring.ru/product/amtip/">https://amonitoring.ru/product/amtip/</a>
Адрес страницы сайта правообладателя в сети «Интернет», на которой размещены информация о стоимости программного обеспечения или порядке ее определения либо сведения о возможности использования программного обеспечения на условиях открытой лицензии или иного безвозмездного лицензионного договора	<a href="https://amonitoring.ru/product/amtip/">https://amonitoring.ru/product/amtip/</a>
Код (коды) продукции в соответствии с Общероссийским классификатором продукции по видам экономической деятельности	62 Продукты программные и услуги по разработке программного обеспечения; консультационные и аналогичные услуги в области информационных технологий

# Как мы производим ЭД



# Что это за данные



## AM TI feeds

Индикаторы компрометации IoC (вредоносные IP-адреса, Домены, хеши, URL'ы) с комплексными сведениями о них

В базе ПМ более **50 млн** индикаторов компрометации

Ежемесячный прирост базы индикаторов компрометации **4%**

Получение сведений от SOC «ПМ» и регуляторов

## БРП AM Rules

Правила обнаружения вторжений (сигнатуры) для сетевых и хостовых средств защиты информации

Первые на российском рынке начали выпускать собственные сигнатуры с **2016** года

В базе ПМ более **50 000** актуальных сигнатур AM Rules

Ежемесячно в базе БРП AM Rules прибавляется до **1000** новых сигнатур

## AM URL фильтрация

База категорированных Интернет-ресурсов (доменов) для использования в сетевых средствах защиты информации и управления политиками доступов

