



ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

**infotecs**

# Эксплуатация и отличительные особенности **БРП** в **IDS** и **TIAS**

**Галкин Николай**

Руководитель НИК  
«Перспективный мониторинг»

**Старовойт Светлана**

Руководитель продуктового решения  
«ИнфоТеКС»



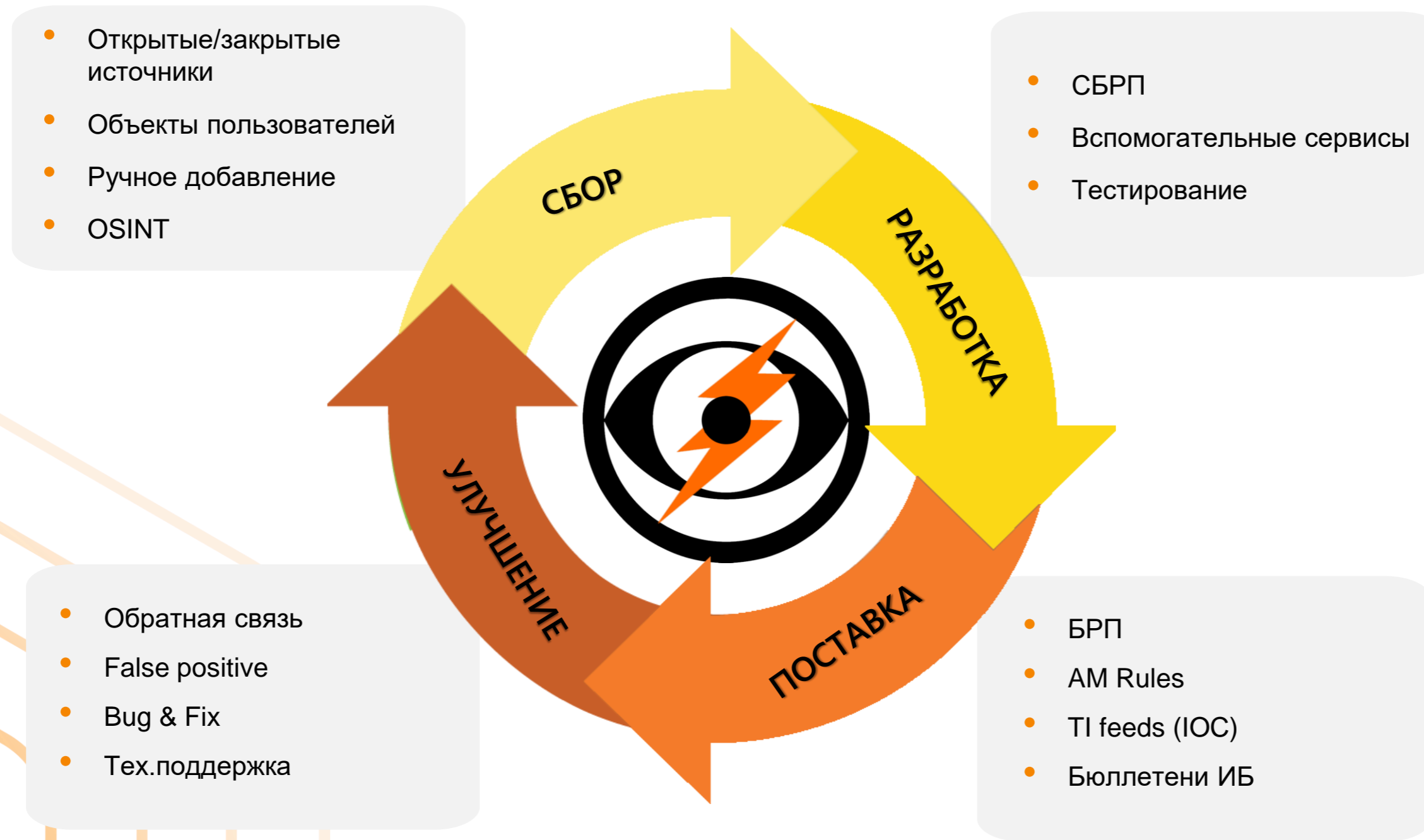
# Направление **исследования киберугроз**



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

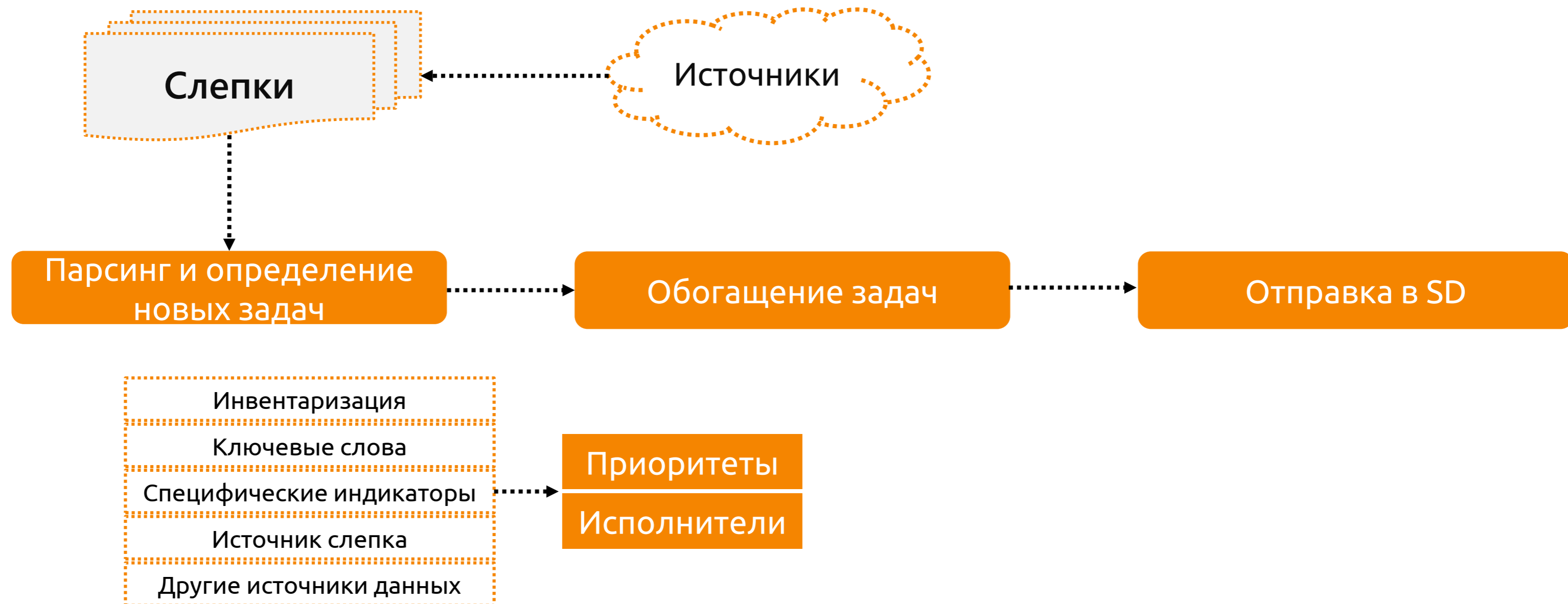
# Процесс разработки правил





# 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

Группа exploit Автор правила [dropdown]  
Группа ТИА attacks Classify [icon]  
CVE 2023-33532 2023-33533  
MITRE ATT&CK T1190 - Exploit Public-Facing Application

Исходный текст

```
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"AM EXPLOIT NETGEAR Multiple Products Multiple OS Command Injection (CVE-2023-33532, CVE-2023-33533)"; flow:established,to_server; content:"POST"; content:"/ipv6_fix.cgi?"; http_uri; content:"id="; http_uri; distance:0; content:"ipv6_wan_ipaddr"; http_client_body; fast_pattern:only; flowbits:isset,AM.Generic.command_injection; reference:url,github.com/D2y6p/CVE/blob/main/Netgear/CVE-2023-33532; reference:cve,2023-33532; classtype:application-attack; sid:3252856; rev:1; metadata: affected_asset dst, affected_os Unix, affected_product netgear:d6220, affected_product netgear:d8500, affected_product netgear:d8500_firmware, affected_product netgear:r6250, affected_product netgear:r6250_firmware, affected_product netgear:r6700, affected_product netgear:r6700_firmware, affected_product netgear:r6900, affected_product netgear:r6900_firmware, affected_vendor netgear, attack_target Networking_Equipment, attack_target Web_Server, tag T1190, tias_category Exploitation;)
```

