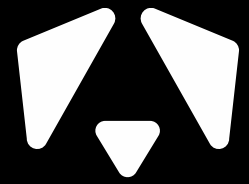
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Поисковые огни и лазерные прицелы



ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Автоматизация процесса киберразведки при производстве данных экспертизы для СЗИ

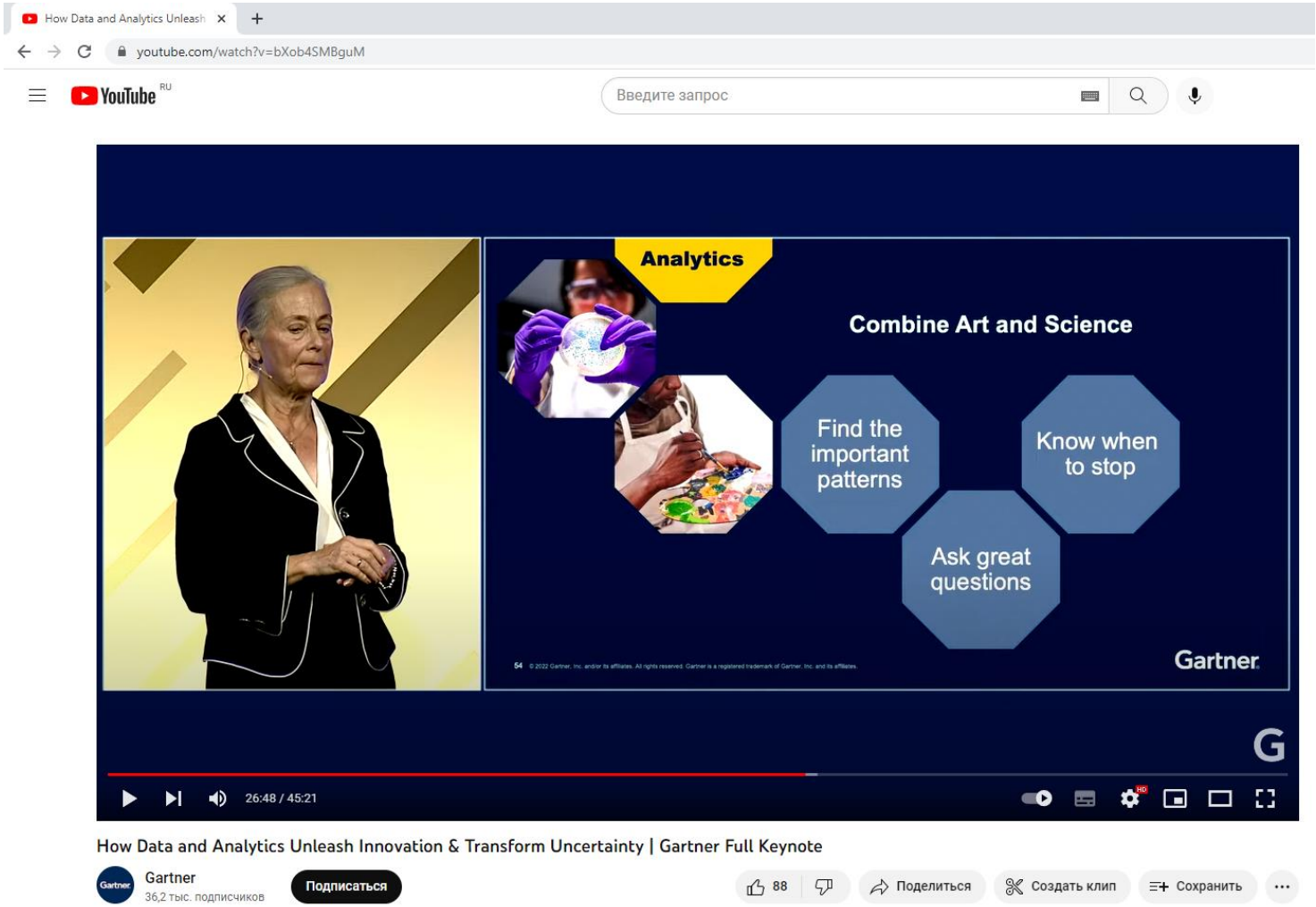
Александр Гусев

Руководитель направления исследования киберугроз

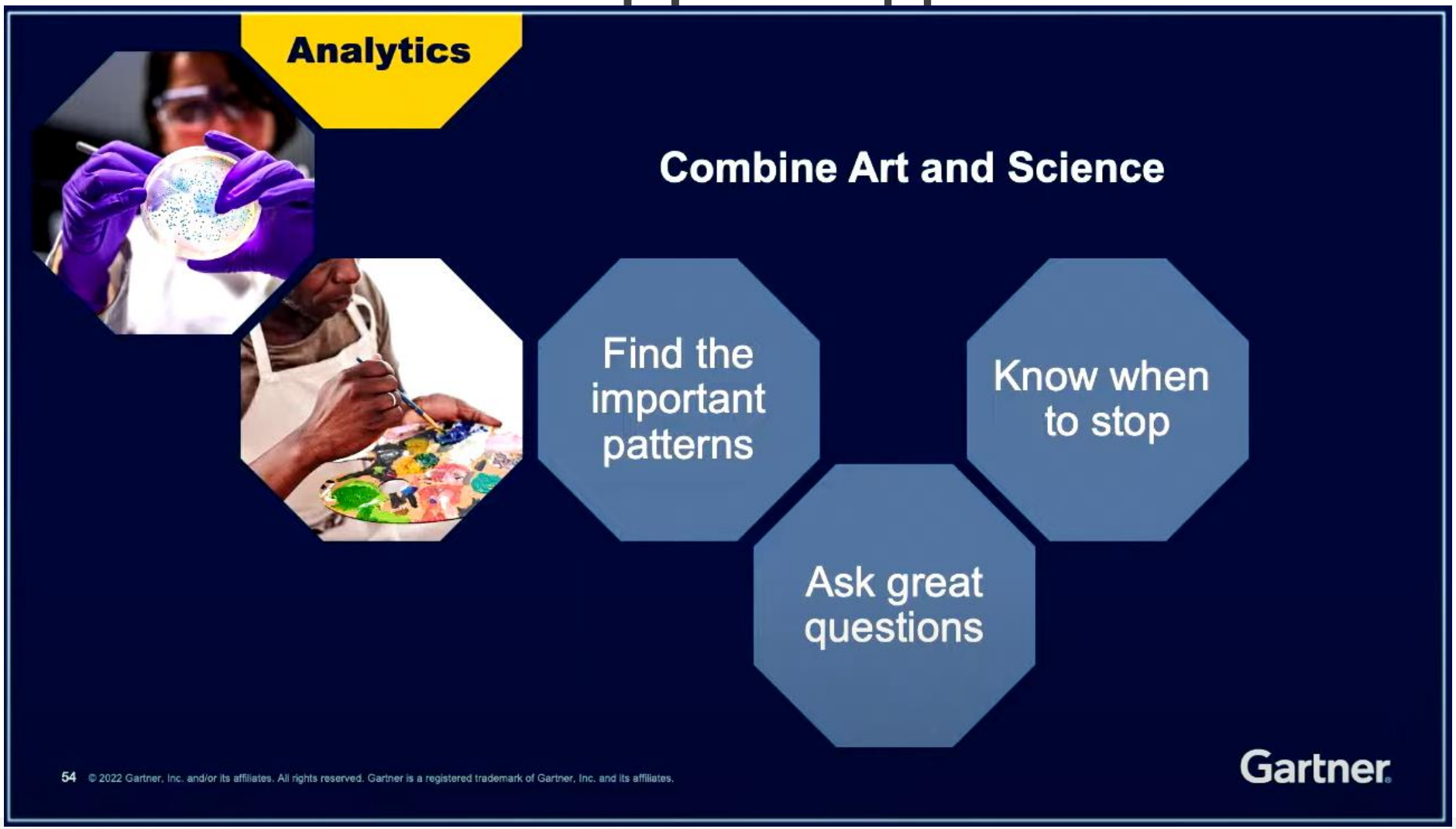
Почему именно сейчас интересна тема автоматической кибербразведки

