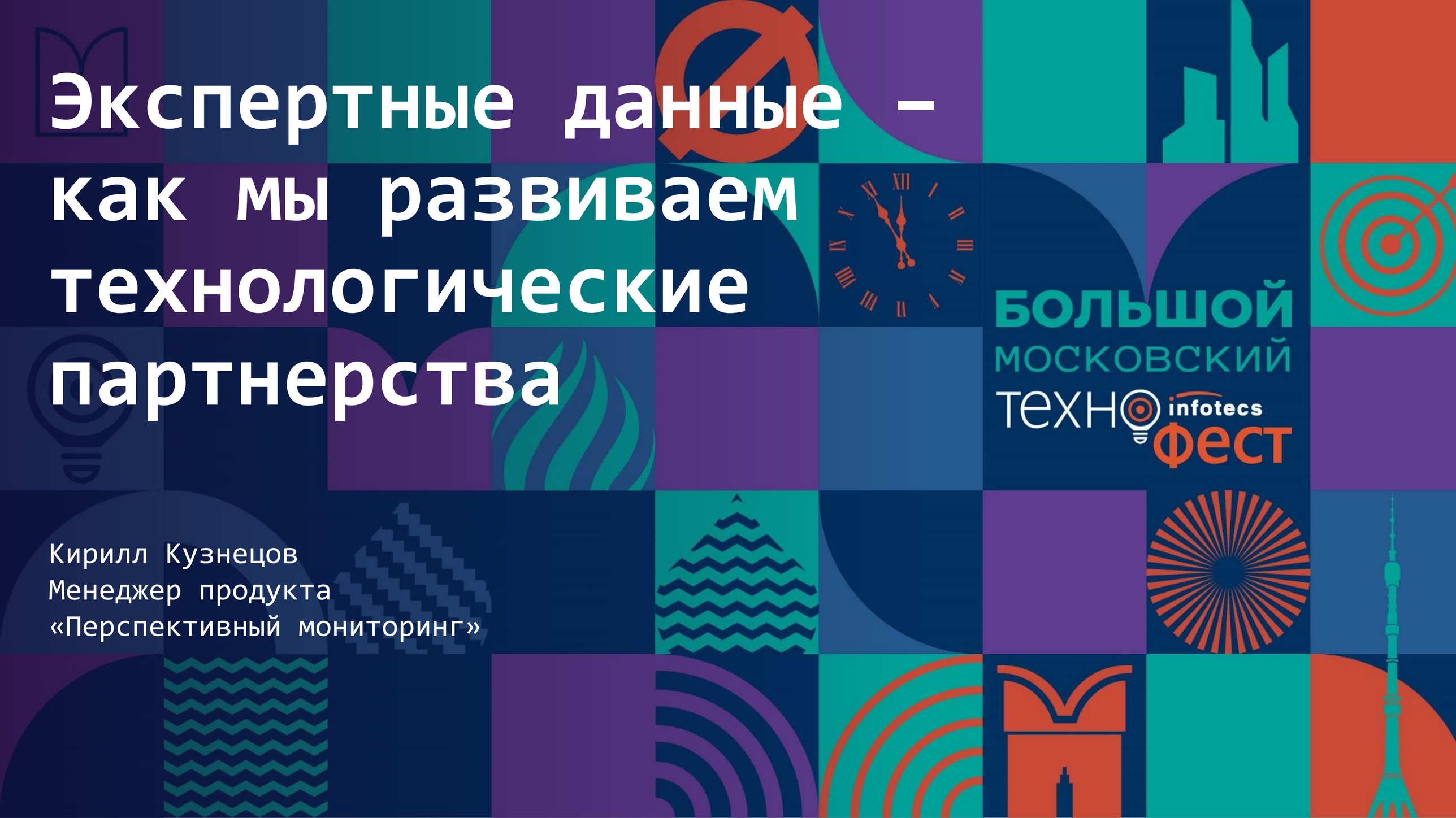
Экспертные данные – как мы развиваем технологические партнерства



Кирилл Кузнецов
Менеджер продукта
«Перспективный мониторинг»

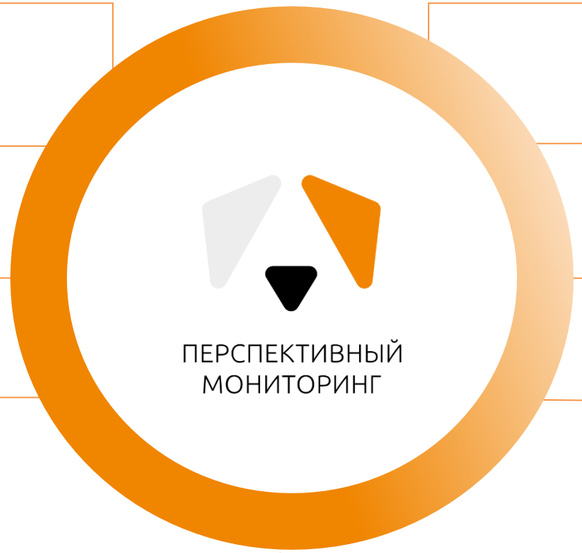
Направления деятельности ПМ

Исследование защищенности

- 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 Threat Intelligence Portal
- Киберполигон Ampire

Семейство продуктов
Экспертные данные

Экспертные данные

— **семейство продуктов**, разработанных «Перспективным мониторингом» для предоставления сведений о компьютерных угрозах, хакерских атаках и уязвимостях ПО. Позволяют службам информационной безопасности выстраивать более эффективную стратегию защиты организации