**100+** миллионов ресурсов

Категорирование современными ML-алгоритмами

Ежемесячный прирост **15%**



# Форматы поставки данных



БРП AM Rules

Сетевые правила

Хостовые правила

Комплексная информация об индикаторах компрометации



SURICATA



OSSEC

STIX 2.1

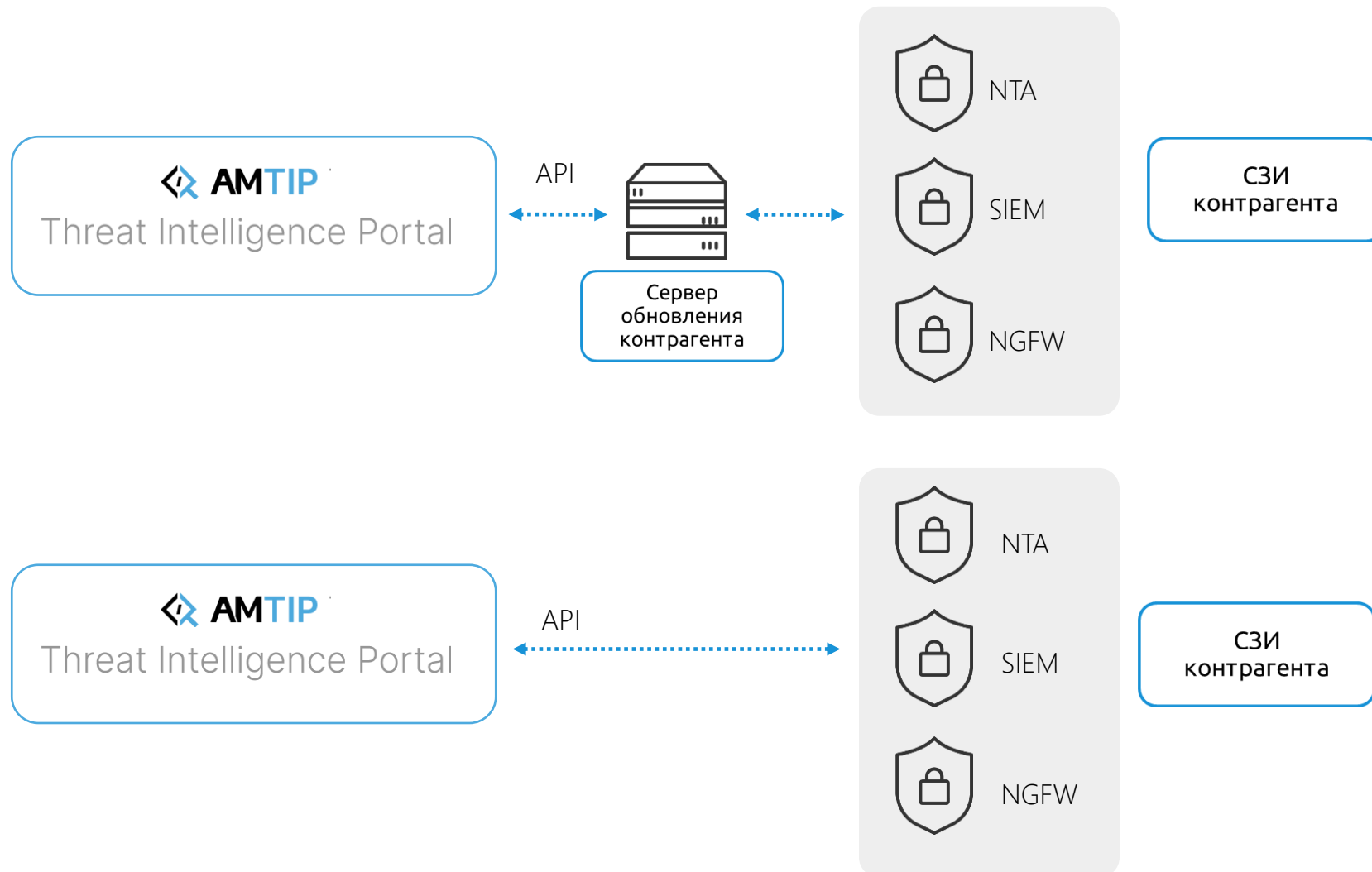


SNORT

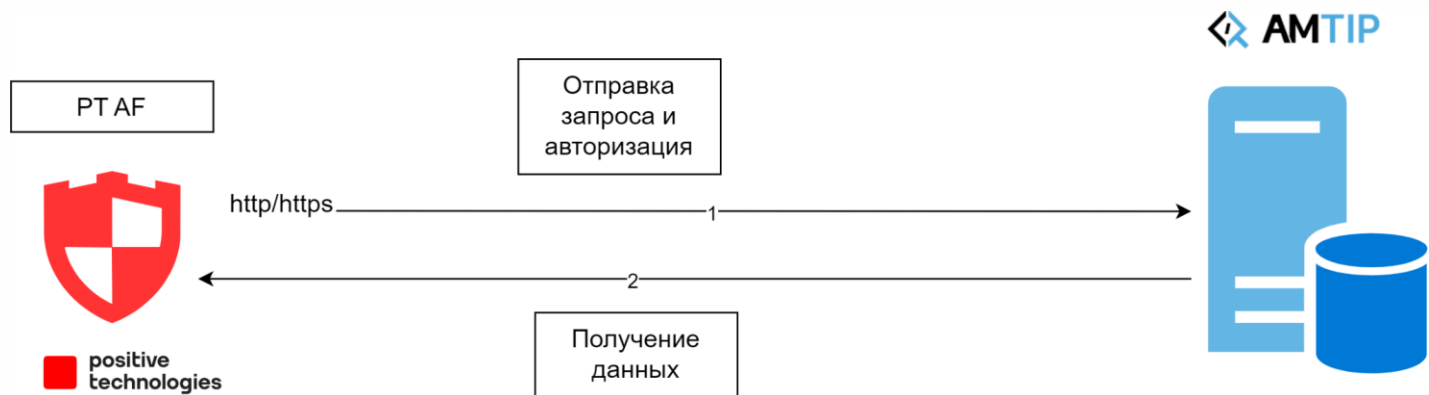


YARA

# Поставка данных (ЭД) в СЗИ

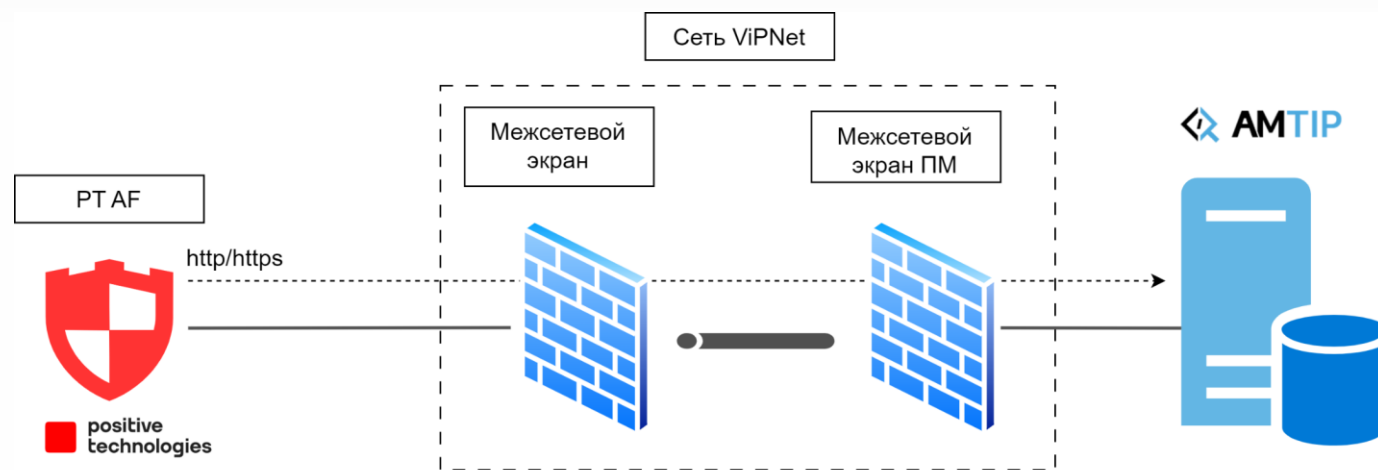


# Как уже реализовано с PT AF



Вариант 1 – PT AF находится у заказчика «снаружи» и напрямую обращается к portalу по http/https для получения файла с вредоносными IP-адресами

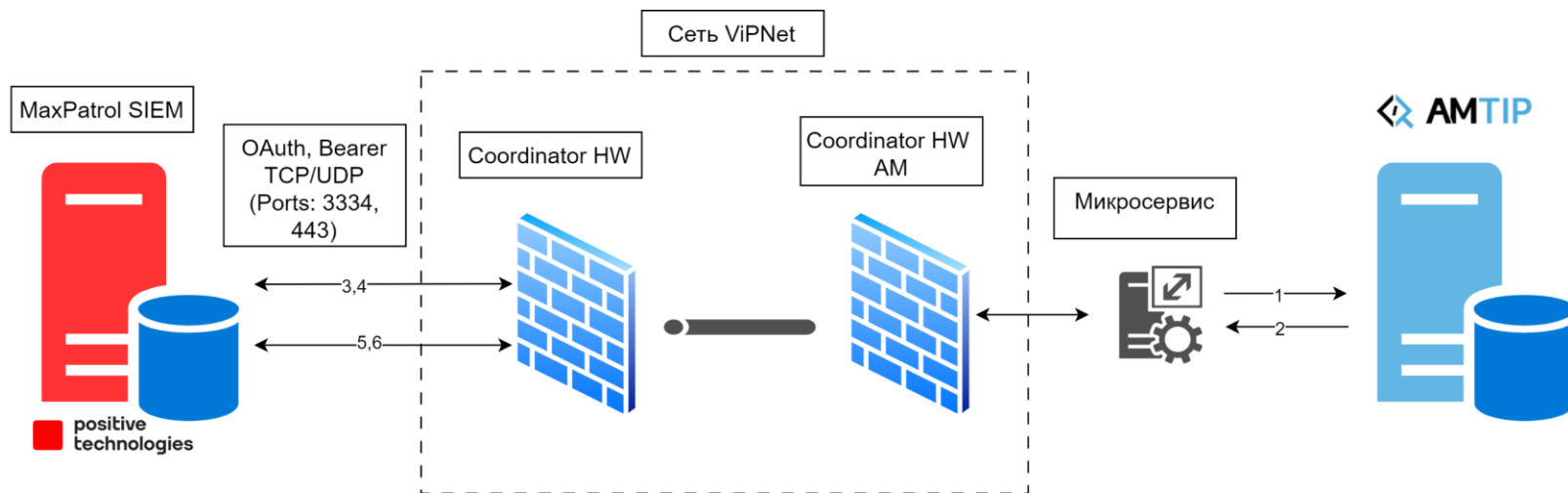
Вариант 2 – PT AF находится внутри сети заказчика и обращается к portalу по http/https через межсетевой экран для получения файла с вредоносными IP-адресами



# Интеграция с SIEM MaxPatrol



SIEM MaxPatrol находится внутри сети клиента



При первой итерации микросервис отдает актуальные данные об угрозах за 1 месяц, после чего предоставляет обновленные данные за прошедший день

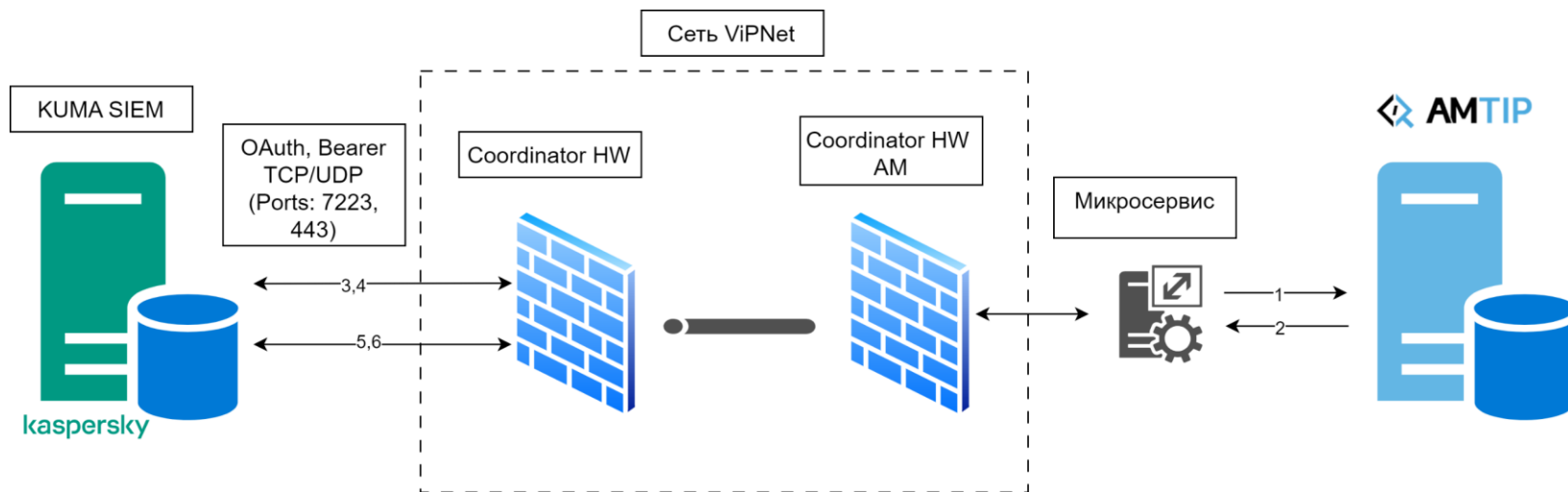
Интеграция AM TIP с SIEM MaxPatrol реализована следующим образом:

На стороне ПМ реализован микросервис, который забирает данные об угрозах и далее через межсетевые экраны (координаторы) обращается к SIEM MaxPatrol, проходит процесс авторизации и после чего отдает сведения об угрозах

# Интеграция с SIEM KUMA



SIEM KUMA находится внутри сети клиента



При первой итерации микросервис отдает актуальные данные об угрозах за 1 месяц, после чего предоставляет обновленные данные за прошедший день

Интеграция AM TIP с SIEM KUMA реализована следующим образом:

На стороне ПМ реализован микросервис, который забирает данные об угрозах и далее через межсетевые экраны (координаторы) обращается к SIEM KUMA, проходит процесс авторизации и после чего отдает сведения об угрозах

# Атака «нулевого» дня?



82.147.84.132  
Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - OpenSSL Bundled)

**Общая информация** Атакующая сессия Низкий риск

Дата и время начала: 01.03.2026 19:07:44  
Дата и время окончания: 01.03.2026 19:07:47  
Длительность: 00:00:03  
Предсказание подтверждено: Да | Нет