- 817 наводок появилось в нашей системе за октябрь 2022 (39 на рабочий день)
- Если собирать меньше – можно что-то пропустить
- Если собирать столько же или больше – никаких людей без продвинутой аналитики не хватит

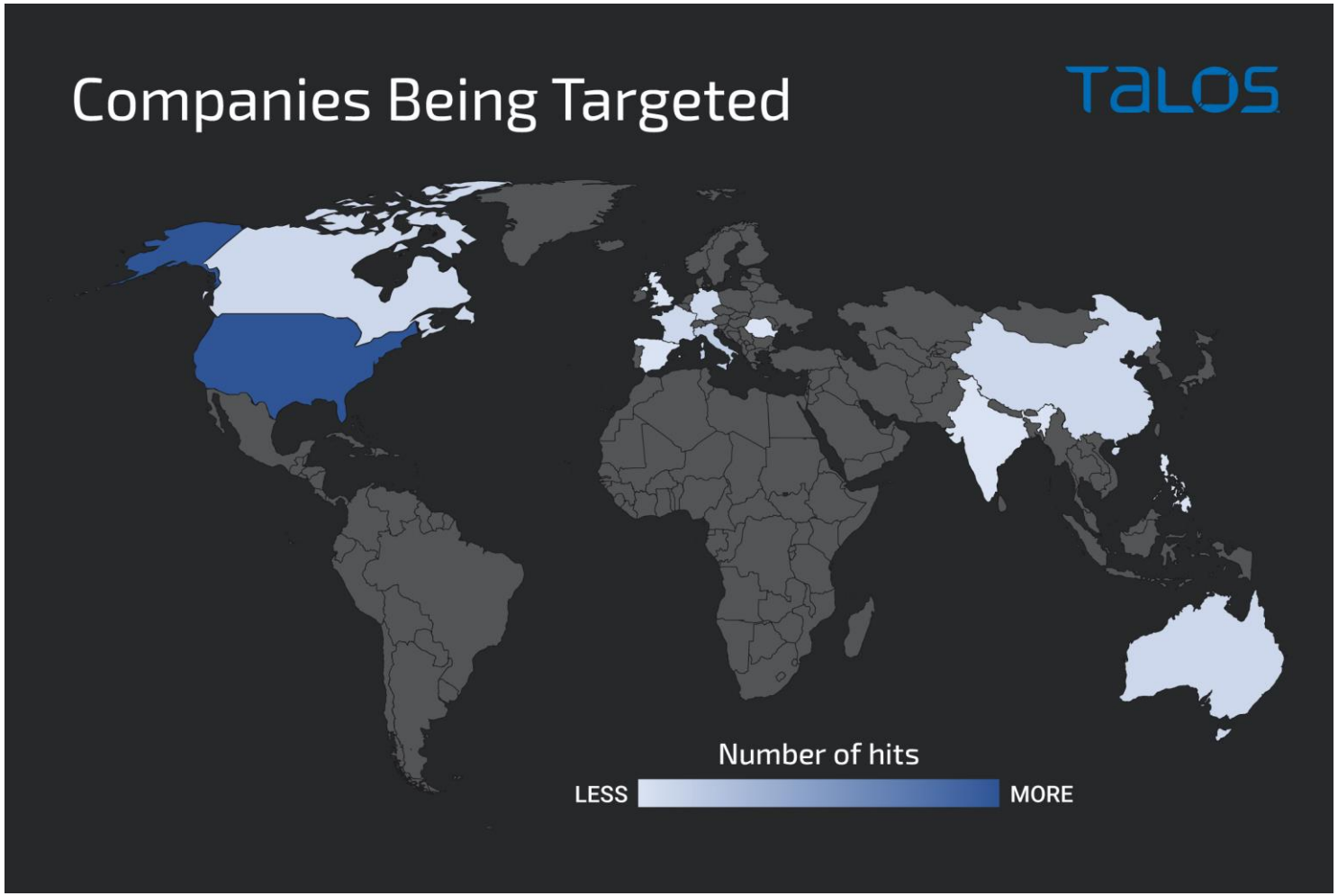
Почему именно сейчас интересна тема автоматической кибербразведки