AM Threat Intelligence Portal

БРП AM Rules **AM TI feeds** **AM URL фильтрация**

Что это за данные

AM TI feeds

индикаторы компрометации IoC (вредоносные IP-адреса, домены, хеши, URL’ы) с комплексными сведениями о них

- Только валидированные IoC’и
- Собственная экспертиза благодаря SOC и исследователям
- Получение сведений от гос. регуляторов

БРП AM Rules

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

- Экспертиза с 2016 года
- Ежедневное обновление и актуализация базы
- 35 000 образцов вредоносного кода на ежедневном анализе

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%

Применимость данных в СЗИ

Класс СЗИ	Тип СЗИ	AM TI Feeds	БРП AM Rules	База URL
Аналитические	IRP, SOAR, SIEM, TI Platform	+	—	—
Сетевые	NGFW, IDS/IPS, WAF	+	+	+
Хостовые	EDR, EPP	+	+	—

Наши текущие партнеры

VolgaBlob

- Smart Monitor

R-Vision

- R-TIP

Эшелон
комплексная безопасность

- eSensor NTA
- SEIM
- NGFW

infotecs

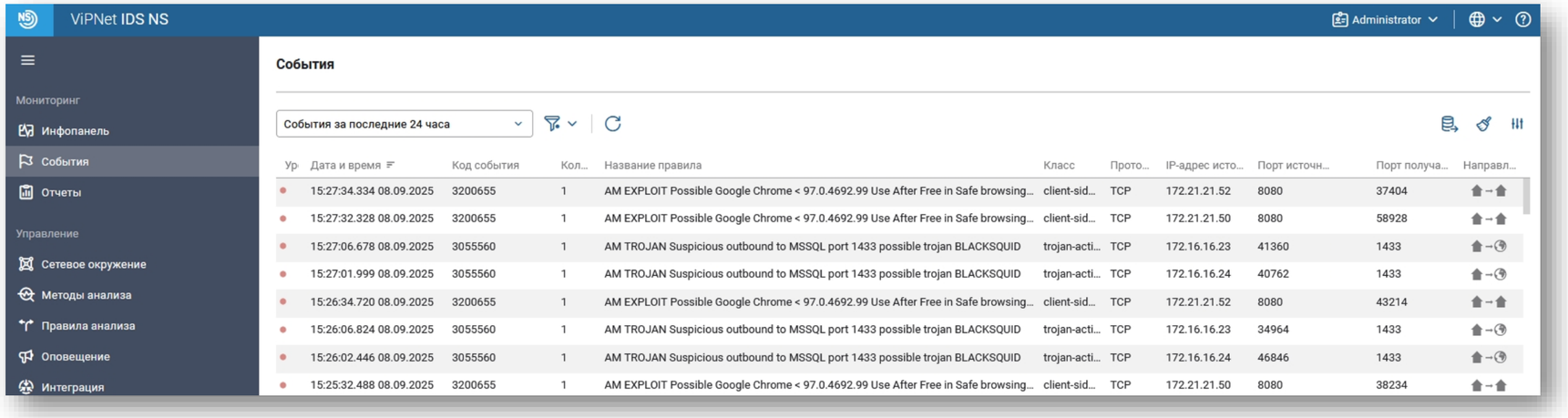
- ViPNet Coordinator HW 4/5
- ViPNet IDS HS
- ViPNet IDS NS
- ViPNet EPP
- ViPNet TIAS
- ViPNet xFirewall 4/5

