Обогащение СЗИ и расследования инцидентов с помощью TIP

Артём Савчук

Технический директор компании «Перспективный мониторинг»

инфотекс ТЕХНОДЕСТ

Белый поток

Направления деятельности

Исследование защищённости

- Пентест
- Аудит ИБ
- Оценка соответствия требованиям Банка России
- Категорирование объектов КИИ

SOC

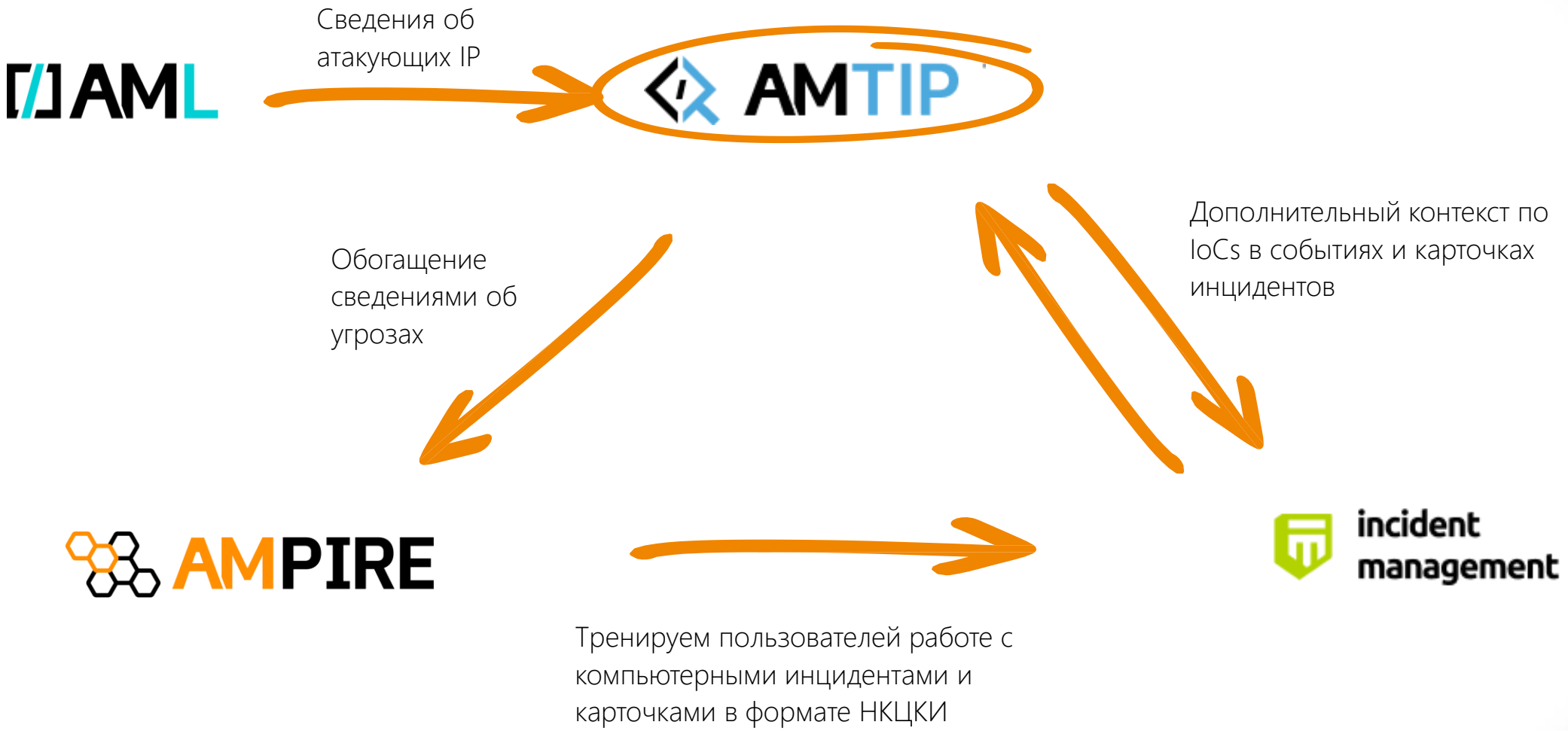
- Коммерческий SOC
- Корп. центр ГосСОПКА (А)
- Расследование инцидентов ИБ
- Группа быстрого реагирования

Продукты

- AM Rules
- IMS
- AM TI Portal
- AML
- Киберполигон Ampire

Сквозная экспертиза по всем направлениям деятельности

Экосистема продуктов ПМ



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 решающий правил AM Rules

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

amtip.ru

Свидетельства и лицензии AM Rules

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации базы данных

№ 2016620316

«База данных сигнатурных правил обнаружения атак AM Rules»

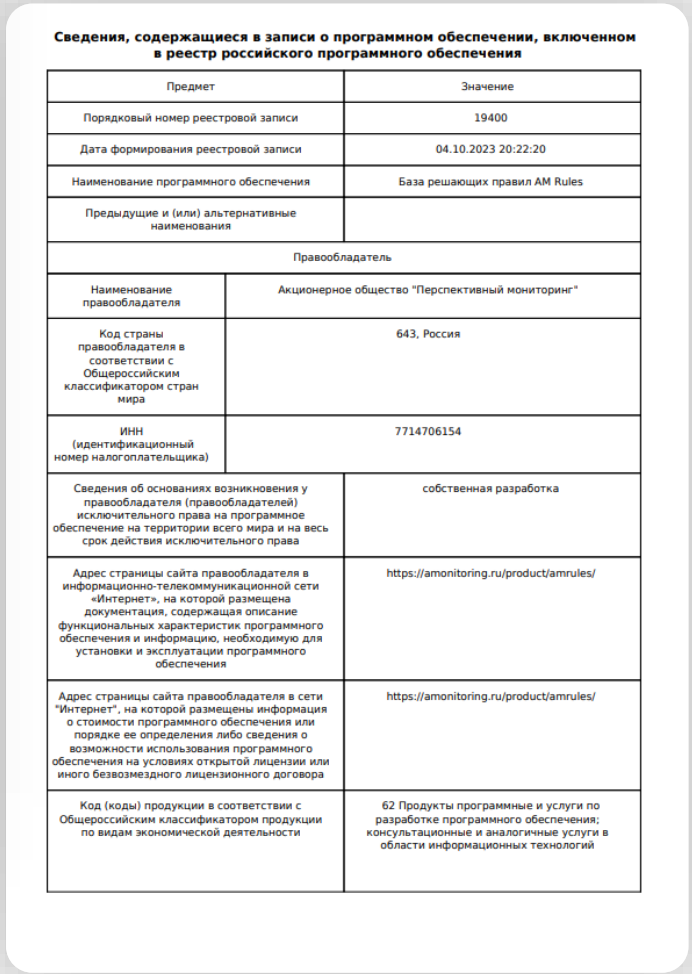
Правообладатель: *Закрытое акционерное общество «Перспективный мониторинг» (RU)*

Авторы: *Головенков Евгений Владимирович (RU), Богданов Роман Сергеевич (RU), Минаков Андрей Геннадьевич (RU)*

Заявка № **2015621242**
Дата поступления **09 октября 2015 г.**
Дата государственной регистрации в Реестре баз данных ***03 марта 2016 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев



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
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	https://amonitoring.ru/product/amrules/
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	https://amonitoring.ru/product/amrules/
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 AM TIP

Продукт зарегистрирован в Роспатенте

и Реестре отечественного ПО

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024614349

AM Threat Intelligence Portal

Правообладатель: *АКЦИОНЕРНОЕ ОБЩЕСТВО "ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ" (RU)*

Заявка № 2024613368

Дата поступления 22 февраля 2024 г.

Дата государственной регистрации в Реестре программ для ЭВМ *22 февраля 2024 г.*

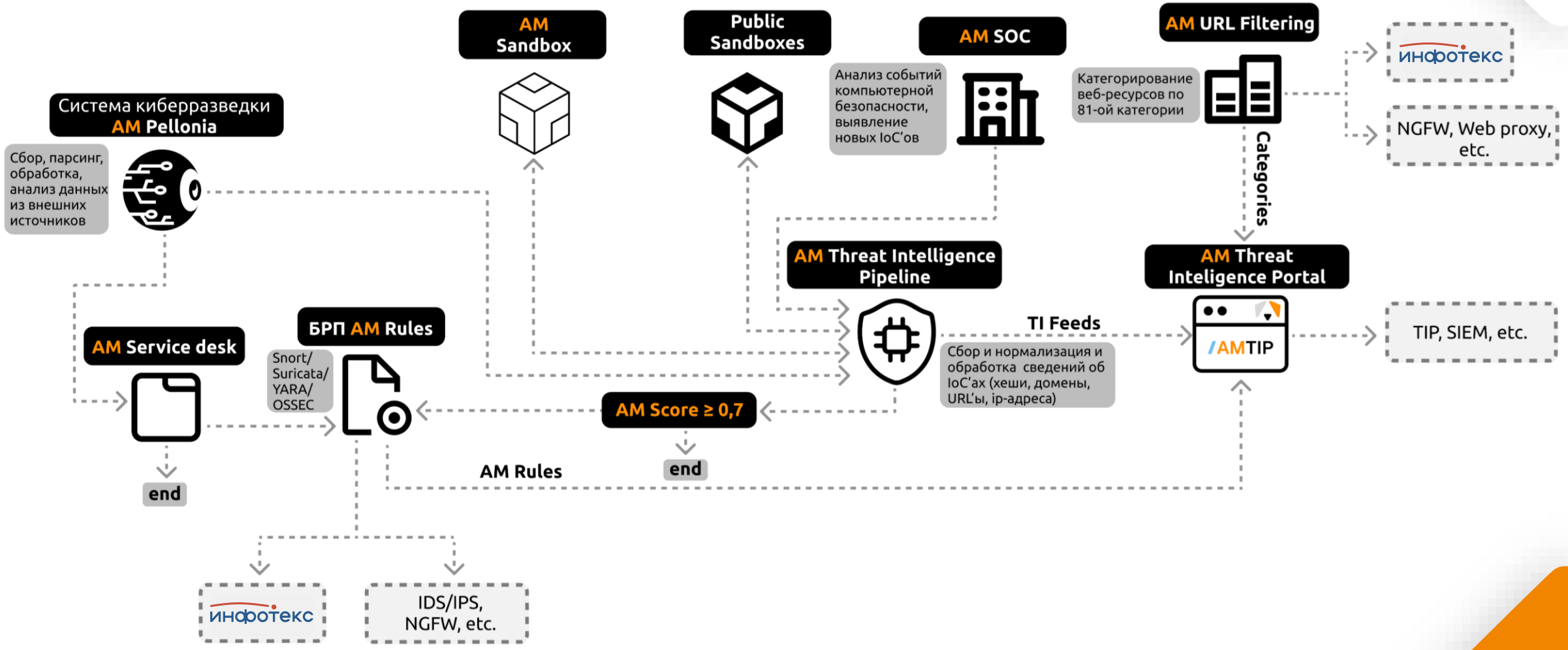
Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