Исходный текст (suricata)

```
alert http any any -> $HOME_NET any (msg:"AM EXPLOIT NETGEAR Multiple Products Multiple firmware OS Command Injection (CVE-2023-33532, CVE-2023-33533)"; flow:established,to_server; content:"POST"; http_method; content:"/ipv6_fix.cgi?"; http_uri; content:"id="; distance:0; http_uri; content:"ipv6_wan_ipaddr"; http_client_body; flowbits:isset,AM.Generic.command_injection; reference:cve,2023-33532; reference:url,github.com/D2y6p/CVE/blob/main/Netgear/CVE-2023-33532; reference:cve,2023-33533; classtype:web-application-attack; sid:3252856; rev:1; metadata: affected_asset dst, affected_os Unix, affected_product netgear:d6220, affected_product netgear:d6220_firmware, affected_product netgear:d8500, affected_product netgear:d8500_firmware, affected_product netgear:r6250, affected_product netgear:r6250_firmware, affected_product netgear:r6700, affected_product netgear:r6700_firmware, affected_product netgear:r6900, affected_product netgear:r6900_firmware, affected_vendor netgear, attack_target Networking_Equipment, attack_target Web_Server, tag T1190, tias_category Exploitation;)
```

**Короткое описание**  
Правило реагирует на попытку эксплуатации уязвимости внедрения команд ОС в NETGEAR множественных продуктов со множеством прошивок

**Описание правила**  
Уязвимость заключается в недостаточной проверке данных и позволяет использовать команды ОС в передаваемом параметре 'ipv6\_wan\_ipaddr', что приведет к исполнению внедренных команд на маршрутизаторе

Для эксплуатации уязвимости удаленный злоумышленник должен отправить специально сформированный POST-запрос к уязвимому конечному адресу '/ipv6\_fix.cgi'. Тело запроса должно содержать параметр 'ipv6\_wan\_ipaddr' со внедренными командами ОС

Уязвимые продукты и версии прошивок:  
- R6250 с версией прошивки до 1.0.4.48 включительно  
- D6220 с версией прошивки до 1.0.0.80 включительно  
- D8500 с версией прошивки до 1.0.3.60 включительно  
- R6700 с версией прошивки до 1.0.2.26 включительно  
- R6900 с версией прошивки до 1.0.2.26 включительно

Критичность Высокая Тип атаки Эксплуатация уязвимостей (vulnerabilities) Название платформы [dropdown]

affected_product	* netgear:d8500_firmware * netgear:r6250 * netgear:r6250_firmware * netgear:r6700 * netgear:r6700_firmware * netgear:r6900 * netgear:r6900_firmware
affected_vendor	* netgear
attack_target	* Networking_Equipment * Web_Server
tag	* T1190
tias_category	* Exploitation

Референсы

Ключ	Значение
cve	2023-33532
url	github.com/D2y6p/CVE/blob/main/Netgear/CVE-2023-33532
cve	2023-33533

Рсар [input] Детектировать [checkbox checked] Snort [checkbox checked] Suricata [checkbox checked]

CVE-2023-33532\_CVE-2023-33533.pcap [play icon]

































# Система БРП: поддержка продуктов

IDS NS | Правила | Профилирование | Сравнить БРП | Сборка NS 1687: Подтвержден ✓ | Сборка xF 1037: Подтвержден ✓ | Сборка HW 133: Подтвержден

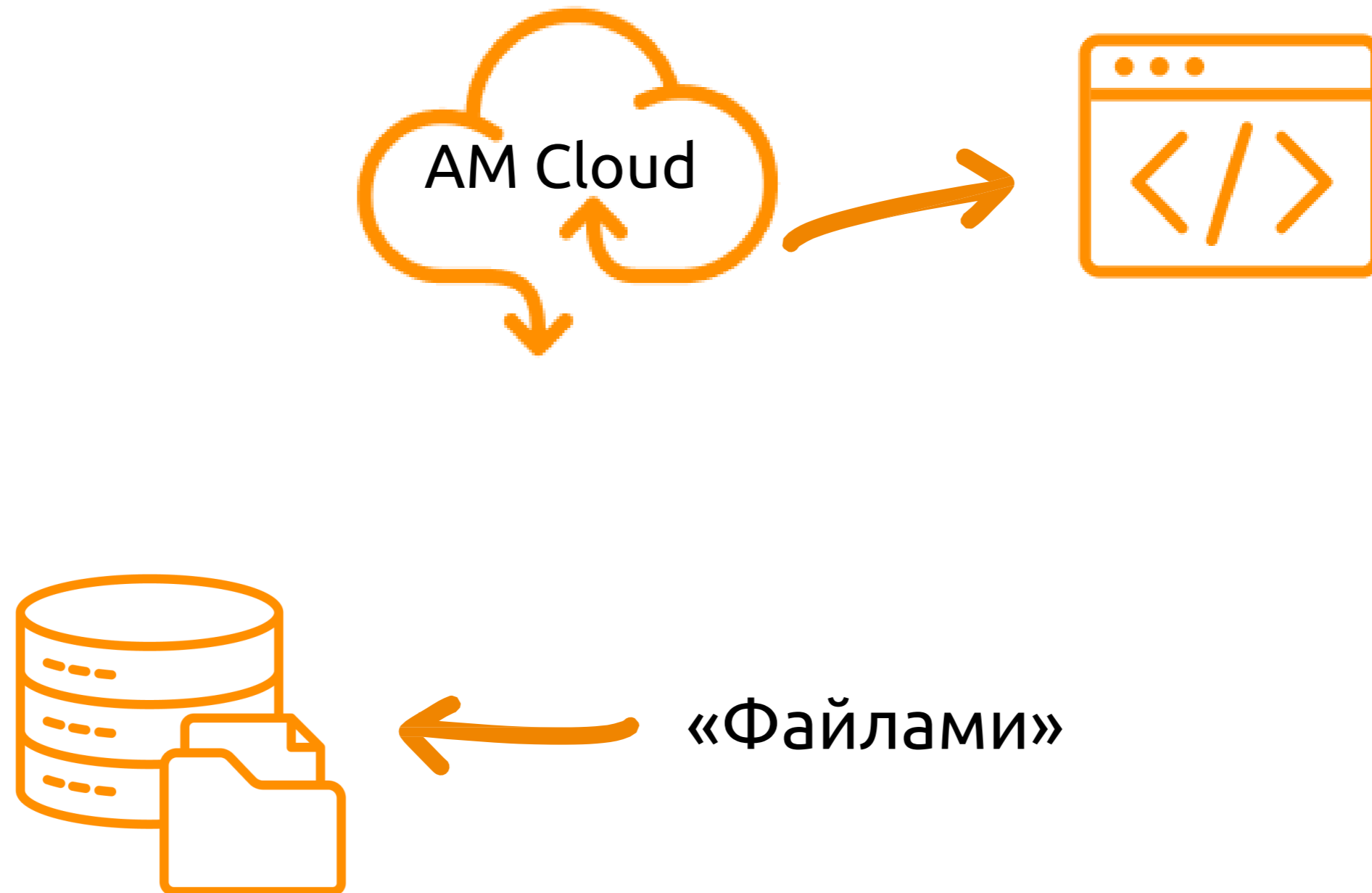
### Сборка NS

Подтвердить ✓ | Пересобрать ↻ | Создать +

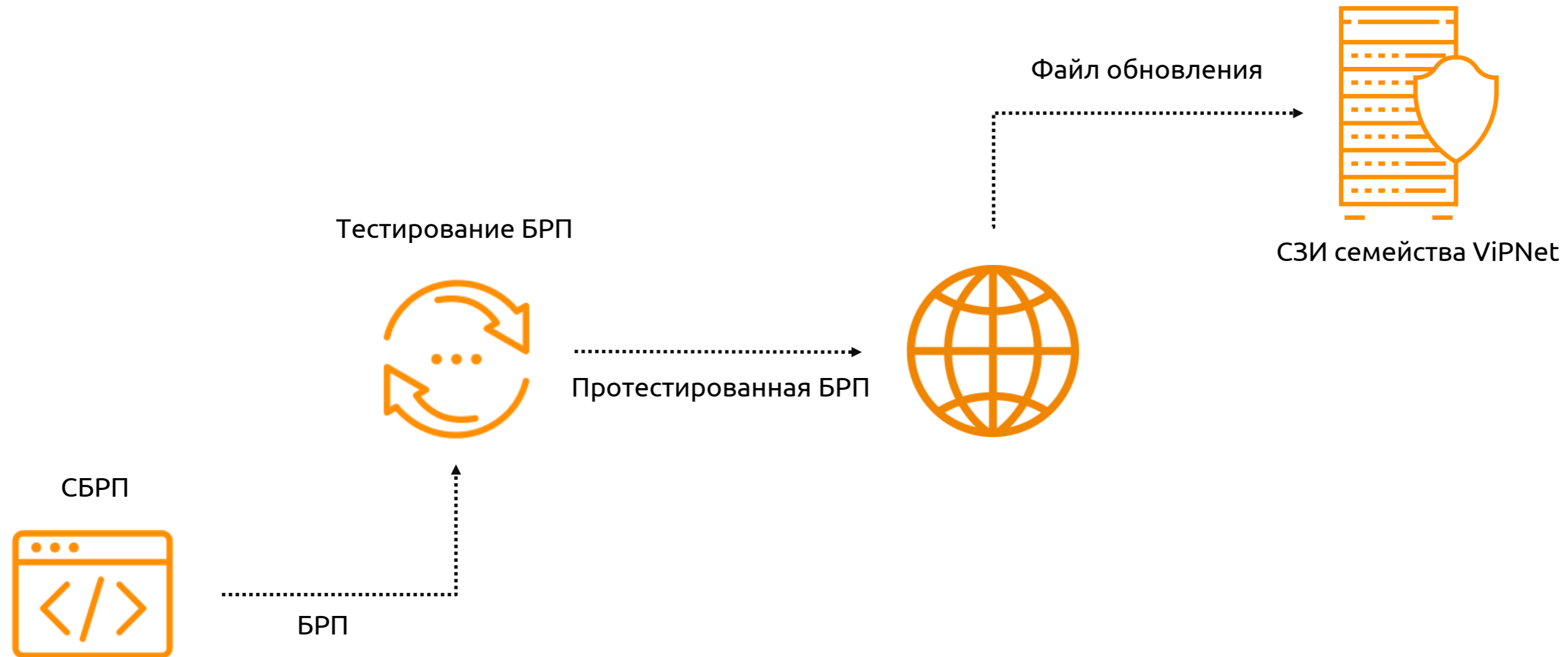
Правил с неизвестными метаданными: 0 | Геоданные: ✓ | Обновление FTP: **загружено**