Парсер: Test  
Версия модели: 04-02-2026\_5  
Количество строк: 9  
Файл с логами: Скачать  
Риск подтвержден: Да | Нет

Логи сессии (9)

№	IP	Time	Code	Request	Response	Model
1	82.147.84.132	01 Mar / 2026 : 19:07:44 +0300	302	GET /cgi-bin/api.values.get?request=68:phone_model HTTP/1.1	138	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - OpenSSL Bundled)
2	82.147.84.132	01 Mar / 2026 : 19:07:44 +0300	0.043 404	GET /cgi-bin/api.values.get?request=68:phone_model HTTP/1.1	19630	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - OpenSSL Bundled)
3	82.147.84.132	01 Mar / 2026 : 19:07:44 +0300	0.043 404	GET /cgi-bin/api.values.get?request=68:phone_model HT...	19205 http://185.37.60.205:443/cgi-bin/api.values.get?request=6...	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - Open...
4	82.147.84.132	01 Mar / 2026 : 19:07:45 +0300	0.042 404	GET /cgi-bin/api.values.get?request=68:phone_model HTTP/1.1	19630	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - OpenSSL Bundled)
5	82.147.84.132	01 Mar / 2026 : 19:07:45 +0300	302	GET /cgi-bin/api.values.get?request=68:phone_model HTTP/1.1	138	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - OpenSSL Bundled)
6	82.147.84.132	01 Mar / 2026 : 19:07:45 +0300	0.043 404	GET /cgi-bin/api.values.get?request=68:phone_model HT...	19205 http://185.37.60.205:443/cgi-bin/api.values.get?request=6...	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - Open...
7	82.147.84.132	01 Mar / 2026 : 19:07:46 +0300	0.044 404	GET /cgi-bin/api.values.get?request=68:phone_model HTTP/1.1	19630	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - OpenSSL Bundled)
8	82.147.84.132	01 Mar / 2026 : 19:07:46 +0300	302	GET /cgi-bin/api.values.get?request=68:phone_model HTTP/1.1	138	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - OpenSSL Bundled)
9	82.147.84.132	01 Mar / 2026 : 19:07:47 +0300	0.044 404	GET /cgi-bin/api.values.get?request=68:phone_model HT...	19205 http://185.37.60.205:443/cgi-bin/api.values.get?request=6...	Mozilla/5.0 (compatible; Grandstream-Scanner/1.0 - Open...

Система с версией модели "04-02-2026\_5" определила в даты 26.02.2026, 01.03.2026 и 02.03.2026 сессии с запросами к URL "/cgi-bin/api.values.get?request=68:phone\_model" как атакующие, а эти запросы являются попыткой эксплуатации "CVE-2026-2329", который был обнаружен 18.02.2026, то есть после того как была собрана сама модель

# Успешная интеграция СЗИ



Smart Monitor



eSensor

NTA



ViPNet  
Coordinator HW 4/5



ViPNet  
EPP



{KOMRAD}  
Enterprise SIEM

SEIM



ViPNet  
IDS HS



ViPNet  
TIAS

## R-Vision



R-TIP



РУБИКОН  
www.rubikon.ru

NGFW



ViPNet  
IDS NS



ViPNet  
xFirewall 4/5

# Совместимость протестирована



PT Application  
Firewal

MaxPatrol  
SIEM



SIEM KUMA



MISP

SNORT

И прочее

# AM Incident Management System

## Система управления инцидентами

является «службой одного окна» для всех специалистов, задействованных в процессе управления инцидентами ИБ, удобной как для работников Центра мониторинга, так и для специалистов заказчика.

РОССИЙСКАЯ ФЕДЕРАЦИЯ



ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

RU 2023614105



incident  
management

Номер регистрации  
(свидетельства):  
2023614105

Дата регистрации: 22.02.2023

Номер и дата поступления заявки:  
2023611118 24.01.2023

Дата публикации: 22.02.2023

Контактные реквизиты:  
+79264256054,  
pavel.konovalov@amonitoring.ru

Правообладатель:  
АКЦИОНЕРНОЕ ОБЩЕСТВО «  
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ» (АО «ПМ»)  
(RU)

Название программы для ЭВМ:

«Система управления инцидентами информационной безопасности AM Incident Management System»

**Реферат:**

Программа предназначена для регистрации, учёта и обработки инцидентов информационной безопасности. Позволяет автоматизировать деятельность по управлению жизненным циклом инцидентов информационной безопасности: сбор, регистрация и агрегация информации по инцидентам ИБ; классификация, приоритезация, эскалация инцидентов ИБ; реагирование на инциденты ИБ; формирование отчётности; автоматизированный обмен информацией с регуляторами и внешними СЗИ. ОС: Windows, GNU/Linux, macOS.

# Возможности AM Incident Management System



Управление инцидентами ИБ



Обмен информацией об угрозах ИБ



Учёт ИТ-активов



Построение статистических графиков, дашбордов



Формирование отчётности



Работа с организациями и филиалами



Интеграция с ГосСОПКА



Оперативное оповещение по e-mail, telegram, sms



Обмен информацией об угрозах ИБ  
С **AMTIP**



### Обращения на killswitch домен Wannacry

HRID: 329428394 | Создан: 12.04.23 09:33 | Изменен: 12.04.23 09:33 | Просмотрен: 12.04.23 09:33

Отправить клиенту

Основное **События** История Чат IOCS Затронутые активы

#### Индикаторы +

Тип	IOC	AM Score	Дата обновления	Score
CVE	CVE-2019-5748	0.60	12.03.23 17:56	
CVE	CVE-2019-12346	0.60	12.03.23 17:56	
URL	http://linkoic.com	0.60	12.03.23 17:56	
IP-адрес	11.0.0.8	0.60	12.03.23 17:56	
Домен	iocdomain.com	0.60	12.03.23 17:56	
Хэш	68fa0e99159ca1ba6	0.60	12.03.23 17:56	
Иная	???	0.60	12.03.23 17:56	

Дашборд  
Инциденты  
Организации  
Отчеты  
Пользователи  
Бюллетени  
База знаний  
Активы  
AB  
Профиль

#### СОБЫТИЯ +

ViPNet\_IDS

Дата	Сенсор	Sid	Узел	Источник	Получатель	Событие
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...

# Области применения

## РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ



Система сгенерировала событие ИБ на IP-адрес 217.160.20.223

### Результаты поиска по IoC

217.160.20.223

Основное | Правила обнаружения вторжений 0 | Взаимосвязи 4

AM Score 0.62 | Обнаружений в антивирусах 5/94

#### Основное

Дата первого появления: 25.07.2019 17:14  
Дата последнего обновления: 22.08.2024 13:04  
Местонахождение: Германия, Карлсруэ  
Сеть: 217.160.0.0/16  
ASN: 8560  
Владелец ASN: IONOS SE  
Категории: malware

Чёрные списки: b.barracudacentral.org, cbl.abuseat.org, dnsbl-2.uceprotect.net, dnsbl-3.uceprotect.net, dyna.spamrats.com, spam.dnsbl.sorbs.net, zen.spamhaus.org  
Смотреть всё

Метки образца: malicious, malware

ТТР: TTP, Тактики, Техники  
TAO011, Command and Control

Аналитик ИБ зашел на AM TIP и увидел, что данный IP-адрес действительно является вредоносным

Аналитик приступил к работе со взаимосвязями и увидел также ряд хэшей, которые связаны с исследуемым IP-адресом

### Хэши

Обновлено	Ссылка	Обнаружения
14.07.2024 22:41	<a href="#">49c8656fe030aef2e3c32cc28fed8c5ebfc360f378716e69e14f42c6329d01c9</a>	46 / 66
14.07.2024 20:52	<a href="#">c52165f555d2c406bfd4835a8ec67249a3e60955049049e9426f1a0da4f30136</a>	12 / 69
14.07.2024 23:44	<a href="#">f904bf92d9447de9a0077e18be53cefb1adb16789d0a3a4dbf98e9bf5bafb865</a>	9 / 58
14.07.2024 23:44	<a href="#">2c15346ac601b015b4a9dcc77c7eb8d1495e8ce49f43072507f7c80466d62553</a>	8 / 60

Один из хэшей также оказался вредоносным, в результате из инфраструктуры удалили не только IP-адрес, но и связанные с ним вредоносные объекты