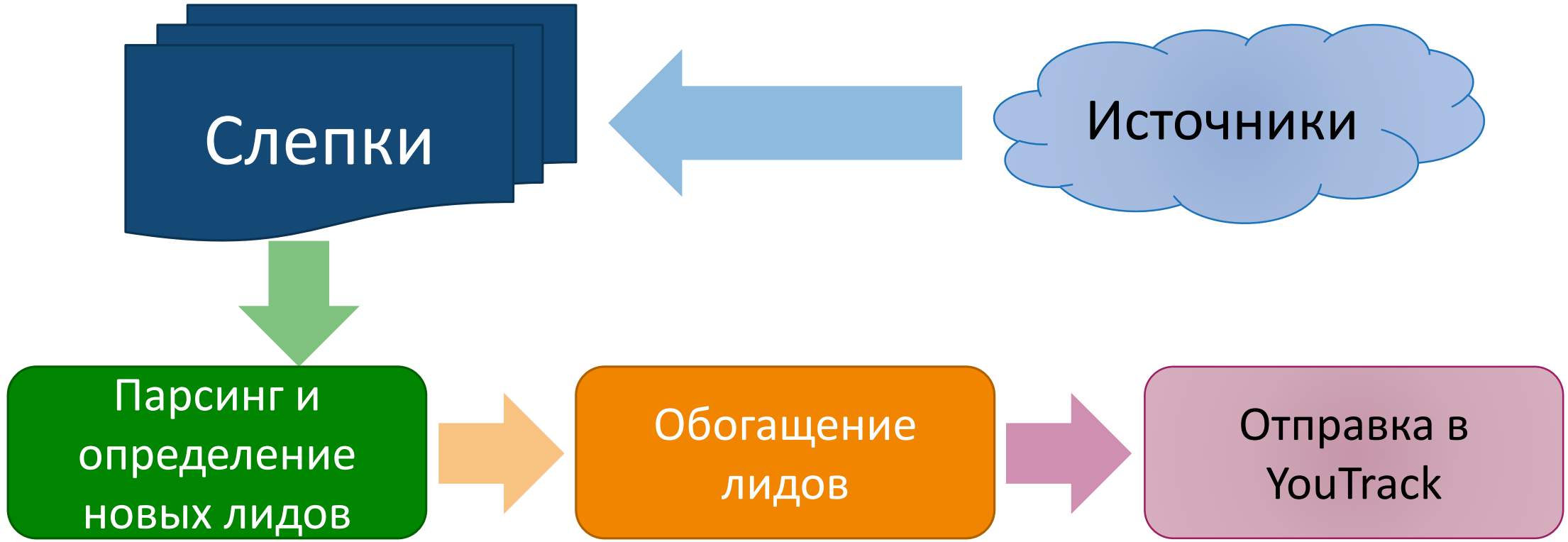
Почему именно сейчас интересна тема автоматической кибербразведки



Почему именно сейчас интересна тема автоматической кибербразведки



Пеллония – система сбора и обработки информации об угрозах, результат работы – автозаведённые в систему управления задачами YouTrack «лиды», или наводки


Слепки
Источники
Парсинг и определение новых лидов
Обогащение лидов
Отправка в YouTrack
Инвентаризация
Ключевые слова
Специфические индикаторы
Источник слепка
Другие источники данных
Приоритеты
Исполнители
Вызовы

Сбор информации

nvd_cve_2022-10-23_...	151 KB	23.10.2022
nvd_cve_2022-10-23_...	151 KB	23.10.2022
nvd_cve_2022-10-24_...	151 KB	24.10.2022
nvd_cve_2022-10-25_...	160 KB	25.10.2022
nvd_cve_2022-10-25_...	160 KB	25.10.2022
nvd_cve_2022-10-26_...	122 KB	26.10.2022
nvd_cve_2022-10-26_...	123 KB	26.10.2022
nvd_cve_2022-10-27_...	110 KB	27.10.2022
nvd_cve_2022-10-27_...	111 KB	27.10.2022
nvd_cve_2022-10-28_...	68 KB	28.10.2022
nvd_cve_2022-10-29_...	76 KB	29.10.2022
nvd_cve_2022-10-29_...	76 KB	29.10.2022
nvd_cve_2022-10-30_...	66 KB	30.10.2022
nvd_cve_2022-10-30_...	66 KB	30.10.2022
nvd_cve_2022-10-31_...	67 KB	31.10.2022

Парсинг

Available for: macOS Monterey 12.5 and later...

CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.x security vulnerabilities *Turritopsis Dohrnii Teo En Ming (Nov 07)*
Subject: CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.x
security vulnerabilities

Good day from Singapore,

Please refer to the following posts. The story is developing.

[1] OpenSSL Gives Heads Up to Critical Vulnerability Disclosure, Check
Point Alerts Organizations to Prepare Now
Link:
https://blog.checkpoint.com/2022/10/30/openssl-gives-heads-up-to-critical-vulnerability-disclosure-check-point-alerts-organizations-to-prepare-now/...

APPLE-SA-2022-10-27-15 Additional information for APPLE-SA-2022-10-24-7 Safari 16.1 *Apple Product Security via Fulldisclosure (Oct*

Парсинг

Beautiful Soup 4

```
def parse_seclists_fulldisc_html(html: str) -> List[Entry]:
    soup = get_html_soup(html)
    blockquote_set = soup("blockquote")
    latest_entries_raw = [latest_entry for latest_entry in blockquote_set
                          if latest_entry.attrs["id"] == "latest-fulldisclosure"]
    latest_entries = latest_entries_raw[0]
    entries = latest_entries("p", class_="excerpt")
    res = []
    for entry in entries:
        nameblock = entry('a')[0]
        name = filter_unprintable(nameblock.text)
        link = nameblock.attrs["href"]
        res.append(Entry({
            "name": name,
            "link": link
        }))
    return res
```

Парсинг

```
In [1]: import bs4

In [2]: from souparser import get_html_soup

In [3]: html = """<p class="excerpt"><strong><a href="https://seclists.org/fulldisclosure/2022/Nov/0">CVE-2022-3602 a
   ...: nd CVE-2022-3786 Critical OpenSSL 3.0.xsecurity vulnerabilities</a></strong><em>Turritopsis Dohrnii Teo En Mi
   ...: ng (Nov 07)</em><br/>Subject: CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.x<br/>security vulnerabili
   ...: ties<br/><br/>Good day from Singapore,<br/><br/>Please refer to the following posts. The story is developing.
   ...: <br/><br/>[1] OpenSSL Gives Heads Up to Critical Vulnerability Disclosure, Check<br/>Point Alerts Organizatio
   ...: ns to Prepare Now<br/>Link: <br/><a href="https://blog.checkpoint.com/2022/10/30/openssl-gives-heads-up-to-cr
   ...: itical-vulnerability-disclosure-check-point-alerts-organizations-to-prepare-now/" rel="nofollow">https://blog
   ...: .checkpoint.com/2022/10/30/openssl-gives-heads-up-to-critical-vulnerability-disclosure-check-point-alerts-org
   ...: anizations-to-prepare-now/</a>...<br/></p>"""

In [4]: soup = get_html_soup(html)

In [5]: nameblock = soup('a')[0]

In [6]: nameblock
Out[6]: <a href="https://seclists.org/fulldisclosure/2022/Nov/0">CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.
xsecurity vulnerabilities</a>

In [7]: name = nameblock.text

In [8]: name
Out[8]: 'CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.xsecurity vulnerabilities'
```