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	https://amonitoring.ru/product/amtip/
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	https://amonitoring.ru/product/amtip/
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

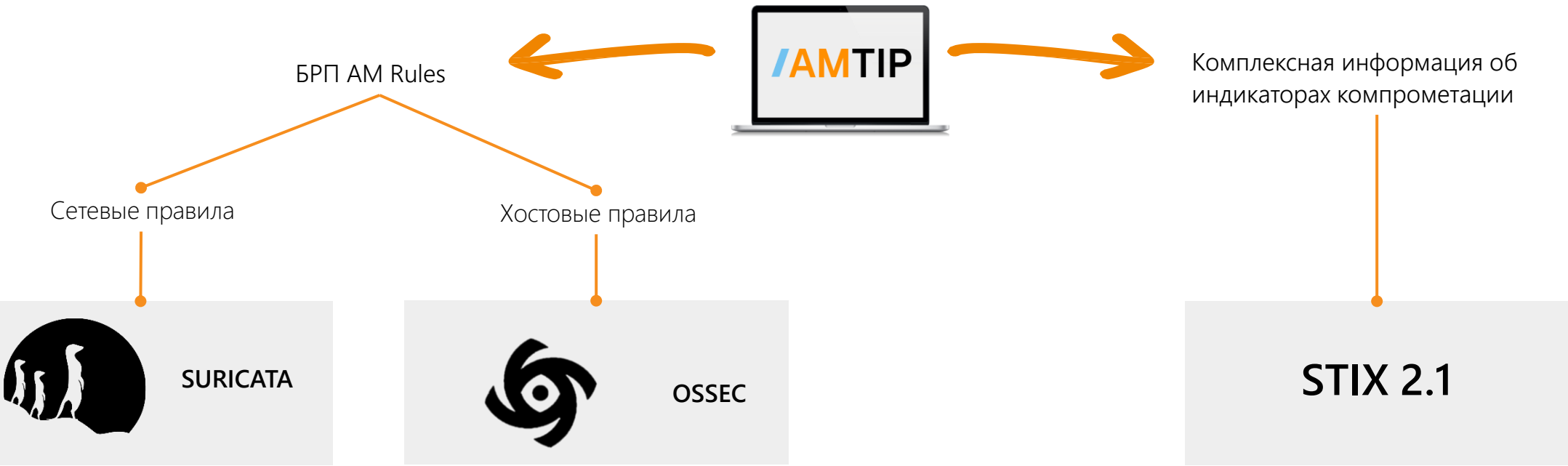
- Первые на российском рынке начали выпускать собственные сигнатуры с 2016 года
- В базе ПМ более 50 000 актуальных сигнатур AM Rules
- Ежемесячно в базе БРП AM Rules прибавляется до 1000 новых сигнатур

AM URL фильтрация

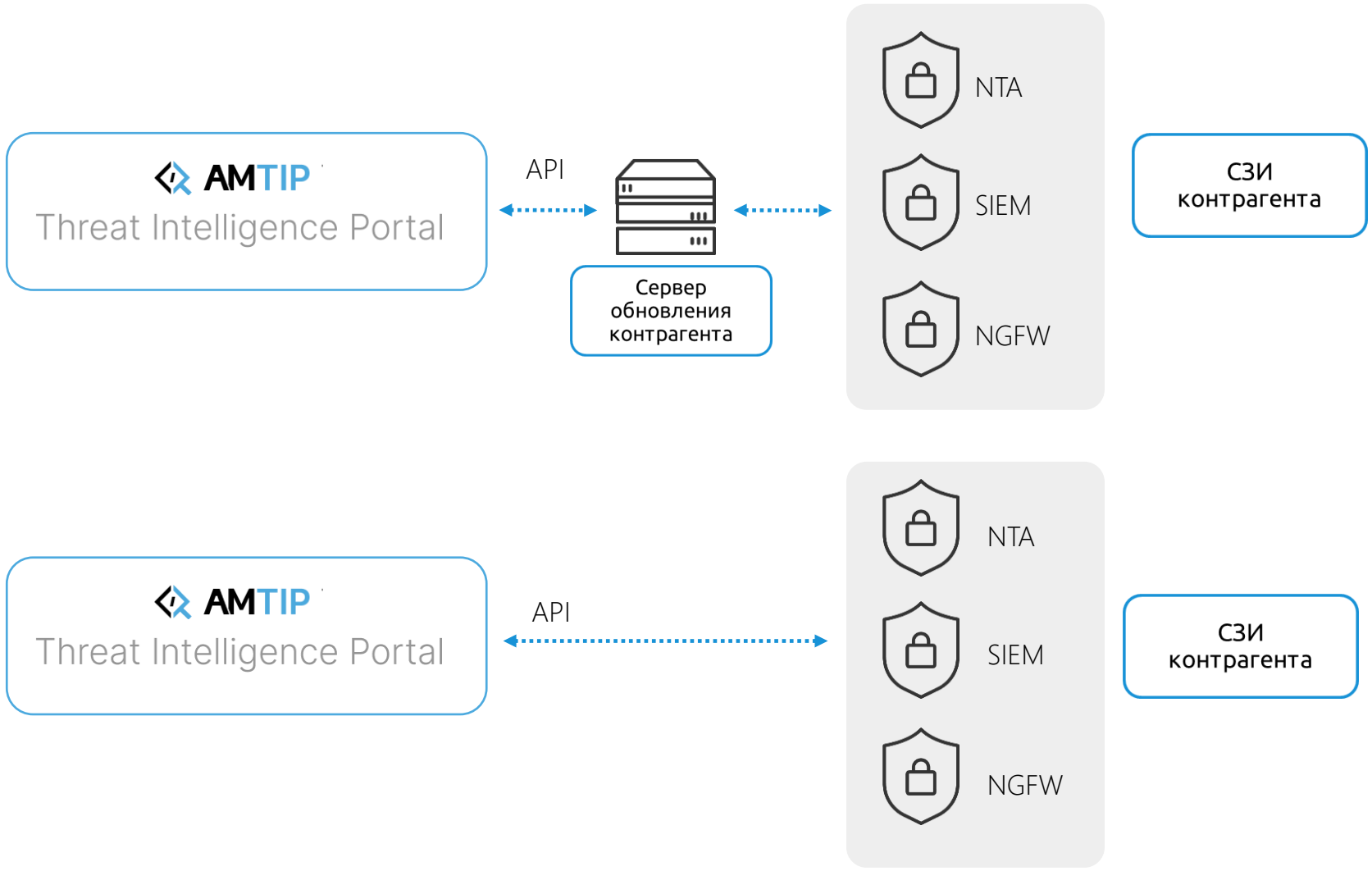
База категорированных Интернет-ресурсов (доменов) для использования в сетевых средствах защиты информации и управления политиками доступов

- 100+ миллионов ресурсов
- Категорирование современными ML-алгоритмами
- Ежемесячный прирост 15%