# Области применения РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ



Результаты поиска по IoC  
208.100.26.245

Основное | Правила обнаружения вторжений | Взаимосвязи | Обновить сведения

AM Score: 0.8 | Обнаружений в антивирусах: 13/94

**Основное**

Дата первого появления: 05.12.2022 15:12  
Дата последнего обновления: 22.08.2024 14:14  
Местонахождение: Соединённые Штаты Америки, Чикаго  
Сеть: 208.100.0.0/19  
ASN: 32748  
Владелец ASN: STEADFAST  
Категория: malware

**Черные списки**

Inquest, human, dnsbl-2.uceprotect.net, dnsbl-3.uceprotect.net, bl.emailbasura.org, cbl.abuseat.org, zen.spamhaus.org, pbl.spamhaus.org, sbl.spamhaus.org

**Метки образца**

malicious, malware

**ТТР**

TTP: Тактики, Техники  
TA0011: Command and Control

Сокращение времени работы аналитиком ИБ над компьютерным инцидентом до 5 минут

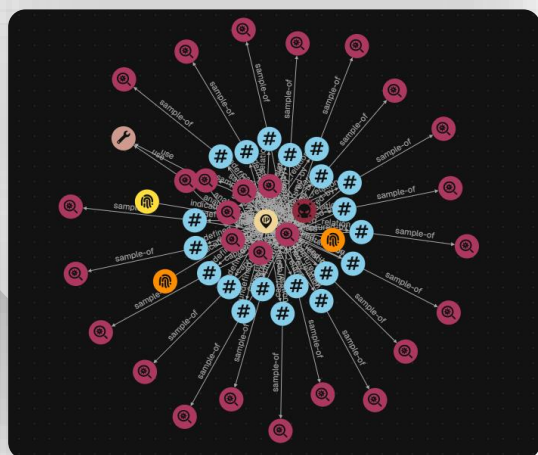
Вся ключевая информация об индикаторе представлена в одном сервисе, что помогает сокращать время поиска информации и не прибегать к нескольким узконаправленным источникам: сигнатуры, метки образца, черные списки, место нахождения, категория, взаимосвязи с объектами

AM MALWARE FakeCSUpdater C2 IP

Средняя критичность | ЦУ бот-сети | any

Описание | SNORT | SURICATA

Данное правило обнаруживает коммуникацию с IP, на котором расположен C2-сервер Fake\_CS\_Updater



Сигнатуры и связи дают дополнительный контекст и сужают круг расследования, а граф визуализирует представленные сведения

Обновлено	Ссылка	Обнаружения
14.07.2024 16:04	6380f689fe824614415172258076799bdabada47c0d4f498c01c8f8a98bf6c2	84 / 74
14.07.2024 16:04	0ba1d98c42e6af75e30d5684fe3d4d03c02bb64bc52c97ef71f746b325464f4	84 / 74
14.07.2024 16:04	a89dabc78895396846d733852190e3f65628431921b664f2fab338c29b9f01	84 / 74
14.07.2024 16:04	383f069e091c65f177987527a89f90fbdb515f148fcd765863tr0607108d	83 / 74

# Обзор функциональности



## КИБЕРКАРТА

- Просмотр аналитической информации по угрозам на карте мира и цветовая индикация стран в соответствии с процентом исходящих угроз по отношению к России,
  - Отображения ТОП-10 атакующих стран и IP-адресов,
  - Отображения ТОП-10 самых часто встречаемых угроз,
  - Отображения ТОП-10 самых часто встречаемых идентификаторов уязвимостей (CVE),
  - Ежедневное обновление информации и наличие фильтров отображения данных
- Просмотр комплексной информации по IoC (хэши, домены, IP-адреса, URL) в веб-интерфейсе,
  - Просмотр базы решающих правил AM Rules по идентификаторам уязвимости (CVE),
  - Возможность выгрузки комплексной информации по IoC из веб-интерфейса в формате STIX 2.1,
  - Возможность просмотра в веб-интерфейсе и выгрузки базы решающих правил AM Rules по IoC в форматах Snort, Suricata, YARA, OSSEC,
  - Оценка вредоносности ресурса на основе собственной методики скоринга AM SCORE



## TI LOOKUP

- Возможность получения базы решающих правил AM Rules по конкретному индикатору компрометации по API,
- Возможность получения комплексной информации об индикаторе компрометации с помощью API



## ИНТЕГРАЦИЯ

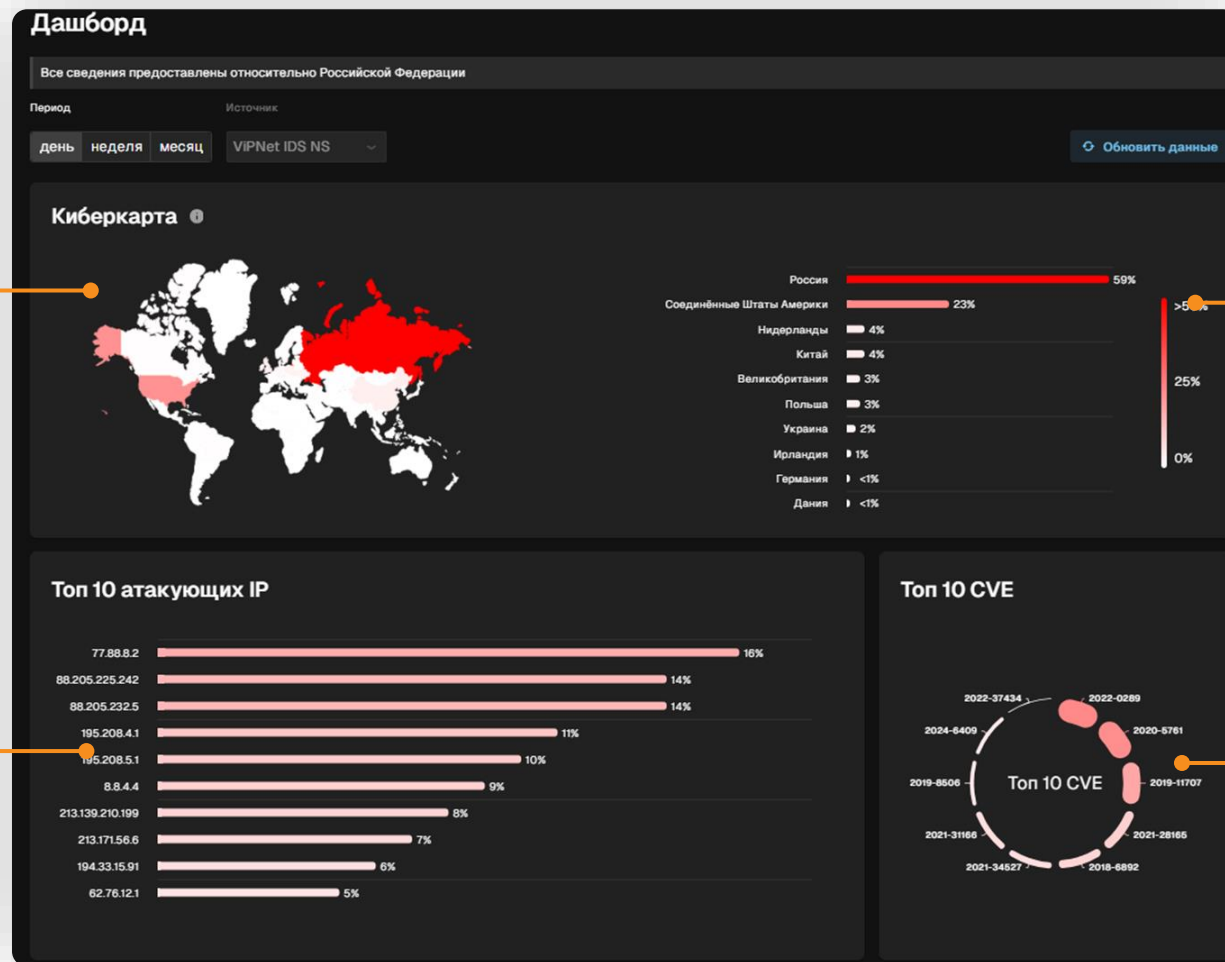
## NEW TI Reports (ver.2.35)

- Это новый раздел, в котором пользователи AM TIP получают доступ к аналитическим отчётам с результатами последних расследований и данными о новейших методах и инструментах, используемых злоумышленниками в ходе APT-атак.