Версия	Дата изменения	Статус	Сборки	Файлы
1689	05.12.23 18:20	Ожидается подтверждение	eas	 changelog(suricata)  changelog(without pipeline)  ver.3.8  ver.3.8-test  tests    ver.3.8-scada  ver.3.10  ver.3.6-scada
				 ver.3.9  ver.3.0  ver.3.1  ver.3.2  ver.3.3  ver.3.4  ver.3.5  ver.3.6  tests    changelog
				 ver.3.7  tests    suricata_adv  suricata   snort

# Способы доставки AM Rules



# Способы доставки БРП



# БРП АО «ПМ» в цифрах

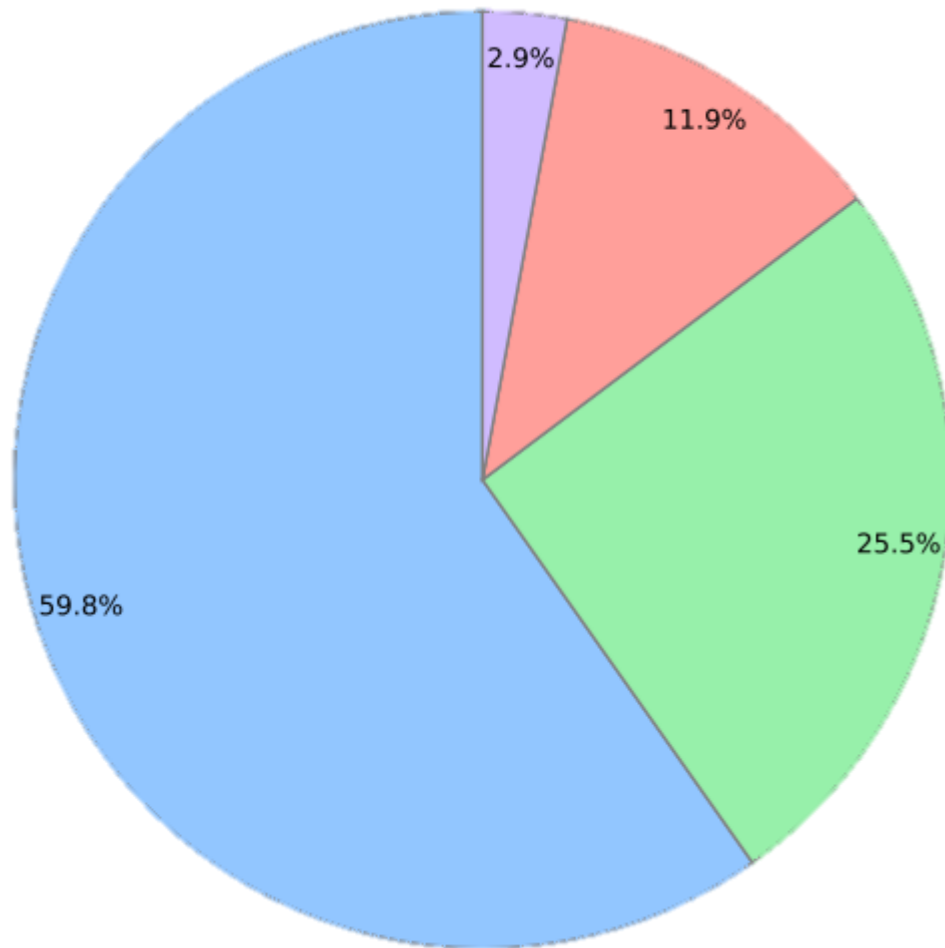


Snort / Suricata / YARA / OSSEC  
> 400 000 правил/сигнатур

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

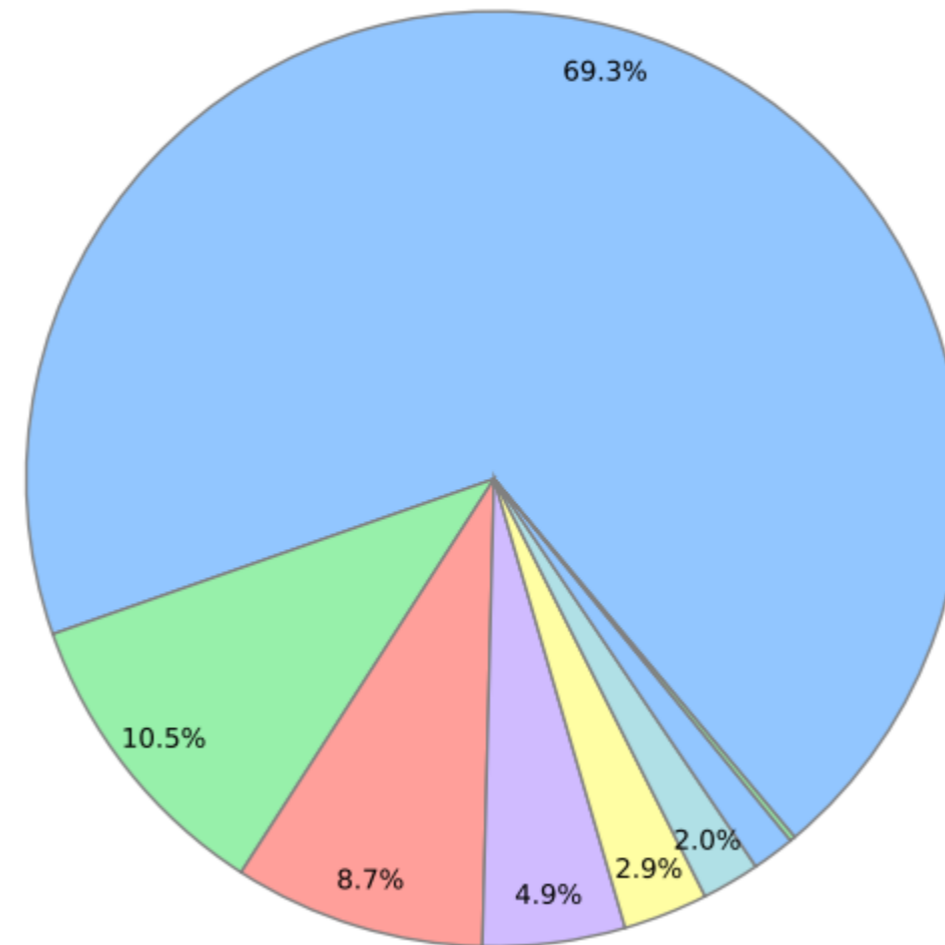
# БРП АО «ПМ» в цифрах: IDS NS

Распределение правил по группам угроз



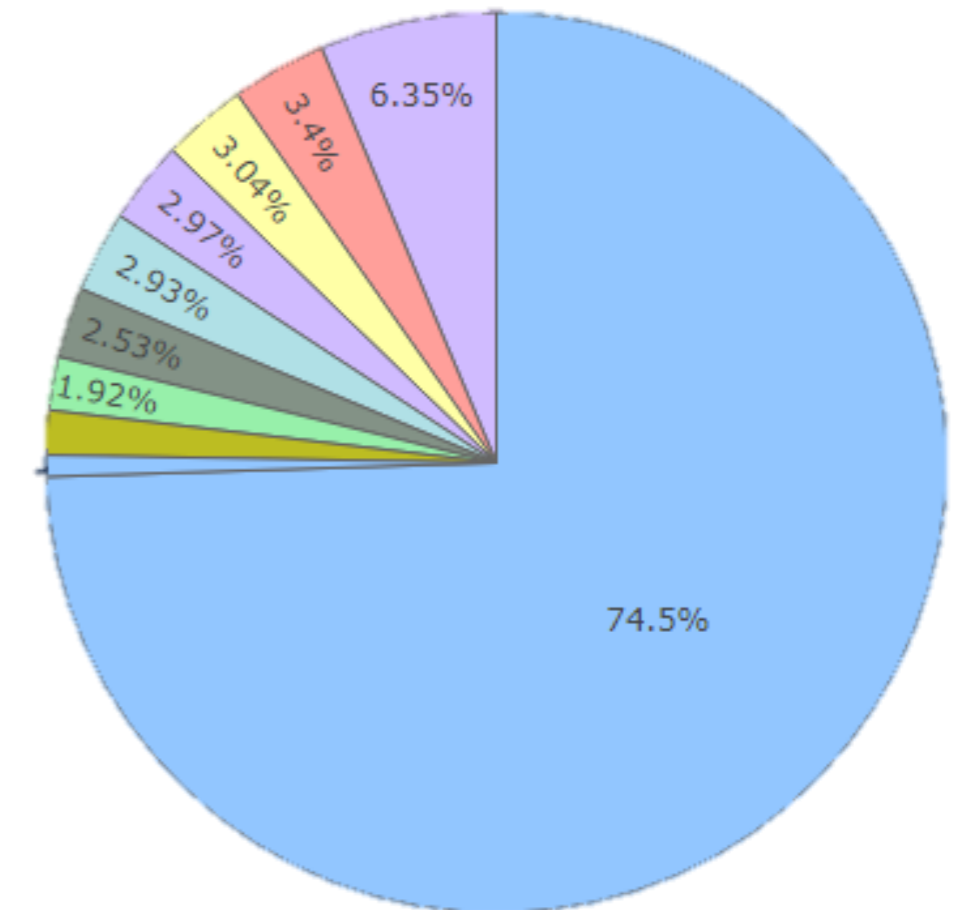
Others, 59.8%	29887
TROJAN, 25.5%	12732
EXPLOIT, 11.9%	5927
MALWARE, 2.9%	1446

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

<input type="checkbox"/>	Статус	Тип	Доступные опции	Актуальность
<input type="checkbox"/>	Не отправлена	TIAS	Обновление ПО, Обновление экспертных данных	Актуальна
<input type="checkbox"/>	Не отправлена	IDS NS	Обновление базы Malware detection, Обновление ПО, Обновление базы правил	Актуальна
<input type="checkbox"/>	Не отправлена	IDS HS	Обновление ПО, Обновление базы правил	Актуальна

- ✓ 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	<a href="https://updateids.infotecs.ru/">https://updateids.infotecs.ru/</a>
Имя пользователя	1401947-1-3-TIAS
Пароль	(5cEPprP

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



# Сервер обновлений

ViPNet Update Server

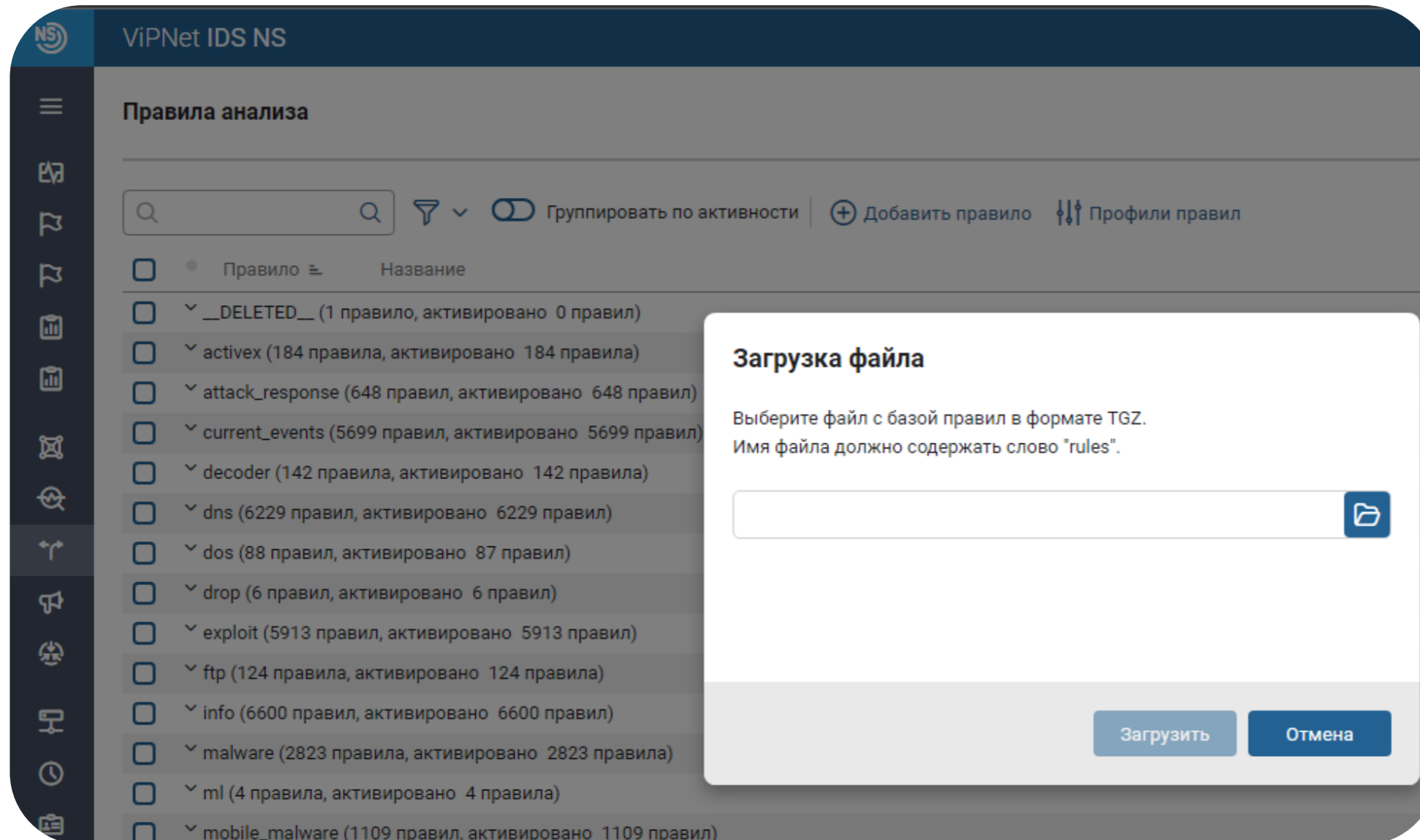
Обновления для ViPNet IDS NS

Базы правил   Базы Malware detection

Поиск обновления  С любой датой создания  Любая версия ПО

Файл обновления	Версия	Дата создания	Размер	Совместимые верси...	SHA1
<a href="#">rules.20231206-151035_eac_ver.3.8.tgz</a>	1690	06.12.2023	27 Мбайт	3.8	dc09b53a854bb176f23945092d27c6e282285f1b
<a href="#">rules.20231206-150820_eac_ver.3.9.tgz</a>	1690	06.12.2023	27 Мбайт	3.9	f86dc825f3fcebc49c3b12b8ddb09ea149ee21ef