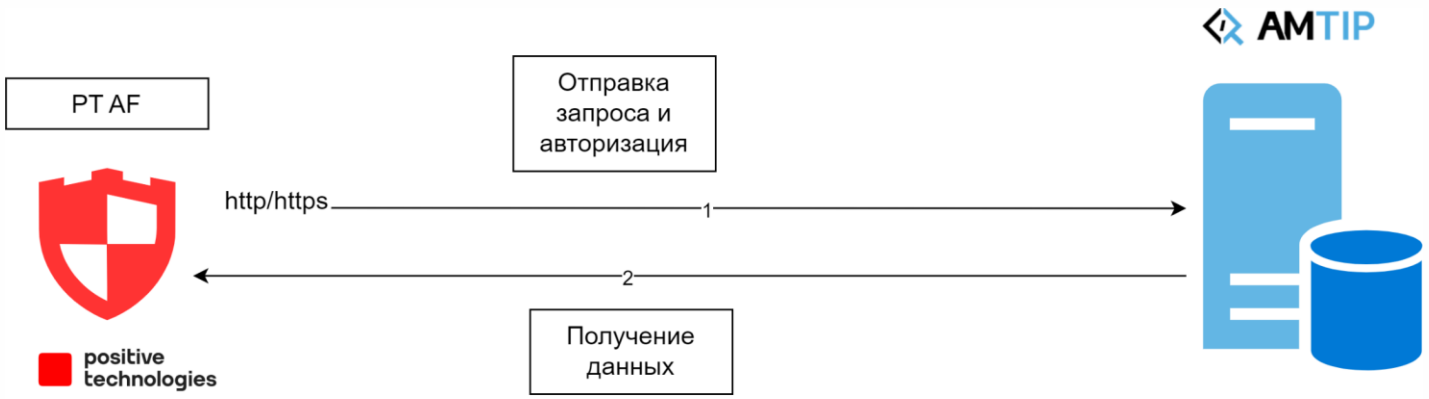
Форматы поставки данных



Поставка данных (ЭД) в СЗИ

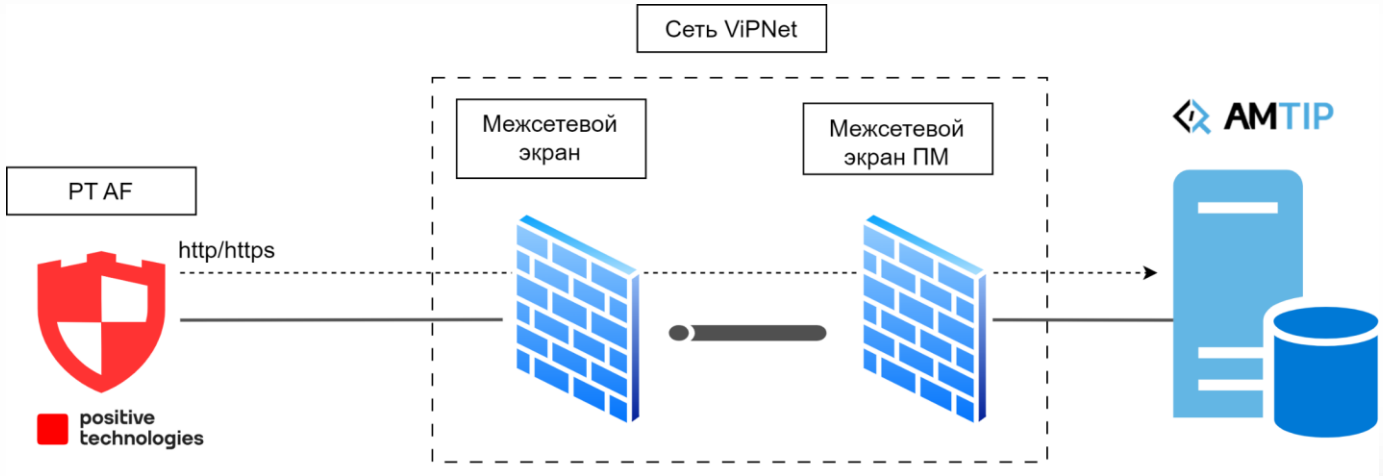


Как уже реализовано с PT AF



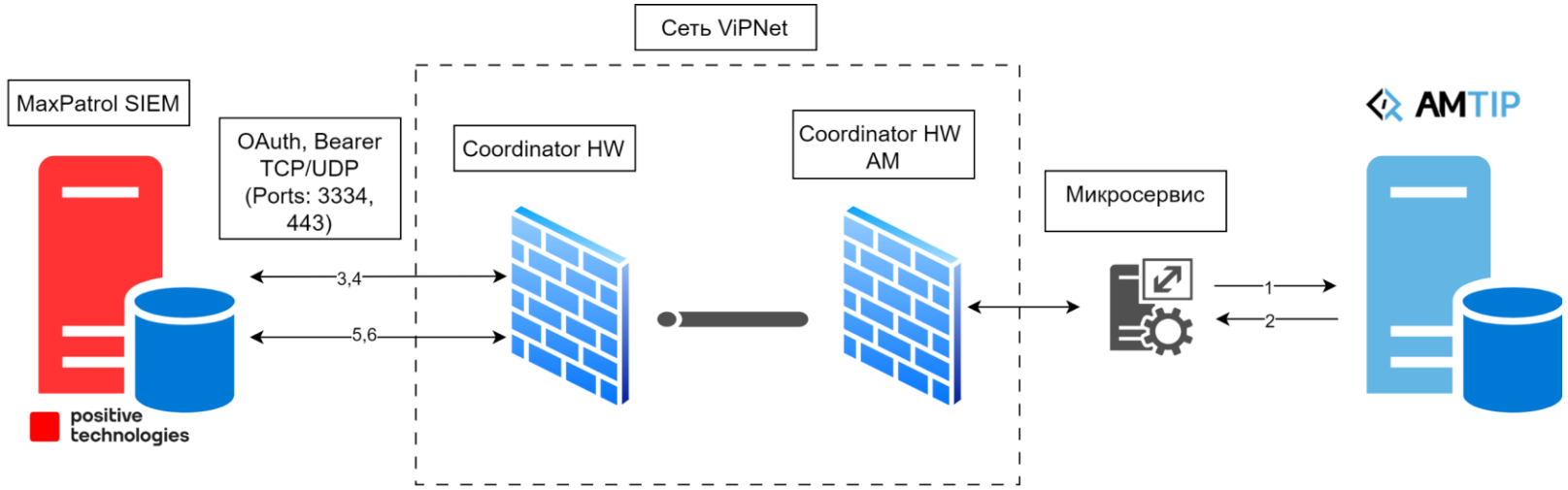
Вариант 1 – PT AF Находится у заказчика «снаружи» и напрямую обращается к порталу по http/https для получения файла с вредоносными IP-адресами

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



Интеграция с SIEM MaxPatrol

SIEM MaxPatrol находится внутри сети клиента



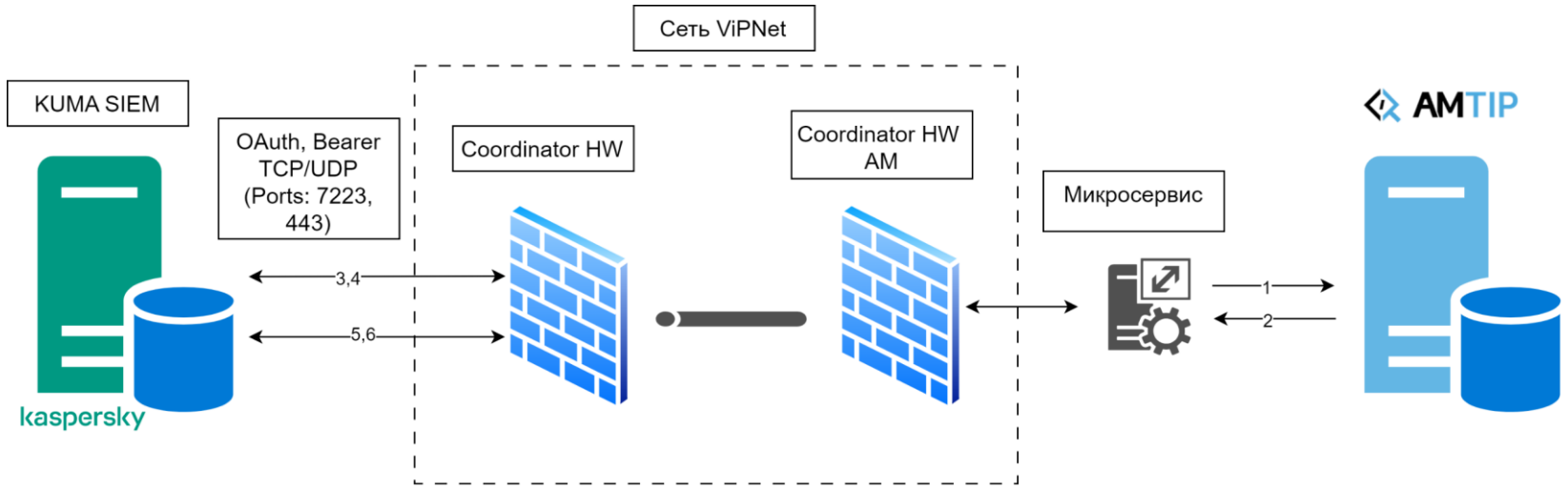
При первой итерации микросервис отдает актуальные данные об угрозах за 1 месяц, после чего предоставляет обновленные данные за прошедший день

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

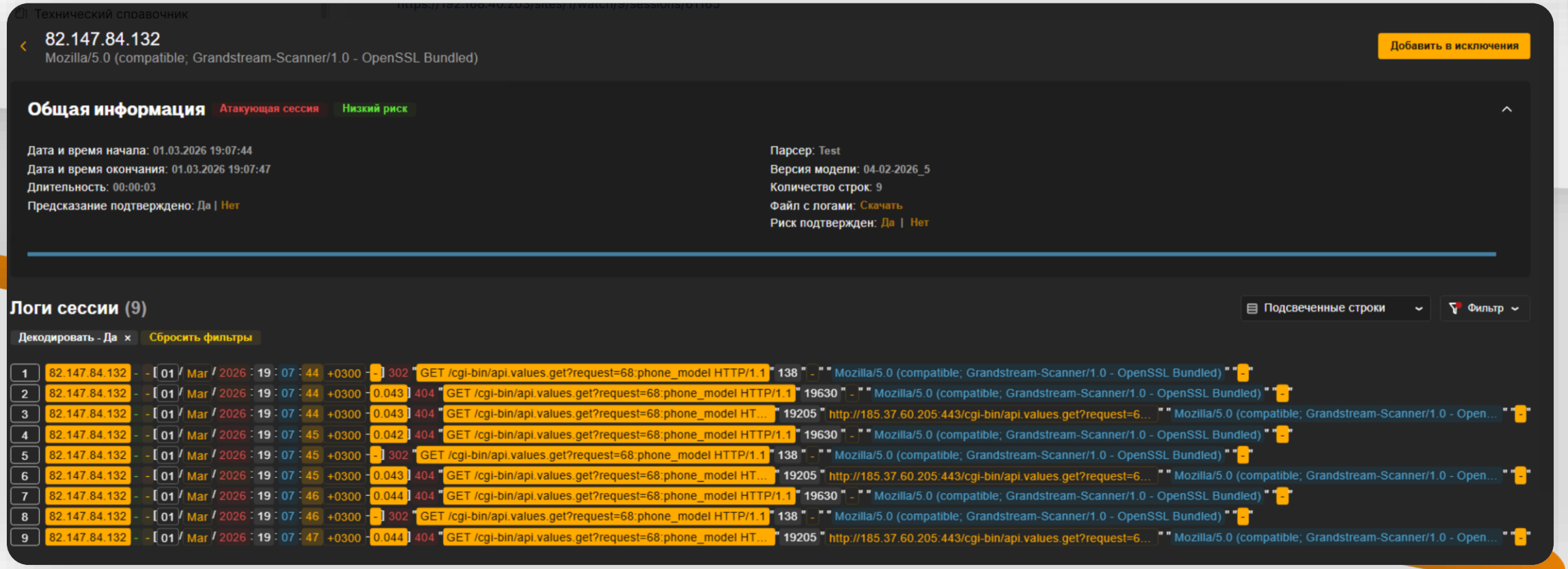


При первой итерации микросервис отдает актуальные данные об угрозах за 1 месяц, после чего предоставляет обновленные данные за прошедший день

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?



