ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

infotecs

Эксплуатация и отличительные особенности БРП в IDS и TIAS

Галкин Николай

Руководитель НИК
«Перспективный мониторинг»

Старовойт Светлана

Руководитель продуктового решения
«ИнфоТеКС»

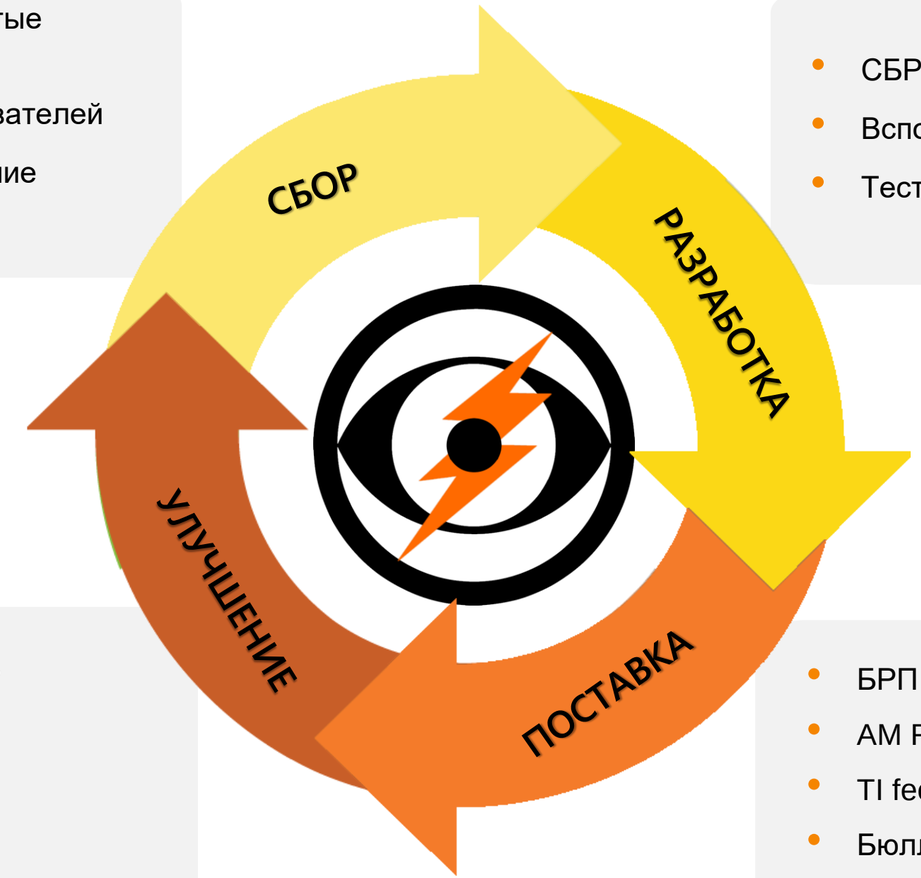
Направление исследования киберугроз

Направление исследования киберугроз (НИК) занимается непрерывным поиском и исследованием угроз ИБ с целью производства соответствующих баз решающих правил (БРП/сигнатур) для СЗИ.

Постоянно исследуем актуальные уязвимости, ВПО, эксплойты и другие угрозы безопасности.; помимо этого, проводим аналитику состояния защищенности СЗИ; являемся частью SOC, что повышает качество сигнатур и их эксплуатации

Процесс разработки правил

- Открытые/закрытые источники
- Объекты пользователей
- Ручное добавление
- OSINT

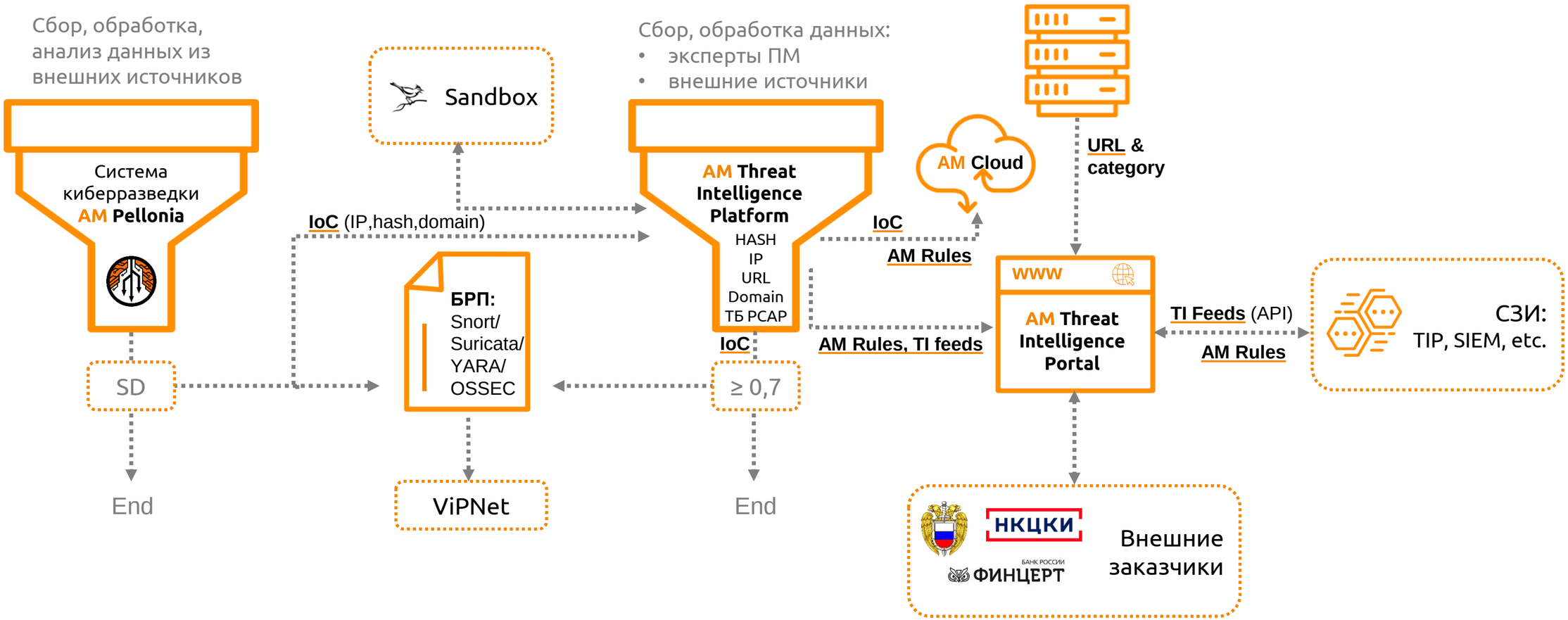


- СБРП
- Вспомогательные сервисы
- Тестирование

- Обратная связь
- False positive
- Bug & Fix
- Тех.поддержка

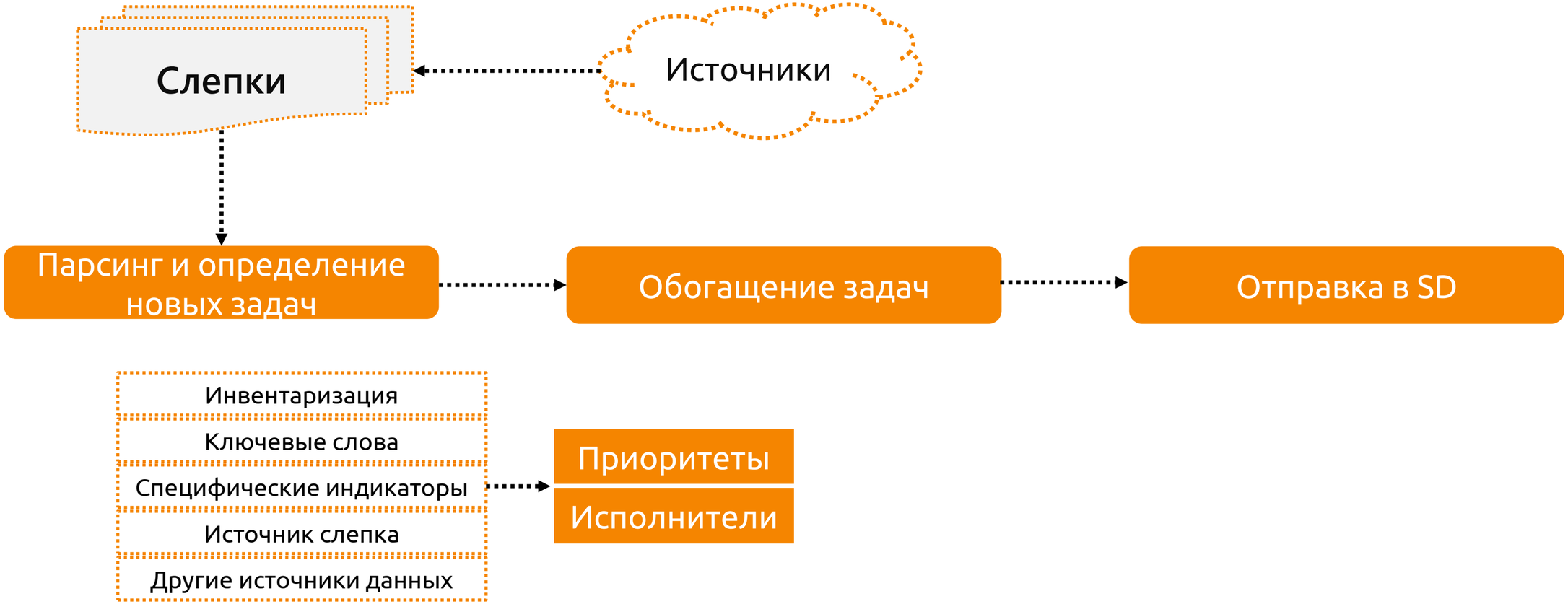
- БРП
- AM Rules
- TI feeds (IOC)
- Бюллетени ИБ

Как устроено



Система AM Pellonia

AM Pellonia – система сбора и обработки информации об угрозах, результат работы – автозаведённые в систему управления задачами.



Работа с публичными источниками

CVE-2022-31686 has been described by the virtualization services provider as a "broken authentication method" vulnerability, and CVE-2022-31687 as a "Broken Access Control" flaw.

"A malicious actor with network access may be able to obtain administrative access without the need to authenticate to the application," VMware said in an advisory for CVE-2022-31686 and CVE-2022-31687.

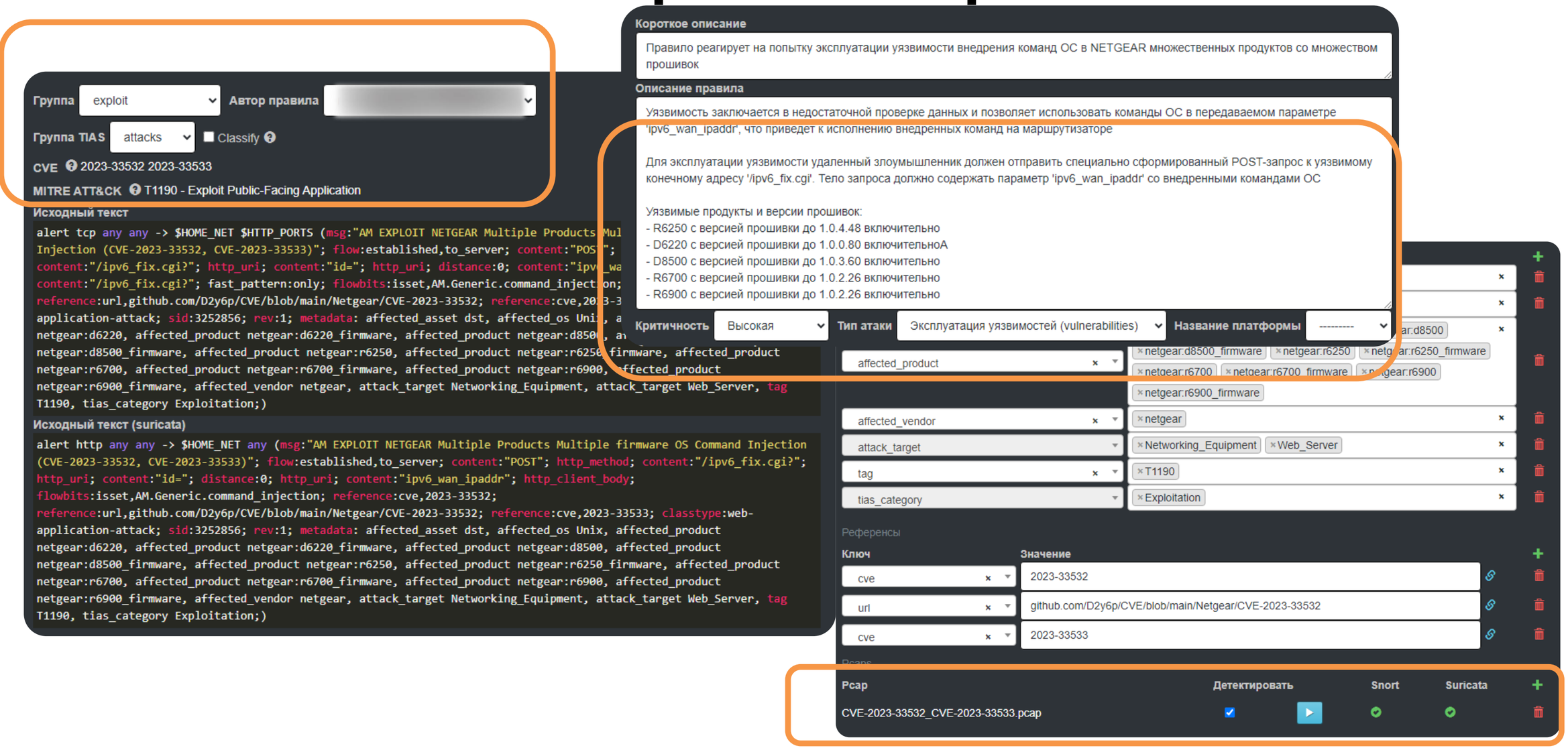
Another vulnerability is a case of a reflected cross-site scripting (XSS) vulnerability (CVE-2022-31688, CVSS score: 6.4) stemming from improper user input sanitization, something that could be exploited to inject arbitrary JavaScript code in the target user's window.