<a href="#">rules.20231206-150754_eac_ver.3.0.tgz</a>	1690	06.12.2023	27.16 Мбайт	3.0	eb3783774fc2baa72b8909821d4ddf81cc7f817e
<a href="#">rules.20231206-150727_eac_ver.3.1.tgz</a>	1690	06.12.2023	27.16 Мбайт	3.1	97298f2c10dd3179c779e114121135c2f9352bee
<a href="#">rules.20231206-150702_eac_ver.3.2.tgz</a>	1690	06.12.2023	27 Мбайт	3.2	4ff49fc92232d61c6156cf1bf0f489b07766b9e3
<a href="#">rules.20231206-150636_eac_ver.3.3.tgz</a>	1690	06.12.2023	27 Мбайт	3.3	f9443f64a948395c7519b692312cb8453fc0c842
<a href="#">rules.20231206-150610_eac_ver.3.4.tgz</a>	1690	06.12.2023	27 Мбайт	3.4	28ea546b2b210c7a67d167e7fea5577e369829c1
<a href="#">rules.20231206-150544_eac_ver.3.5.tgz</a>	1690	06.12.2023	27 Мбайт	3.5	b77e05ae908e1034805837fbc11f26987ca56190
<a href="#">rules.20231206-150517_eac_ver.3.6.tgz</a>	1690	06.12.2023	27 Мбайт	3.6	c4d20947c21d78634cb9ca296468f2d1fca9ac81
<a href="#">rules.20231206-150436_eac_ver.3.7.tgz</a>	1690	06.12.2023	27 Мбайт	3.7	36a6cdf7237ca402e4efd359a504883fd8b0130
<a href="#">rules.20231205-150943_eac_ver.3.8.tgz</a>	1689	05.12.2023	25.78 Мбайт	3.8	1bb5c17f4ec17564c652ac66442e5b7cc6b27025
<a href="#">rules.20231205-150735_eac_ver.3.9.tgz</a>	1689	05.12.2023	25.78 Мбайт	3.9	3f5d7c1d6548994449e4a1aef963326e703422f7
<a href="#">rules.20231205-150711_eac_ver.3.0.tgz</a>	1689	05.12.2023	25.93 Мбайт	3.0	92c9cc28fb97a558811b5bc9af29ea0654e8ffdf
<a href="#">rules.20231205-150646_eac_ver.3.1.tgz</a>	1689	05.12.2023	25.93 Мбайт	3.1	3e870b51b654640d1969d1433e99d81954244183
<a href="#">rules.20231205-150622_eac_ver.3.2.tgz</a>	1689	05.12.2023	25.77 Мбайт	3.2	7e0d4b0f234798d7a92650f13933f086dda52b9d
<a href="#">rules.20231205-150558_eac_ver.3.3.tgz</a>	1689	05.12.2023	25.77 Мбайт	3.3	103f11c1d09a45d75612c51b9b303d99a955424b
<a href="#">rules.20231205-150535_eac_ver.3.4.tgz</a>	1689	05.12.2023	25.77 Мбайт	3.4	1d7c0b494bf2a0d548ac00e4d73e49681497c664
<a href="#">rules.20231205-150512_eac_ver.3.5.tgz</a>	1689	05.12.2023	25.77 Мбайт	3.5	82bed4b3f41d9ab03c803e31488750280ebe16eb
<a href="#">rules.20231205-150448_eac_ver.3.6.tgz</a>	1689	05.12.2023	25.78 Мбайт	3.6	9060762bb9b24be6c4a4470a24ad3e391d995c5f