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

VolgaBlob

Smart Monitor

R-Vision

R-TIP

Эшелон
комплексная безопасность

eSensor NTA

{KOMRAD} Enterprise SIEM SEIM

РУБИКОН NGFW

инфотекс

HW ViPNet Coordinator HW 4/5

HS ViPNet IDS HS

NS ViPNet IDS NS

ViPNet EPP

ViPNet TIAS

xFW ViPNet xFirewall 4/5

Совместимость протестирована

positive technologies

- PT Application Firewal
- MaxPatrol SIEM

kaspersky

- SIEM KUMA

OPEN SOURCE

- 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

RU 2023614105

incident management

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

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»

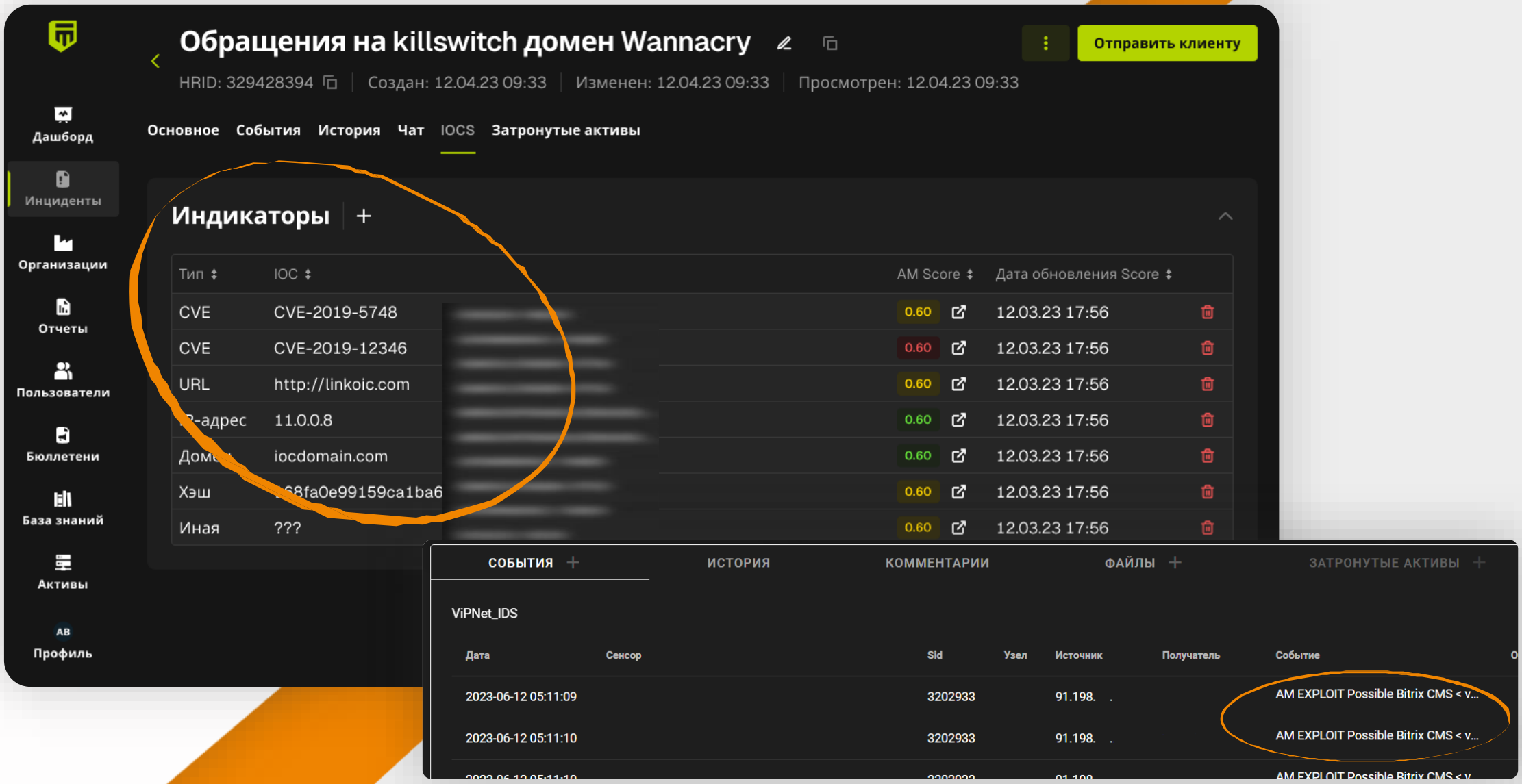
Реферат:
Программа предназначена для регистрации, учёта и обработки инцидентов информационной безопасности. Позволяет автоматизировать деятельность по управлению жизненным циклом инцидентов информационной безопасности: сбор, регистрация и агрегация информации по инцидентам ИБ; классификация, приоритезация,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

Включено в реестр отечественного ПО, реестровая запись №29485 от 29.08.2025

Возможности
AM Incident Management System

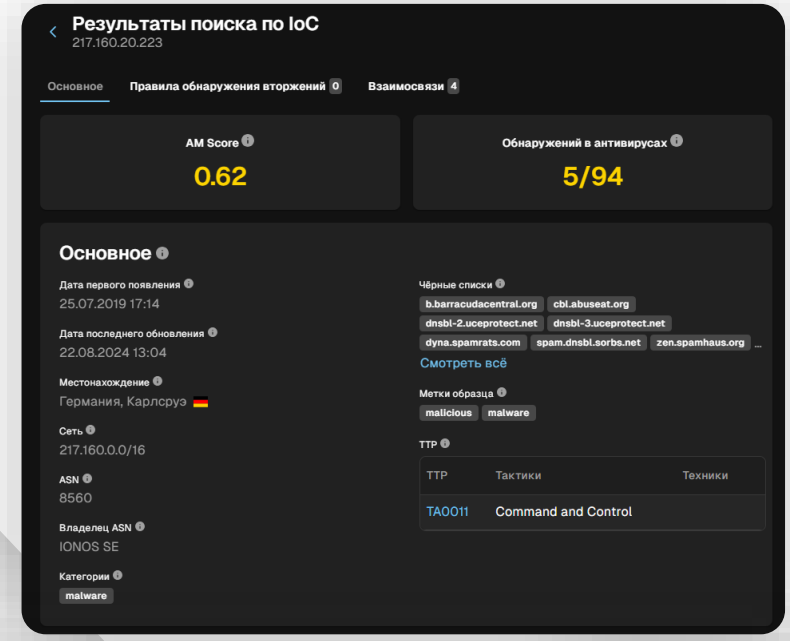
- Управление инцидентами ИБ
- Учёт ИТ-активов
- Формирование отчётности
- Интеграция с ГосСОПКА
- Обмен информацией об угрозах ИБ
- Построение статистических графиков, дашбордов
- Работа с организациями и филиалами
- Оперативное оповещение по e-mail, telegram, sms

Обмен информацией об угрозах ИБ с AMTIP



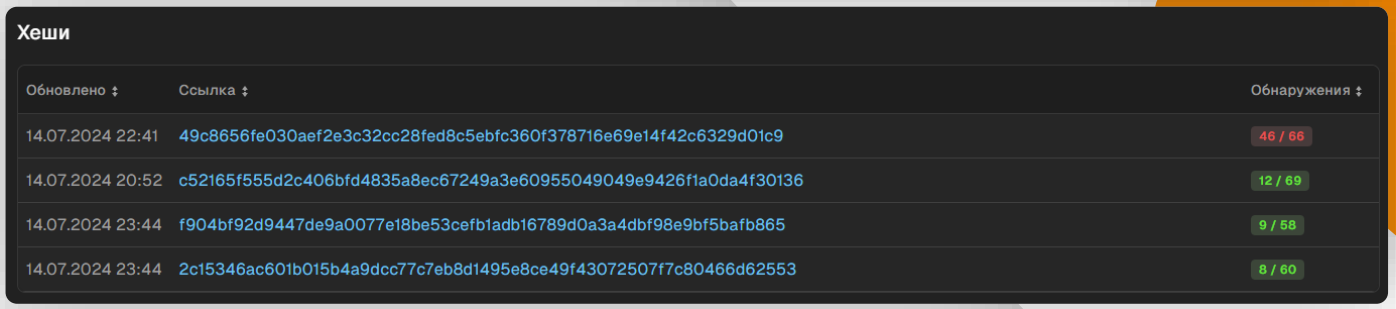
Области применения
РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Система сгенерировала событие ИБ на IP-адрес 217.160.20.223



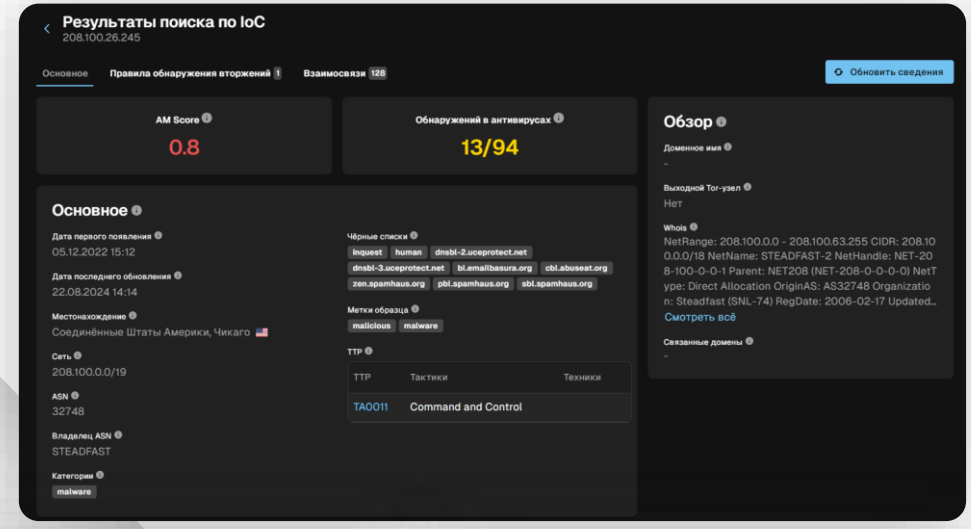
Аналитик ИБ зашел на AM TIP и увидел, что данный IP-адрес действительно является вредоносным

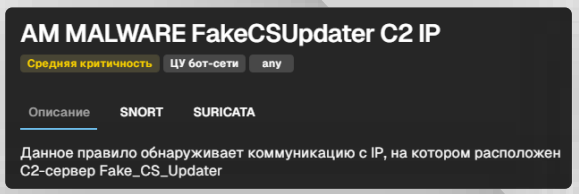
Аналитик приступил к работе со взаимосвязями и увидел также ряд хэшей, которые связаны с исследуемым IP-адресом

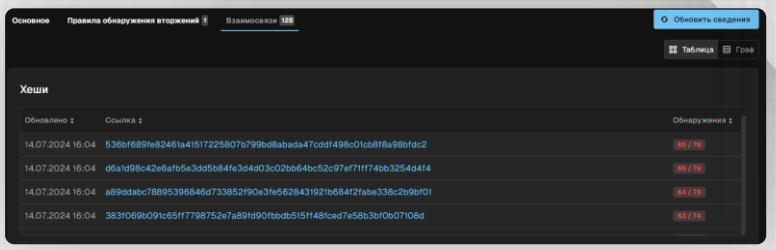


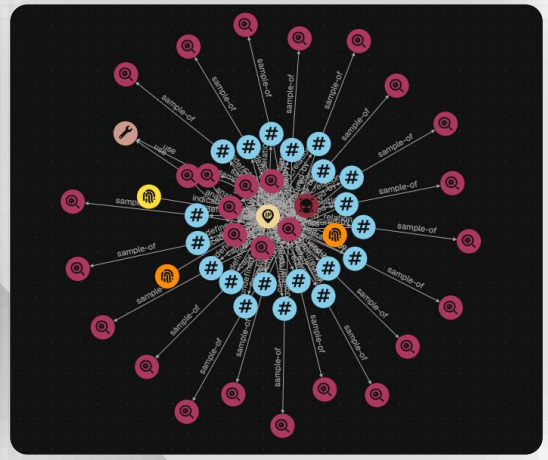
Один из хэшей также оказался вредоносным, в результате из инфраструктуры удалили не только IP-адрес, но и связанные с ним вредоносные объекты

Области применения
РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ









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

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

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

TI LOOKUP

- 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

ИНТЕГРАЦИЯ

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

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.

