

Экспертные данные – как мы развиваем технологические партнерства

Кирилл Кузнецов
Менеджер продукта
«Перспективный мониторинг»

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  ФЕСТ

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

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

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

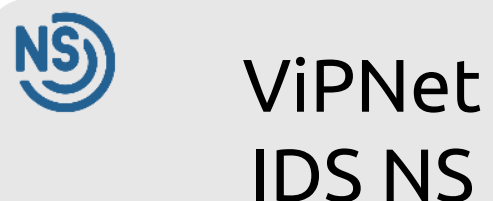
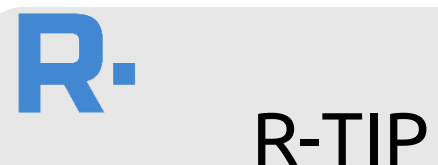
Ежемесячный прирост 15%

Применимость данных в СЗИ



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

Наши текущие партнеры



Здесь могли бы быть Вы

Наши текущие партнеры



И здесь тоже Вы могли бы быть 😊

События в линейке продуктов ViPNet



NS ViPNet IDS NS Administrator

Мониторинг

Инфо панель

События

Отчеты

Управление

Сетевое окружение

Методы анализа

Правила анализа

Оповещение

Интеграция

События

События за последние 24 часа

Ур	Дата и время	Код события	Кол...	Название правила	Класс	Прото...	IP-адрес исто...	Порт источн...	Порт получа...	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

NS ViPNet TIAS amonitoring

Мониторинг

Инфо панель

Инциденты

События

Сетевые

Узловые

Отчеты

Управление

Инфраструктура

Сетевые события

IDS NS, IDS HS, xFirewall, EPP

Категории событий

▼ Источники

Скачать таблицу

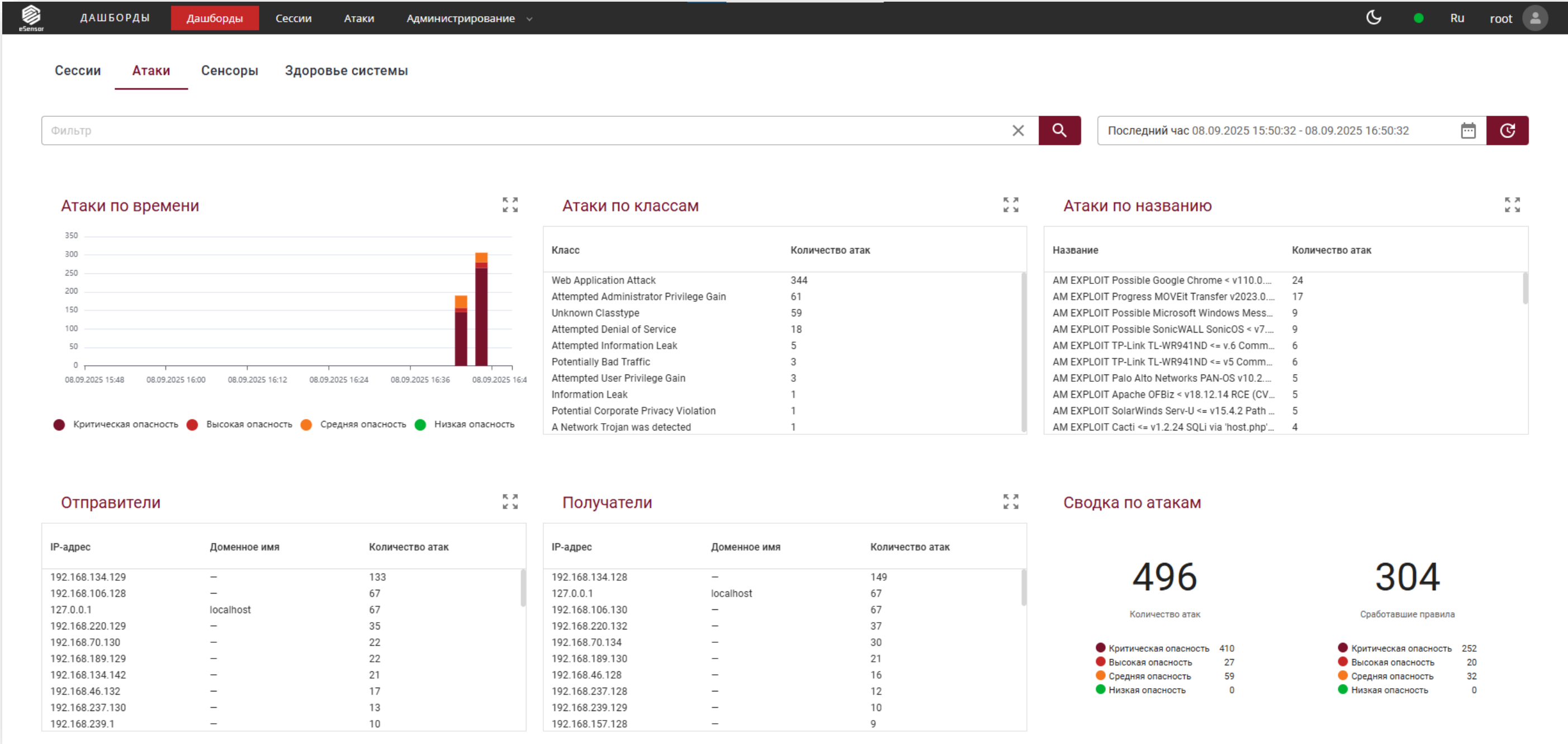
Уровень ...	Правило	К...	IP-адрес источника	IP-адрес сенс
● Критичный	AM EXPLOIT Possible Generic HTTP Parameter Pollution in URI	10		
● Критичный	AM EXPLOIT Possible Generic HTTP Parameter Pollution in URI	2		
● Критичный	AM SQL Generic SQLi in HTTP Body: 'UNION SELECT' query	2		
● Критичный	AM SQL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