Система БРП

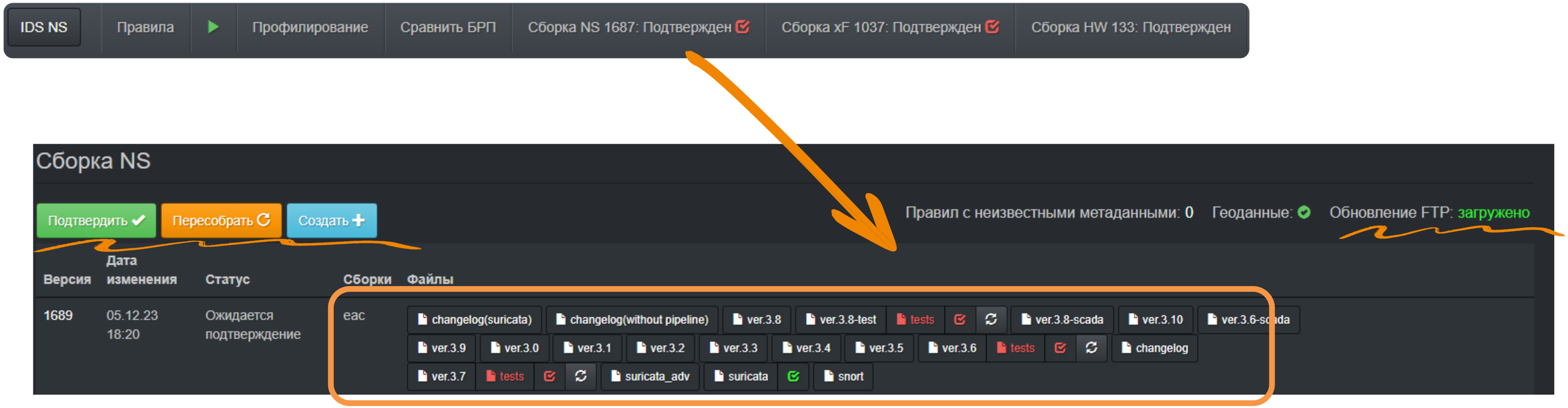
Дата изменения	Группа	SID	Сообщение
29.11.23 15:38	exploit	3251398	AM EXPLOIT Tenda AC8 <= v16.03.34.06 Stack Overflow (CVE-2023-33671)
23.11.23 15:13	exploit	3251397	AM EXPLOIT Generic Possible XXE Injection: 'DOCTYPE ENTITY' in HTTP Body
27.11.23 14:11	exploit	3250053	AM EXPLOIT Tenda AC8 <= v16.03.34.06 Stack Overflow (CVE-2023-33675)
27.11.23 14:09	exploit	3250052	AM EXPLOIT Tenda AC8 <= v16.03.34.06 Stack Overflow (CVE-2023-33673)
29.11.23 14:28	exploit	3250051	AM EXPLOIT Generic Command Injection in HTTP Body: chmod var 2
27.11.23 14:09	exploit	3250050	AM EXPLOIT Tenda AC8 <= v16.03.34.06 Stack Overflow (CVE-2023-33672)
29.11.23 14:28	exploit	3250049	AM EXPLOIT Generic Command Injection in HTTP Body: chmod var 1
16.11.23 15:16	info	3249786	ET INFO DYNAMIC_DNS Query to a (Redacted - Vulgar) Domain
29.11.23 14:28	exploit	3249785	AM EXPLOIT Cisco IOS XE < v17.9.4a RCE Authenticated (CVE-2023-20273)
23.11.23 16:25	exploit	3249784	AM EXPLOIT Possible Bitrix24 CRM <= v22.0.300 RCE via .phar-file Deserialization (CVE-2023-1714)
22.11.23 15:55	exploit	3249783	AM EXPLOIT Bitrix24 CRM <= v22.0.300 Stored XSS (CVE-2023-1720)
23.11.23 16:25	exploit	3249782	AM EXPLOIT Possible Bitrix24 CRM <= v22.0.300 RCE via .php-file Append (CVE-2023-1714)
22.11.23 15:55	exploit	3249781	AM EXPLOIT Possible Bitrix24 CRM <= 22.0.300 DOM XSS via Prototype Pollution (CVE-2023-1717)
01.12.23 14:31	exploit	3249780	AM EXPLOIT Atlassian Confluence < v8.5.1 Broken Access Control (CVE-2023-22515)
22.11.23 15:55	exploit	3249363	AM EXPLOIT Possible Bitrix24 CRM <= v22.0.300 XSS Filter Bypass (CVE-2023-1716)
17.11.23 14:11	exploit	3249362	AM EXPLOIT Bitrix24 CRM <= v22.0.300 XSS Filter Bypass (CVE-2023-1715)
27.11.23 14:11	exploit	3249360	AM EXPLOIT Tenda AC8 <= v16.03.34.06 Stack Overflow (CVE-2023-33670)
27.11.23 14:09	exploit	3249356	AM EXPLOIT Tenda AC8 <= v16.03.34.06 Stack Overflow (CVE-2023-33669)
20.11.23 15:14	trojan	3249355	ET TROJAN TA453 BellaCiao CnC Domain in DNS Lookup (msn-service .co)
10.11.23 14:38	info	3249354	ET INFO Observed DNS Query to .work TLD

Система БРП (БРП - «База решающих правил» [ГОСТ Р 59709-2022]) автоматизирует выпуск сборок БРП для различных продуктов АО «ИнфоТеКС» и AM Rules для внешних Заказчиков.

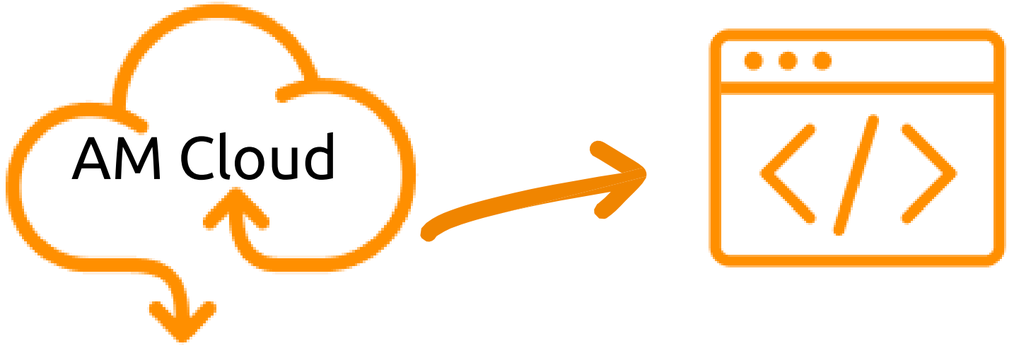
Система БРП: карточка правила

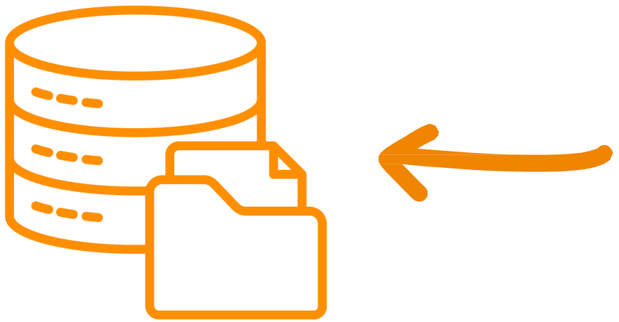


Система БРП: поддержка продуктов



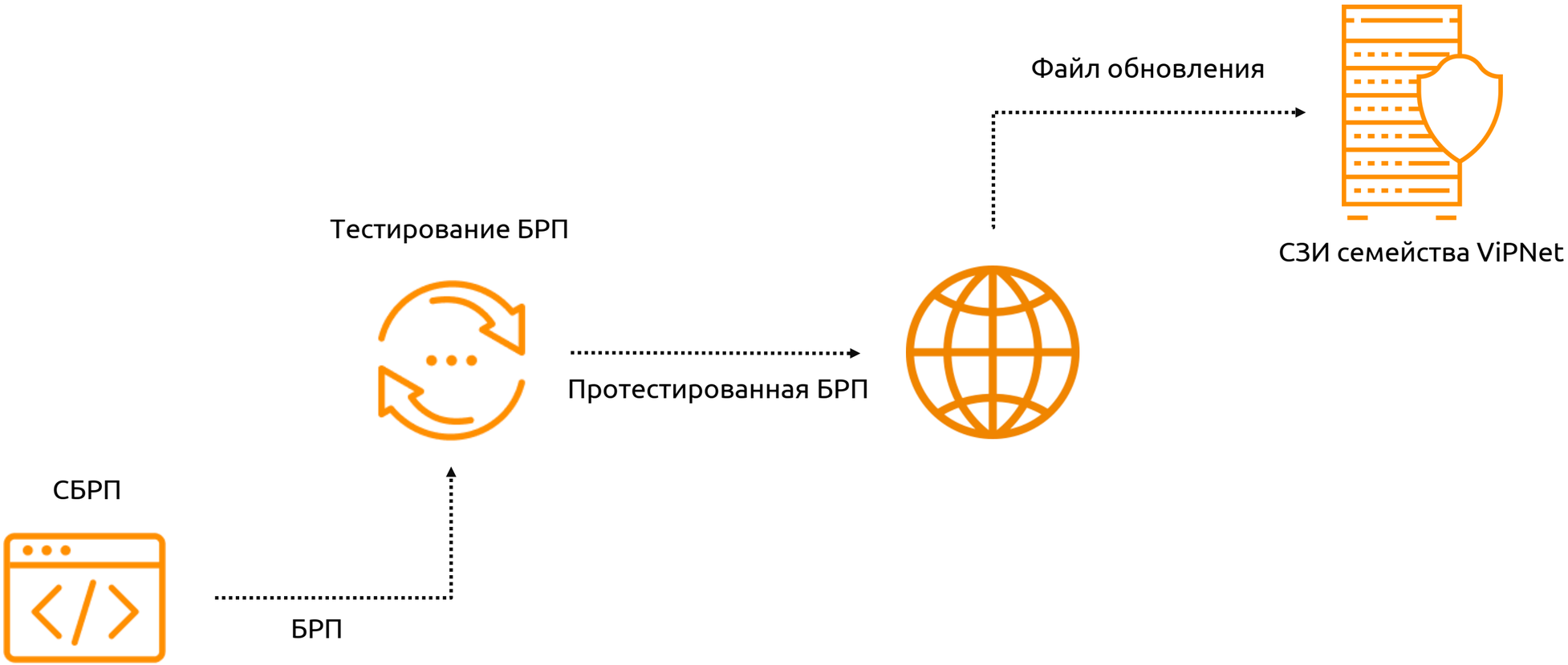
Способы доставки AM Rules





«Файлами»