# Загрузка правил в продуктах



**ViPNet IDS NS**

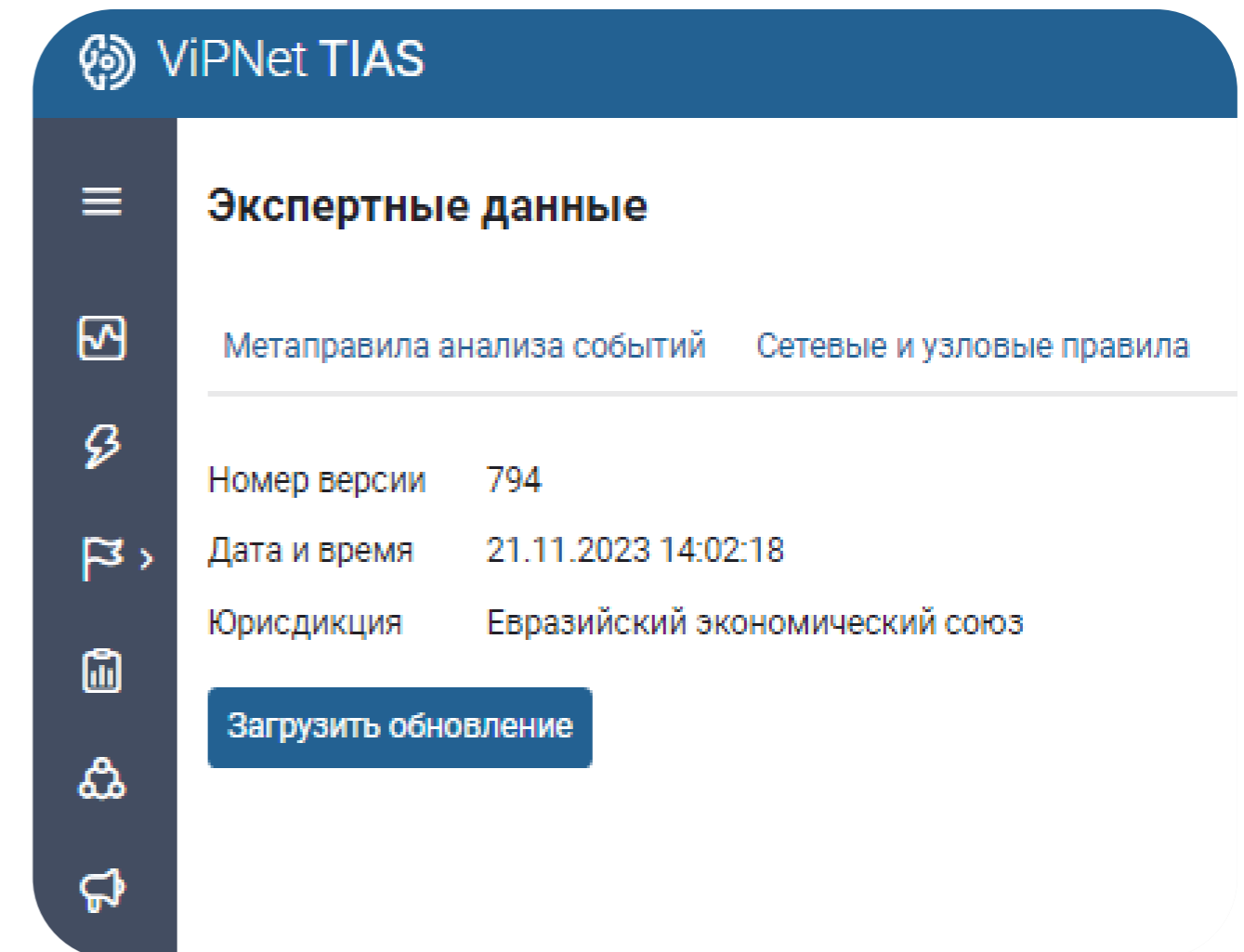
Правила анализа

Поиск:  | Фильтр:  | Группировать по активности:  | Добавить правило:  | Профили правил:

<input type="checkbox"/>	Правило	Название
<input type="checkbox"/>	__DELETED__	(1 правило, активировано 0 правил)
<input type="checkbox"/>	activex	(184 правила, активировано 184 правила)
<input type="checkbox"/>	attack_response	(648 правил, активировано 648 правил)
<input type="checkbox"/>	current_events	(5699 правил, активировано 5699 правил)
<input type="checkbox"/>	decoder	(142 правила, активировано 142 правила)
<input type="checkbox"/>	dns	(6229 правил, активировано 6229 правил)
<input type="checkbox"/>	dos	(88 правил, активировано 87 правил)
<input type="checkbox"/>	drop	(6 правил, активировано 6 правил)
<input type="checkbox"/>	exploit	(5913 правил, активировано 5913 правил)
<input type="checkbox"/>	ftp	(124 правила, активировано 124 правила)
<input type="checkbox"/>	info	(6600 правил, активировано 6600 правил)
<input type="checkbox"/>	malware	(2823 правила, активировано 2823 правила)
<input type="checkbox"/>	ml	(4 правила, активировано 4 правила)
<input type="checkbox"/>	mobile_malware	(1109 правил, активировано 1109 правил)

### Загрузка файла

Выберите файл с базой правил в формате TGZ.  
Имя файла должно содержать слово "rules".



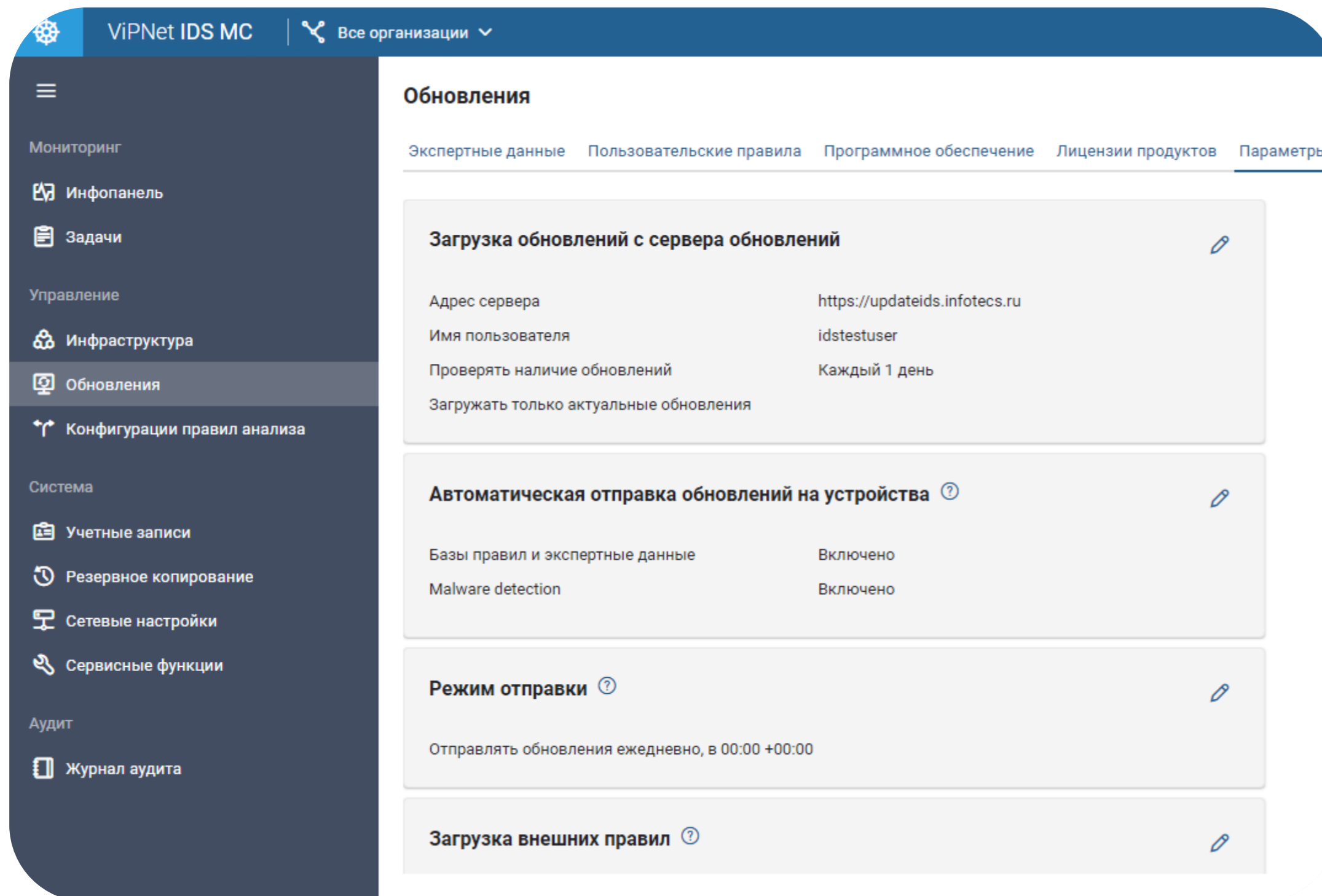
**ViPNet TIAS**

Экспертные данные

Метаправила анализа событий | Сетевые и узловые правила

Номер версии	794
Дата и время	21.11.2023 14:02:18
Юрисдикция	Евразийский экономический союз