Скачать таблицу

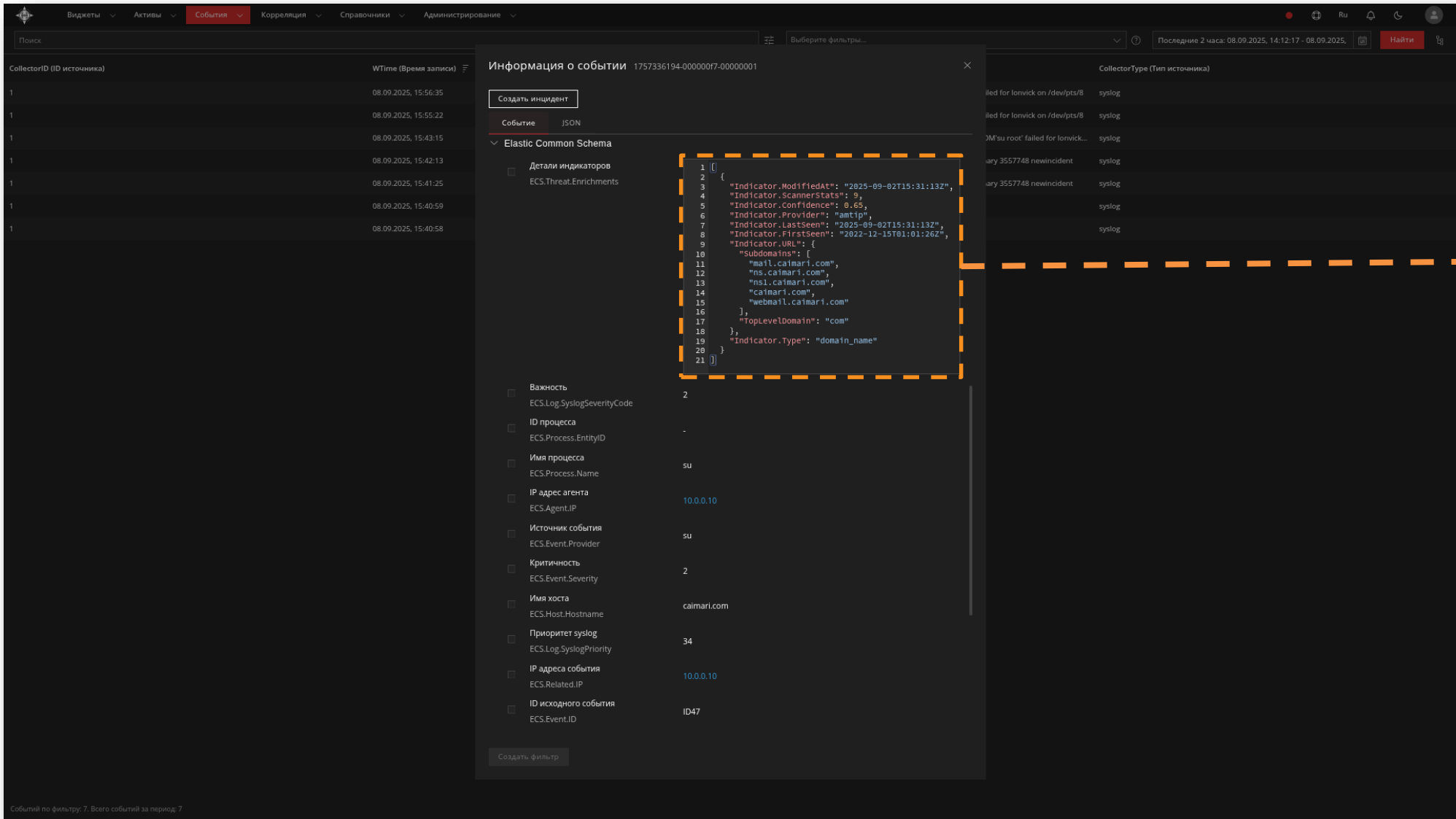
Уровень ...	Правило	Количество	IP-адрес получателя	IP-адрес сенсора	Название се...	Протокол
● Критичный	AM EXPLOIT ...	380			1-IDSHS-34-2...	TCP
● Критичный	AM EXPLOIT ...	12			1-IDSHS-34-2...	TCP
● Критичный	AM EXPLOIT ...	24			1-IDSHS-34-2...	TCP
● Критичный	AM EXPLOIT ...	28			1-IDSHS-34-2...	TCP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