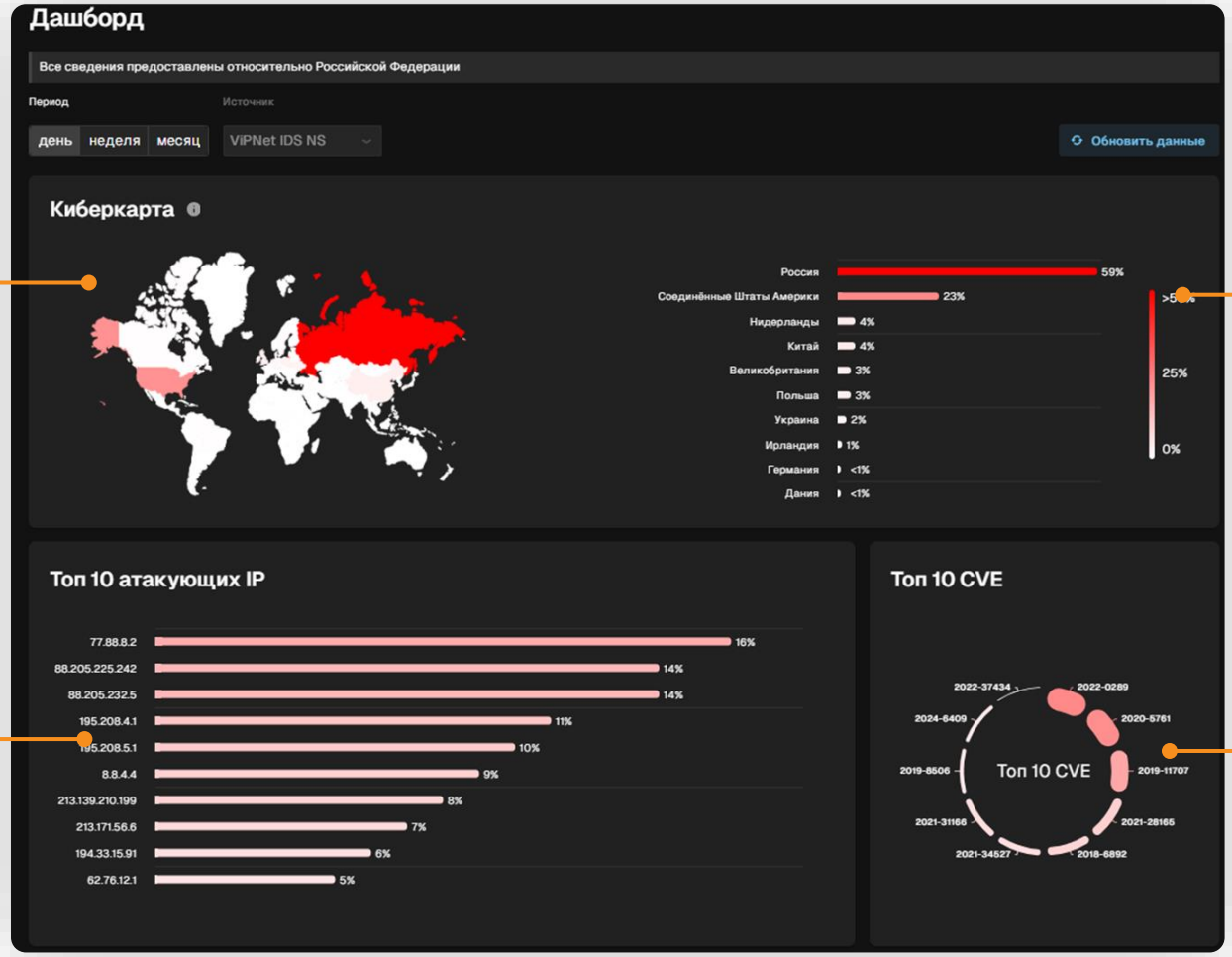
Дашборд

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

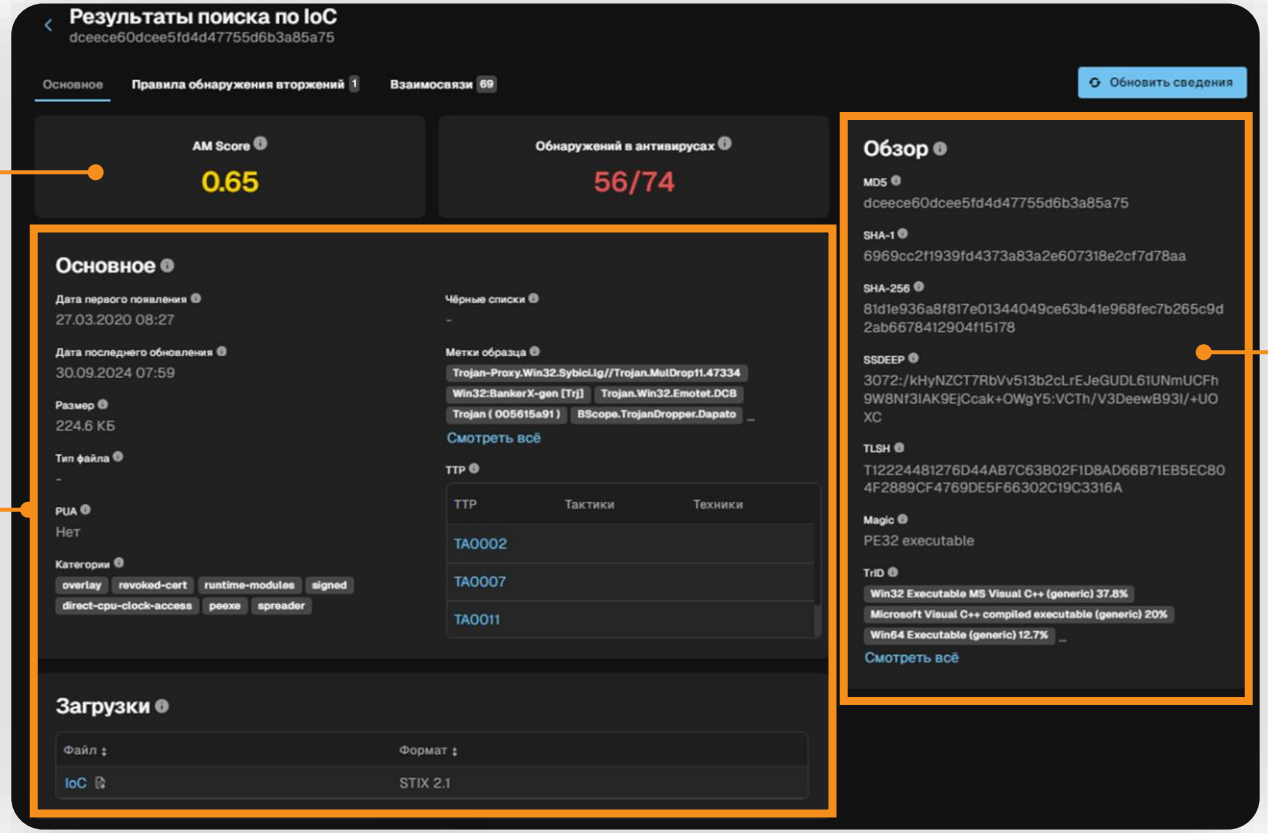
Функциональность TI LOOKUP

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



IoC

Дополниетльные атрибуты индикатора компрометации

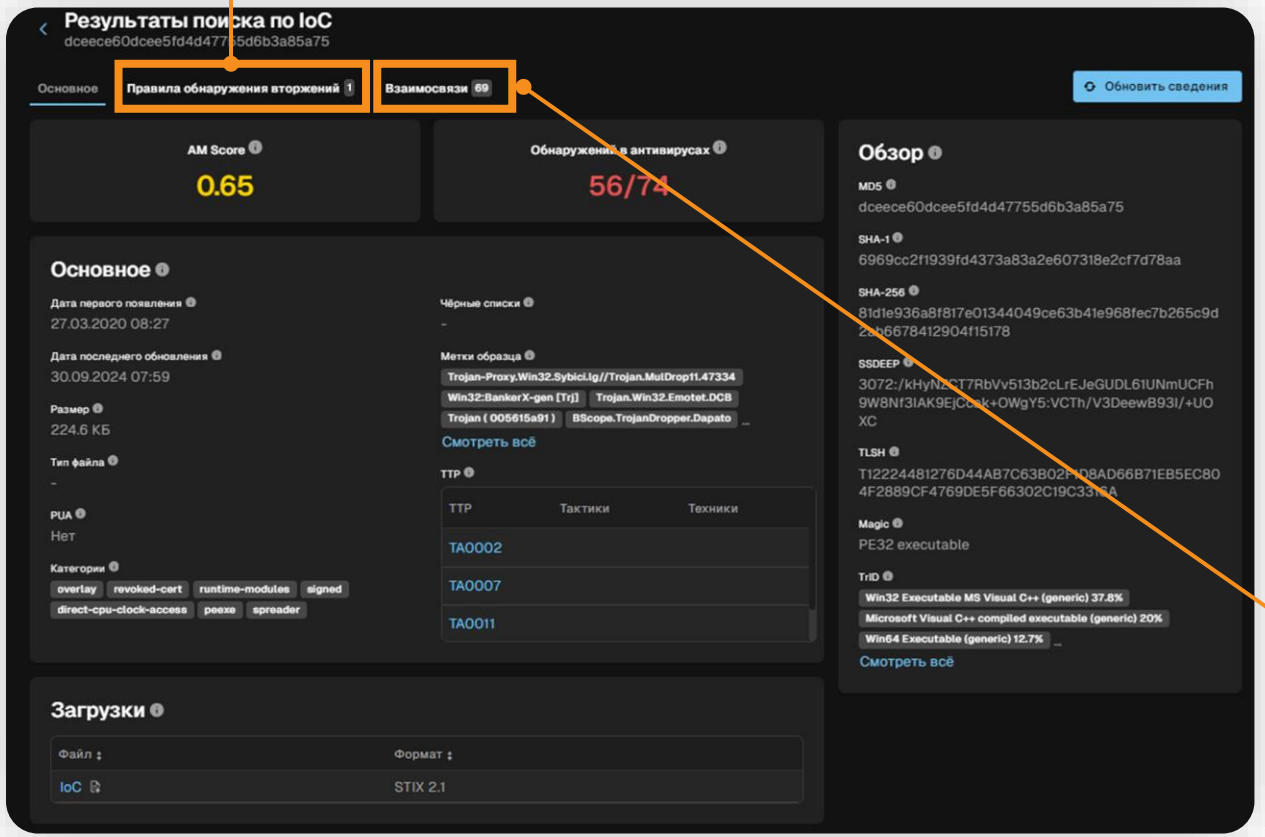
Типы исследуемых объектов:

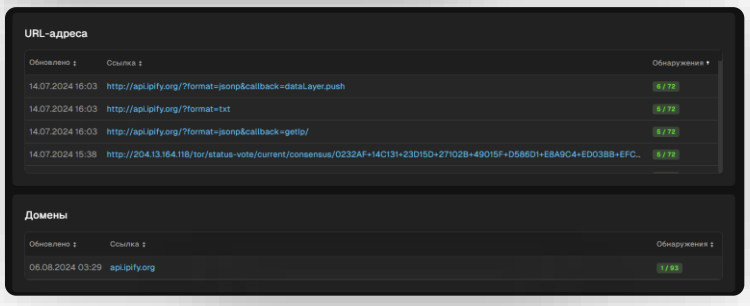
Hash, IP, CVE, Domain, URL

Функциональность TI LOOKUP

БРП AM Rules

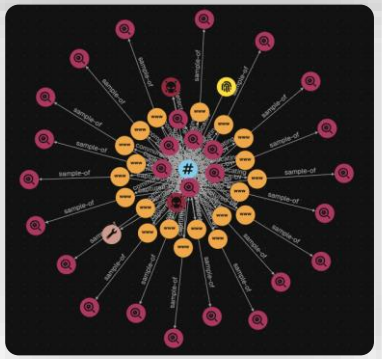
Описание сигнатур по исследуемому объекту с возможностью просмотра и выгрузки правила в форматах Snort, Suricata, YARA, OSSEC





Взаимосвязи

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

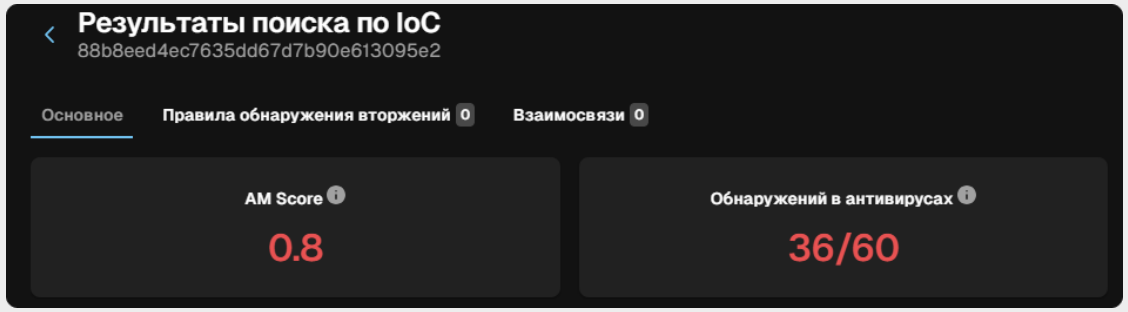


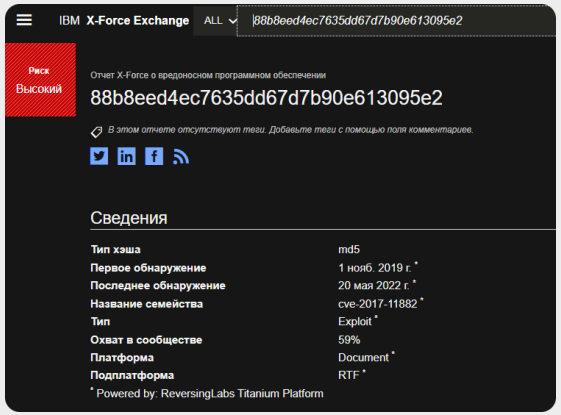
Экспертная оценка AM Score

– оценка вредоносности ресурса
по собственной методологии ПМ

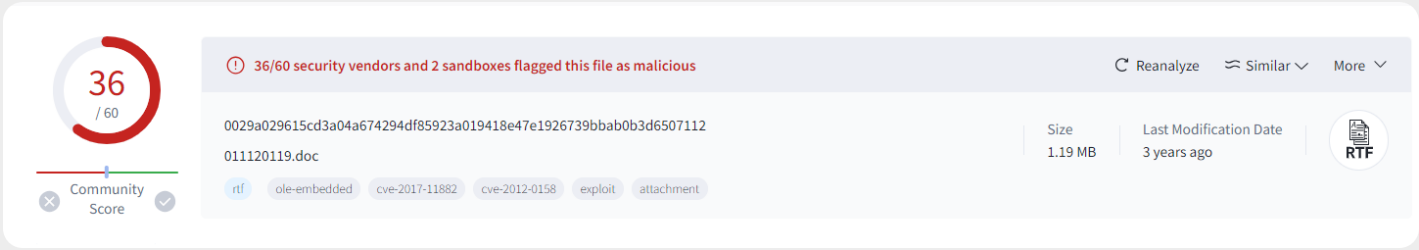
≥0,7	— вредоносный;
≥0,3 <0,7	— недоверенный;
<0,3	— не квалифицирован как вредоносный