# Автоматическое обновление баз правил



The screenshot shows the 'Обновления' (Updates) section of the ViPNet IDS MC interface. The left sidebar contains navigation items: Мониторинг, Инфопанель, Задачи, Управление, Инфраструктура, Обновления (highlighted), Конфигурации правил анализа, Система, Учетные записи, Резервное копирование, Сетевые настройки, Сервисные функции, Аудит, and Журнал аудита. The main content area has tabs for 'Экспертные данные', 'Пользовательские правила', 'Программное обеспечение', 'Лицензии продуктов', and 'Параметры'. The 'Параметры' tab is active, showing several configuration cards:

- Загрузка обновлений с сервера обновлений**:
  - Адрес сервера: `https://updateids.infotecs.ru`
  - Имя пользователя: `idstestuser`
  - Проверять наличие обновлений: `Каждый 1 день`
  - Загружать только актуальные обновления
- Автоматическая отправка обновлений на устройства**:
  - Базы правил и экспертные данные: `Включено`
  - Malware detection: `Включено`
- Режим отправки**:
  - Отправлять обновления ежедневно, в 00:00 +00:00
- Загрузка внешних правил**

Использовать прокси-сервер

Тип прокси-сервера

HTTP (HTTP/1.1)

HTTP (HTTP/1.1)

HTTP (HTTP/1.0)

HTTPS

Socks 4

Socks 5

Socks 4A

Socks 5 Hostname

**Режим автоматической отправки обновлений**

- Отправлять обновления сразу после загрузки на ViPNet IDS MC
- Не отправлять обновления автоматически
- Отправлять обновления по расписанию

Время выполнения  в

# Только актуальные обновления



ViPNet IDS MC | Все организации

admin

### Обновления

Экспертные данные | Пользовательские правила | Программное обеспечение | Лицензии продуктов | Параметры

Загрузить файл | Удалить | Очистить

Удалить неактуальные обновления

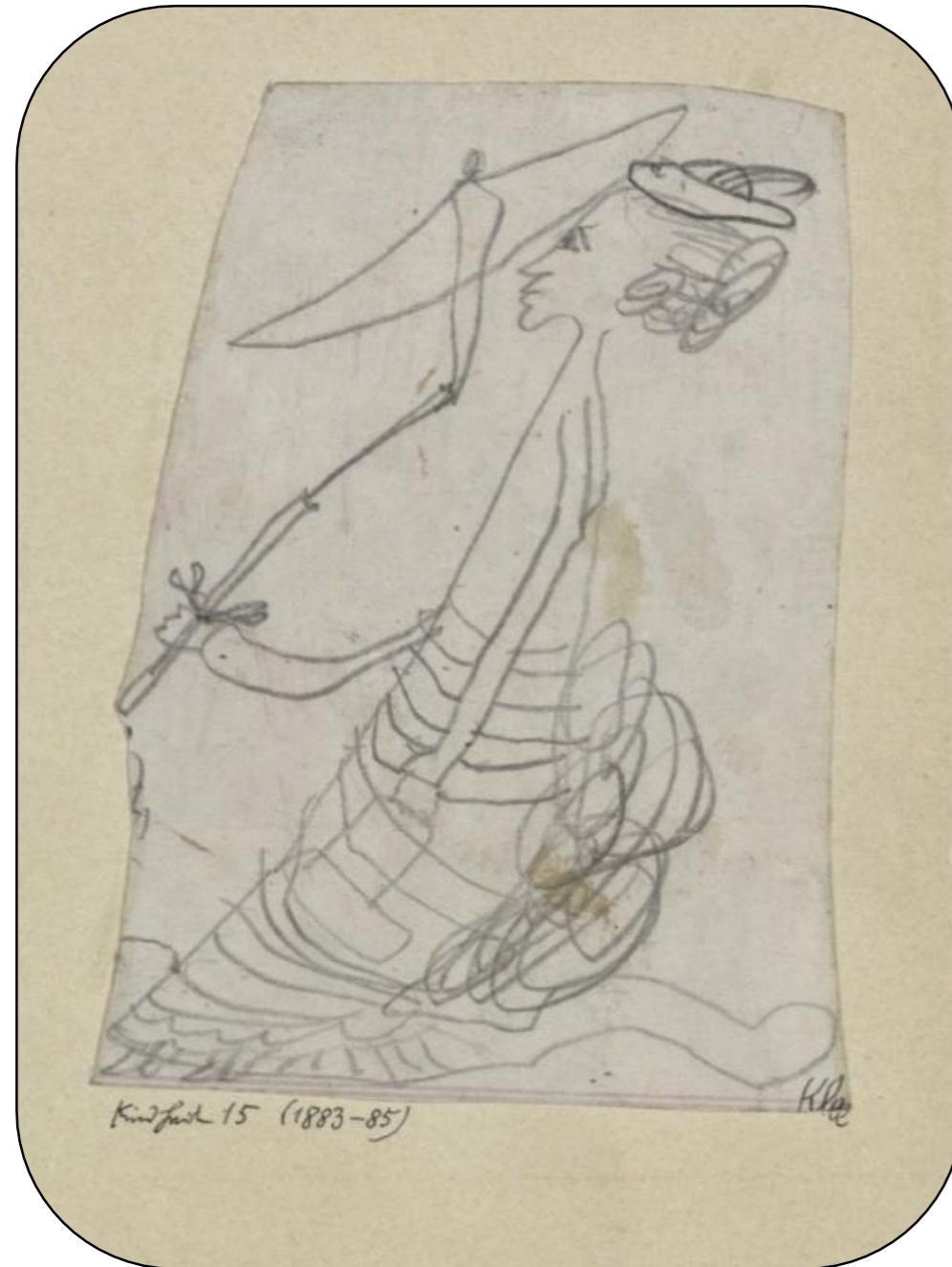
<input type="checkbox"/>	Дата создания	Тип	Версия обновления	Версии ПО	Источник	О...	Размер	Загружено
<input type="checkbox"/>	17:31:34 07.12.2023	TIAS	806	3.8, 3.8.0, 3.8.1	IDS MC		37.8 Мбайт	18:34:10 07.12.2023
<input type="checkbox"/>	05:07:16 07.12.2023	Malware detection IDS NS	5965	3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3....	IDS MC		9.4 Мбайт	16:33:16 07.12.2023
<input type="checkbox"/>	18:10:35 06.12.2023	IDS NS	1690	3.8	IDS MC		27.0 Мбайт	16:40:17 07.12.2023
<input type="checkbox"/>	18:08:20 06.12.2023	IDS NS	1690	3.9	IDS MC		27.0 Мбайт	16:40:33 07.12.2023
<input type="checkbox"/>	18:07:02 06.12.2023	IDS NS	1690	3.2	IDS MC		27.0 Мбайт	16:38:52 07.12.2023
<input type="checkbox"/>	18:06:36 06.12.2023	IDS NS	1690	3.3	IDS MC		27.0 Мбайт	16:39:08 07.12.2023
<input type="checkbox"/>	18:06:10 06.12.2023	IDS NS	1690	3.4	IDS MC		27.0 Мбайт	16:39:23 07.12.2023
<input type="checkbox"/>	18:05:44 06.12.2023	IDS NS	1690	3.5	IDS MC		27.0 Мбайт	16:39:39 07.12.2023
<input type="checkbox"/>	18:05:17 06.12.2023	IDS NS	1690	3.6	IDS MC		27.0 Мбайт	16:39:49 07.12.2023
<input type="checkbox"/>	18:04:36 06.12.2023	IDS NS	1690	3.7	IDS MC		27.0 Мбайт	16:40:05 07.12.2023
<input type="checkbox"/>	15:38:26 06.12.2023	TIAS	805	3.8, 3.8.0, 3.8.1	IDS MC		37.7 Мбайт	16:37:38 06.12.2023
<input type="checkbox"/>	15:38:23 06.12.2023	TIAS	805	3.7.0, 3.7, 3.7.1	IDS MC		44.0 Мбайт	16:37:11 06.12.2023
<input type="checkbox"/>	15:38:20 06.12.2023	TIAS	805	3.5.0, 3.5, 3.5.1, 3.6, 3.6.0, ...	IDS MC		43.9 Мбайт	16:36:41 06.12.2023
<input type="checkbox"/>	15:38:17 06.12.2023	TIAS	805	3.3, 3.3.1	IDS MC		8.6 Мбайт	16:35:51 06.12.2023
<input type="checkbox"/>	15:38:14 06.12.2023	TIAS	805	3.4, 3.4.1	IDS MC		43.9 Мбайт	16:36:15 06.12.2023