События в линейке продуктов ГК Эшелон



Примеры сработок
баз решающих правил
AM Rules в NTA
eSensor

События в линейке продуктов ГК Эшелон

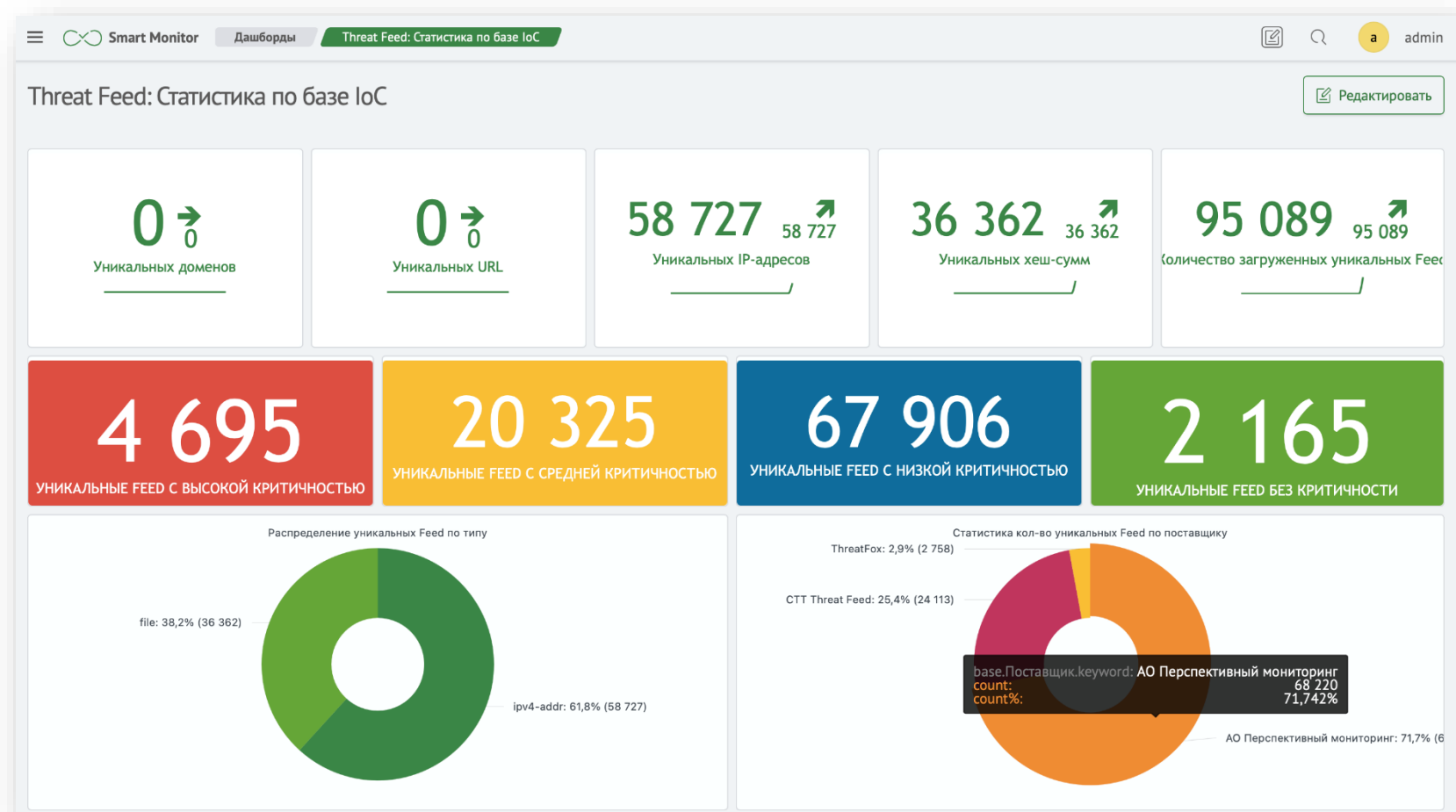


```
1 [
2   {
3     "Indicator.ModifiedAt": "2025-09-02T15:31:13Z",
4     "Indicator.ScannerStats": 9,
5     "Indicator.Confidence": 0.65,
6     "Indicator.Provider": "amtip",