Парсинг

```
In [1]: import bs4

In [2]: from souparser import get_html_soup

In [3]: html = """<p class="excerpt"><strong><a href="https://seclists.org/fulldisclosure/2022/Nov/0">CVE-2022-3602 a
   ...: nd CVE-2022-3786 Critical OpenSSL 3.0.xsecurity vulnerabilities</a></strong><em>Turritopsis Dohrnii Teo En Mi
   ...: ng (Nov 07) </em><br/>Subject: CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0 x<br/>security vulnerabili
   ...: ties<br/><br/>Good day from Singapore,<br/><br/>Please refer to the following posts. The story is developing.
   ...: <br/><br/>[1] OpenSSL Gives Heads Up to Critical Vulnerability Disclosure, Check<br/>Point Alerts Organizatio
   ...: ns to Prepare Now<br/>Link: <br/><a href="https://blog.checkpoint.com/2022/10/30/openssl-gives-heads-up-to-cr
   ...: itical-vulnerability-disclosure-check-point-alerts-organizations-to-prepare-now/" rel="nofollow">https://blog
   ...: .checkpoint.com/2022/10/30/openssl-gives-heads-up-to-critical-vulnerability-disclosure-check-point-alerts-org
   ...: anizations-to-prepare-now/</a>...<br/></p>"""

In [4]: soup = get_html_soup(html)

In [5]: nameblock = soup('a')[0]

In [6]: nameblock
Out[6]: <a href="https://seclists.org/fulldisclosure/2022/Nov/0">CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.
xsecurity vulnerabilities</a>

In [7]: name = nameblock.text

In [8]: name
Out[8]: 'CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.xsecurity vulnerabilities'
```

Парсинг

```
In [1]: import bs4

In [2]: from souparser import get_html_soup

In [3]: html = """<p class="excerpt"><strong><a href="https://seclists.org/fulldisclosure/2022/Nov/0">CVE-2022-3602 a
   ...: nd CVE-2022-3786 Critical OpenSSL 3.0.xsecurity vulnerabilities</a></strong><em>Turritopsis Dohrnii Teo En Mi
   ...: ng (Nov 07)</em><br/>Subject: CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.x<br/>security vulnerabili
   ...: ties<br/><br/>Good day from Singapore,<br/><br/>Please refer to the following posts. The story is developing.
   ...: <br/><br/>[1] OpenSSL Gives Heads Up to Critical Vulnerability Disclosure, Check<br/>Point Alerts Organizatio
   ...: ns to Prepare Now<br/>Link: <br/><a href="https://blog.checkpoint.com/2022/10/30/openssl-gives-heads-up-to-cr
   ...: itical-vulnerability-disclosure-check-point-alerts-organizations-to-prepare-now/" rel="nofollow">https://blog
   ...: .checkpoint.com/2022/10/30/openssl-gives-heads-up-to-critical-vulnerability-disclosure-check-point-alerts-org
   ...: anizations-to-prepare-now/</a>...<br/></p>"""

In [4]: soup = get_html_soup(html)

In [5]: nameblock = soup('a')[0]

In [6]: nameblock
Out[6]: <a href="https://seclists.org/fulldisclosure/2022/Nov/0">CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.
xsecurity vulnerabilities</a>

In [7]: name = nameblock.text

In [8]: name
Out[8]: 'CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.xsecurity vulnerabilities'
```

Парсинг

```
In [1]: import bs4

In [2]: from souparser import get_html_soup

In [3]: html = """<p class="excerpt"><strong><a href="https://seclists.org/fulldisclosure/2022/Nov/0">CVE-2022-3602 a
   ...: nd CVE-2022-3786 Critical OpenSSL 3.0.xsecurity vulnerabilities</a></strong><em>Turritopsis Dohrnii Teo En Mi
   ...: ng (Nov 07)</em><br/>Subject: CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.x<br/>security vulnerabili
   ...: ties<br/><br/>Good day from Singapore,<br/><br/>Please refer to the following posts. The story is developing.
   ...: <br/><br/>[1] OpenSSL Gives Heads Up to Critical Vulnerability Disclosure, Check<br/>Point Alerts Organizatio
   ...: ns to Prepare Now<br/>Link: <br/><a href="https://blog.checkpoint.com/2022/10/30/openssl-gives-heads-up-to-cr
   ...: itical-vulnerability-disclosure-check-point-alerts-organizations-to-prepare-now/" rel="nofollow">https://blog
   ...: .checkpoint.com/2022/10/30/openssl-gives-heads-up-to-critical-vulnerability-disclosure-check-point-alerts-org
   ...: anizations-to-prepare-now/</a>...<br/></p>"""

In [4]: soup = get_html_soup(html)

In [5]: nameblock = soup('a')[0]

In [6]: nameblock
Out[6]: <a href="https://seclists.org/fulldisclosure/2022/Nov/0">CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.
xsecurity vulnerabilities</a>

In [7]: name = nameblock.text

In [8]: name
Out[8]: 'CVE-2022-3602 and CVE-2022-3786 Critical OpenSSL 3.0.xsecurity vulnerabilities'
```

Обогащение

packet storm

WiFi File Transfer 1.0.8 Cross Site Scripting

Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Backdoor.Win32.Redkod.d MVID-2022-0649 Hardcoded Credential

Authored by malvuln | Site malvuln.com

MiniDVBLinux 5.4 Remote Root Command Injection

Authored by LiquidWorm | Site zeroscience.mk

pfSense pfBlockerNG 2.1.4_26 Shell Upload

Authored by IHTeam, jheysel-r7 | Site metasploit.com

Spring Cloud Gateway 3.1.0 Remote Code Execution

Authored by Ayan Saha | Site metasploit.com

Webile 1.0.1 Directory Traversal

Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Обогащение

packet storm

WiFi File Transfer 1.0.8 Cross Site Scripting
Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Backdoor.Win32.Redkod.d MVID-2022-0649 Hardcoded Credential
Authored by malvuln | Site malvuln.com

MiniDVBLinux 5.4 Remote Root Command Injection
Authored by Liquidvvorm | Site zeroscience.mk

pfSense pfBlockerNG 2.1.4_26 Shell Upload
Authored by IHTeam, jheysel-r7 | Site metasploit.com

Spring Cloud Gateway 3.1.0 Remote Code Execution
Authored by Ayan Saha | Site metasploit.com