Страница 1

Показывать 100 объектов

# 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



## Точно

- Меньше ложно-положительных срабатываний;
- Адаптированные правила



## Оптимально

- Снижение нагрузки на сенсор



## Сложно

- Есть квалифицированные специалисты, которые понимают что делают

# Управление профилями

## Профили правил

Использовать профили правил

Профили помогут вам адаптировать список активных правил анализа сенсора под вашу защищаемую сеть и используемые в ней сервисы, что позволит более качественно выявлять атаки и угрозы, минимизирует количество ложных срабатываний, а также повысит эффективность работы сенсора. Пожалуйста, активируйте профили для защиты систем и сервисов вашей сети в соответствии с описаниями (правила, не входящие в профили, останутся без изменений).

АСУТП

Профиль содержит специфические правила, детектирующие атаки на различное промышленное оборудование и их протоколы (Siemens, Schneider electric, MODBUS и т.д).

Клиент-серверное ПО

Профиль содержит специфические правила, детектирующие атаки на различное клиент-серверное ПО, которое нельзя четко разграничить на клиентский или серверный профиль.

DNS-серверы

Профиль содержит специфические правила, детектирующие атаки на различные DNS серверы.

Мобильные устройства

Данный профиль необходим для защиты мобильных устройств в сети. Профиль содержит правила для операционных систем iOS, Android, а также правила, специфичные для мобильных приложений.

Рабочие станции

Профиль содержит правила, специфичные для защиты рабочих станций (под управлением ОС семейств Windows, Linux, macOS), а также пользовательских приложений.

Почтовые серверы

Профиль активирует правила для обнаружения атак на почтовые серверы использующие протоколы smtp, imap, pop3

Сохранить

Отмена

## Профили правил

Использовать профили правил

Профили помогут вам адаптировать список активных правил анализа сенсора под вашу защищаемую сеть и используемые в ней сервисы, что позволит более качественно выявлять атаки и угрозы, минимизирует количество ложных срабатываний, а также повысит эффективность работы сенсора. Пожалуйста, активируйте профили для защиты систем и сервисов вашей сети в соответствии с описаниями (правила, не входящие в профили, останутся без изменений).

Профиль необходимо активировать при эксплуатации в защищаемой сети веб-серверов и веб-платформ, таких как SharePoint, nginx, Apache Tomcat и многих других. Профиль задействует правила, специфичные для атак на веб серверы и встроенные в них базы данных.

Устройства интернета вещей

Профиль содержит специфические правила, детектирующие атаки на различные устройства интернета вещей и протоколы работы с ними.

Сетевое оборудование

Профиль содержит правила, детектирующие атаки на различное сетевое оборудование типа «коммутатор», «маршрутизатор» (Cisco, D-Link и прочие).

IP-телефония

Профиль содержит специфические правила, детектирующие атаки на оборудование и протоколы IP-телефонии.

Файловые хранилища

Профиль содержит специфические правила, детектирующие атаки на различные файловые хранилища и протоколы работы с ними (TFTP, FTP и т.д).

Серверы

Профиль содержит специфические правила, детектирующие атаки на различное серверное оборудование и ПО по управлению/конфигурации, не вошедшее в другие группы.

Серверы баз данных

Профиль содержит правила, детектирующие атаки на различные базы данных: MS SQL, PostgreSQL, MySQL и прочие.

SMB хранилища

Профиль необходимо задействовать при использовании в защищаемой сети файловых хранилищ на базе SMB протокола.

Сохранить

Отмена



# Управление конфигурациями



## Конфигурации правил анализа

Создать Удалить Показать различия

<input type="checkbox"/>	Название конфигурации правил	Дата изменения	Совместимость с версией ПО
<input type="checkbox"/>	Конфигурация 10:08:44 08.12.2023	10:10:48 08.12.2023	3.9
<input type="checkbox"/>	Конфигурация для Томского офиса	10:17:07 08.12.2023	3.8
<input checked="" type="checkbox"/>	Конфигурация Москва, тестовая инфраструктура	10:17:48 08.12.2023	3.9
<input type="checkbox"/>	Конфигурация для тестирования периметра	10:18:30 08.12.2023	3.9

## Конфигурация Москва, тестовая инфраструктура

Все группы правил Все правила Группа правил IDS MC

Новое правило Изменить ^ Удалить настройки

<input checked="" type="checkbox"/>	Наименование	Активность >	
<input checked="" type="checkbox"/>	_DELETED	Сохранение пакетов >	Включить
<input type="checkbox"/>	activex	Возможность переопределения >	Выключить
<input type="checkbox"/>	attack_response		
<input checked="" type="checkbox"/>	botcc		
<input type="checkbox"/>	chat		
<input checked="" type="checkbox"/>	ciarmy		
<input checked="" type="checkbox"/>	compromised		
<input checked="" type="checkbox"/>	current_events		

## Конфигурация Москва, тестовая инфраструктура

Дата последнего изменения 10:17:48 08.12.2023  
Совместимость с версией ПО 3.9

Элементы применения Результирующее множество

Элементы иерархии, к которым применена данная конфигурация правил

- Поиск Редактировать
- Gazprom
  - BP
  - Shell
  - IDS NS ip12

# Настройка правил в IDS NS

## Правила анализа

<input type="checkbox"/>	Правило	Название	Активность	Класс
<input type="checkbox"/>	2102043	GPL ATTACK_RESPONSE isakmp login failed	<input checked="" type="checkbox"/>	misc-activity
<input type="checkbox"/>	3097929	AM EXPLOIT Possible Credential Disclosure in Tiandy IPC/NVR 9.12.7	<input checked="" type="checkbox"/>	web-application-attack
<input type="checkbox"/>	3097930	AM EXPLOIT Possible Shell Upload in WordPress FileManager plugin	<input type="checkbox"/>	web-application-attack
<input type="checkbox"/>	3098807	AM EXPLOIT MantisBT < 2.3.0 Remote Code Execution via 'neato_tool' config option	<input checked="" type="checkbox"/>	web-application-attack
<input type="checkbox"/>	3100390	AM EXPLOIT MedDream PACS Server 6.8.3.751 PHP-shell Command Execution	<input checked="" type="checkbox"/>	web-application-attack
<input type="checkbox"/>	3107185	ET ATTACK_RESPONSE Backdoor reDuh http initiate	<input checked="" type="checkbox"/>	trojan-activity
<input type="checkbox"/>	3123822	ET ATTACK_RESPONSE Backdoor reDuh http tunnel	<input type="checkbox"/>	trojan-activity
<input type="checkbox"/>	3124316	AM ATTACK_RESPONSE Generic Request to .aspx shell on Exchange Server var 1	<input checked="" type="checkbox"/>	web-application-activity
<input type="checkbox"/>	3124318	AM ATTACK_RESPONSE Generic Request to .aspx shell on Exchange Server var 2	<input checked="" type="checkbox"/>	web-application-activity
<input type="checkbox"/>	3160445	ET ATTACK_RESPONSE Non-Local Burp Proxy Error	<input checked="" type="checkbox"/>	successful-admin
<input type="checkbox"/>	3201403	ET ATTACK_RESPONSE Output of id command from HTTP server	<input checked="" type="checkbox"/>	bad-unknown
<input type="checkbox"/>	3210705	ET ATTACK_RESPONSE Metasploit Meterpreter Registry Interation Detected	<input checked="" type="checkbox"/>	successful-user
<input type="checkbox"/>	3226949	ET ATTACK_RESPONSE r57 phpshell footer detected	<input checked="" type="checkbox"/>	web-application-activity
<input type="checkbox"/>	current_events (5699 правил, активировано 5699 правил)			
<input type="checkbox"/>	decoder (142 правила, активировано 142 правила)			
<input type="checkbox"/>	dns (6229 правил, активировано 6229 правил)			
<input type="checkbox"/>	dos (88 правил, активировано 87 правил)			
<input type="checkbox"/>	drop (6 правил, активировано 6 правил)			
<input type="checkbox"/>	exploit (5913 правил, активировано 5913 правил)			
<input type="checkbox"/>	ftp (124 правила, активировано 124 правила)			
<input type="checkbox"/>	info (6600 правил, активировано 6600 правил)			
<input type="checkbox"/>	malware (2823 правила, активировано 2823 правила)			