88b8eed4ec7635dd67d7b90e613095e2





/AMTIP



VIRUSTOTAL

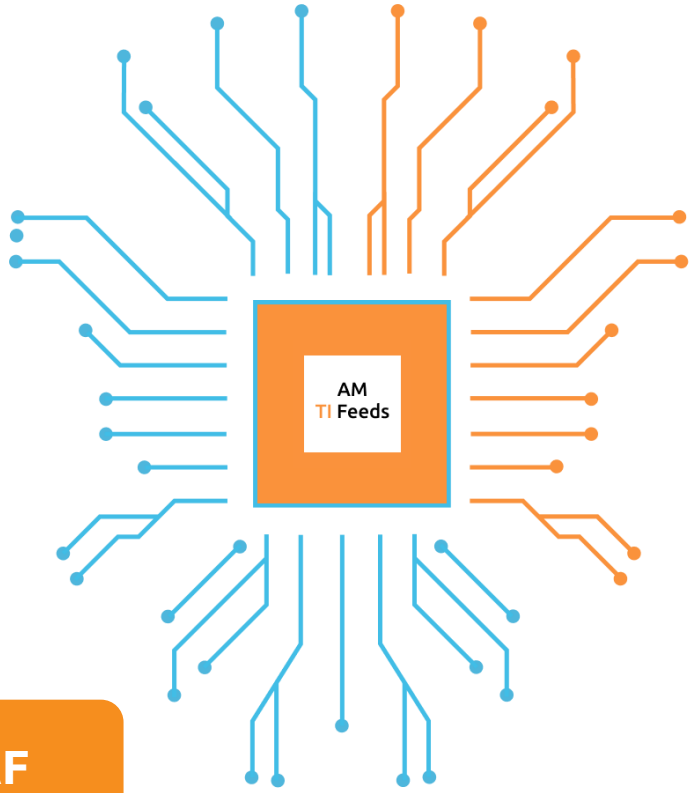
IBM

RST CLOUD

Применимость AM TI Feeds

SIEM

Обнаружение вредоносной активности на ранних этапах



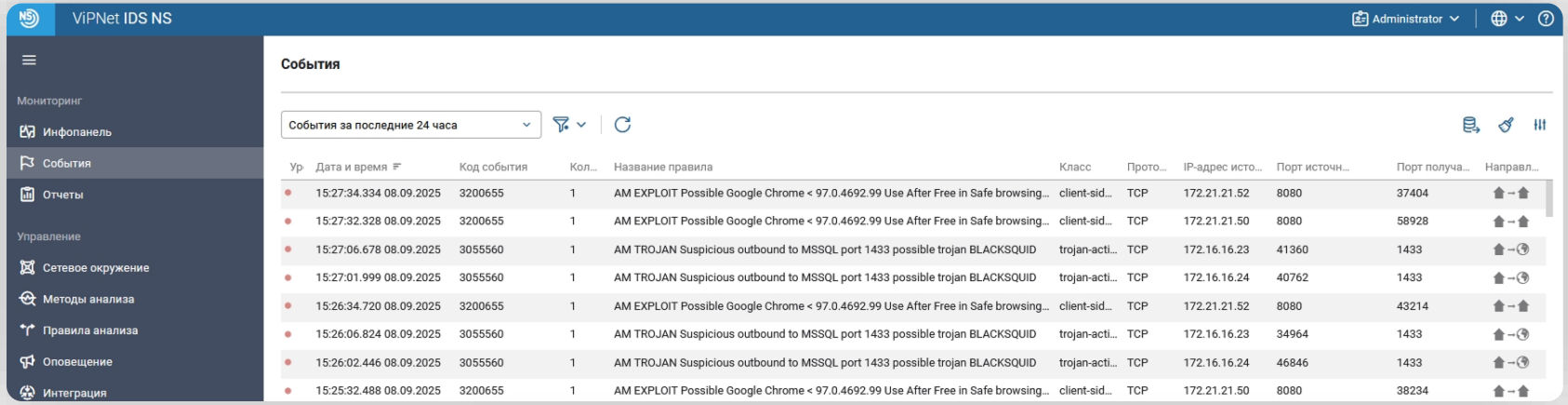
TI-platform

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

IDS/IPS/NGFW/NTA/WAF

Повышение эффективности в работе средств защиты информации

События в линейке продуктов ViPNet

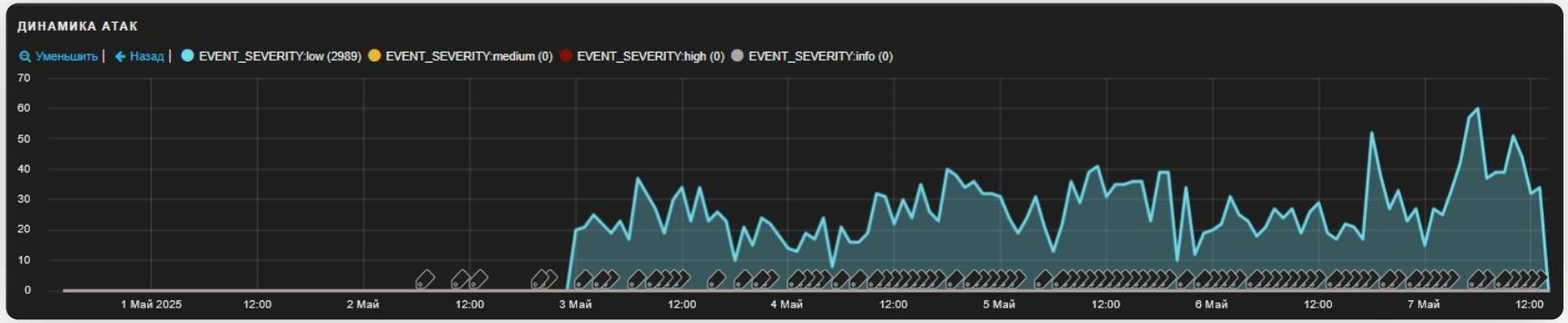


Примеры сработок баз решающих правил AM Rules в ViPNet IDS NS

Примеры сработок баз решающих правил AM Rules в ViPNet TIAS

Подтверждённый эффект

AM TI Feeds были внедрены в WAF клиента 3 мая 2025

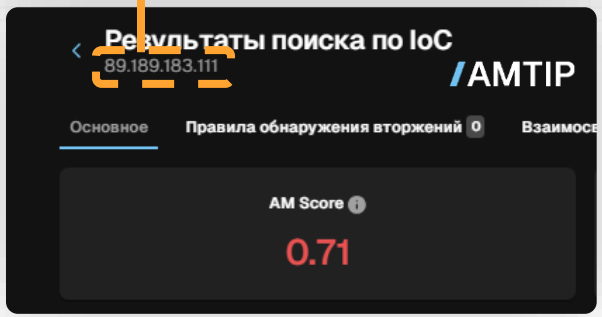


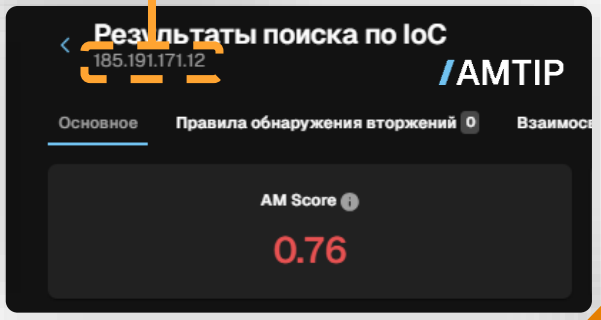
АТАКИ

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 13:5 :28
low	Blacklisted by IP Address	TOR IP Address Blocke...		CLIENT_IP	95.78.246.146	2025-05-07 13:5 :04
low	Blacklisted by IP Address	TOR IP Address Blocke...		CLIENT_IP	185.191.171.16	2025-05-07 13:5 :54
low	Blacklisted by IP Address	TOR IP Address Blocke...		CLIENT_IP	89.189.183.111	2025-05-07 13:5 :30

Благодаря чему удается блокировать ряд атак на сайты клиентов

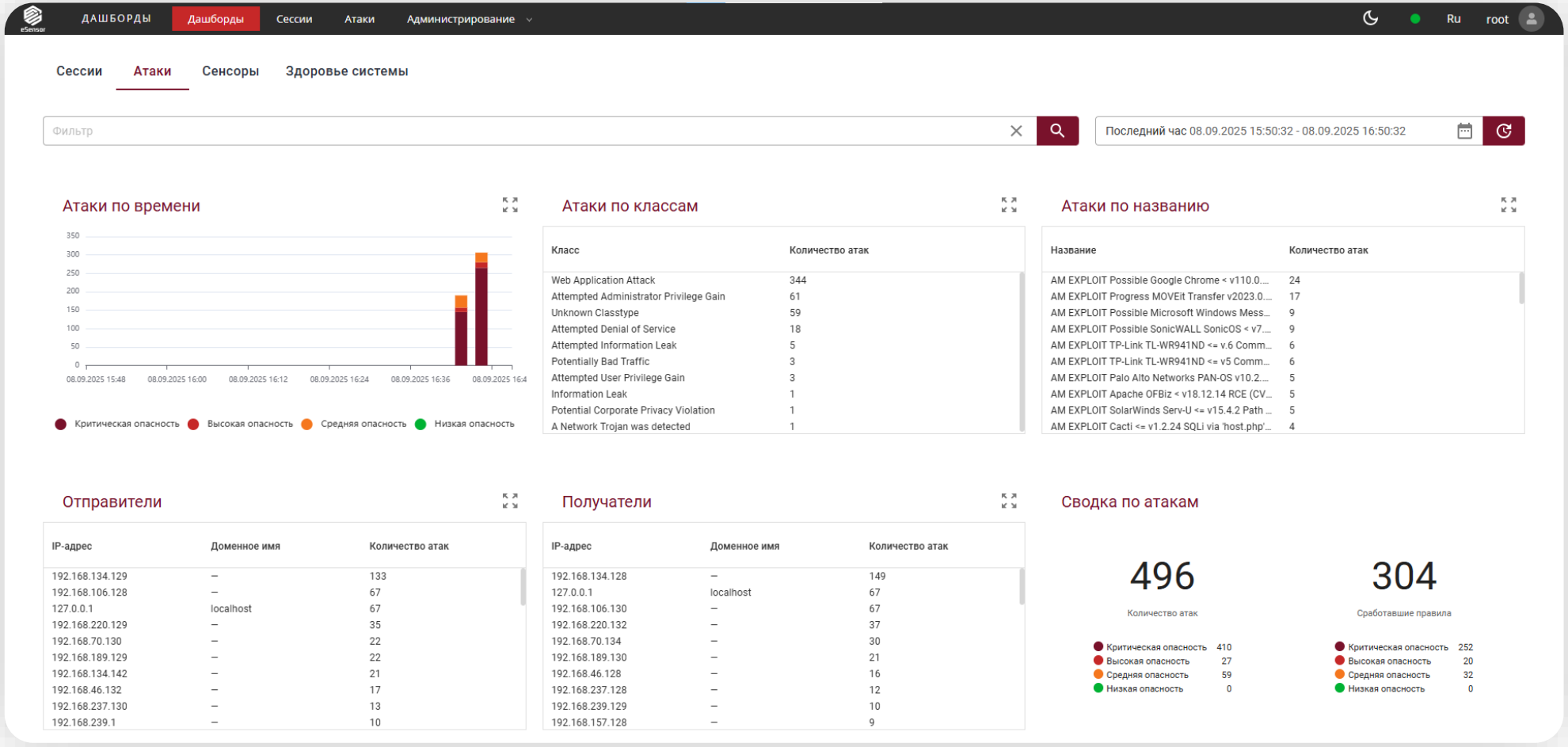




Ежедневно в WAF поставляется обновляемый список из 200 000 вредоносных IP-адресов

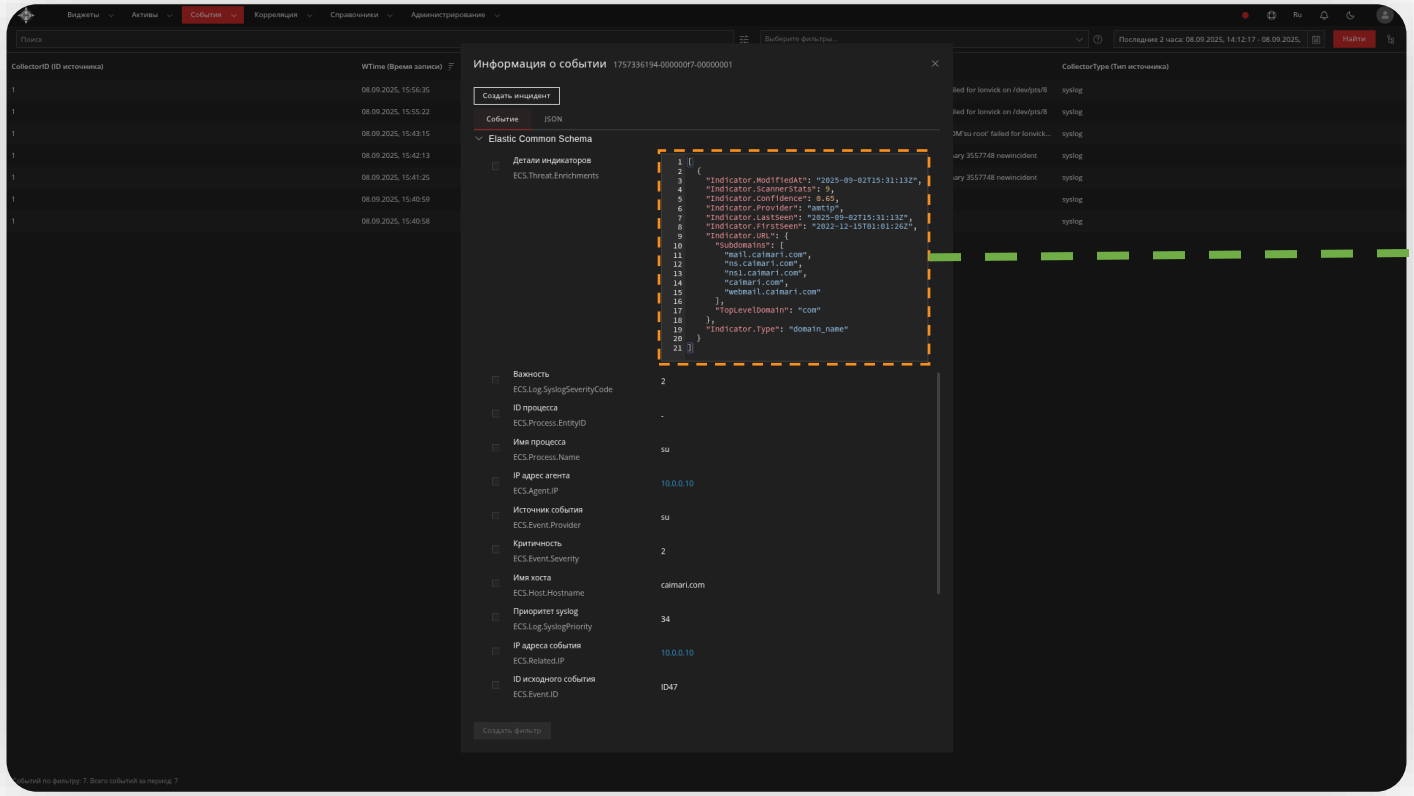
За все время работы было выявлено только 3 ложных блокировки