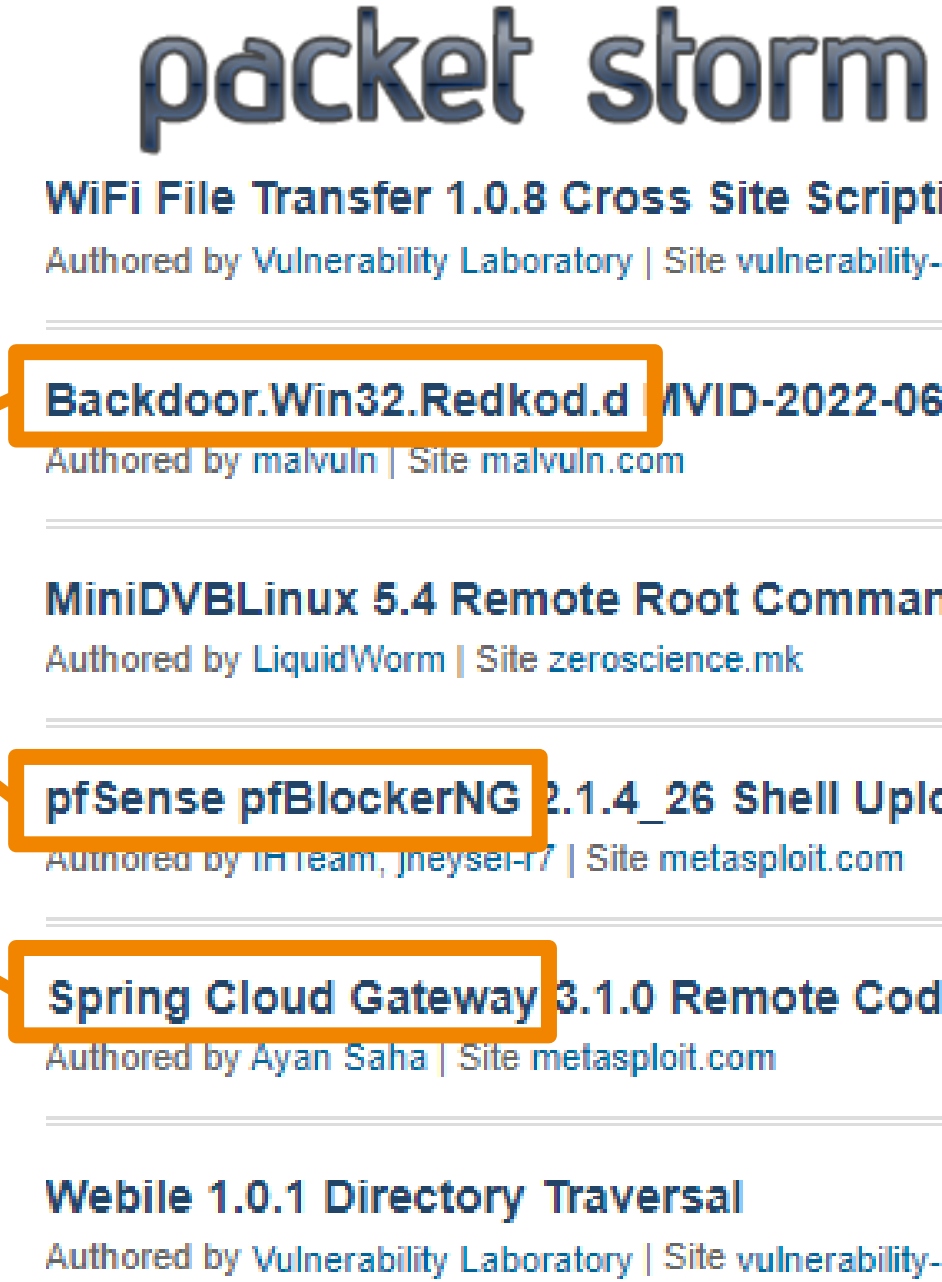
Webile .0.1 Directory Traversal
Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Обогащение

Вредоносное ПО [шаблон именования Касперского]

Свободное известное СЗИ!

Известная библиотека!



Обогащение

packet storm

WiFi File Transfer 1.0.8 Cross Site Scripting

Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Backdoor.Win32.Redkod.d MVID-2022-0649 Hardcoded Credential

Authored by malvuln | Site malvuln.com

MiniDVBLinux 5.4 Remote Root Command Injection

Authored by LiquidWorm | Site zeroscience.mk

pfSense pfBlockerNG 2.1.4_26 Shell Upload

Authored by IHTeam, jheysel-r7 | Site metasploit.com

Spring Cloud Gateway 3.1.0 Remote Code Execution

Authored by Ayan Saha | Site metasploit.com

Webile 1.0.1 Directory Traversal

Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Обогащение

packet storm

WiFi File Transfer 1.0.8 **Cross Site Scripting**
Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Backdoor.Win32.Redkod.d MVID-2022-064 **Hardcoded Credential**
Authored by malvuln | Site malvuln.com

MiniDVBLinux 5. **Remote Root Command Injection**
Authored by LiquidWorm | Site zerosclence.mk

pfSense pfBlockerNG 2.1.4_26 **Shell Upload**
Authored by IHTeam, jheysel-r7 | Site metasploit.com

Spring Cloud Gateway 3.1.0 **Remote Code Execution**
Authored by Ayan Saha | Site metasploit.com

Webile 1.0.1 **Directory Traversal**
Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Обогащение

Отдать человекам в первую очередь

packet storm

WiFi File Transfer 1.0.8 Cross Site Scripting
Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Backdoor.Win32.Redkod.d MVID-2022-064 Hardcoded Credential
Authored by malvuln | Site malvuln.com

MiniDVBLinux 5. Remote Root Command Injection
Authored by LiquidWorm | Site zerosclence.mk

pfSense pfBlockerNG 2.1.4_26 Shell Upload
Authored by IHTeam, jheysel-r7 | Site metasploit.com

Spring Cloud Gateway 3.1.0 Remote Code Execution
Authored by Ayan Saha | Site metasploit.com

Webile 1.0.1 Directory Traversal
Authored by Vulnerability Laboratory | Site vulnerability-lab.com

Обогащение

NVD CVE

Легко выделить эксплоиты, они размечены

НКЦКИ

Нужен анализ текста или дополнительное внимание

HackerNews

Нужен анализ текста или дополнительное внимание, и не факт что эксплоит будет

Обогащение

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.

Обогащение

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.