Здесь могли бы быть Вы

Наши текущие партнеры

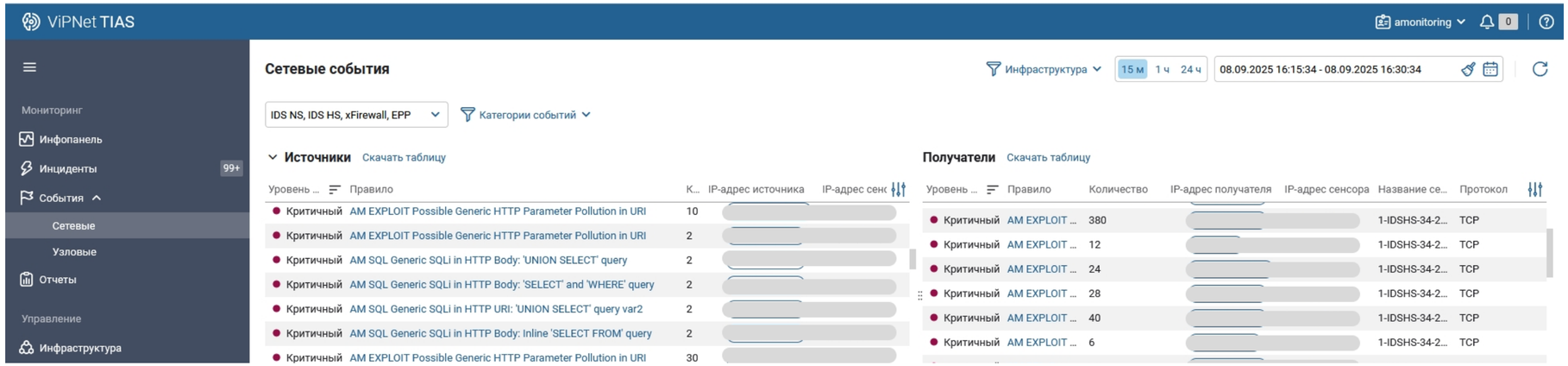
И здесь тоже Вы могли бы быть ☺

События в линейке продуктов ViPNet

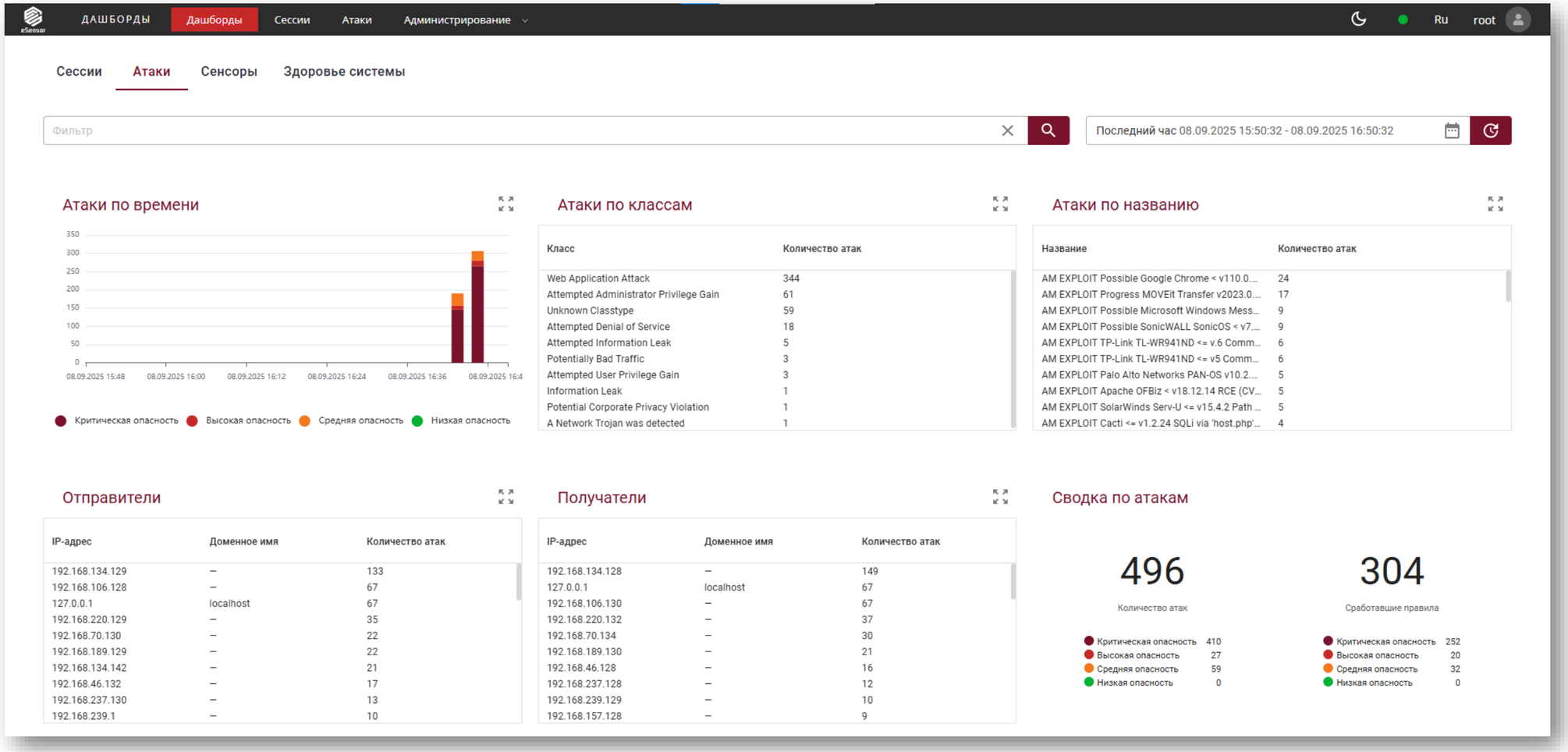


Примеры сработок баз решающих правил AM Rules в ViPNet IDS NS

Примеры сработок баз решающих правил AM Rules в ViPNet TIAS

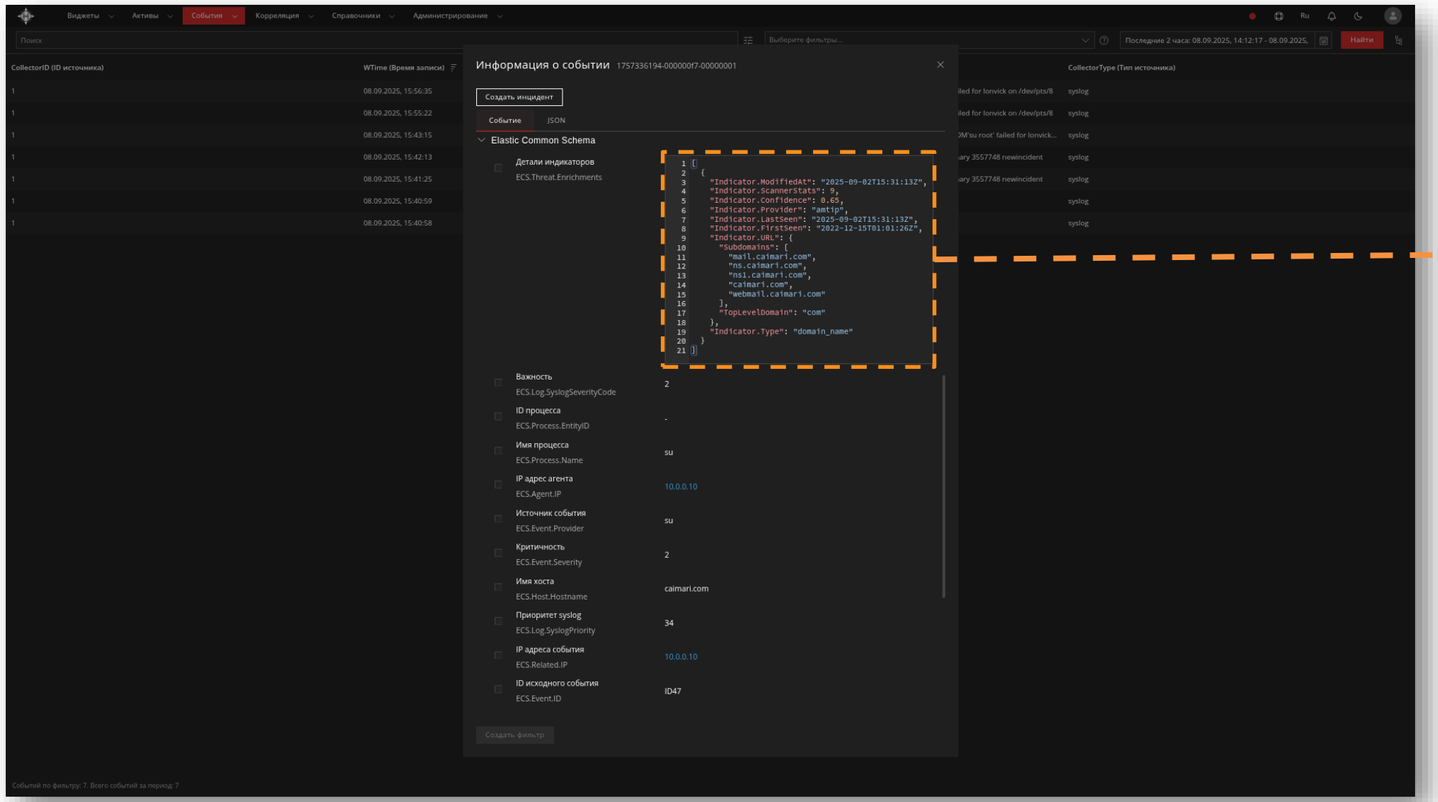


События в линейке продуктов ГК Эшелон



Примеры сработок баз решающих правил AM Rules в NTA eSensor

События в линейке продуктов ГК Эшелон

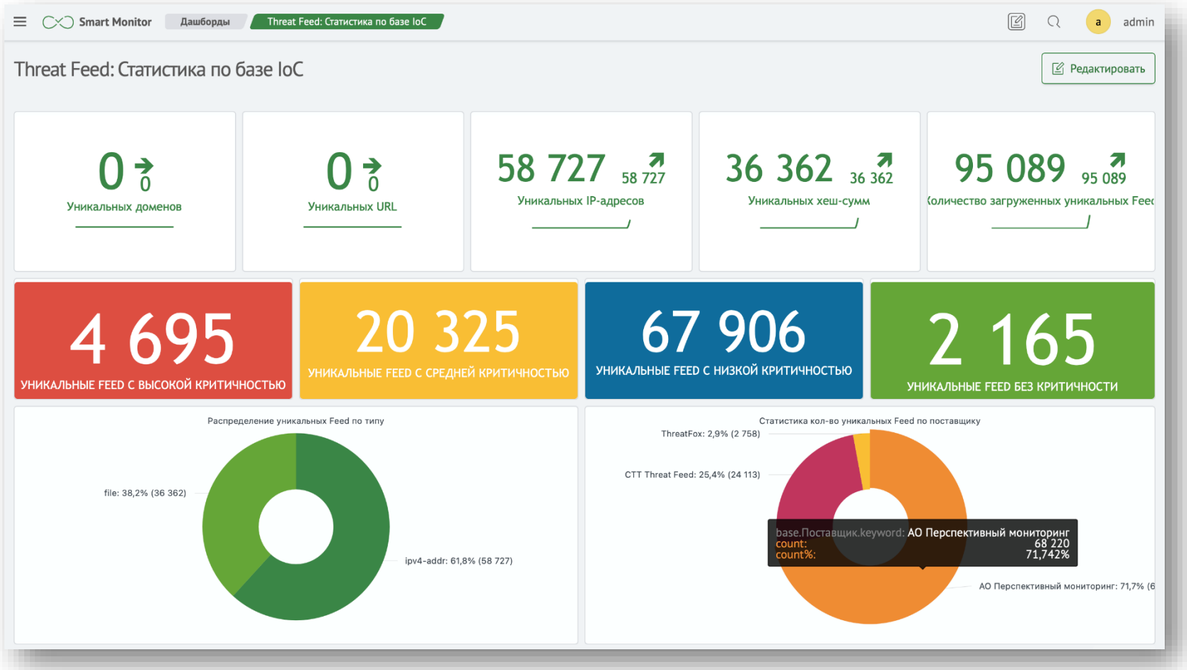


Примеры обогащённой информации в SIEM KOMRAD с помощью AM TI Feeds

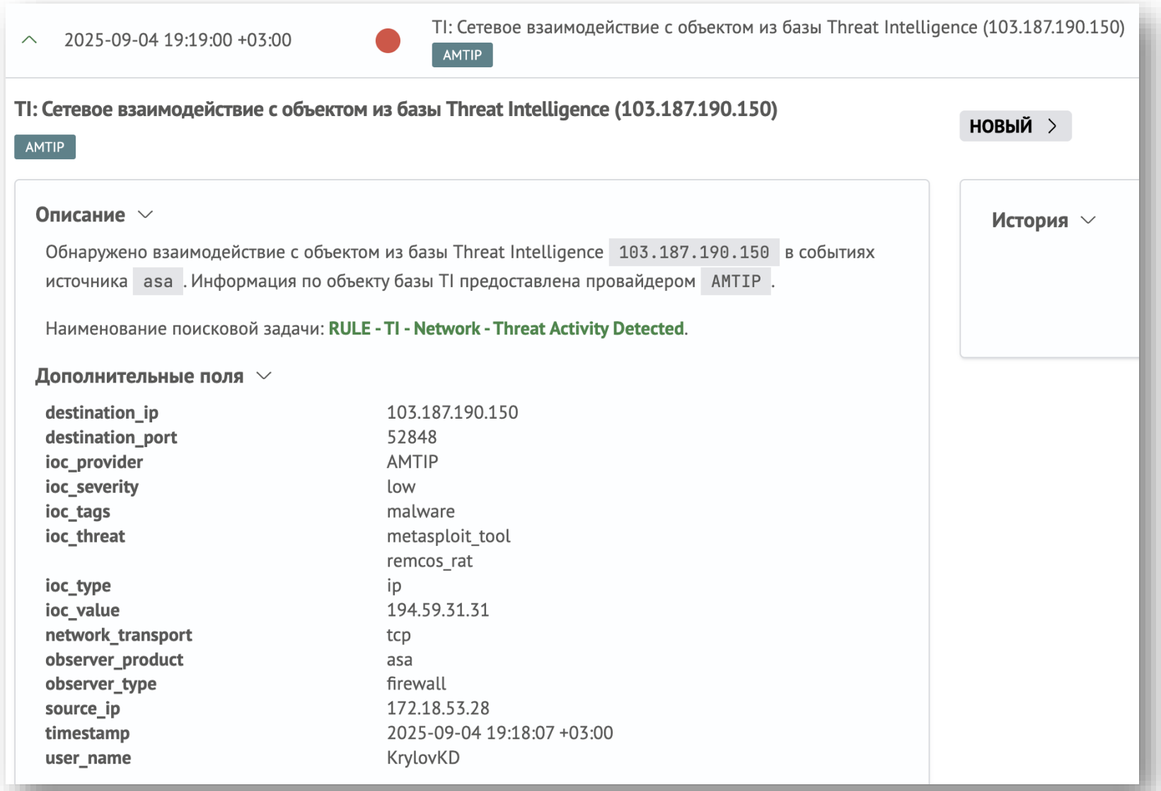
```
[