Способы доставки БРП



БРП АО «ПМ» в цифрах

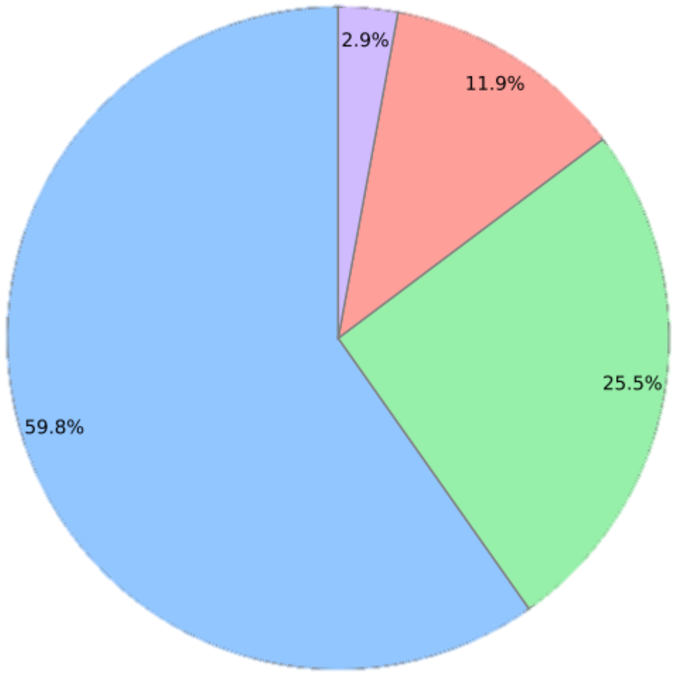
Snort / Suricata / YARA /OSSEC

> 400 000 правил/сигнатур

Периодичность	Сетевые правила	Хостовые правила
В день ~	33	12
В месяц ~	873	319
В год ~	97986	50370
Total ~	295000	132500

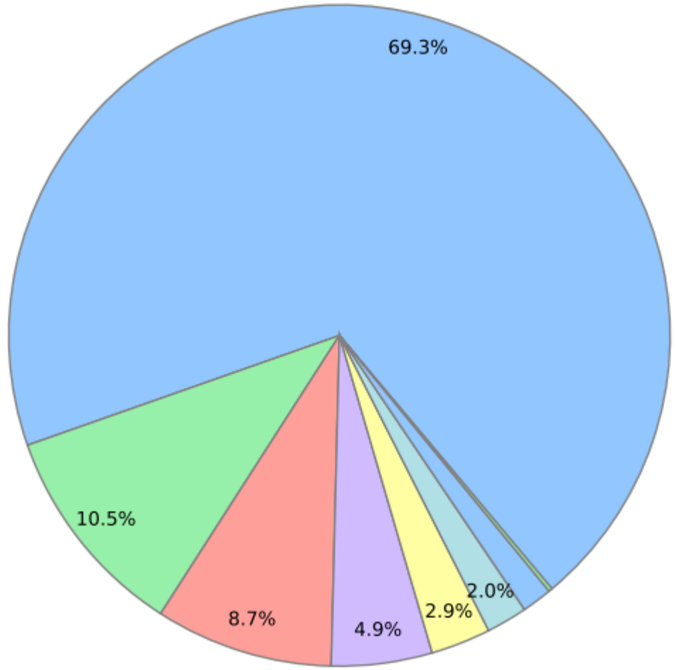
БРП АО «ПМ» в цифрах: IDS NS

Распределение правил по группам угроз



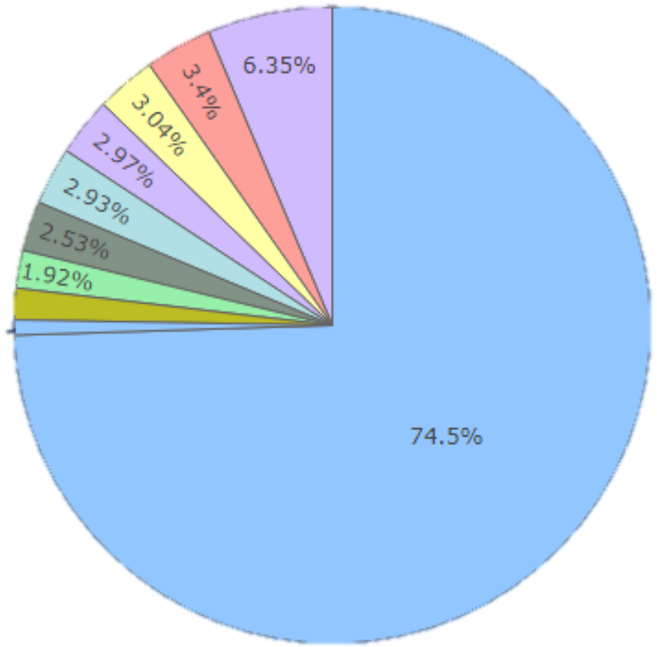
Others, 59.8%	29887
TROJAN, 25.5%	12732
EXPLOIT, 11.9%	5927
MALWARE, 2.9%	1446

Распределение правил по профилям защиты



Рабочие станции, 69.3%	34631
Клиент-серверное ПО, 10.5%	5261
Веб-серверы, 8.7%	4347
Все профили, 4.9%	2460
Специализированные профили, 2.9%	1464
Серверы, 2.0%	1001
Сетевое оборудование, 1.5%	738
АСУ ТП, 0.2%	90

Распределение правил по топ-10 вендорам



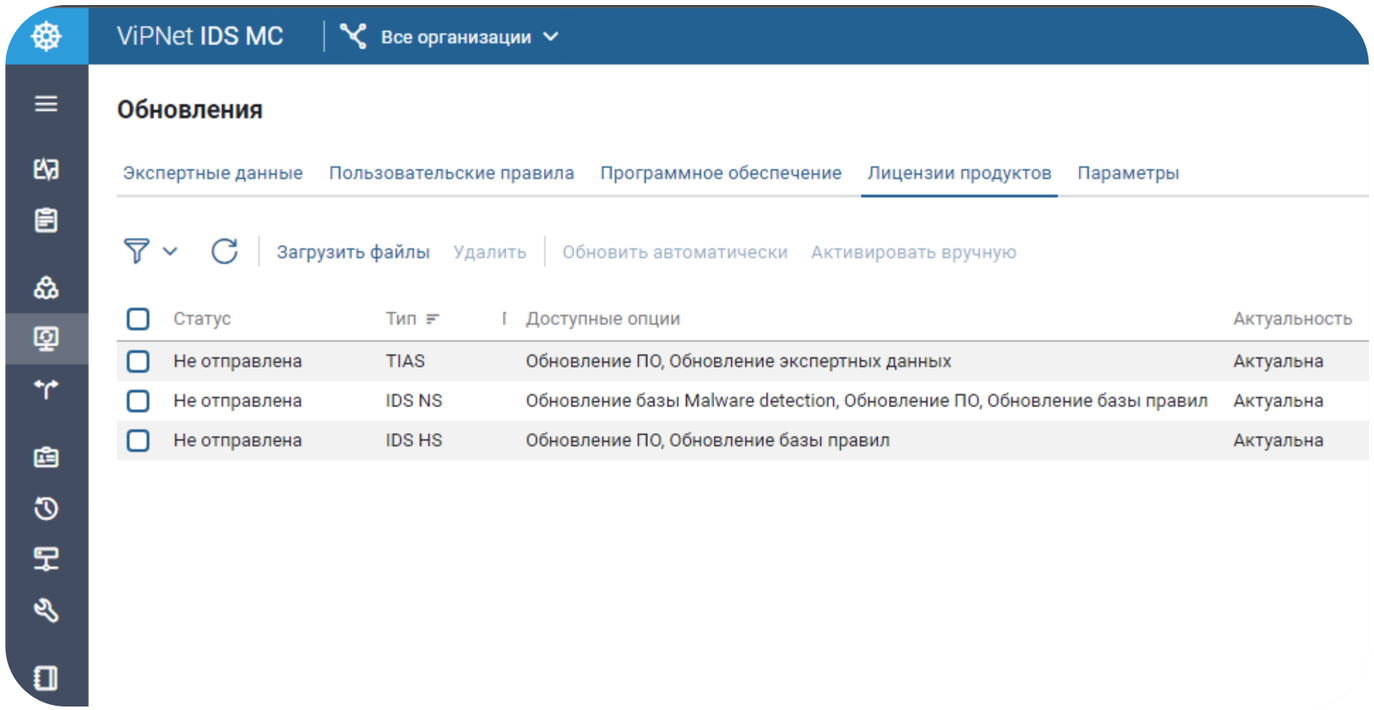
microsoft	4859
linux	414
oracle	222
google	198
hp	194
cisco	191
apple	165
adobe	125
ibm	104
bitrix	50

Доступ к базам правил

Лицензирование обновлений БРП

Подписка на обновления БРП на 1 год включена в стоимость продукта

Через 1 год подписку нужно продлевать



- ✓ Подписка оформляется отдельно для каждого устройства
- ✓ При просроченной подписке обновить БРП/ экспертные данные на устройстве нельзя

Доступ к серверу обновлений

Информация о лицензии:

"Обновление экспертных данных ViPNet TIAS"

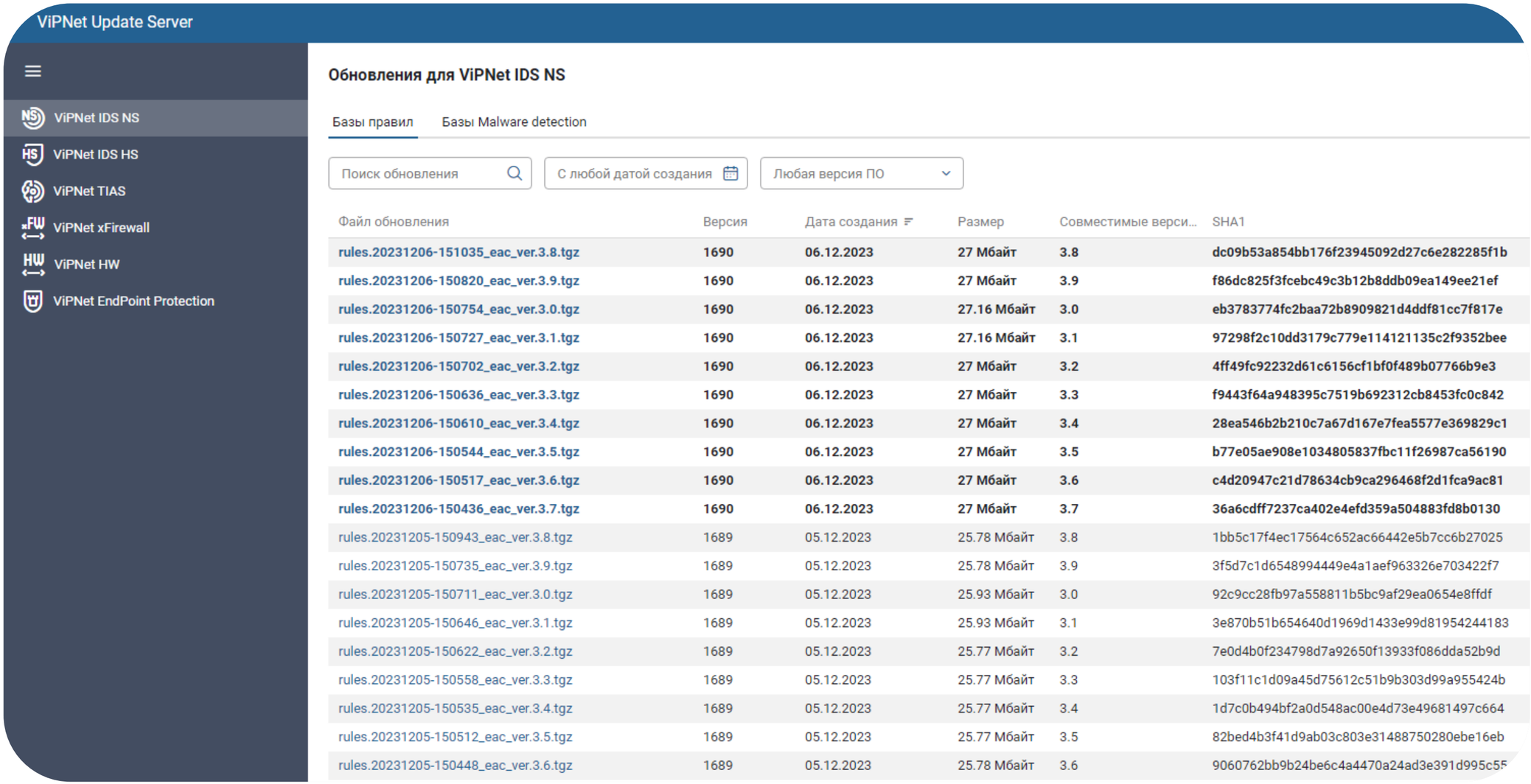
Идентификатор лицензии:	1401947/1/3-TIAS
Дата начала действия учётной записи:	13.02.2019
Дата окончания действия учётной записи:	не ограничено
Конечный пользователь:	Открытое акционерное общество "Информационные технологии и коммуникационные системы"