7     "Indicator.LastSeen": "2025-09-02T15:31:13Z",
8     "Indicator.FirstSeen": "2022-12-15T01:01:26Z",
9     "Indicator.URL": {
10       "Subdomains": [
11         "mail.caimari.com",
12         "ns.caimari.com",
13         "ns1.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)

AMTIP

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

AMTIP

Описание

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

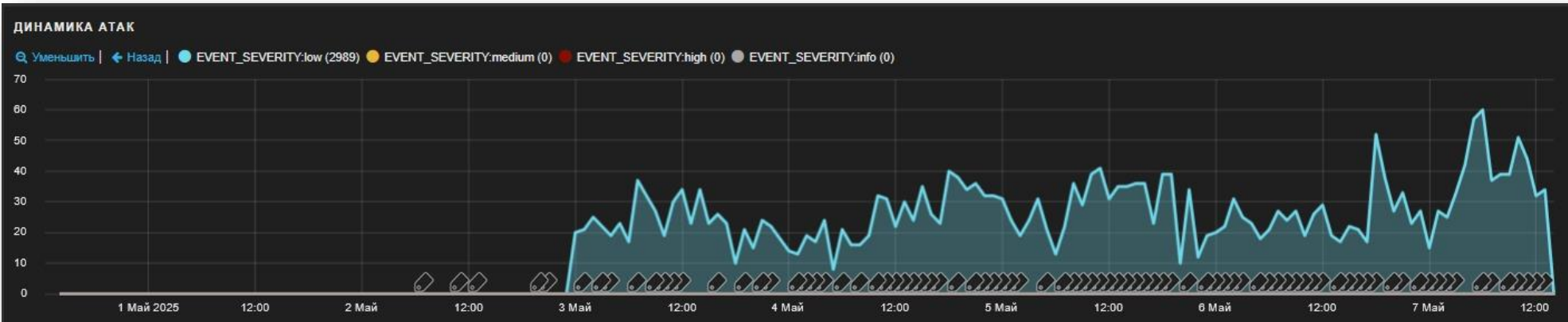
Наименование поисковой задачи: RULE - TI - Network - Threat Activity Detected.

Дополнительные поля

destination_ip	103.187.190.150
destination_port	52848
ioc_provider	AMTIP
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	KrylovKD

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 трафика на WAF