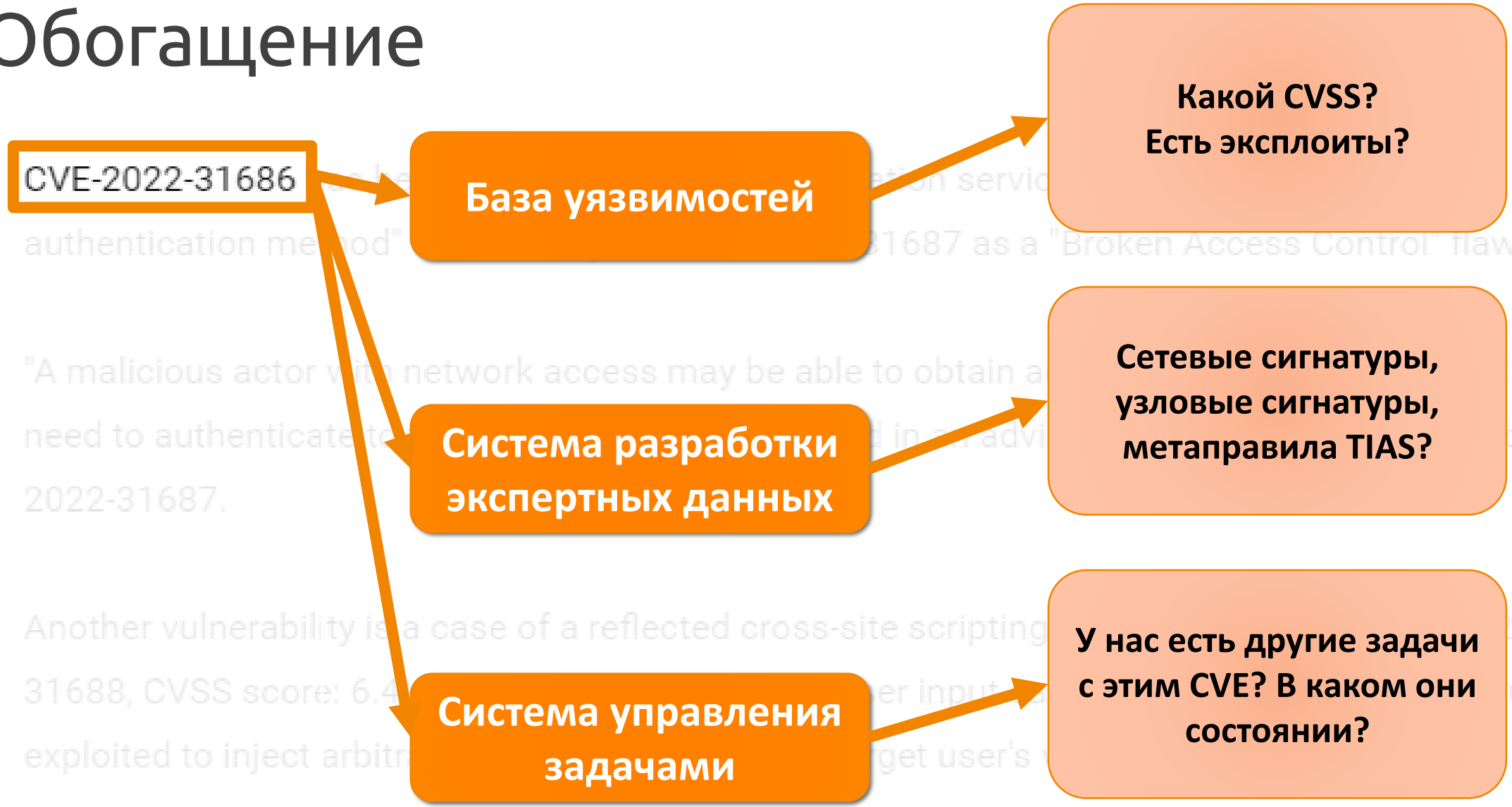
Обогащение

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.

Обогащение


CVE-2022-31686
База уязвимостей
Система разработки экспертных данных
Система управления задачами
Какой CVSS?
Есть эксплоиты?
Сетевые сигнатуры, узловые сигнатуры, метаправила TIAS?
У нас есть другие задачи с этим CVE? В каком они состоянии?

Обогащение

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.

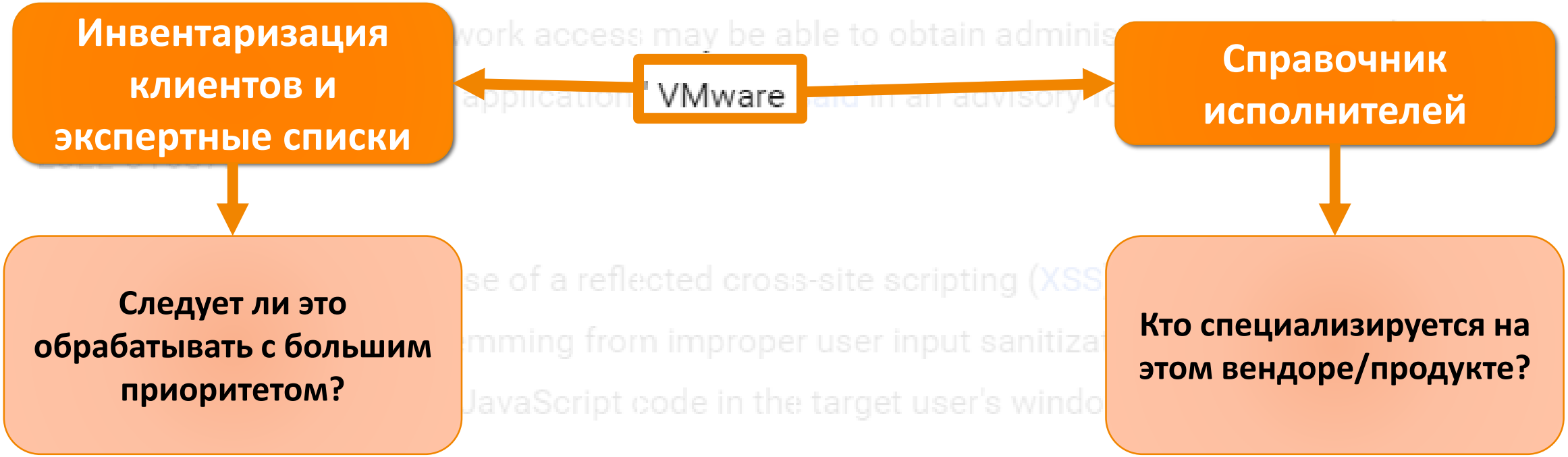
Обогащение

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.