Учетные данные для доступа к серверу обновлений

Адрес сервера обновлений	https://updateids.infotecs.ru/
Имя пользователя	**1401947-1-3-TIAS**
Пароль	**(5cEPprP**

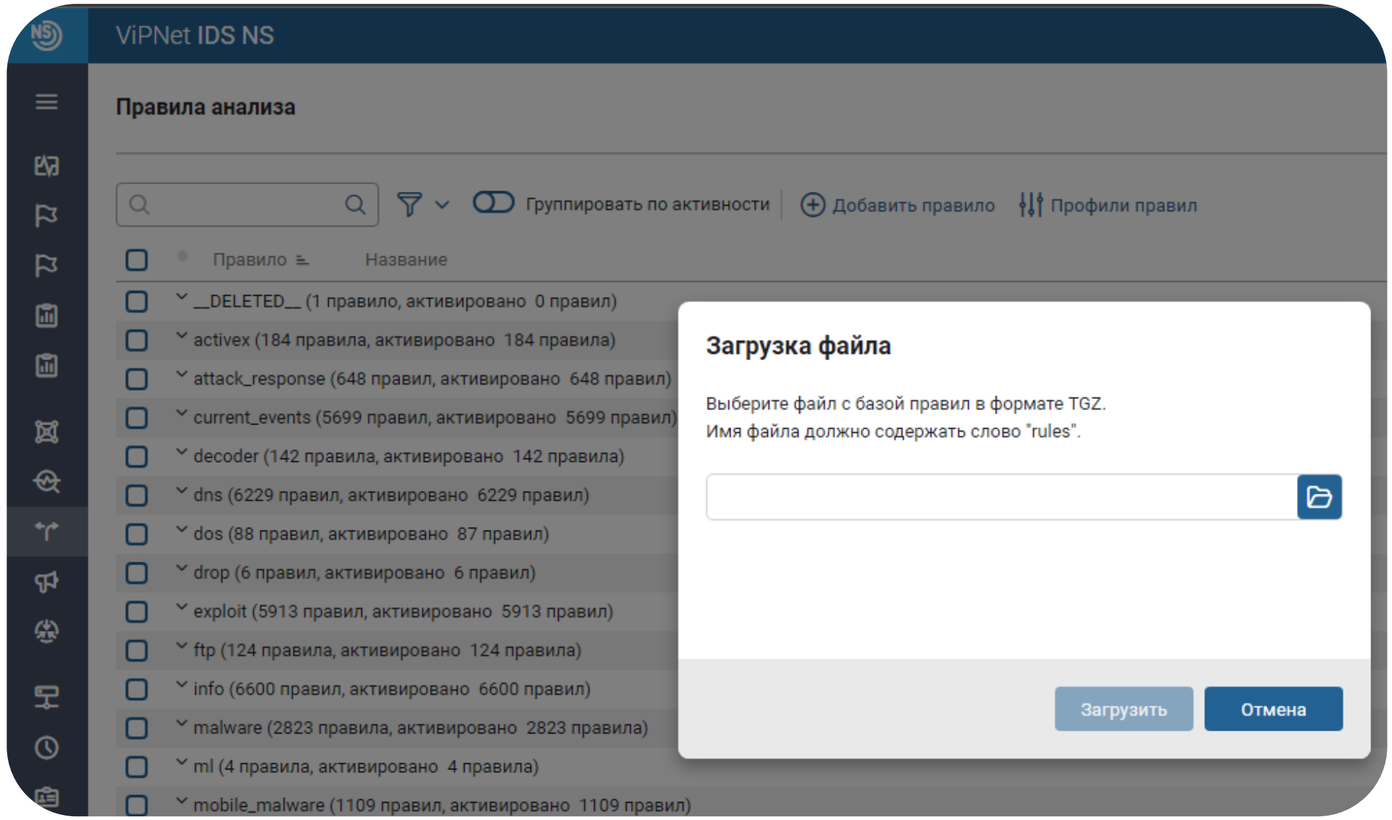
- ✓ Файл lic_XXXXXX-X_DD.MM.YYYY_XXXXXX-X_creds.pdf выдается вместе с лицензией
- ✓ Дата окончания действия учетной записи равна дате окончания подписки на обновления
- ✓ Лицензия для IDS MC дает доступ к обновлениям всех продуктов, подключенных к MC

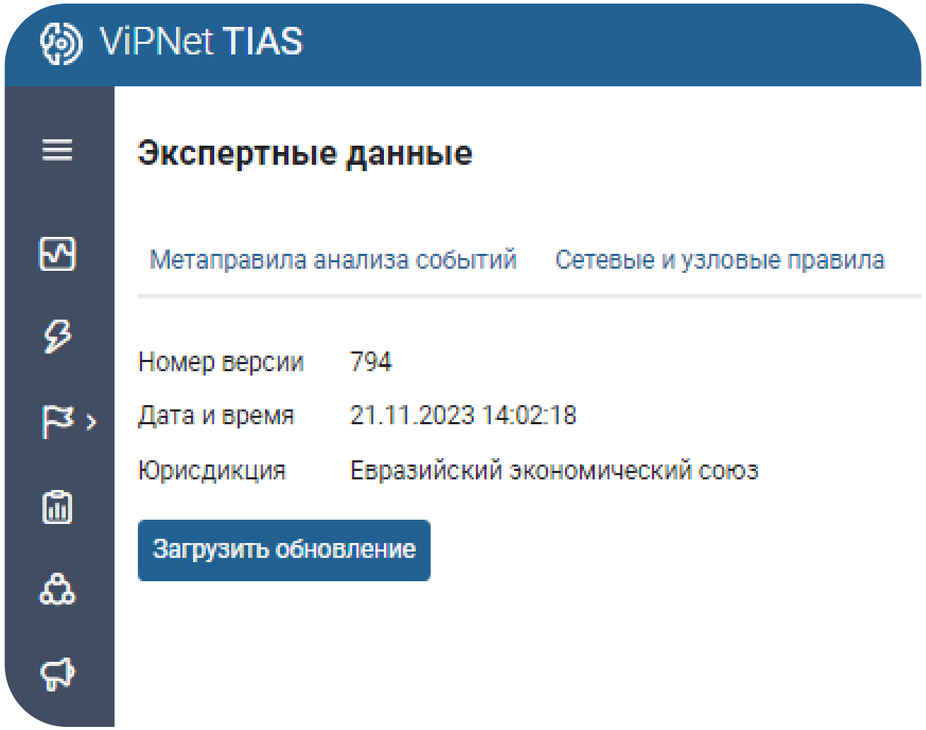
Сервер обновлений



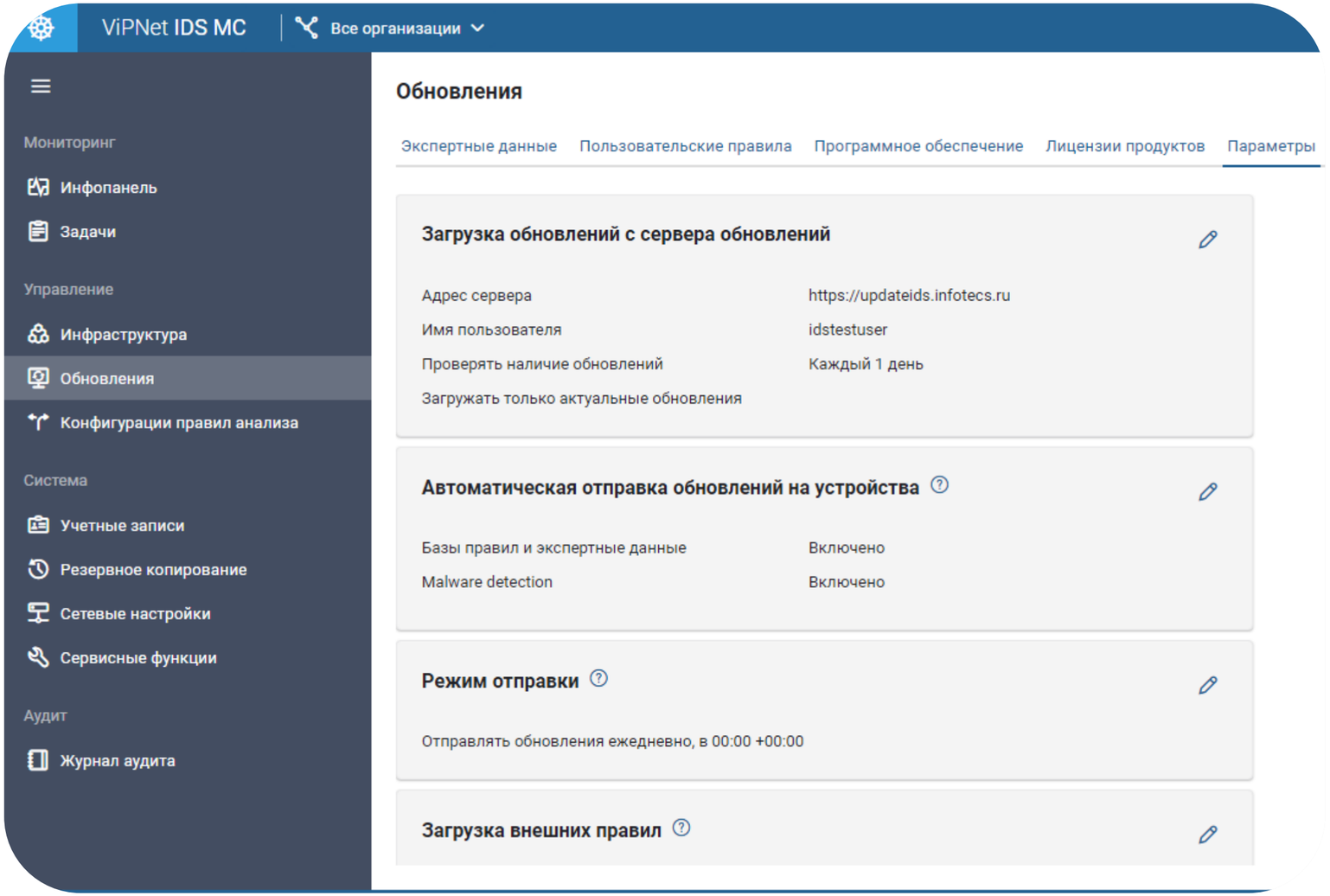
Файл обновления	Версия	Дата создания	Размер	Совместимые верси...	SHA1
rules.20231206-151035_eac_ver.3.8.tgz	1690	06.12.2023	27 Мбайт	3.8	dc09b53a854bb176f23945092d27c6e282285f1b
rules.20231206-150820_eac_ver.3.9.tgz	1690	06.12.2023	27 Мбайт	3.9	f86dc825f3fcebc49c3b12b8ddb09ea149ee21ef
rules.20231206-150754_eac_ver.3.0.tgz	1690	06.12.2023	27.16 Мбайт	3.0	eb3783774fc2baa72b8909821d4ddf81cc7f817e
rules.20231206-150727_eac_ver.3.1.tgz	1690	06.12.2023	27.16 Мбайт	3.1	97298f2c10dd3179c779e114121135c2f9352bee
rules.20231206-150702_eac_ver.3.2.tgz	1690	06.12.2023	27 Мбайт	3.2	4ff49fc92232d61c6156cf1bf0f489b07766b9e3
rules.20231206-150636_eac_ver.3.3.tgz	1690	06.12.2023	27 Мбайт	3.3	f9443f64a948395c7519b692312cb8453fc0c842
rules.20231206-150610_eac_ver.3.4.tgz	1690	06.12.2023	27 Мбайт	3.4	28ea546b2b210c7a67d167e7fea5577e369829c1
rules.20231206-150544_eac_ver.3.5.tgz	1690	06.12.2023	27 Мбайт	3.5	b77e05ae908e1034805837fbc11f26987ca56190
rules.20231206-150517_eac_ver.3.6.tgz	1690	06.12.2023	27 Мбайт	3.6	c4d20947c21d78634cb9ca296468f2d1fca9ac81
rules.20231206-150436_eac_ver.3.7.tgz	1690	06.12.2023	27 Мбайт	3.7	36a6cdff7237ca402e4efd359a504883fd8b0130
rules.20231205-150943_eac_ver.3.8.tgz	1689	05.12.2023	25.78 Мбайт	3.8	1bb5c17f4ec17564c652ac66442e5b7cc6b27025
rules.20231205-150735_eac_ver.3.9.tgz	1689	05.12.2023	25.78 Мбайт	3.9	3f5d7c1d6548994449e4a1aef963326e703422f7
rules.20231205-150711_eac_ver.3.0.tgz	1689	05.12.2023	25.93 Мбайт	3.0	92c9cc28fb97a558811b5bc9af29ea0654e8ffdf
rules.20231205-150646_eac_ver.3.1.tgz	1689	05.12.2023	25.93 Мбайт	3.1	3e870b51b654640d1969d1433e99d81954244183
rules.20231205-150622_eac_ver.3.2.tgz	1689	05.12.2023	25.77 Мбайт	3.2	7e0d4b0f234798d7a92650f13933f086dda52b9d
rules.20231205-150558_eac_ver.3.3.tgz	1689	05.12.2023	25.77 Мбайт	3.3	103f11c1d09a45d75612c51b9b303d99a955424b
rules.20231205-150535_eac_ver.3.4.tgz	1689	05.12.2023	25.77 Мбайт	3.4	1d7c0b494bf2a0d548ac00e4d73e49681497c664
rules.20231205-150512_eac_ver.3.5.tgz	1689	05.12.2023	25.77 Мбайт	3.5	82bed4b3f41d9ab03c803e31488750280ebe16eb
rules.20231205-150448_eac_ver.3.6.tgz	1689	05.12.2023	25.78 Мбайт	3.6	9060762bb9b24be6c4a4470a24ad3e391d995c55