  {
    "Indicator.ModifiedAt": "2025-09-02T15:31:13Z",
    "Indicator.ScannerStats": 9,
    "Indicator.Confidence": 0.65,
    "Indicator.Provider": "amtip",
    "Indicator.LastSeen": "2025-09-02T15:31:13Z",
    "Indicator.FirstSeen": "2022-12-15T01:01:26Z",
    "Indicator.URL": {
      "Subdomains": [
        "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

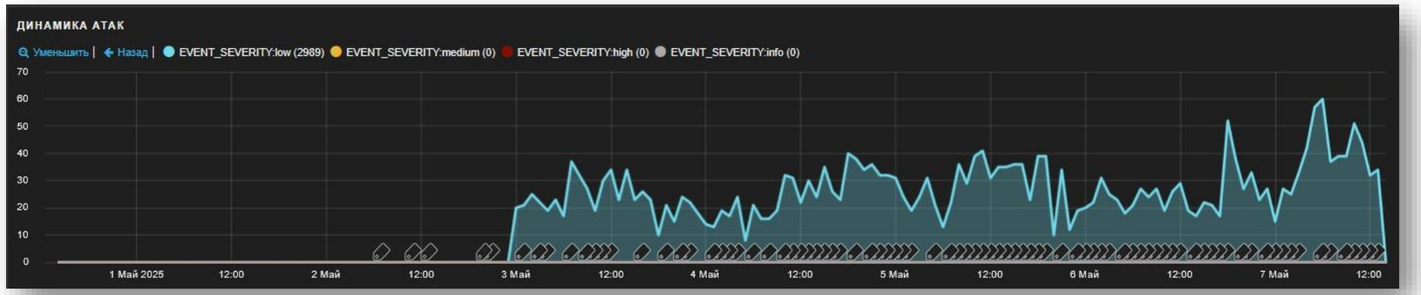


AM TI Feeds в SIEM Smart Monitor



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

Блокировка вредоносного траффика на WAF



AM TI Feeds были интегрированы в WAF клиента 3 мая 2025 года, после чего WAF начал блокировать вредоносный траффик