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

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

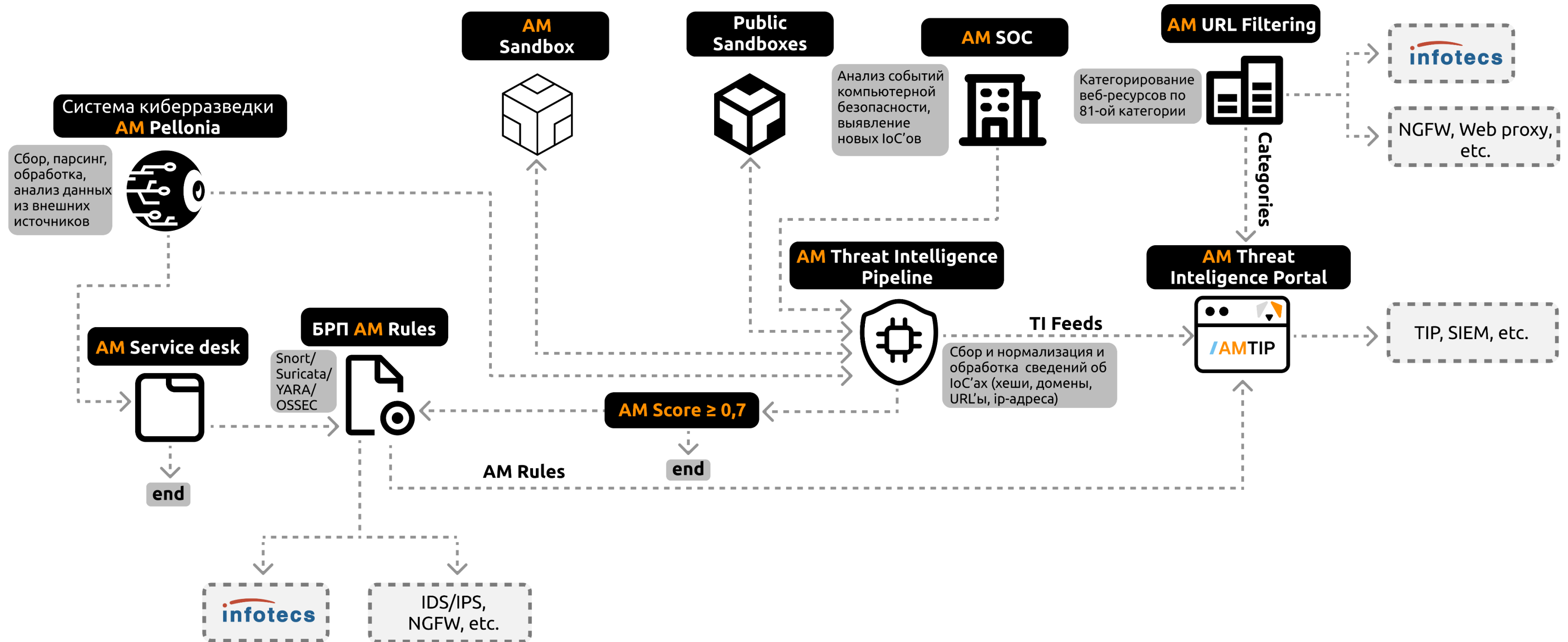
2

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

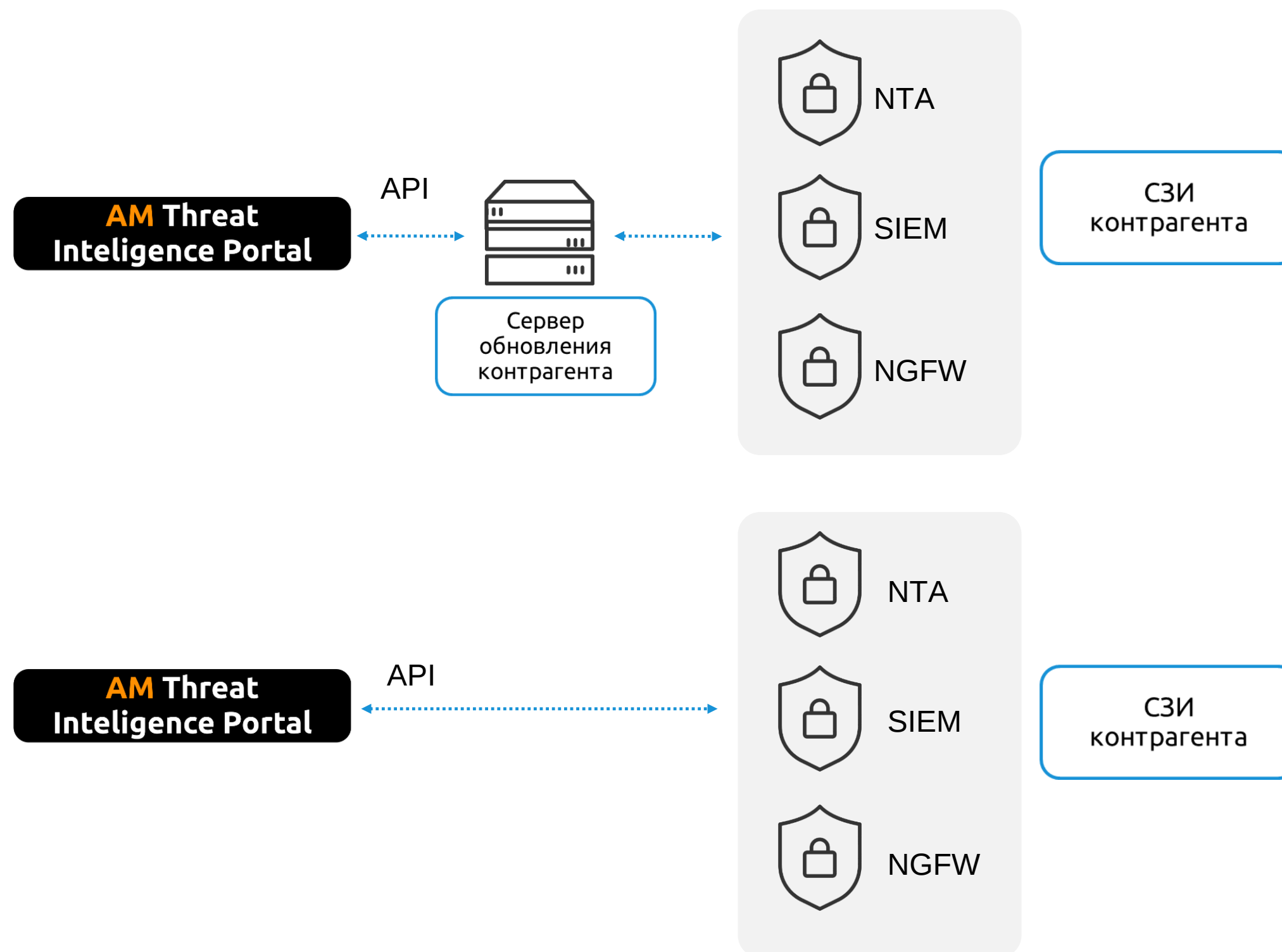


Включен в реестр отечественного ПО,
реестровая запись №22808 от 06.06.2024

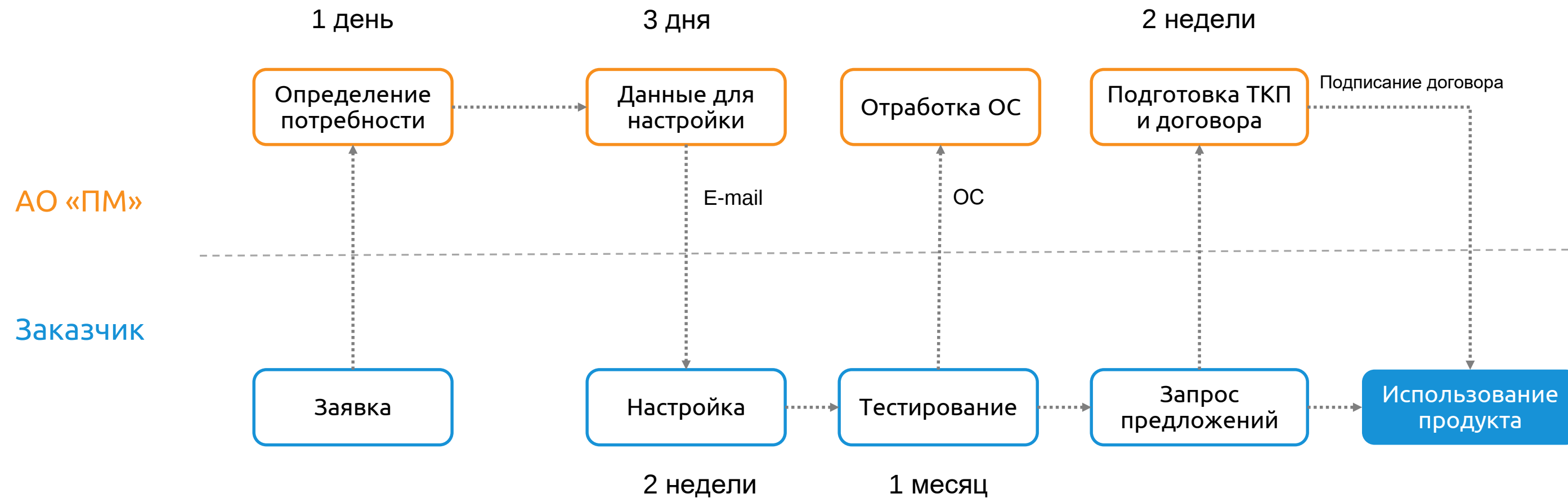