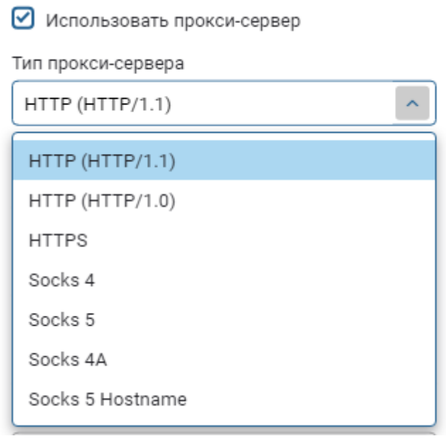
Загрузка правил в продуктах

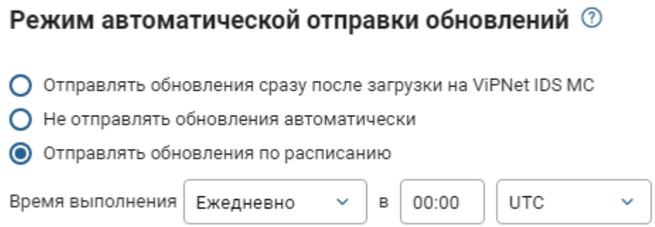




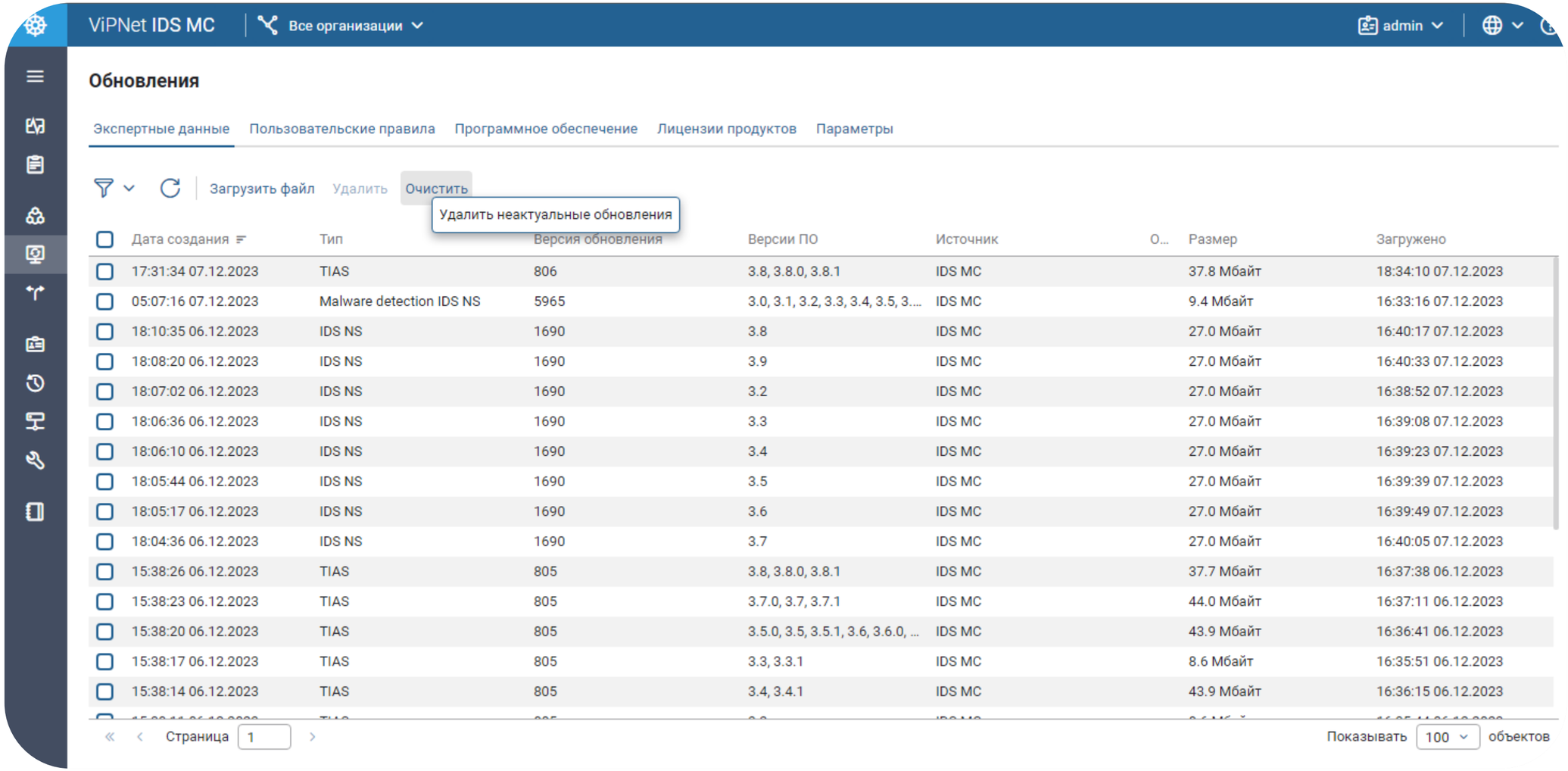
Автоматическое обновление баз правил







Только актуальные обновления



Работа с правилами
в продуктах

Профили и конфигурации

Пауль Клее. Дама с зонтиком

Клод Моне. Дама с зонтиком

Когда что использовать?

Быстро
- Ввод в эксплуатацию и первичная настройка сенсоров;
- Не требуется оптимизация работы сенсоров

Просто
- Нет квалифицированных специалистов;
- Типичный трафик не требующий тонкой настройки

Грубо
- Может быть много ложно-положительных срабатываний

конфигурации

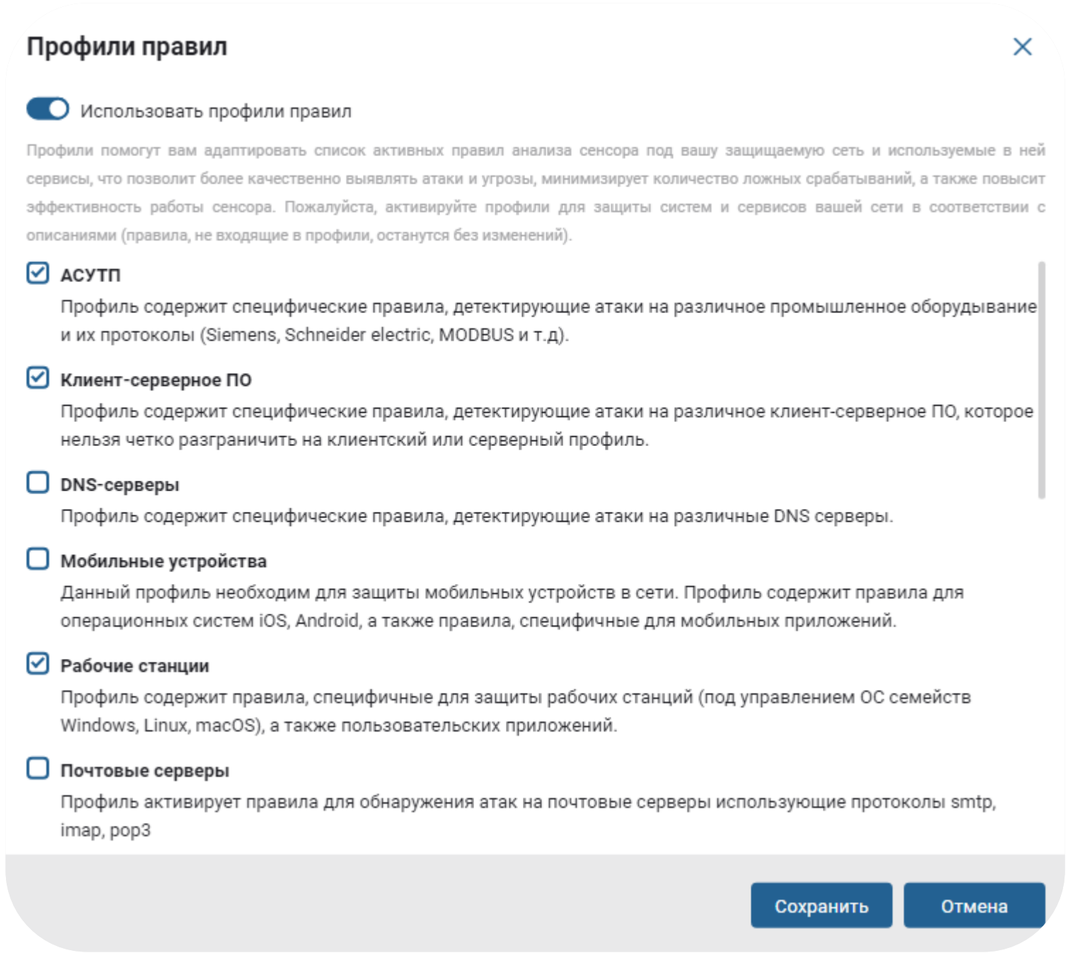
профили

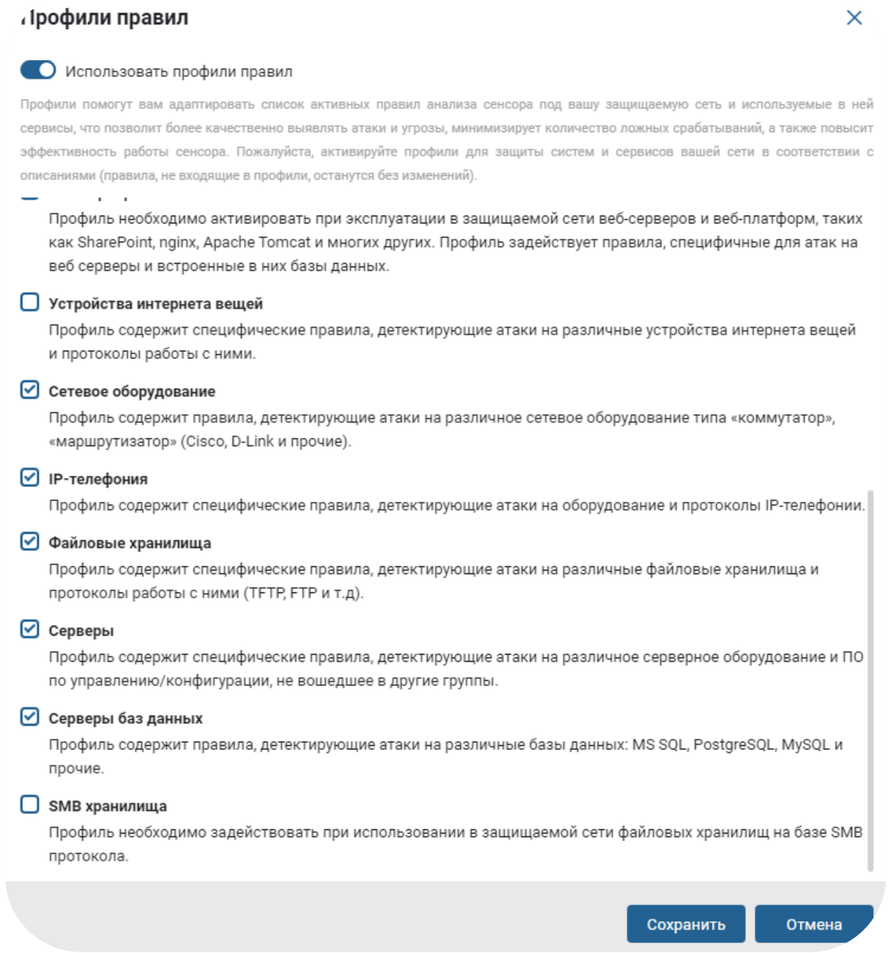
Точно
- Меньше ложно-положительных срабатываний;
- Адаптированные правила