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

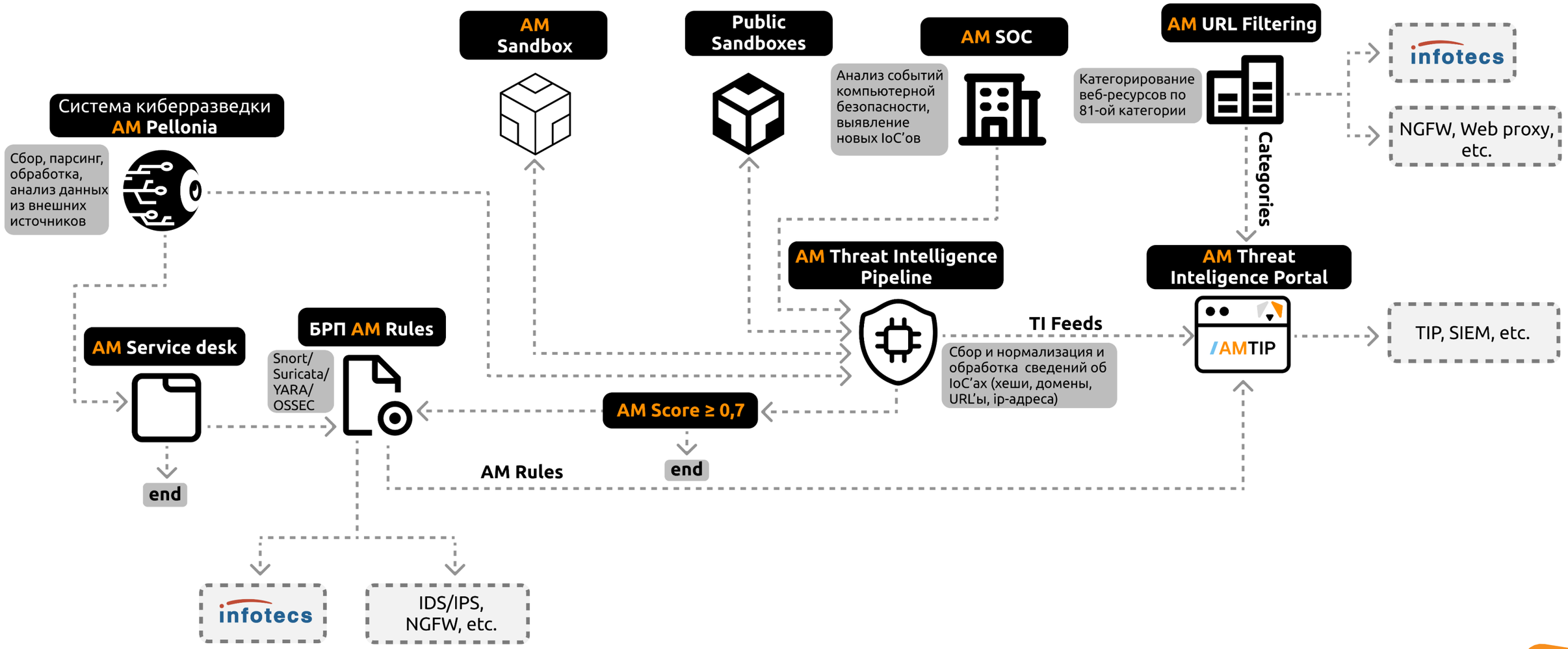
За все время работы было выявлено только 3 ложных блокировки

EVENT_SEVERITY	EVENT_TAG.NAME	EVENT_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 13:55:28
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP		2025-05-07 13:55:04
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP	185.191.171.16	2025-05-07 13:54:54
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP		2025-05-07 13:54:30
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP		2025-05-07 13:54:28
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP		2025-05-07 13:54:05