amtip.ru

Как поставляем данные

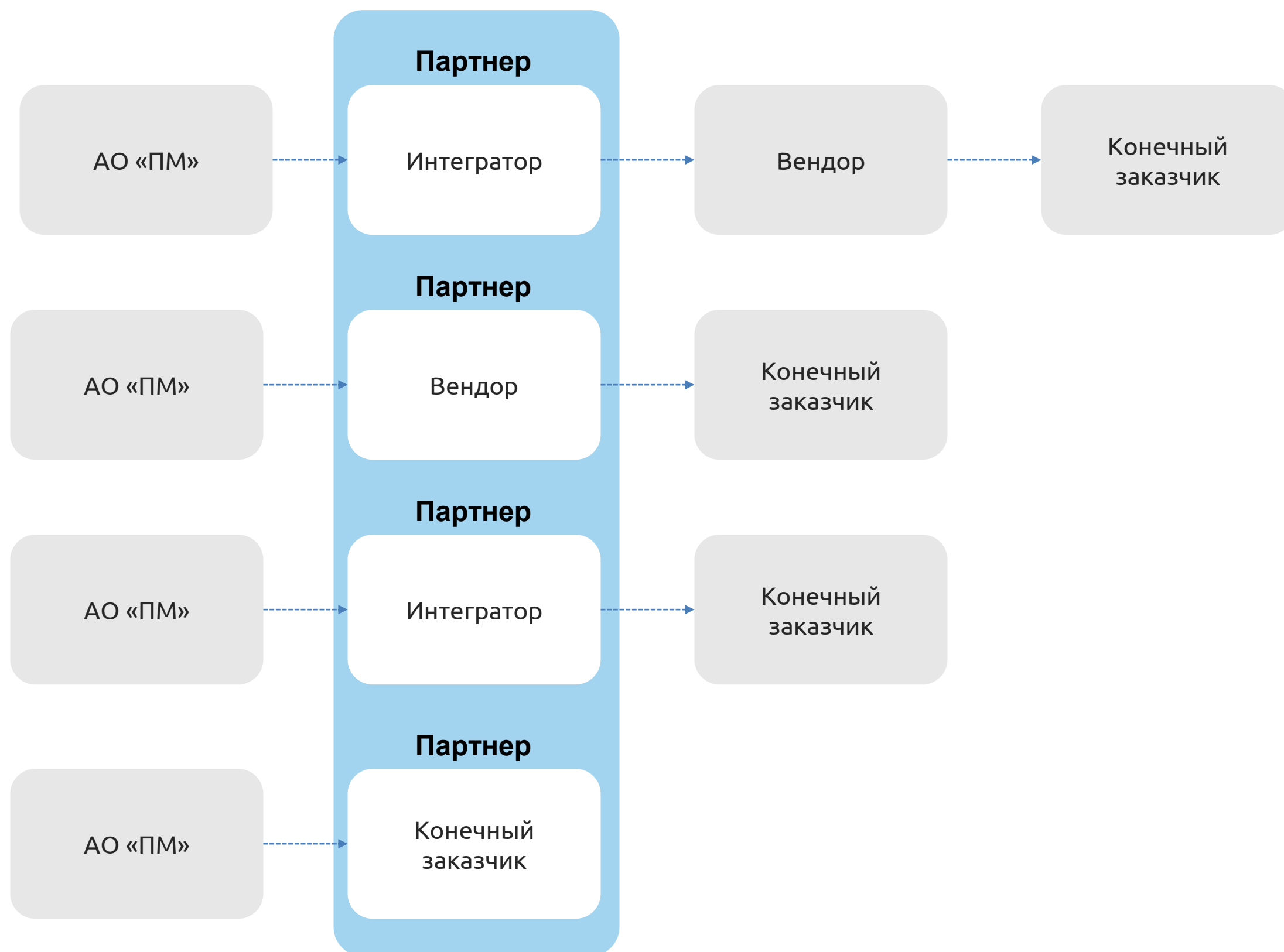


Как организован процесс



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!



t.me/pm_public

amonitoring.ru

amtip.ru

Кирилл Кузнецов

менеджер продукта,
«Перспективный мониторинг»

Kirill.Kuznetsov@amonitoring.ru

ТЕХНО infotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