Применить изменения

Отменить изменения

## Правило AM ATTACK\_RESPONSE Generic Request to .aspx shell on Exchange Server var 1

Идентификатор: 3124316, группа: attack\_response

Идентификатор правила	3124316
Класс	web-application-activity
Уровень важности	Средний
Активность	Правило используется
Сохранение пакетов	Производится
Группа	attack_response
Название правила	AM ATTACK_RESPONSE Generic Request to .aspx shell on Exchange Server var 1
Описание	Правило обнаруживает ответную (вторичную) часть атаки (например, попытку запустить произвольный код на ранее взломанный ресурс или отправку команды управления на такой ресурс)
Включено в профили	Веб-серверы

Текст:

```
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg: "AM ATTACK_RESPONSE Generic Request to .aspx shell on Exchange Server var 1";flow: established,to_server;content: "/owa/auth/";http_uri;content: ".aspx";http_uri;distance: 0;flowbits: isset,AM.Generic.command_injection;reference: url,symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-exchange-server-protection;class type: web-application-activity;sid: 3124316;rev: 7;metadata: affected_asset dst, affected_product exchange, affected_product n/a, affected_vendor n/a, attack_target Web_Server, tag AM.ARMA, tag T1190, tias_category Exploitation)
```

Добавить тег

# Изменение правила в IDS NS

## Редактирование правила

Правило: AM ATTACK\_RESPONSE Generic Request to .aspx shell on Exchange Server var 1

[Конструктор](#) [Редактор](#)

Протокол	IP-адрес источника	Порт источника
<input type="text" value="tcp"/>	<input type="text" value="any"/>	<input type="text" value="any"/>
Направление	IP-адрес получателя	Порт получателя
<input type="text" value="-&gt;"/>	<input type="text" value="\$HOME_NET"/>	<input type="text" value="\$HTTP_PORTS"/>

Параметры правила:

msg	"AM ATTACK_RESPONSE Generic Request to .aspx shell on Exchange Server var 1"
flow	established,to_server
content	"/owa/auth/"
http_uri	
content	".aspx"
http_uri	
distance	0
flowbits	isset,AM.Generic.command_injection
reference	<input type="text" value="url"/> <input type="text" value="symantec-enterprise-blogs.security.com/blogs/threat-intelligence..."/>
classtype	web-application-activity
sid	3124316
rev	7
metadata	affected_asset dst, affected_product exchange, affected_product n/a, affected_vendor n/a, attack_target Web_Server, tag AM.ARMA, tag T1190, tias_category Exploitation

[+](#) Добавить параметр ▼

[Сохранить изменения](#) [Отменить](#)

## Добавление копии правила

Правило: AM ATTACK\_RESPONSE Generic Request to .aspx shell on Exchange Server var 2 (копия 3124318)

[Конструктор](#) [Редактор](#)

Правило

```
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg: "AM ATTACK_RESPONSE Generic Request to .aspx shell on Exchange Server var 2 (копия 3124318)";flow: established,to_server;content: "/ecp/auth/";http_uri;content: ".aspx";http_uri;distance: 0;flowbits: isset,AM.Generic.command_injection;reference: url,symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-exchange-server-protection;classtype: web-application-activity;rev: 8;metadata: affected_asset: dst : affected_product exchange : affected_product n/a : affected_vendor n/a : attack_target Web_Server : tag AM.ARMA : tag T1190 : tias_category Exploitation;sid: 4000000)
```

[Сохранить изменения](#) [Отменить](#)

# Работа с правилами в TIAS



## Экспертные данные

Метаправила анализа событий | Сетевые и узловые правила | Модель машинного обучения | Отчеты сканеров уязвимостей | Обновление экспертных данных

Создать метаправило | Загрузить пользовательские метаправила | Скачать таблицу

928 метаправил

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

# Пользовательские **метаправила**

## Метаправило анализа последовательности событий

Общие

Доступ к метаправилу

Объекты инфраструктуры

Условия срабатывания

Шаблон карточки инцидента

### \* Условия срабатывания

Добавьте от 2 до 10 звеньев анализируемых событий. Расположите звенья в порядке возникновения событий. Для срабатывания метаправила необходимо наличие хотя бы одного события из каждого звена.

Добавить звено

#### 1. Сетевые события

Пораженный актив      Получатель

Интервал выборки событий, с      0

Правила анализа на сенсорах

2 правила

1:3206898    AM SHELLCODE Microsoft Windows x86 Reverse Shell (MSF variant via UDP)

1:3207062    AM SHELLCODE Linux x86 Reverse Connect Stage via metasploit (UDP)

#### 2. Узловые события

Пораженный актив      Устройство

Интервал выборки событий, с      600

Правила анализа на сенсорах

4 правила

100107      Подозрение на обход UAC (exploiting environment variables)

100320      Обнаружен вредоносный объект Win32\_Exploit\_Agent\_NOW

## Экспертные данные

Метаправила анализа событий

Сетевые и узловые правила

+ Создать метаправило

Загрузить пользовательские мет

Критическое сетевое событие

Критическое узловое событие

Повторяющееся сетевое событие

Последовательность событий

Набор событий

Контроль доступа по GeolP

Testing "/esc/" in Microsoft Excel

53 copy 1

47 copy 1

77 copy 1

Provider class before sending a

Scanning detected the SMB (MS-17-010) violation copy 1

Сохранить

Отмена

# 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 срабатывания 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 3243817, 2025701). После установки сегодня базы правил 1668 на IDS правил за день примерно 20000,

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-адреса сервера мониторинга и сервер обновлений, сервер обновлений используется для доставки обновлений для приложений.

14, 3243816,

вы для сравнения

11:03

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/relations>).

Изменено 09:12



925470897-19...3077749.pcap

108 байт

09:12



1.20 КБ

Коллеги, всем привет!

Помогите разобраться в правильности детектирования:

## 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 срабатывание.

Просьба разобраться.

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

привет!

о, пожалуйста, по внесению корректировок в правила на IDS NS.

ключить определенный адрес, для которого не нужно это правило детектировать. Я добавил его но детектирование событий продолжается. Что делаю не так?)

08:23

Коллеги, добрый день!



IDS\_packet\_time-...pcap

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



IDS\_packet\_senso...pcap

517 байт

Коллеги, всем привет! Подскажите по правилу 3243120, похоже на фолс: в данных случаях в параметре log не передаются специальные символы " ' / @ = \* [ ] ( )

06:23



100...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»

AM Threat Intelligence Portal

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:N**  
**Объект уязвимости:** Класс Marshaller протокола OpenWire в Apache ActiveMQ  
**Требования к атакующему:** Удаленный неаутентифицированный  
**Максимальный результат атаки:** Удаленное исполнение кода

Правила/Сигнатуры

sid	Время изменения	Название	Группы	TTP
3220816	25.11.23 05:04	AM EXPLOIT Possible Microsoft Outlook NTLM-relay Attack via phishing e-mail (CVE-2023-23397)	exploit	T1566

Краткое описание: Правило реагирует на возможную попытку атаки NTLM Relay посредством фишингового письма, содержащего эксплуатацию уязвимости повышения привилегий в Microsoft Outlook

Полное описание: 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: \* |1f 85 00 00| - идентификатор параметра "PidLidReminderFileParameter" \* |1c 85 00 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"

Исходный текст: alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET [25,110,143,193,587,995] (msg:"AM EXPLOIT Possible Microsoft Outlook NTLM-relay Attack via phishing e-mail (CVE-2023-23397)"; flow:established,to\_server; content:"|1f 85 00 00|"; fast\_pattern; content:"|08 20 06 00 00 00 00 c0 00 00 00 00 00 46|"; distance:0; content:"|1c 85 00 00|"; content:"|02 20 06 00 00 00 00 00 00 00 00 00 46|"; distance:0; content:"|5c 00 5c 00|"; reference:cve,2023-23397; reference:url,msec.co.uk/2023/03/exploiting-cve-2023-23397-microsoft-outlook-elevation-of-privilege-vulnerability; reference:url,msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397; reference:url,github.com/sqrZeroKnowledge/CVE-2023-23397\_EXPLOIT\_0DAY/blob/main/HsgKitTestTool/AppointmentTest.cs; classtype:file-format; sid:3220816; rev:1; metadata: affected\_asset dst, affected\_os Windows, affected\_product microsoft:365\_apps, affected\_product microsoft:office, affected\_product microsoft:outlook, affected\_vendor microsoft, attack\_target Client\_Endpoint, attack\_target Mail\_Server, tag T1566, tias\_category Exploitation, tias\_category Phish;)

Критичность: Высокая  
Типы атаки: Эксплуатация уязвимостей  
Платформы: windows

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-

# 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 IoT



Интеграция с TI-платформой



Сервис инцидент-менеджмента



ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

**infotecs**

# Спасибо за внимание!



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



[infotecs.ru](https://infotecs.ru)

## Галкин Николай

Руководитель НИК  
«Перспективный мониторинг»

[nikolay.galkin@amonitoring.ru](mailto:nikolay.galkin@amonitoring.ru)

## Старовойт Светлана

Руководитель продуктового решения  
«ИнфоТеКС»

[starovoytsg@infotecs.ru](mailto:starovoytsg@infotecs.ru)