# Дашборд

## Киберкарта

На Киберкарте в режиме реального времени отображается цветовая индикация стран, из которых фиксируются угрозы по отношению к РФ за выбранный период



## ТОП 10 атакующих IP

Рейтинг атакующих IP из выбранной на карте страны по отношению к РФ с выбранным периодом и источниками в процентах по убыванию

## ТОП атакующих стран

Рейтинг стран, из которых зафиксированы угрозы по отношению к РФ с выбранным периодом и источниками в процентах по убыванию

## ТОП 10 CVE

Рейтинг эксплуатируемых CVE из выбранной на карте страны по отношению к РФ с выбранным периодом и источниками, которые чаще всего фиксируются в событиях безопасности продуктов ИнфоТеКС и ПМ

# Функциональность TI LOOKUP



## AM Score

Оценка вредоносности ресурса на основе методики ПМ. Цветовая индикация результата позволяет ускорить реакцию на угрозу

## IoC

Комплексные сведения об индикаторе компрометации с возможностью выгрузки IoC в формате STIX 2.1

Результаты поиска по IoC  
dceese60dcee5fd4d47755d6b3a85a75

Основное Правила обнаружения вторжений 1 Взаимосвязи 69 Обновить сведения

AM Score 0.65 Обнаружений в антивирусах 56/74

**Основное**

Дата первого появления 27.03.2020 08:27  
Дата последнего обновления 30.09.2024 07:59  
Размер 224.6 КБ  
Тип файла -  
PUA Нет  
Категории overlay revoked-cert runtime-modules signed direct-cpu-clock-access peexe spreader

Чёрные списки -  
Метки образца Trojan-Proxy.Win32.Sybil.Ig//Trojan.MulDrop11.47334 Win32:BankerX-gen [Trj] Trojan.Win32.Emotet.DCB Trojan (005615a91) BScore.TrojanDropper.Dapato ...  
Смотреть все

TTP

TTP	Тактики	Техники
TA0002		
TA0007		
TA0011		

**Обзор**

MDS dceese60dcee5fd4d47755d6b3a85a75  
SHA-1 6969cc2f1939fd4373a83a2e607318e2cf7d78aa  
SHA-256 81d1e936a8f817e01344049ce63b41e968fec7b265c9d2ab6678412904f15178  
SSDEEP 3072:/kHyNZCT7RbVv513b2cLrEJeGUDL61UNmUCFh9W8Nf3IAK9EjCcak+OWgY5:VCTh/V3DeewB93l/+UOXC  
TLSH T12224481276D44AB7C63B02F1D8AD66B71EB5EC804F2889CF4769DE6F66302C19C3316A  
Magic PE32 executable  
TrID Win32 Executable MS Visual C++ (generic) 37.6% Microsoft Visual C++ compiled executable (generic) 20% Win64 Executable (generic) 12.7% ...  
Смотреть все

**Загрузки**

Файл	Формат
IoC	STIX 2.1

## IoC

Дополнительные атрибуты индикатора компрометации

Типы исследуемых объектов:

Hash, IP, CVE, Domain, URL

# Функциональность TI LOOKUP



## БРП AM Rules

Описание сигнатур по исследуемому объекту с возможностью просмотра и выгрузки правила в форматах Snort, Suricata, YARA, OSSEC

Результаты поиска по IoC  
dceese60dcee5fd4d47755d6b3a85a75

Основное Правила обнаружения вторжений 1 Взаимосвязи 69 Обновить сведения

AM Score 0.65 Обнаружения в антивирусах 56/74

Основное  
Дата первого появления 27.03.2020 08:27  
Дата последнего обновления 30.09.2024 07:59  
Размер 224.6 КБ  
Тип файла -  
PUA Нет  
Категории overlay, revoked-cert, runtime-modules, signed, direct-cpu-clock-access, peexe, spreader

Обзор  
MD5 dceese60dcee5fd4d47755d6b3a85a75  
SHA-1 6969cc2f1939fd4373a83a2e607318e2cf7d78aa  
SHA-256 81de936a8f817e01344049ce63b41e968fec7b265c9d2eb6678412904f15178  
SSDEEP 3072:/kHyNcCT7RbVv513b2cLrEJeGUDL61UNmUCFh9W8Nf3IAK9EJcck+OWgY5:VCTn/V3DeewB93I/+UOXC  
TLSH T12224481276D44B7C63B02F08AD66B71EB5EC804F2889CF4769DE5F66302C19C3315A  
Magic PE32 executable  
TrID Win32 Executable MS Visual C++ (generic) 37.6%, Microsoft Visual C++ compiled executable (generic) 20%, Win64 Executable (generic) 12.7%

Загрузки  
Файл ioc Формат STIX 2.1

AM EXPLOIT Possible Microsoft Outlook NTLM-relay Attack via phishing e-mail (CVE-2023-23397)

Высокая критичность Эксплуатация уязвимостей windows

Описание SNORT SURICATA

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: \* [ff 85 00 00] - идентификатор параметра "PidLidReminderFileParameter" \* [5c 00 5c 00] - идентификатор параметра "PidLidReminderOverride" \* [5c 00 5c 00] - "\\", указывающее на наличие UNC-пути до сетевого ресурса \* [08 20 06 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 c0 00 00 00 00 00 46] - GUID множества параметров, к которому принадлежит "PidLidReminderOverride".

URL-адреса

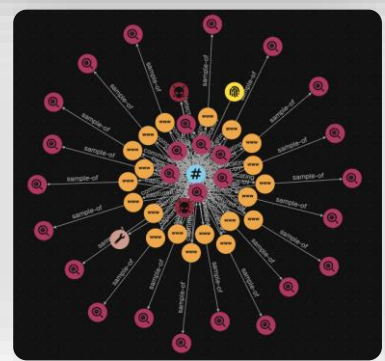
Обновлено	Ссылка	Обнаружение
14.07.2024 16:03	<a href="http://api.ipify.org/?format=json&amp;callback=dataLayer.push">http://api.ipify.org/?format=json&amp;callback=dataLayer.push</a>	5/78
14.07.2024 16:03	<a href="http://api.ipify.org/?format=json&amp;callback=gzip">http://api.ipify.org/?format=json&amp;callback=gzip</a>	5/78
14.07.2024 16:03	<a href="http://api.ipify.org/?format=json&amp;callback=gzip">http://api.ipify.org/?format=json&amp;callback=gzip</a>	5/78
14.07.2024 16:38	<a href="http://204.13.164.118/tor/status-vote/current/consensus/0232AF+14C131+23D15D+27102B+49015F+D586D1+EA9C4+ED03BB+EFC...">http://204.13.164.118/tor/status-vote/current/consensus/0232AF+14C131+23D15D+27102B+49015F+D586D1+EA9C4+ED03BB+EFC...</a>	4/78

Домены

Обновлено	Ссылка	Обнаружение
06.08.2024 03:29	<a href="http://api.ipify.org">api.ipify.org</a>	1/83

## Взаимосвязи

Информация о связанных индикаторах компрометации и адаптивный граф со связями и комплексными сведениями об индикаторе компрометации



# Экспертная оценка AM Score

– оценка вредоносности ресурса по собственной методологии ПМ

- ≥0,7** — вредоносный;
- ≥0,3 <0,7** — недоверенный;
- <0,3** — не квалифицирован как вредоносный

# 88b8eed4ec7635dd67d7b90e613095e2

Результаты поиска по IoC  
88b8eed4ec7635dd67d7b90e613095e2

Основное Правила обнаружения вторжений 0 Взаимосвязи 0

AM Score **0.8**

Обнаружений в антивирусах **36/60**

/AMTIP

36 / 60 Community Score

⚠ 36/60 security vendors and 2 sandboxes flagged this file as malicious

0029a029615cd3a04a674294df85923a019418e47e1926739bbab0b3d6507112

011120119.doc

Size 1.19 MB Last Modification Date 3 years ago

rtf ole-embedded cve-2017-11882 cve-2012-0158 exploit attachment

Reanalyze Similar More

VIRUSTOTAL

IBM X-Force Exchange ALL 88b8eed4ec7635dd67d7b90e613095e2

Риск **Высокий**

Отчет X-Force о вредоносном программном обеспечении  
88b8eed4ec7635dd67d7b90e613095e2

В этом отчете отсутствуют теги. Добавьте теги с помощью поля комментариев.