События в линейке продуктов ГК Эшелон

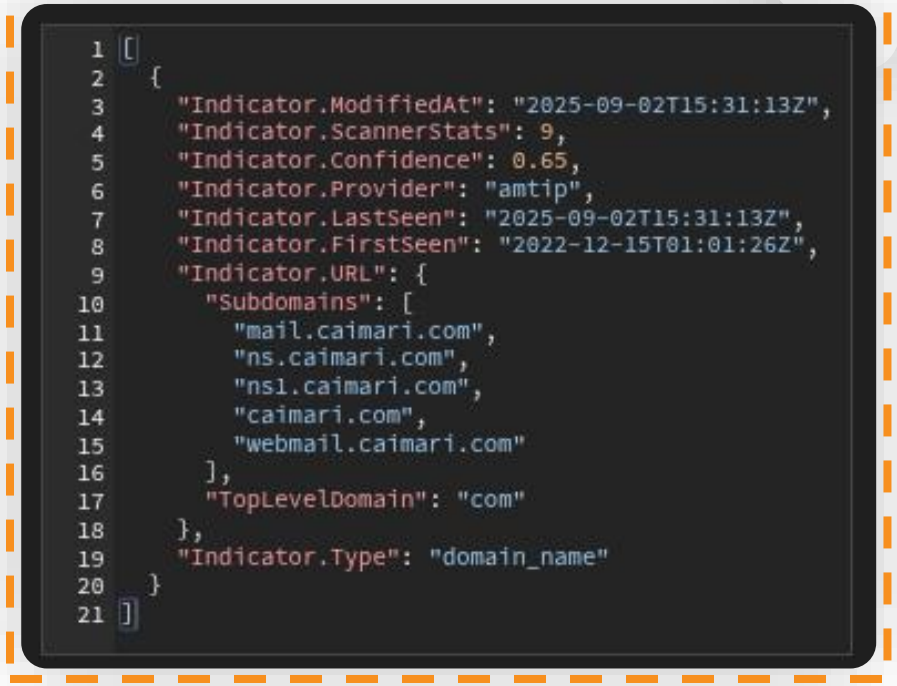


Примеры сработок баз решающих правил AM Rules в NTA eSensor

События в линейке продуктов ГК Эшелон



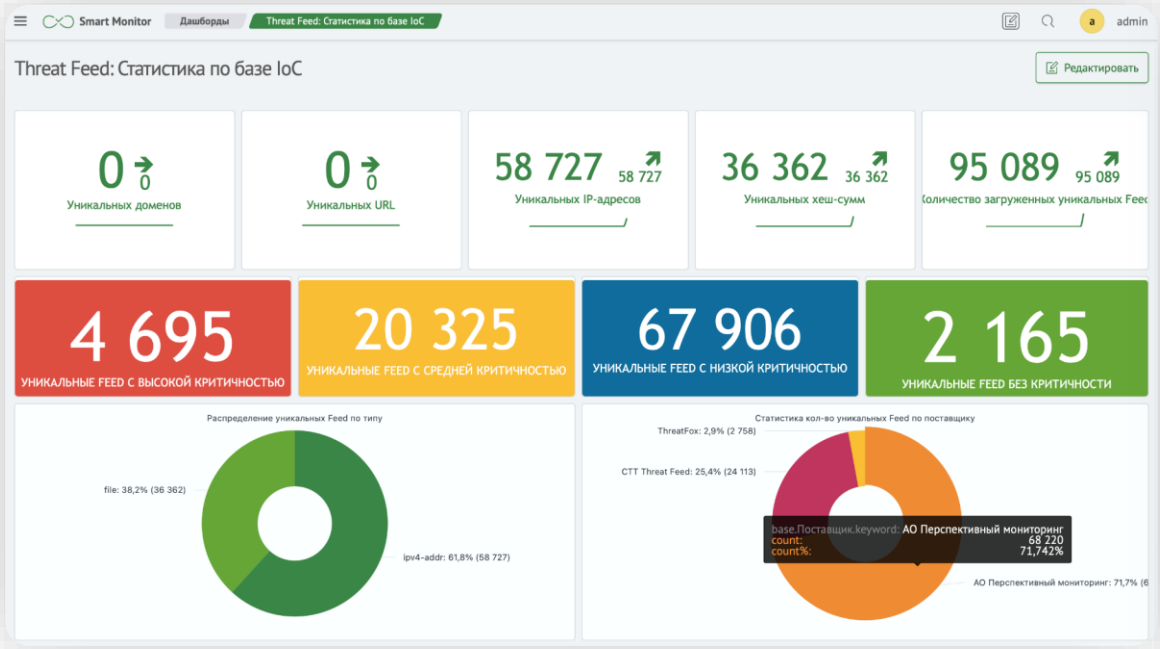
Примеры обогащённой информации в SIEM KOMRAD с помощью AM TI Feeds



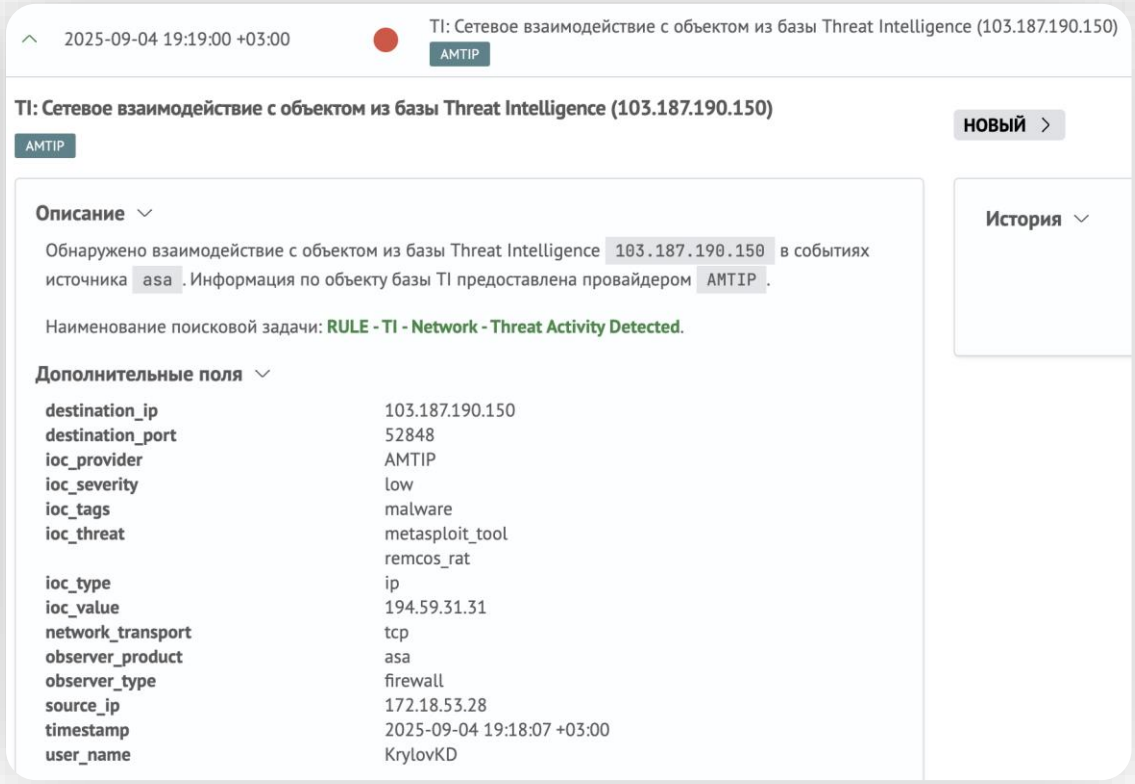
```
[
  {
    "Indicator.ModifiedAt": "2025-09-02T15:31:13Z",
    "Indicator.ScannerStats": 9,
    "Indicator.Confidence": 0.65,
    "Indicator.Provider": "amtip",
    "Indicator.LastSeen": "2025-09-02T15:31:13Z",
    "Indicator.FirstSeen": "2022-12-15T01:01:26Z",
    "Indicator.URL": {
      "Subdomains": [
        "mail.caimari.com",
        "ns.caimari.com",
        "ns1.caimari.com",
        "caimari.com",
        "webmail.caimari.com"
      ],
      "TopLevelDomain": "com"
    },
    "Indicator.Type": "domain_name"
  }
]
```

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

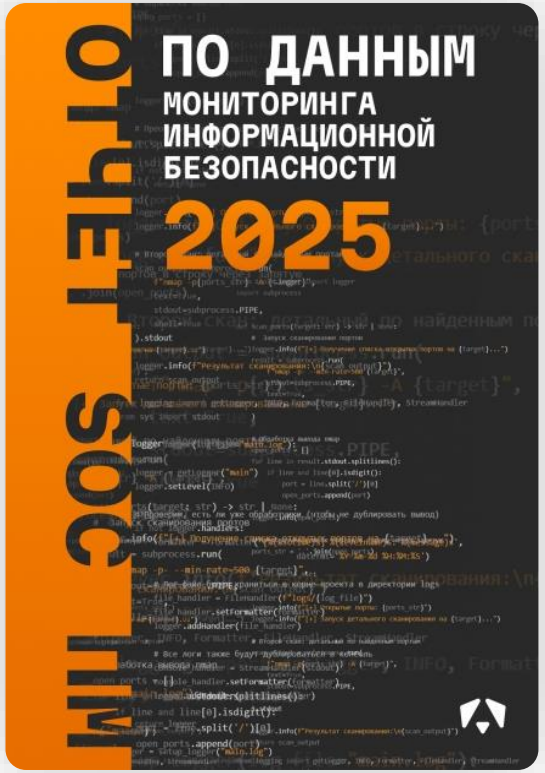


Благодаря AM TI Feeds можно обогащать события, которые поступают в SIEM,а также писать правила корреляции для формирования инцидентов при нахождении вредоносного объекта

Публичные результаты

MeshAgent

Отчёт SOC ПМ



Ландшафт киберугроз

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо за внимание!

Артём Савчук

Технический директор,
«Перспективный мониторинг»

amonitoring.ru

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

инфотекс Академия | Учебный центр инфотекс | AMPIRE | TELEOFIS | КОМФОРТЕЛ оператор связи бизнес-класса | РУТОКЕН компания ТРАКТИВ | TS Solution | AXOFT

Подписывайтесь на наши соцсети