Оптимально
- Снижение нагрузки на сенсор

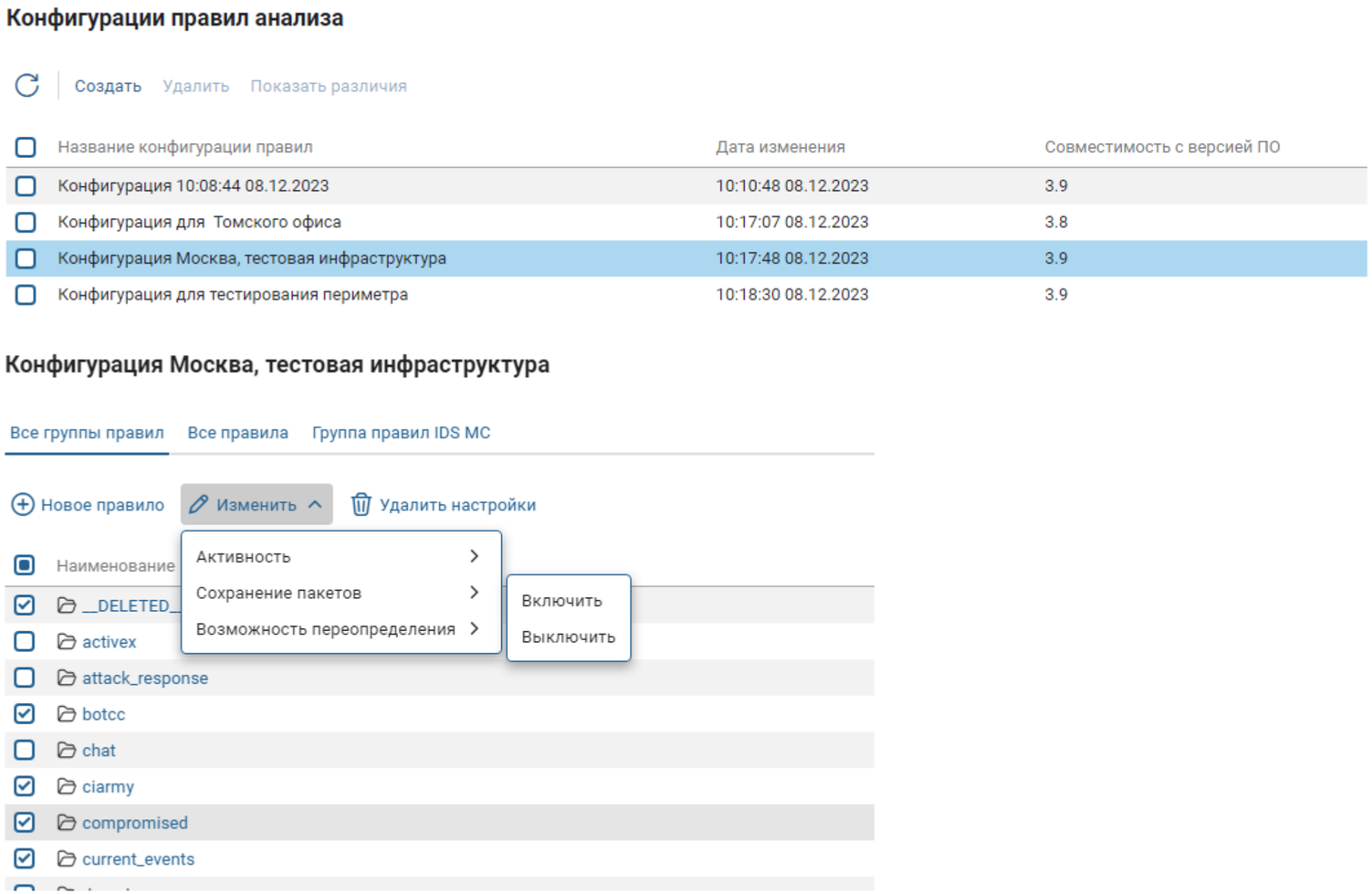
Сложно
- Есть квалифицированные специалисты, которые понимают что делают