Сведения

Тип хэша	md5
Первое обнаружение	1 нояб. 2019 г. *
Последнее обнаружение	20 мая 2022 г. *
Название семейства	cve-2017-11882 *
Тип	Exploit *
Охват в сообществе	59%
Платформа	Document *
Подплатформа	RTF *

\* Powered by: ReversingLabs Titanium Platform

IBM

Indicator Report  
88b8eed4ec7635dd67d7b90e613095e2

Reputation Score

0

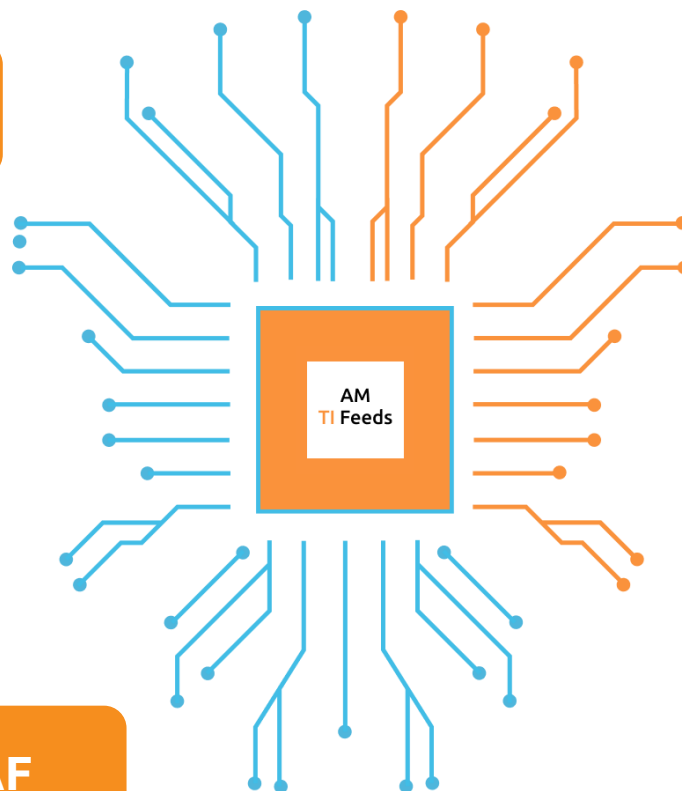
RST CLOUD

# Применимость AM TI Feeds



## SIEM

Обнаружение вредоносной активности на ранних этапах



## IDS/IPS/NGFW/NTA/WAF

Повышение эффективности в работе средств защиты информации

## TI-platform

Увеличение охвата индикаторов компрометации и предоставление дополнительного контекста по IoC'am

# События в линейке продуктов ViPNet



ViPNet IDS NS Administrator

### События

События за последние 24 часа

Ур.	Дата и время	Код события	Кол...	Название правила	Класс	Прото...	IP-адрес исто...	Порт источн...	Порт получ...	Направл...
●	15:27:34.334 08.09.2025	3200655	1	AM EXPLOIT Possible Google Chrome < 97.0.4692.99 Use After Free in Safe browsing...	client-sid...	TCP	172.21.21.52	8080	37404	←→
●	15:27:32.328 08.09.2025	3200655	1	AM EXPLOIT Possible Google Chrome < 97.0.4692.99 Use After Free in Safe browsing...	client-sid...	TCP	172.21.21.50	8080	58928	←→
●	15:27:06.678 08.09.2025	3055560	1	AM TROJAN Suspicious outbound to MSSQL port 1433 possible trojan BLACKSQUID	trojan-acti...	TCP	172.16.16.23	41360	1433	←→
●	15:27:01.999 08.09.2025	3055560	1	AM TROJAN Suspicious outbound to MSSQL port 1433 possible trojan BLACKSQUID	trojan-acti...	TCP	172.16.16.24	40762	1433	←→
●	15:26:34.720 08.09.2025	3200655	1	AM EXPLOIT Possible Google Chrome < 97.0.4692.99 Use After Free in Safe browsing...	client-sid...	TCP	172.21.21.52	8080	43214	←→
●	15:26:06.824 08.09.2025	3055560	1	AM TROJAN Suspicious outbound to MSSQL port 1433 possible trojan BLACKSQUID	trojan-acti...	TCP	172.16.16.23	34964	1433	←→
●	15:26:02.446 08.09.2025	3055560	1	AM TROJAN Suspicious outbound to MSSQL port 1433 possible trojan BLACKSQUID	trojan-acti...	TCP	172.16.16.24	46846	1433	←→
●	15:25:32.488 08.09.2025	3200655	1	AM EXPLOIT Possible Google Chrome < 97.0.4692.99 Use After Free in Safe browsing...	client-sid...	TCP	172.21.21.50	8080	38234	←→

Примеры сработок баз решающих правил AM Rules в ViPNet IDS NS

Примеры сработок баз решающих правил AM Rules в ViPNet TIAS

ViPNet TIAS amonitoring

### Сетевые события

IDS NS, IDS HS, xFirewall, EPP Категории событий

15 М 1 ч 24 ч 08.09.2025 16:15:34 - 08.09.2025 16:30:34

Источники

Уровень	Правило	К...	IP-адрес источника	IP-адрес сенс
● Критичный	AM EXPLOIT Possible Generic HTTP Parameter Pollution in URI	10		
● Критичный	AM EXPLOIT Possible Generic HTTP Parameter Pollution in URI	2		
● Критичный	AM SQL Generic SQLi in HTTP Body: 'UNION SELECT' query	2		
● Критичный	AM SQL Generic SQLi in HTTP Body: 'SELECT' and 'WHERE' query	2		
● Критичный	AM SQL Generic SQLi in HTTP Body: 'UNION SELECT' query var2	2		
● Критичный	AM SQL Generic SQLi in HTTP Body: Inline 'SELECT FROM' query	2		
● Критичный	AM EXPLOIT Possible Generic HTTP Parameter Pollution in URI	30		

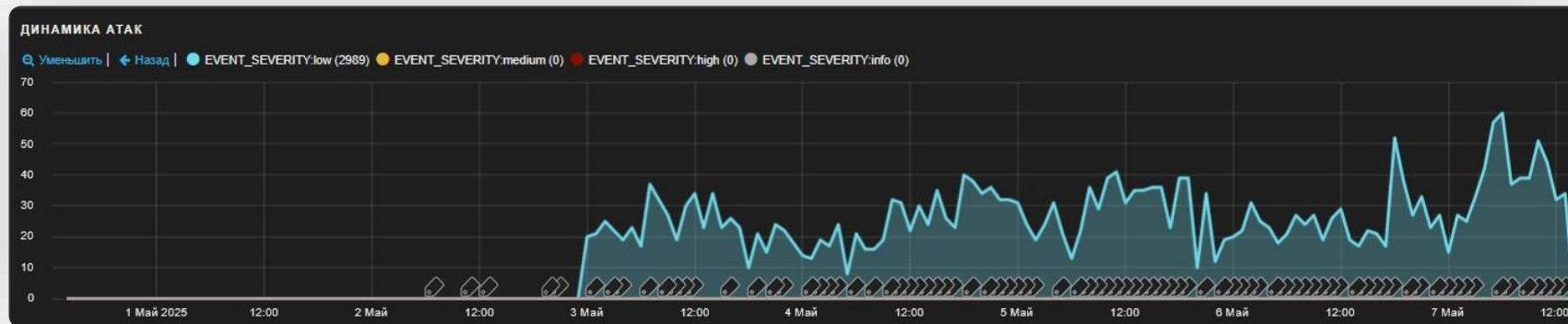
Получатели

Уровень	Правило	Количество	IP-адрес получателя	IP-адрес сенсора	Название се...	Протокол
● Критичный	AM EXPLOIT ...	380			1-IDSHS-34-2...	TCP
● Критичный	AM EXPLOIT ...	12			1-IDSHS-34-2...	TCP
● Критичный	AM EXPLOIT ...	24			1-IDSHS-34-2...	TCP
● Критичный	AM EXPLOIT ...	28			1-IDSHS-34-2...	TCP
● Критичный	AM EXPLOIT ...	40			1-IDSHS-34-2...	TCP
● Критичный	AM EXPLOIT ...	6			1-IDSHS-34-2...	TCP