Обогащение

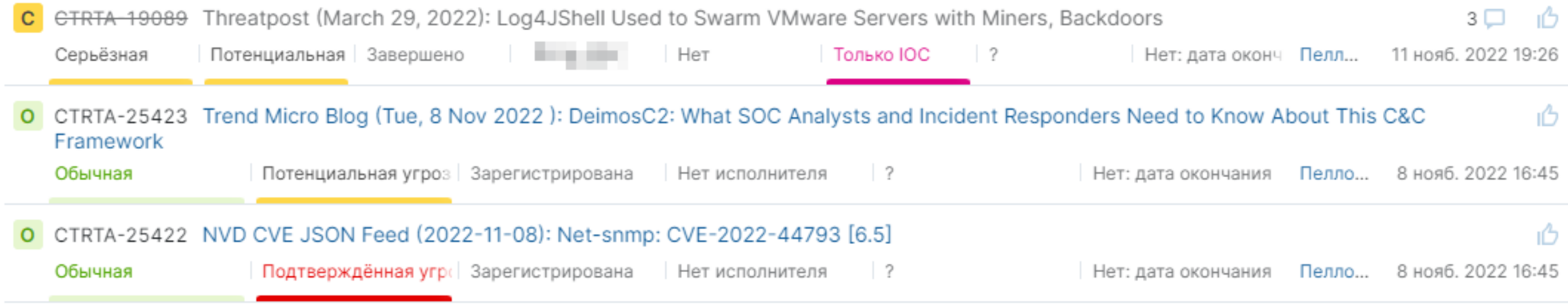

Инвентаризация клиентов и экспертные списки
VMware
Справочник исполнителей
Следует ли это обрабатывать с большим приоритетом?
Кто специализируется на этом вендоре/продукте?

Заводим задачи в YouTrack

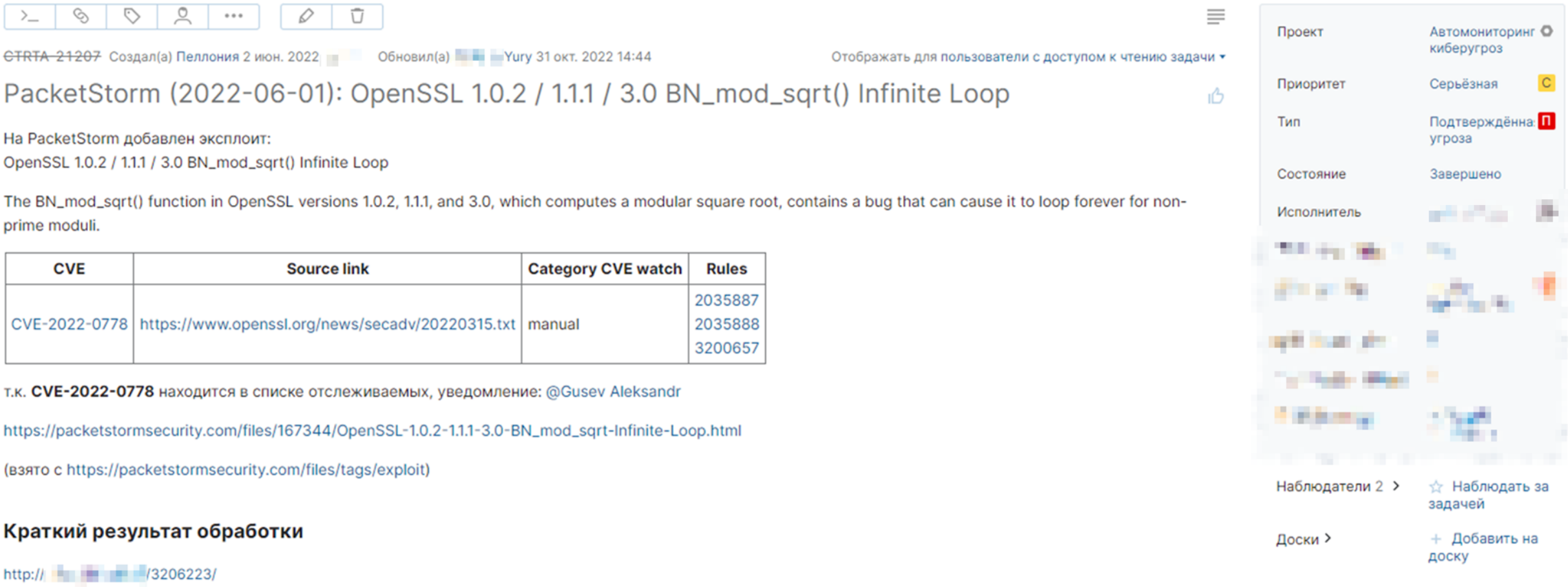
Приоритет	Найден исполнитель	Нет исполнителя	Всего
Повышен	202	0	**202**
Обычный	75	508	**583**
Понижен	0	32	**32**

202/817 = 24.7% наводок получают повышенный приоритет

Заводим задачи в YouTrack



Заводим задачи в YouTrack



~~CTRTA-21207~~ Создал(а) Пеллония 2 июн. 2022 Обновил(а) Yury 31 окт. 2022 14:44 Отображать для пользователи с доступом к чтению задачи

PacketStorm (2022-06-01): OpenSSL 1.0.2 / 1.1.1 / 3.0 BN_mod_sqrt() Infinite Loop

На PacketStorm добавлен эксплоит:
OpenSSL 1.0.2 / 1.1.1 / 3.0 BN_mod_sqrt() Infinite Loop

The BN_mod_sqrt() function in OpenSSL versions 1.0.2, 1.1.1, and 3.0, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli.

CVE	Source link	Category CVE watch	Rules
CVE-2022-0778	https://www.openssl.org/news/secadv/20220315.txt	manual	2035887 2035888 3200657

т.к. **CVE-2022-0778** находится в списке отслеживаемых, уведомление: @Gusev Aleksandr

https://packetstormsecurity.com/files/167344/OpenSSL-1.0.2-1.1.1-3.0-BN_mod_sqrt-Infinite-Loop.html

(взято с https://packetstormsecurity.com/files/tags/exploit)

Краткий результат обработки

http:// /3206223/

Проект: Автомониторинг киберугроз
Приоритет: Серьёзная
Тип: Подтверждённая угроза
Состояние: Завершено
Исполнитель
Наблюдатели 2 ☆ Наблюдать за задачей
Доски ＋ Добавить на доску

Заводим задачи в YouTrack

~~CTRTA-21207~~ Создал(а) Пеллония 2 июн. 2022 Обновил(а) Yury 31 окт. 2022 14:44 Отображать для пользователи с доступом к чтению задачи

PacketStorm (2022-06-01): OpenSSL 1.0.2 / 1.1.1 / 3.0 BN_mod_sqrt() Infinite Loop

На PacketStorm добавлен эксплоит:
OpenSSL 1.0.2 / 1.1.1 / 3.0 BN_mod_sqrt() Infinite Loop

The BN_mod_sqrt() function in OpenSSL versions 1.0.2, 1.1.1, and 3.0, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli.