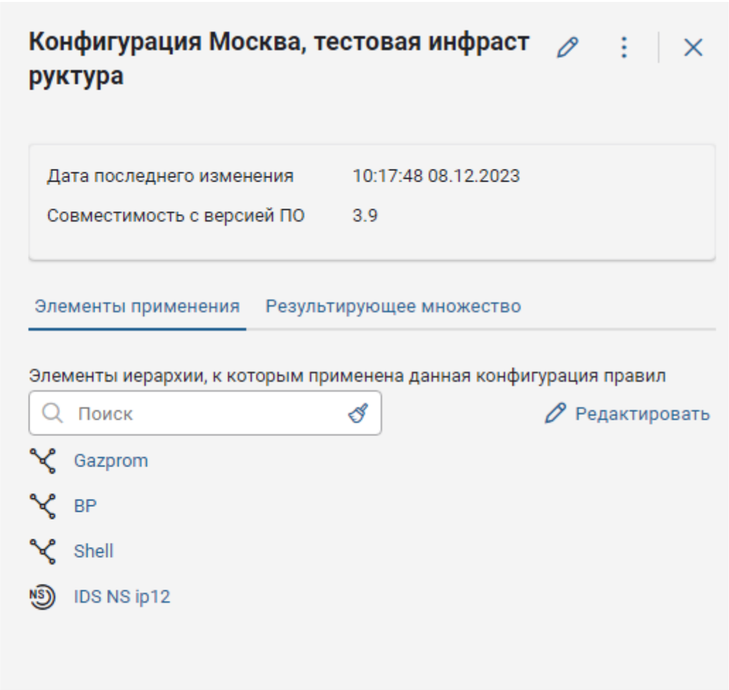
Управление профилями



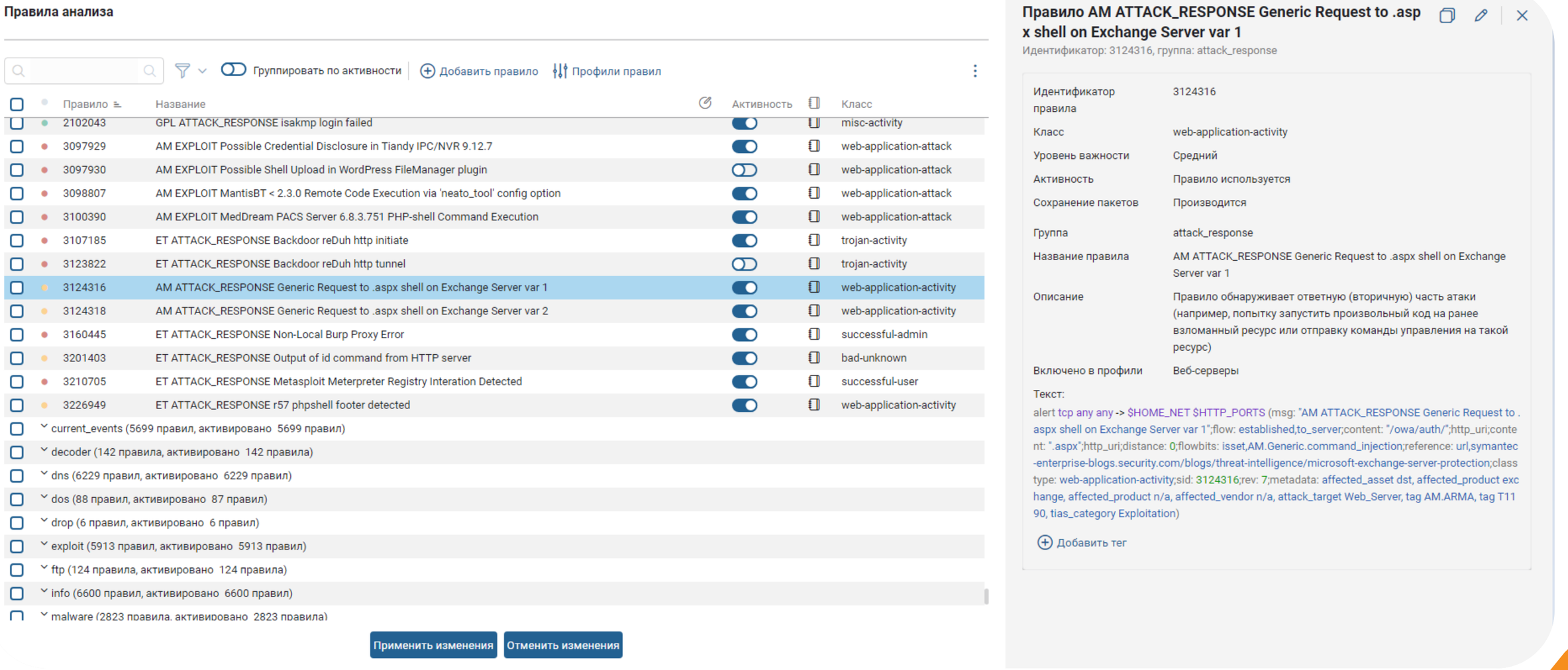


Управление конфигурациями

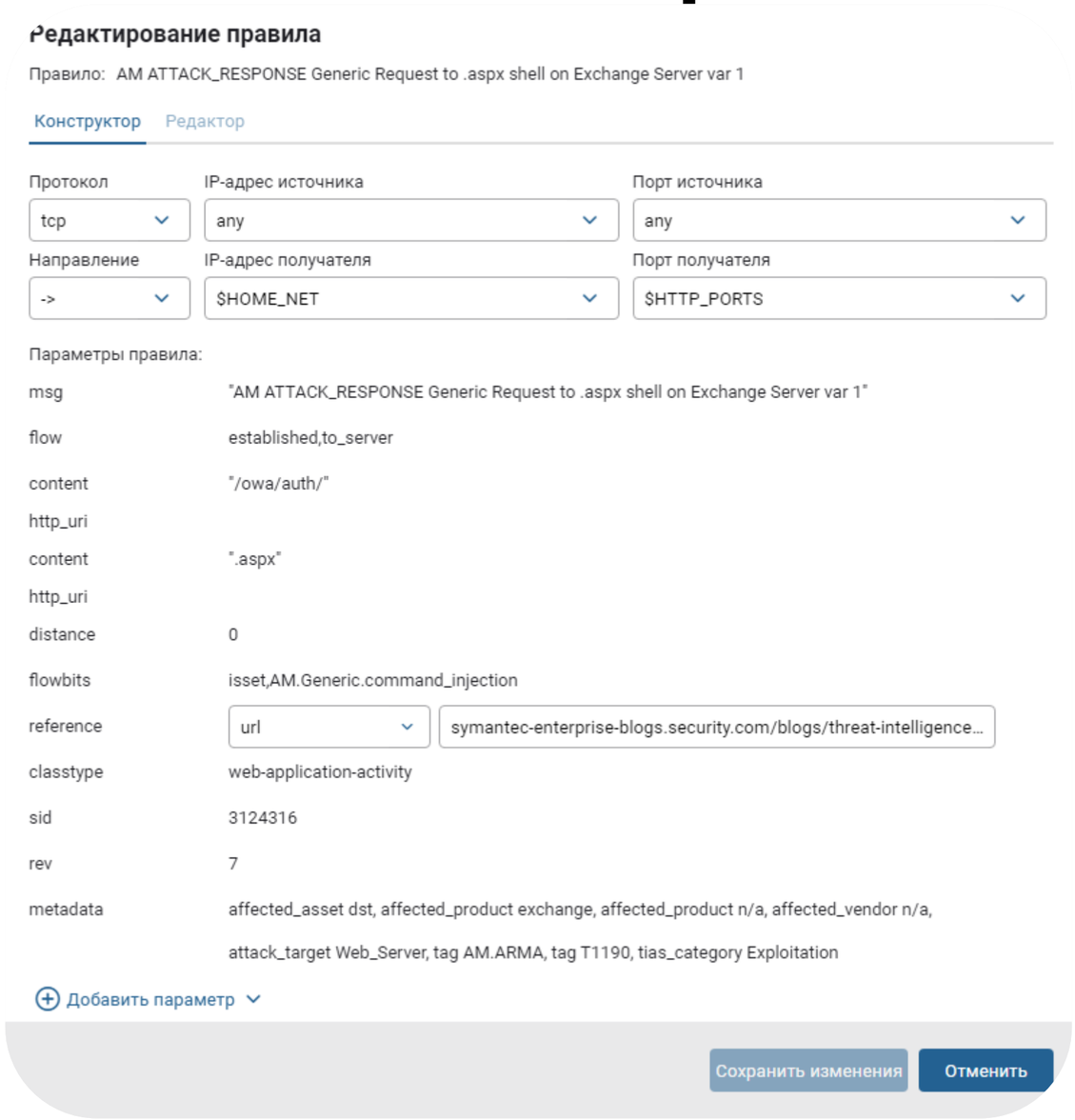


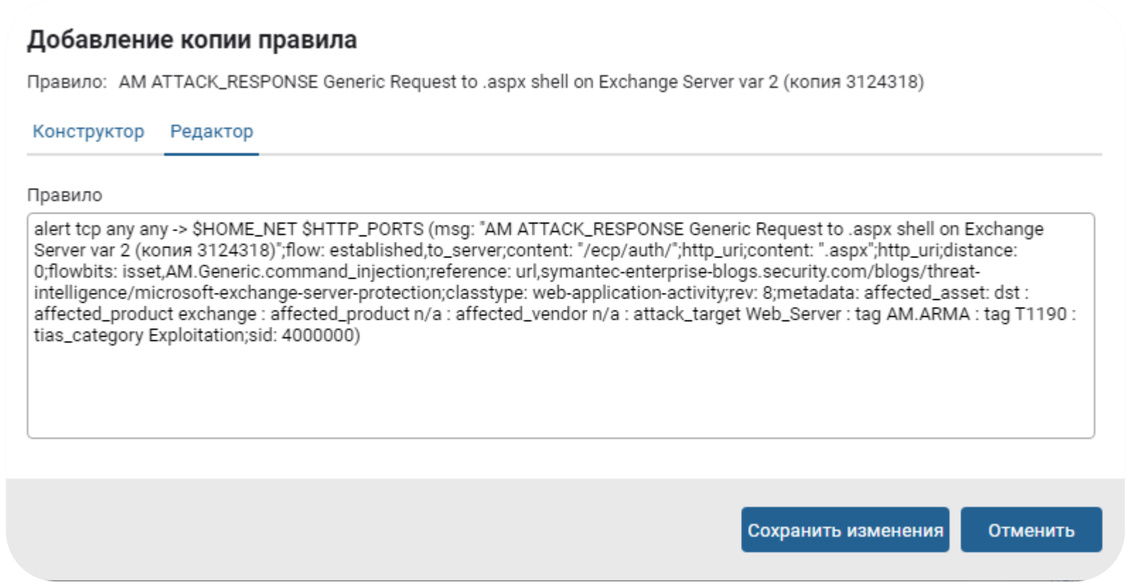


Настройка правил в IDS NS

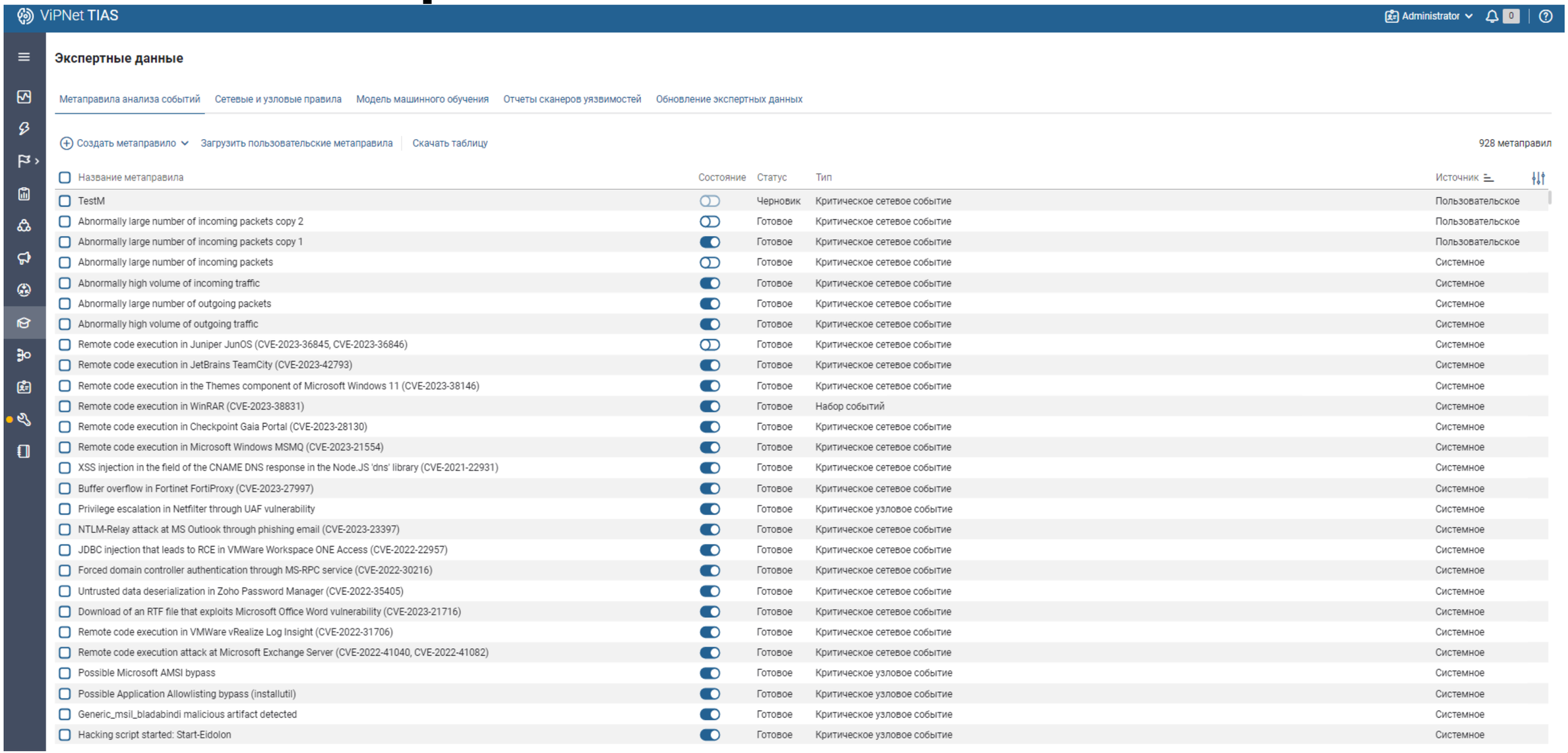


Изменение правила в IDS NS



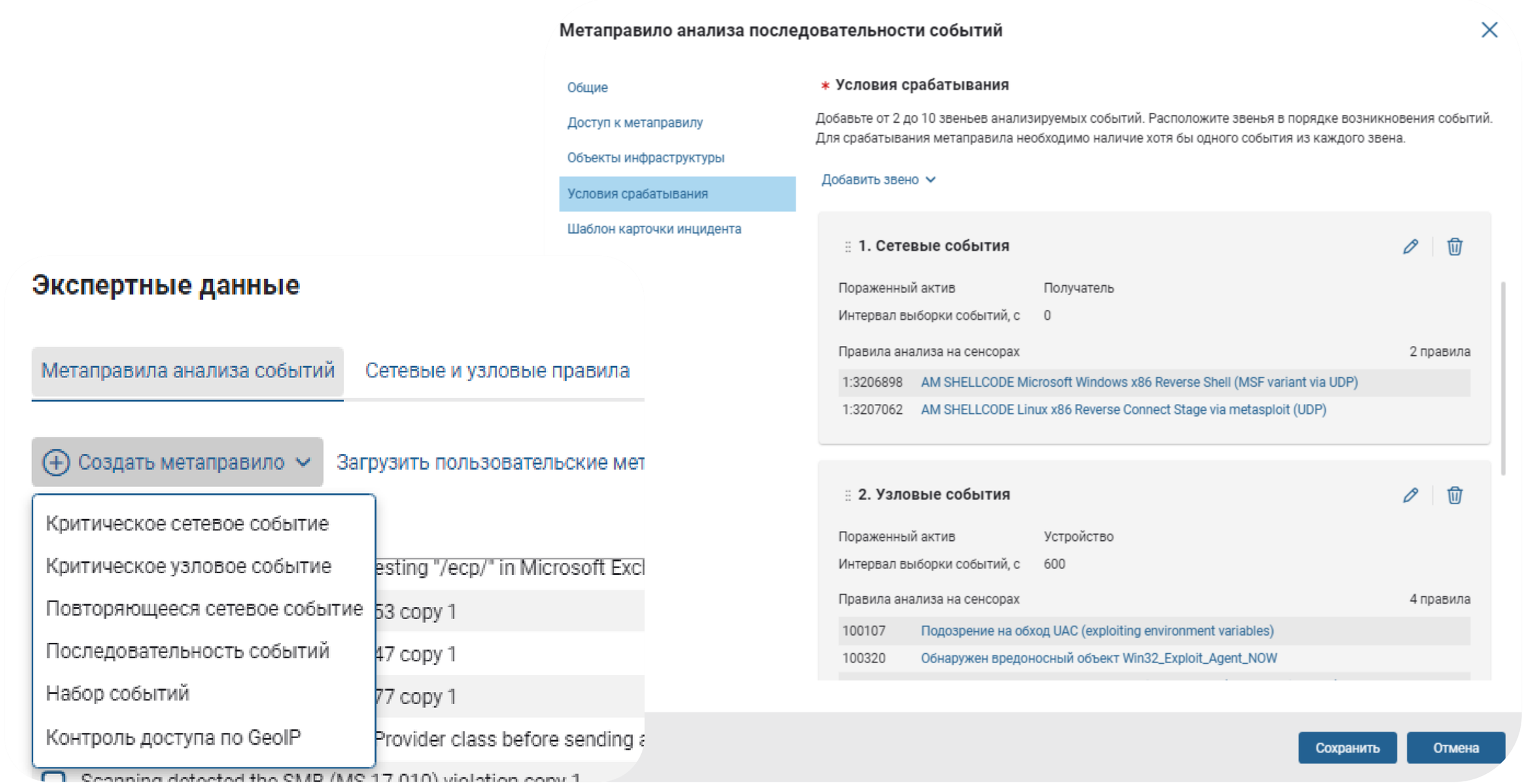


Работа с правилами в TIAS



Название метаправила	Состояние	Статус	Тип	Источник
TestM		Черновик	Критическое сетевое событие	Пользовательское
Abnormally large number of incoming packets copy 2		Готовое	Критическое сетевое событие	Пользовательское
Abnormally large number of incoming packets copy 1		Готовое	Критическое сетевое событие	Пользовательское
Abnormally large number of incoming packets		Готовое	Критическое сетевое событие	Системное
Abnormally high volume of incoming traffic		Готовое	Критическое сетевое событие	Системное
Abnormally large number of outgoing packets		Готовое	Критическое сетевое событие	Системное
Abnormally high volume of outgoing traffic		Готовое	Критическое сетевое событие	Системное
Remote code execution in Juniper JunOS (CVE-2023-36845, CVE-2023-36846)		Готовое	Критическое сетевое событие	Системное
Remote code execution in JetBrains TeamCity (CVE-2023-42793)		Готовое	Критическое сетевое событие	Системное
Remote code execution in the Themes component of Microsoft Windows 11 (CVE-2023-38146)		Готовое	Критическое сетевое событие	Системное
Remote code execution in WinRAR (CVE-2023-38831)		Готовое	Набор событий	Системное
Remote code execution in Checkpoint Gaia Portal (CVE-2023-28130)		Готовое	Критическое сетевое событие	Системное
Remote code execution in Microsoft Windows MSMQ (CVE-2023-21554)		Готовое	Критическое сетевое событие	Системное
XSS injection in the field of the CNAME DNS response in the Node.JS 'dns' library (CVE-2021-22931)		Готовое	Критическое сетевое событие	Системное
Buffer overflow in Fortinet FortiProxy (CVE-2023-27997)		Готовое	Критическое сетевое событие	Системное
Privilege escalation in Netfilter through UAF vulnerability		Готовое	Критическое узловое событие	Системное
NTLM-Relay attack at MS Outlook through phishing email (CVE-2023-23397)		Готовое	Критическое сетевое событие	Системное
JDBC injection that leads to RCE in VMWare Workspace ONE Access (CVE-2022-22957)		Готовое	Критическое сетевое событие	Системное
Forced domain controller authentication through MS-RPC service (CVE-2022-30216)		Готовое	Критическое сетевое событие	Системное
Untrusted data deserialization in Zoho Password Manager (CVE-2022-35405)		Готовое	Критическое сетевое событие	Системное
Download of an RTF file that exploits Microsoft Office Word vulnerability (CVE-2023-21716)		Готовое	Критическое сетевое событие	Системное
Remote code execution in VMWare vRealize Log Insight (CVE-2022-31706)		Готовое	Критическое сетевое событие	Системное
Remote code execution attack at Microsoft Exchange Server (CVE-2022-41040, CVE-2022-41082)		Готовое	Критическое сетевое событие	Системное
Possible Microsoft AMSI bypass		Готовое	Критическое узловое событие	Системное
Possible Application Allowlisting bypass (installutil)		Готовое	Критическое узловое событие	Системное
Generic_msil_bladabindi malicious artifact detected		Готовое	Критическое узловое событие	Системное
Hacking script started: Start-Eidolon		Готовое	Критическое узловое событие	Системное

Пользовательские метаправила



Почему у меня ~~не~~ работают правила???

На IDS NS регистрируются события ET WEB_SERVER Possible Attempt to Get SQL Server Version in URI using SELECT VERSION
Просьба проверить корректность срабатыания правила, пример срабатывания во вложении.
Version 3.9.0-652121
Hardware platform ViPNet IDS NS2000 Q2
Sensor name DVGD - ViPNet IDS NS2000 1819564370

После установки Базы правил 1668 на IDS стало приходить [redacted] 14, 3243816, 3243817, 2025701). После установки сегодня базы правил 1 [redacted] вы для сравнения за вчерашний день было примерно 20000, [redacted] на IDS правил за день примерно 350. Просьба сообщить в чем причина такого количества

[redacted]
rule.id: 3205686

description: AM DOS Eclipse Jetty Attempted DoS via TLS Traffic with Large Frame (CVE-2021-28165)

Со слов Заказчика, необходимо для данного правила внести в исключение ip-адре[redacted]мониторинг и сервер обновлений, сервер обновлений используется для доставки обновлений для приложений). 11:03

[redacted]
Коллеги, добрый день. Подскажите по сигнатуре http://rules.cm.am.int/3077749/ Похоже, фолсит на использование VPN: обращения к ресурсам (23.227.143.219, 23.227.142.26, 209.205.197.226), используемым для монетизации бесплатных приложений (go1.monetizemyapp.net), в том числе EasyVPN (https://www.virustotal.com/gui/file/0f0fb6d0fd2c78732901dd7bd244a06508c84ccbe71209fce68f910e00ee48f2/relation[redacted]s). Изменено 09:12