# Подтверждённый эффект



AM TI Feeds были  
внедрены в WAF  
клиента 3 мая 2025



АТАКИ

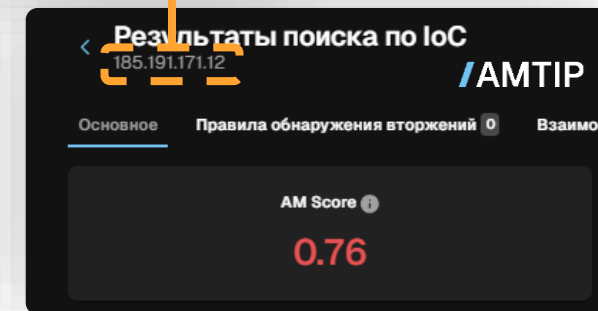
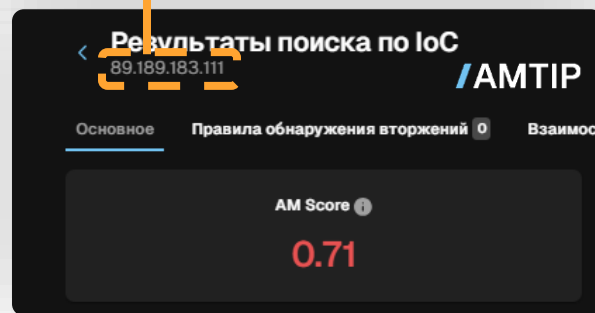
0 до 40 из 2989 доступных записей

EVENT_SEVERITY	EVENT_TAG_NAME	EVENT_NAME	POLICY_NAME	MATCHED.VARIABLE_N...	CLIENT_IP	TIMESTAMP
low	Blacklisted by IP Address	TOR IP Address Blocke...		CLIENT_IP	185.191.171.12	2025-05-07 13:51:28
low	Blacklisted by IP Address	TOR IP Address Blocke...		CLIENT_IP	95.78.246.146	2025-05-07 13:51:04
low	Blacklisted by IP Address	TOR IP Address Blocke...		CLIENT_IP	185.191.171.16	2025-05-07 13:51:54
low	Blacklisted by IP Address	TOR IP Address Blocke...		CLIENT_IP	89.189.183.111	2025-05-07 13:51:30

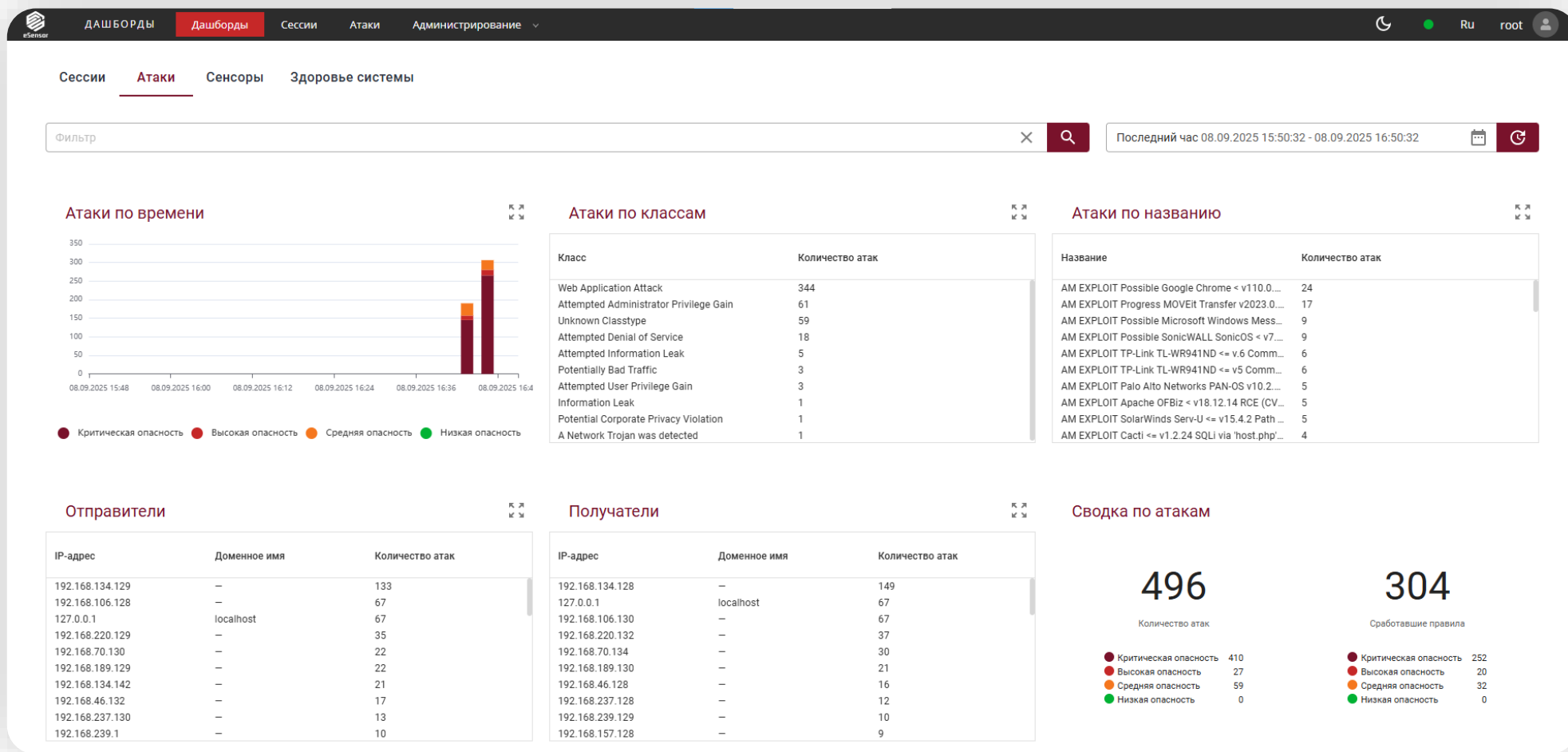
Благодаря чему удастся блокировать ряд атак  
на сайты клиентов

Ежедневно в WAF поставляется обновляемый список из  
200 000 вредоносных IP-адресов