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP	185.191.171.16	2025-05-07 13:54:00
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP	185.191.171.13	2025-05-07 13:53:02
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP	185.191.171.9	2025-05-07 13:50:30
low	Blacklisted by IP Address	TOR IP Address Blocke...	CLIENT_IP	156.59.198.136	2025-05-07 13:47:47

Какой профит?

1. Дополнительный доход
2. Усиление эффективности СЗИ за счет ЭД
3. Усиление бренда

Как мы собираем и производим ЭД



Как поставляем данные

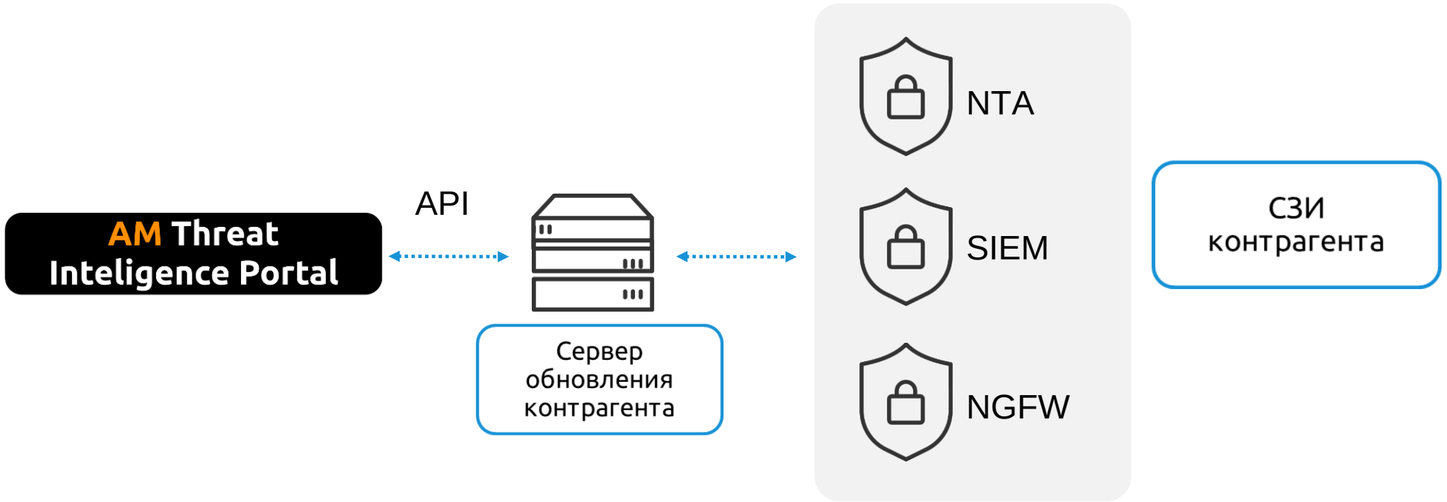
Поставка ПО осуществляется через
AM Threat Intelligence Portal по интеграции
С возможностью ежедневного обновления данных