CVE	Source link	Category CVE watch	Rules
CVE-2022-0778	https://www.openssl.org/news/secadv/20220315.txt	manual	2035887 2035888 3200657

т.к. **CVE-2022-0778** находится в списке отслеживаемых, уведомление: @Gusev Aleksandr

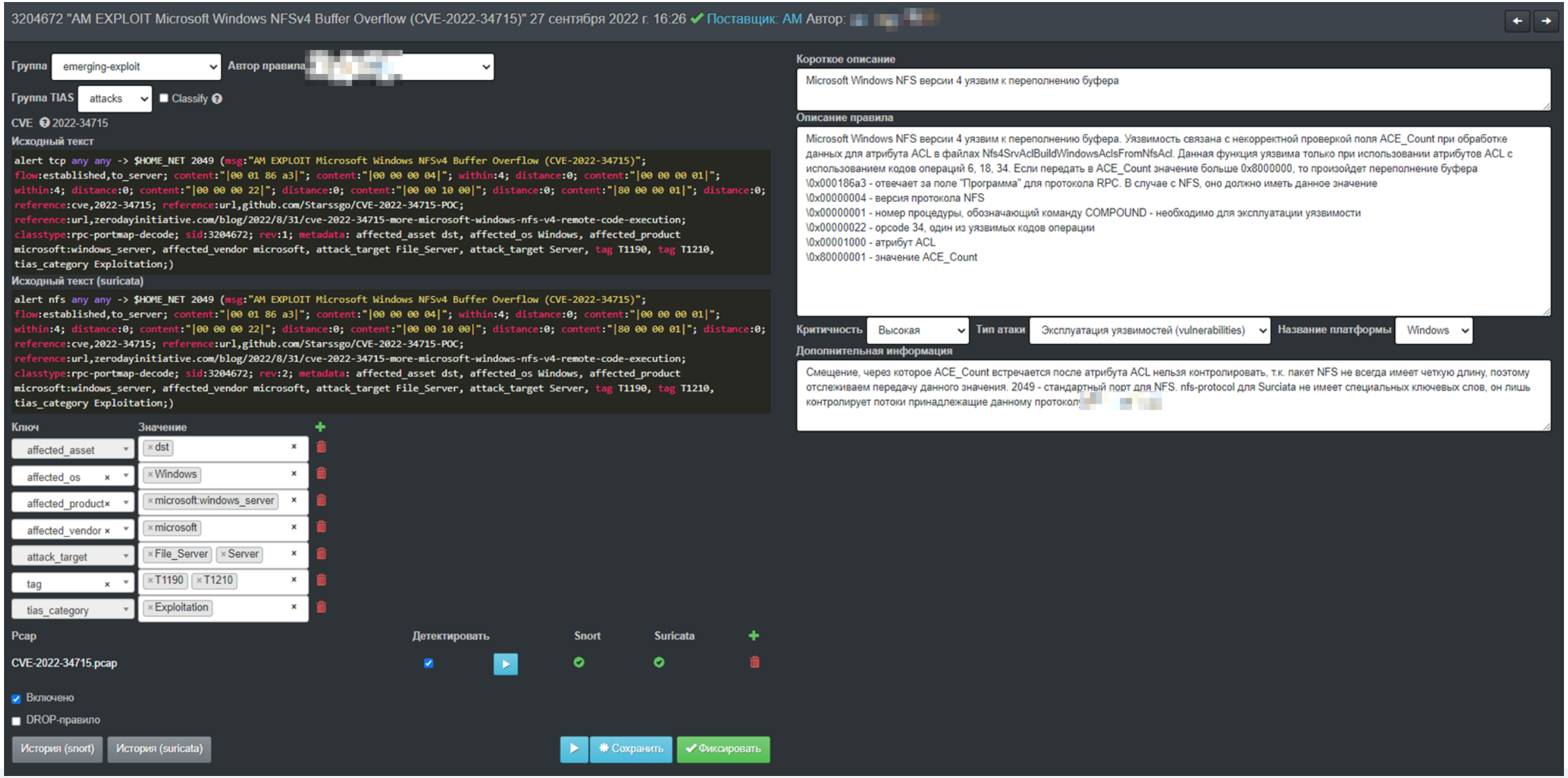
https://packetstormsecurity.com/files/167344/OpenSSL-1.0.2-1.1.1-3.0-BN_mod_sqrt-Infinite-Loop.html

(взято с https://packetstormsecurity.com/files/tags/exploit)

Краткий результат обработки

http:// /3206223/

Создаём сетевое правило



Управление процессом

1. Первичная оценка лида
2. Если есть полезные данные, производим ЭД
3. Если произведена единица ЭД, подлежащая оценке, она валидируется штатным сотрудником, он даёт обратную связь (так можно и со стажёрами)
4. Если ЭД удовлетворяет валидатора, она верифицируется руководителем, как ответственным за выпуск, и отправляется на тестовый контур

Управление процессом

Формализуй это!

- На любую нетривиальную повторяющуюся задачу должны быть хотя бы рекомендации, лучше руководство, ещё лучше – чеклисты, по которым можно сверять качество результата
- Если два человека допустили одну ошибку по два раза – это наверняка надо закрепить во внутреннем стандарте
- Если это уже закреплено во внутреннем стандарте, но ошибки всё равно регулярны – стандарт можно и нужно доуточнять
- Если вы автоматизируете сами (а не отдаёте это выделенным программистам) – обязательно разработайте внутренний стандарт стиля кода

Управление процессом

- Регуляторная гильотина – слишком длинные стандарты нужно разбивать или автоматизировать, если пункт стандарта тривиален – его нужно автоматизировать и удалить из стандарта
- Команда должна хорошо понимать внутреннюю логику процессов и метрики оценки результатов, это помогает не только принимать самостоятельные решения, но и лучше видеть, что можно автоматизировать
- Не недооценивайте свои человеческие ресурсы - *при должной организации процессов обучения и контроля* даже студенты хотят и могут автоматизировать, более того, их легче учить писать чистый код, чем тех, кто в работе пользуется программированием годами, и автоматизация позволяет всем заниматься менее рутинными и более увлекательными задачами

Результаты

Основными результатами процесса являются экспертные данные в виде

- Правил сетевых и узловых IDPS и NGFW
- Правил EDR
- Метаправил TIAS
- Threat Intelligence-фидов

Широкое применение автоматизации и эффективная её организация позволяют добиться следующих эффектов:

Результаты

- Качество ЭД улучшается – компетенции специалистов развиваются быстрее, а автоматика страхует их от более тривиальных недоработок
- Скорость выпуска ЭД увеличивается – кроме того, что автоматике отдаются классы ЭД, которые обычно делаются «руками» (т.к. эти руки автоматизируют себя), алгоритмы снимают со специалистов часть работы
- Процессы становятся прозрачнее и контролируемее – правильно организованная автоматика позволяет контролировать себя и собирать внутри себя статистику, а системы управления задачами уже предоставляют часть необходимого функционала

Спасибо!

Александр Гусев

Aleksandr.Gusev@amonitoring.ru