За все время работы было выявлено только 3 ложных  
блокировки

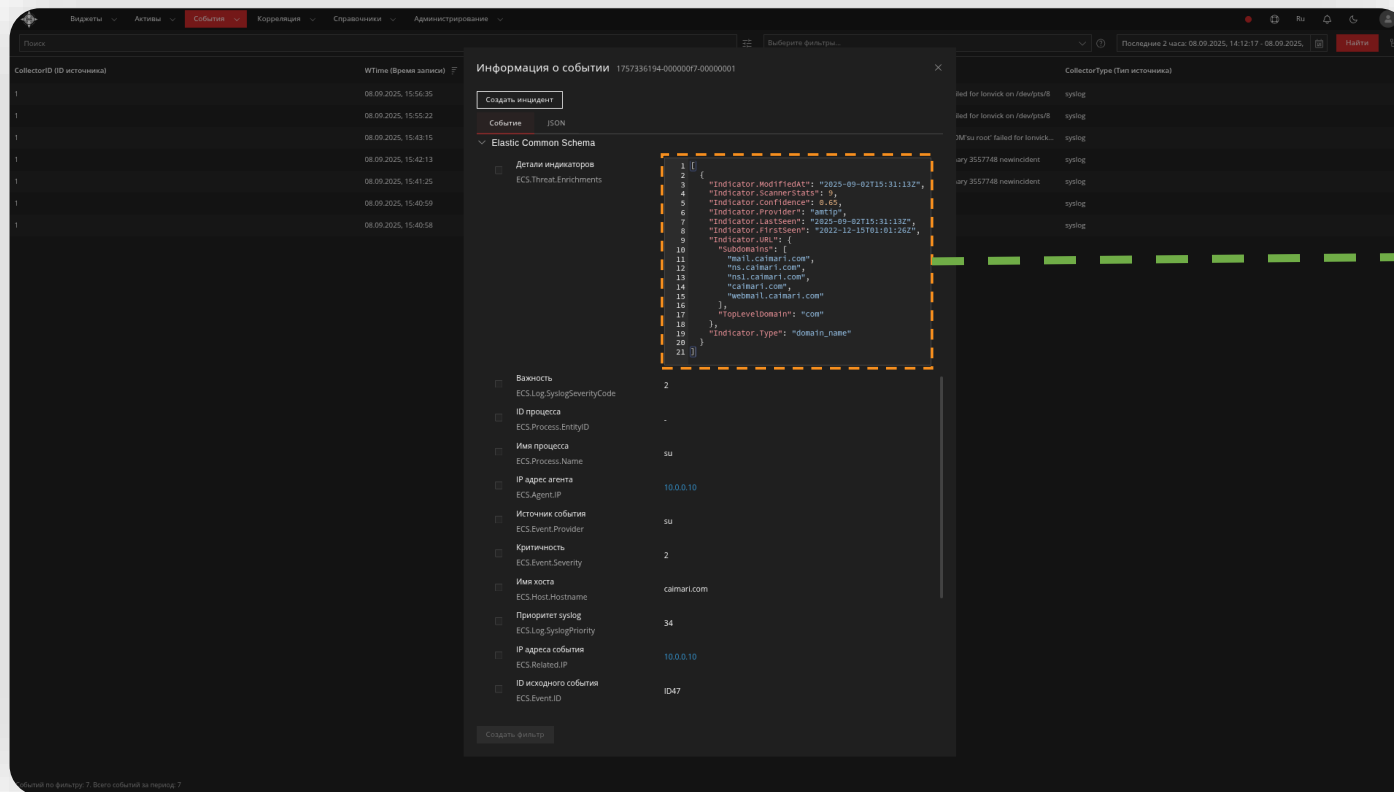


# События в линейке продуктов ГК Эшелон



Примеры сработок  
баз решающих  
правил **AM Rules**  
в NTA eSensor

# События в линейке продуктов ГК Эшелон

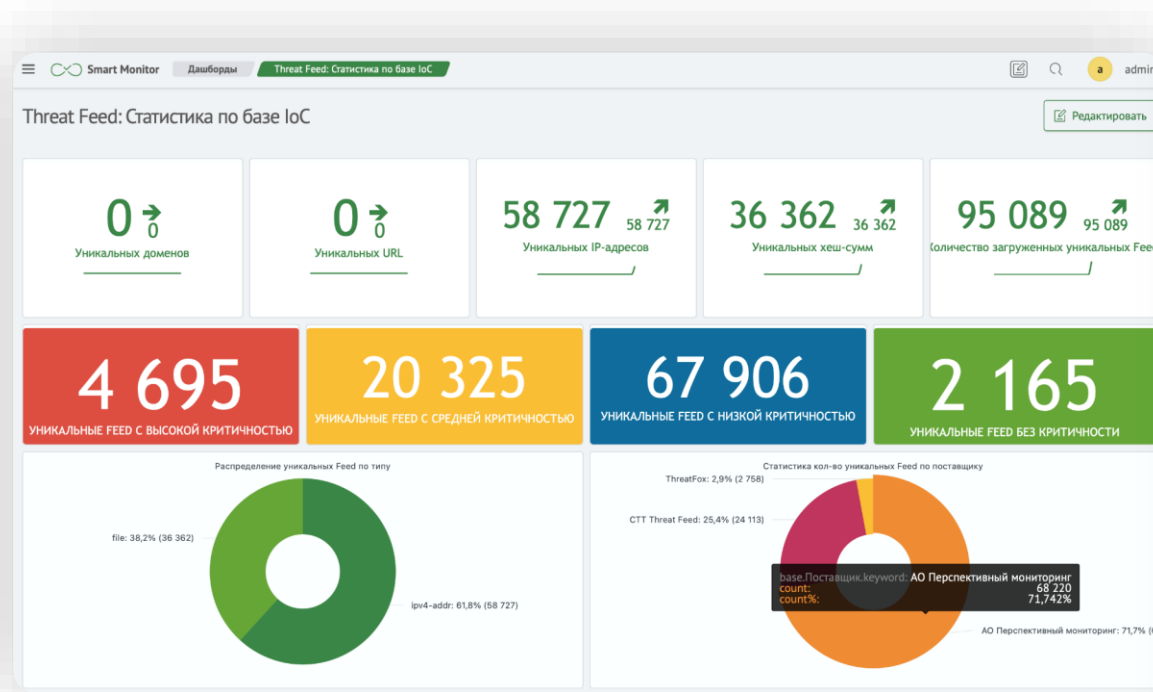


```
1 [
2   {
3     "Indicator.ModifiedAt": "2025-09-02T15:31:13Z",
4     "Indicator.ScannerStats": 9,
5     "Indicator.Confidence": 0.65,
6     "Indicator.Provider": "amtip",
7     "Indicator.LastSeen": "2025-09-02T15:31:13Z",
8     "Indicator.FirstSeen": "2022-12-15T01:01:26Z",
9     "Indicator.URL": {
10      "subdomains": [
11        "mail.caimari.com",
12        "ns.caimari.com",
13        "nsl.caimari.com",
14        "caimari.com",
15        "webmail.caimari.com"
16      ],
17      "TopLevelDomain": "com"
18    },
19     "Indicator.Type": "domain_name"
20   }
21 ]
```

Примеры обогащённой информации в SIEM KOMRAD с помощью AM TI Feeds

Благодаря AM TI Feeds, SIEM показывает уровень вредоносности индикатора, количество обнаружений в антивирусах, связанные домены и поддомены с объектом

# События в SIEM Smart Monitor



AM TI Feeds в SIEM Smart Monitor

2025-09-04 19:19:00 +03:00

TI: Сетевое взаимодействие с объектом из базы Threat Intelligence (103.187.190.150)

АМТИП

ТИ: Сетевое взаимодействие с объектом из базы Threat Intelligence (103.187.190.150) **НОВЫЙ**

АМТИП

**Описание**

Обнаружено взаимодействие с объектом из базы Threat Intelligence 103.187.190.150 в событиях источника asa. Информация по объекту базы TI предоставлена провайдером АМТИП.

Наименование поисковой задачи: **RULE - TI - Network - Threat Activity Detected.**

**Дополнительные поля**

destination_ip	103.187.190.150
destination_port	52848
ioc_provider	АМТИП
ioc_severity	low
ioc_tags	malware
ioc_threat	metasploit_tool remcos_rat
ioc_type	ip
ioc_value	194.59.31.31
network_transport	tcp
observer_product	asa
observer_type	firewall
source_ip	172.18.53.28
timestamp	2025-09-04 19:18:07 +03:00
user_name	KrytovKD

**История**

Благодаря AM TI Feeds можно обогащать события, которые поступают в SIEM, а также писать правила корреляции для формирования инцидентов при нахождении вредоносного объекта

# Публичные результаты



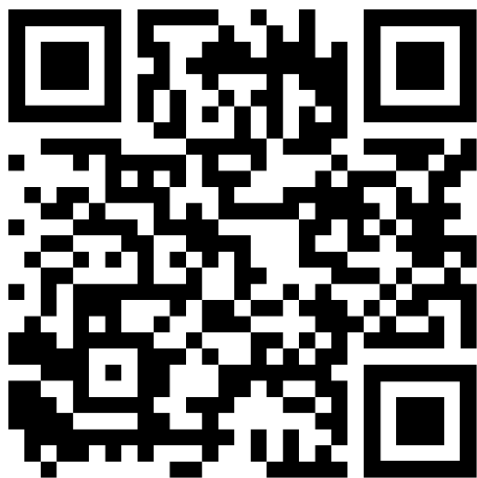
Отчёт SOC ПМ



Ландшафт киберугроз



MeshAgent



# Спасибо за внимание!

Артём Савчук  
Технический директор,  
«Перспективный мониторинг»



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

САНКТ  
ПЕТЕРБУРГ

инфотекс  
ТЕХНОДЕСТ

Подписывайтесь  
на наши соцсети



инфотекс  
Академия

УЧЕБНЫЙ  
ЦЕНТР  
ИНФОТЕКС

AMPIRE

TELEOFIS®

КОМФОРТЕЛ  
оператор связи бизнес-класса

РУТОКЕН  
МОНИТОРИНГ  
ПРАКТИВ

TS Solution

AUXOFT®