925470897-19...3077749.pcap
108 байт 09:12

Коллеги, добрый день. Интересует ваше видение, как можно реализовать фильтрацию ложных срабатываний средств обнаружения вторжений (IDS NS, HS), в рамках модификации базы решающих правил последних. 16:00

[redacted]
привет!
[redacted]ожалуйста, по внесению корректировок в правила на IDS NS.
[redacted]ключить определенный адрес, для которого не нужно это правило детектировать. Я добавил его [redacted]но детектирование событий продолжается. Что делаю не так?) 08:23

[redacted].pcap
1.20 КБ
Коллеги, всем привет!

Помогите разобраться в правильности детектирования:

Срабатывает правило 119.16
alert (msg:"HI CLIENT LARGE CHUNK";sid:16;gid:119;rev:1;metadata:rule-typ[redacted]
В инструкции не нашел описания поля «metadata».
Просьба сообщить на что конктретно оно срабатывает.

[redacted]
IDS_packet_time-[redacted]cap
62.59 КБ
Коллеги, добрый день! http://rules.cm.am.int/3131779/ генерирует большое количество событий. Посмотрите, пожалуйста. 13:57

IDS_packet_ti...-3131779.pcap
62.59 КБ
Изменено 13:57

Description:

IDS NS 3.9.0 фиксирует события, на адреса, которые не в
Настроено $External_Net - any, $Home_Net - 172.24.0.0/16
Фиксируются же события, где в качестве источника и по
Почему IDS отслеживает то, чего нет в сетевом окружен

Description:

На IDS NS регистрируются события AM EXPLOIT Possible Nginx DNS Resolver Heap Overflow via 'CNAME' (CVE-2021-23017)
Правило срабатывает при обращении клиента выполнить DNS запрос к доменам:
extension-updates.geo.opera.com
v10.events.data.microsoft.com
s01.upd.kaspersky.com
dns.msftncsi.com

Примеры .pcap с IDS во вложении.
Судя по всему имеет место быть ложное срабатыание.
Просьба разобраться.

[redacted]
IDS_packet_senso[redacted].pcap
517 байт
Коллгери, всем привет! Подскажите по правилу 3243120, похоже на фолс: в данных случаях в параметре log не передаются специальные символы " ' / @ = * [ ] ( ) 06:23

[redacted].pcap
1.03 КБ 06:23

FAQ

~ 75% случаев связанных с неправильной работой правил происходят из-за некорректно настроенного сетевого окружения (EXTERNAL_NET/HOME_NET)

~ 20% по причине отсутствия своевременного обновления баз правил

~ 5% доля ложноположительных срабатываний, которые происходят из-за некорректной работы самих правил: функциональных особенностей СЗИ или особенностей IT-инфраструктуры, и/или недостаточной детектирующей способности

Обратная связь

Одним из основным каналов связи между эксплуатантами БРП и направлением исследования киберугроз является служба поддержки АО «Инфотекс» или Центр Мониторинга АО «ПМ»

Дополнительным каналом взаимодействия могут являться корпоративная почта или мессенджеры

Исправление дефектов занимает от 1 до 5 дней.

Актуальная информация об угрозах

Информационный бюллетень Центра мониторинга АО «ПМ»

Название документа	**Уязвимость удаленного исполнения кода в Apache ActiveMQ**
Разослан	2023-11-27
Идентификатор	AM-2023-ALE-1127-02
Описание угрозы	**CVE-2023-46604**

CVSSv3.1: 10.0, AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H

Объект уязвимости: Класс Marshaller протокола OpenWire в Apache ActiveMQ

Требования к атакующему: Удаленный неаутентифицированный

Максимальный результат атаки: Удаленное исполнение кода

Меры противодействия

Обновить ПО до актуальной версии, следовать указаниям из бюллетеня безопасности Apache:

- https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt

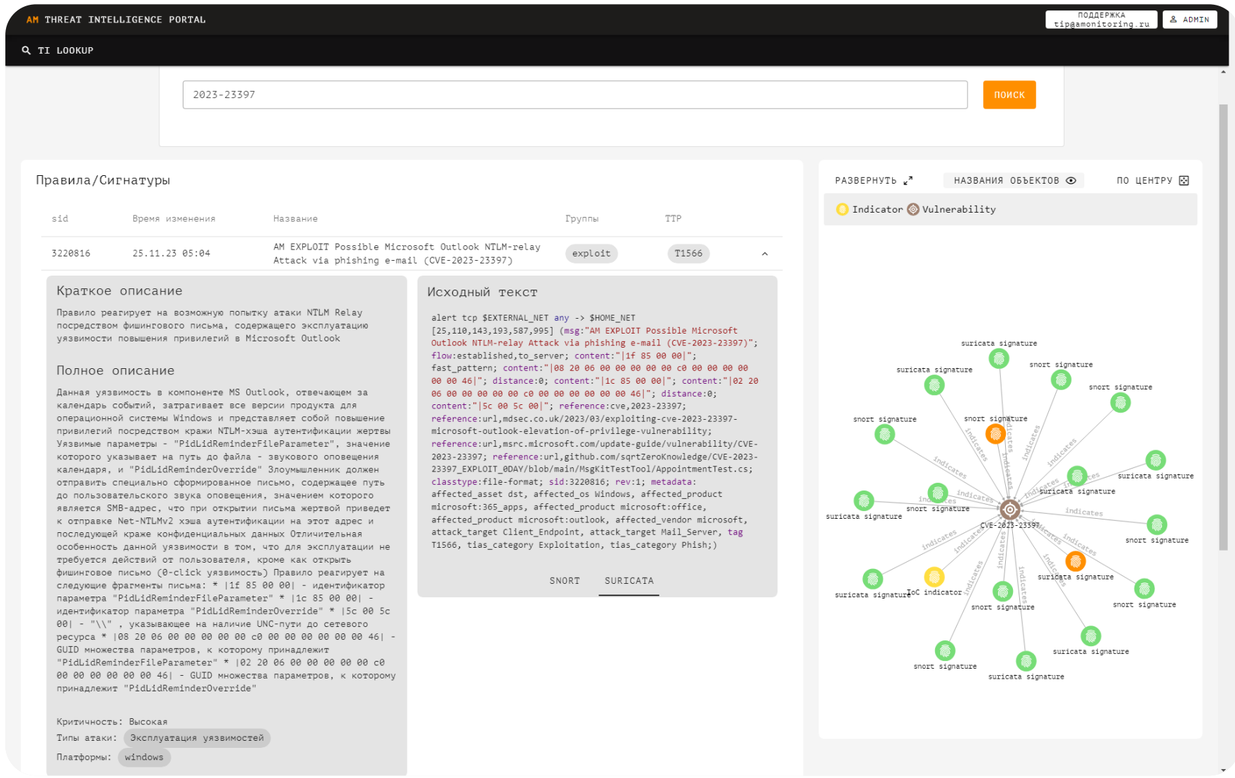
Использовать правила ViPNet IDS NS:

- sid 3252852 "AM EXPLOIT Apache ActiveMQ < v5.18.3 Java Deserialization RCE via 'FileSystemXmlApplicationContext' (CVE-2023-46604)"
- sid 3252842 "AM EXPLOIT [ET] Apache ActiveMQ < v5.18.3 Java Deserialization RCE via 'ClassPathXmlApplicationContext' (CVE-2023-46604)"
- sid 3252853 "AM EXPLOIT [ET] Possible Apache ActiveMQ < v5.18.3 RCE Server Response (CVE-2023-46604)"

Использовать метаправило ViPNet TIAS:

- Удаленное исполнение кода в Apache ActiveMQ (CVE-2023-

AM Threat Intelligence Portal



Экспертные данные в TIAS

Системные ЭД

- ✓ База узловых и сетевых правил
- ✓ База метаправил
- ✓ База индикаторов компрометации
- ✓ База геопозиционных данных
- ✓ База размеченных инцидентов
- ✓ Справочники шаблонов инцидентов

Пользовательские ЭД

- ✓ Пользовательские правила IDS
- ✓ Данные сканеров уязвимостей
- ✓ Пользовательские метаправила
- ✓ Сценарии реагирования
- ✓ Размеченные инциденты

Планы интеграции с сервисами ПМ

- Расширенные сценарии работы с IoC
- Интеграция с TI-платформой
- Сервис инцидент-менеджмента

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

infotecs

Спасибо
за внимание!

amonitoring.ru

infotecs.ru

Галкин Николай

Руководитель НИК
«Перспективный мониторинг»

nikolay.galkin@amonitoring.ru

Старовойт Светлана

Руководитель продуктового решения
«ИнфоТеКС»

starovoytsg@infotecs.ru