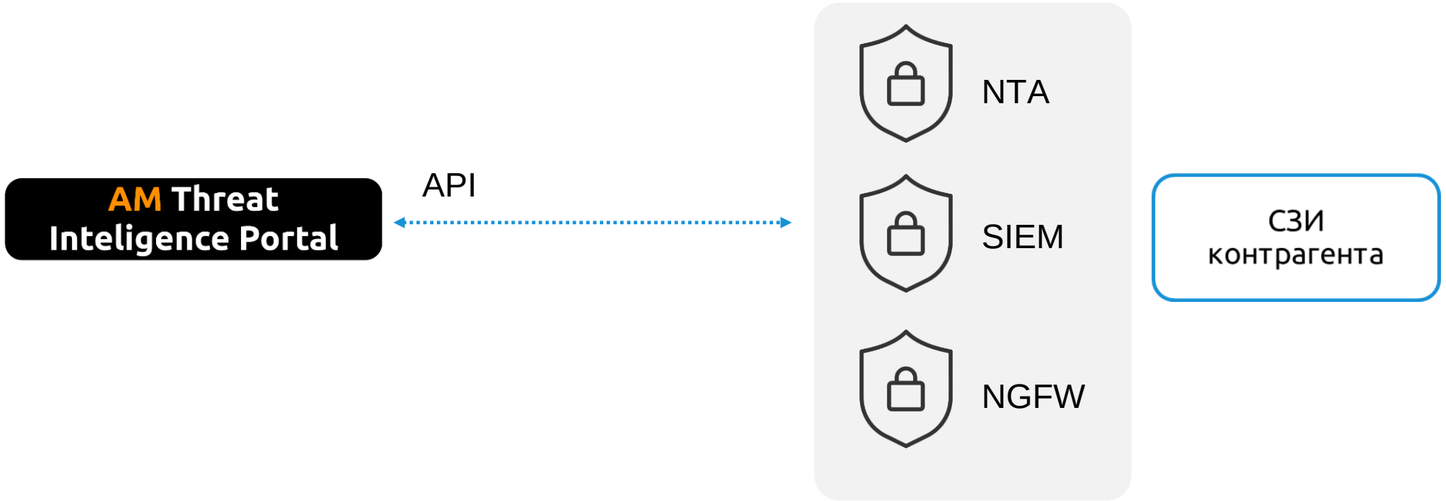
– веб-сервис, предоставляющий сведения о киберугрозах, на основе многолетней экспертизы ПМ

amtip.ru

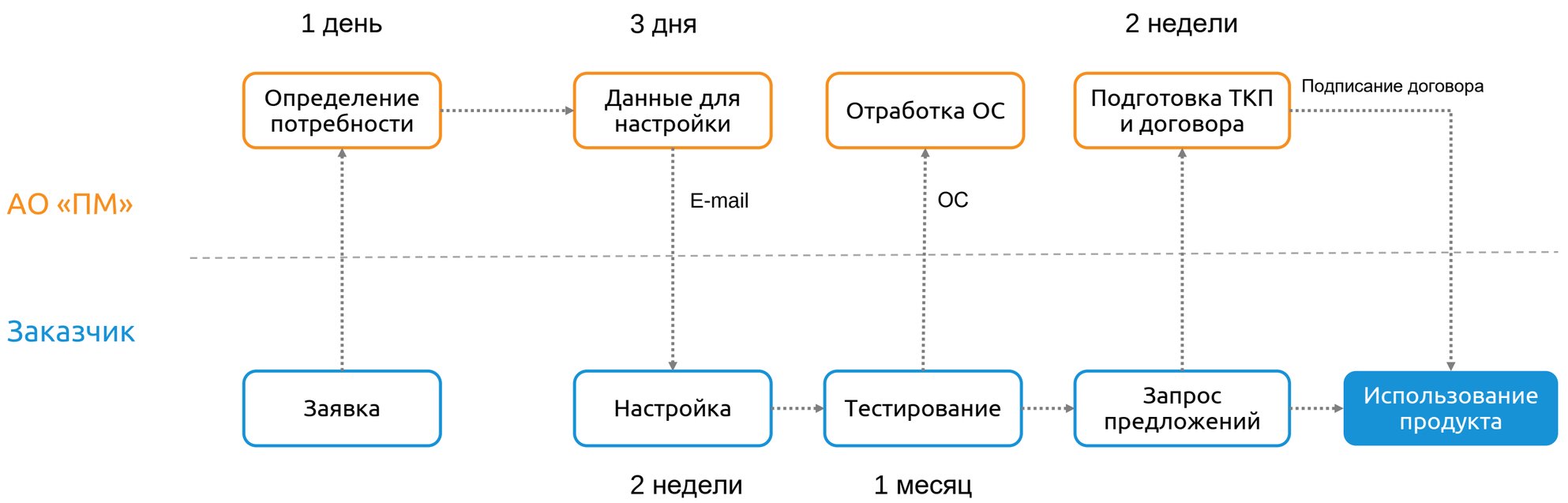
Включен в реестр отечественного ПО,
реестровая запись №22808 от 06.06.2024

Как поставляем данные



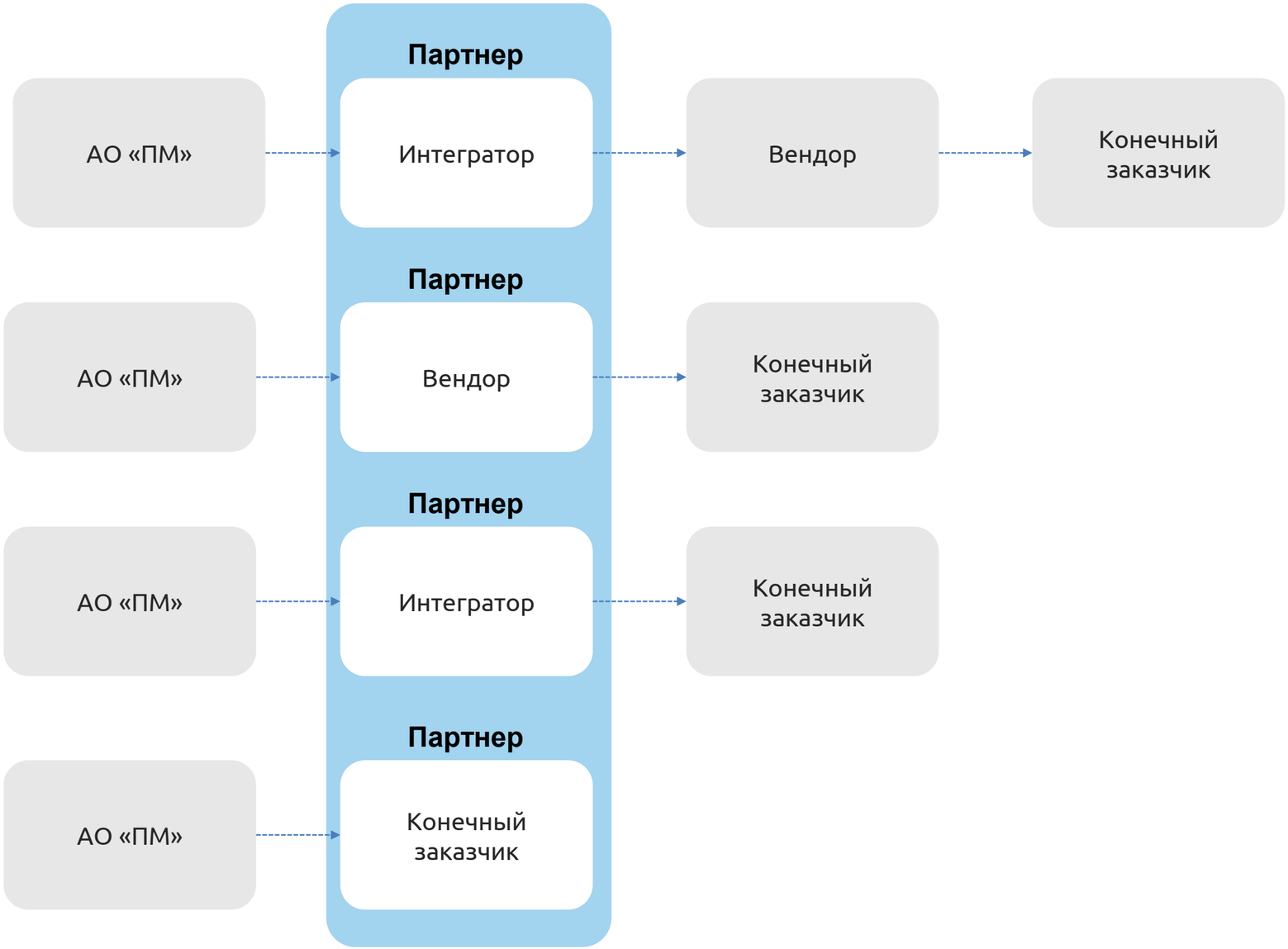


Как организован процесс



- 2 месяца от заявки до старта использования продукта

Мы открыты к сотрудничеству



Почему мы

01

Мы гибкие

Подстроимся под любые потребности и архитектурные сложности

02

Профессионализм

Имеем подтвержденный опыт в интеграции в ПАК конечного заказчика без участия вендора

03

Низкий порог входа

Низкая стоимость относительно аналогичных конкурентных решений

04

Экспертиза

Ведем экспертизу с 2016 года и поставляем только валидированные данные

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Кирилл Кузнецов

менеджер продукта,
«Перспективный мониторинг»

Kirill.Kuznetsov@amonitoring.ru

t.me/pm_public amonitoring.ru amtip.ru

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA
NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ
GLOBAL DIGITAL SPACE
CISOCLUB
РУТОКЕН КОМПАНИЯ АКТИВ
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ
АВАНГАРД
ARinteg
АТБ ЭЛЕКТРОНИКА
infotecs {/-cademy}
merlion
УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС