

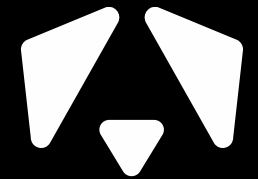


ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ



# Поисковые огни и лазерные прицелы

Автоматизация процесса  
киберразведки при производстве  
данных экспертизы для СЗИ



ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

Александр Гусев

Руководитель направления исследования киберугроз

# Почему именно сейчас интересна тема автоматической киберразведки



- **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 киберразведки



How Data and Analytics Unleash Innovation & Transform Uncertainty | Gartner Full Keynote

youtube.com/watch?v=bXob4SMBguM

Введите запрос

**Analytics**

**Combine Art and Science**

Find the important patterns

Ask great questions

Know when to stop

Gartner

26:48 / 45:21

Gartner 36,2 тыс. подписчиков

Подписаться

88

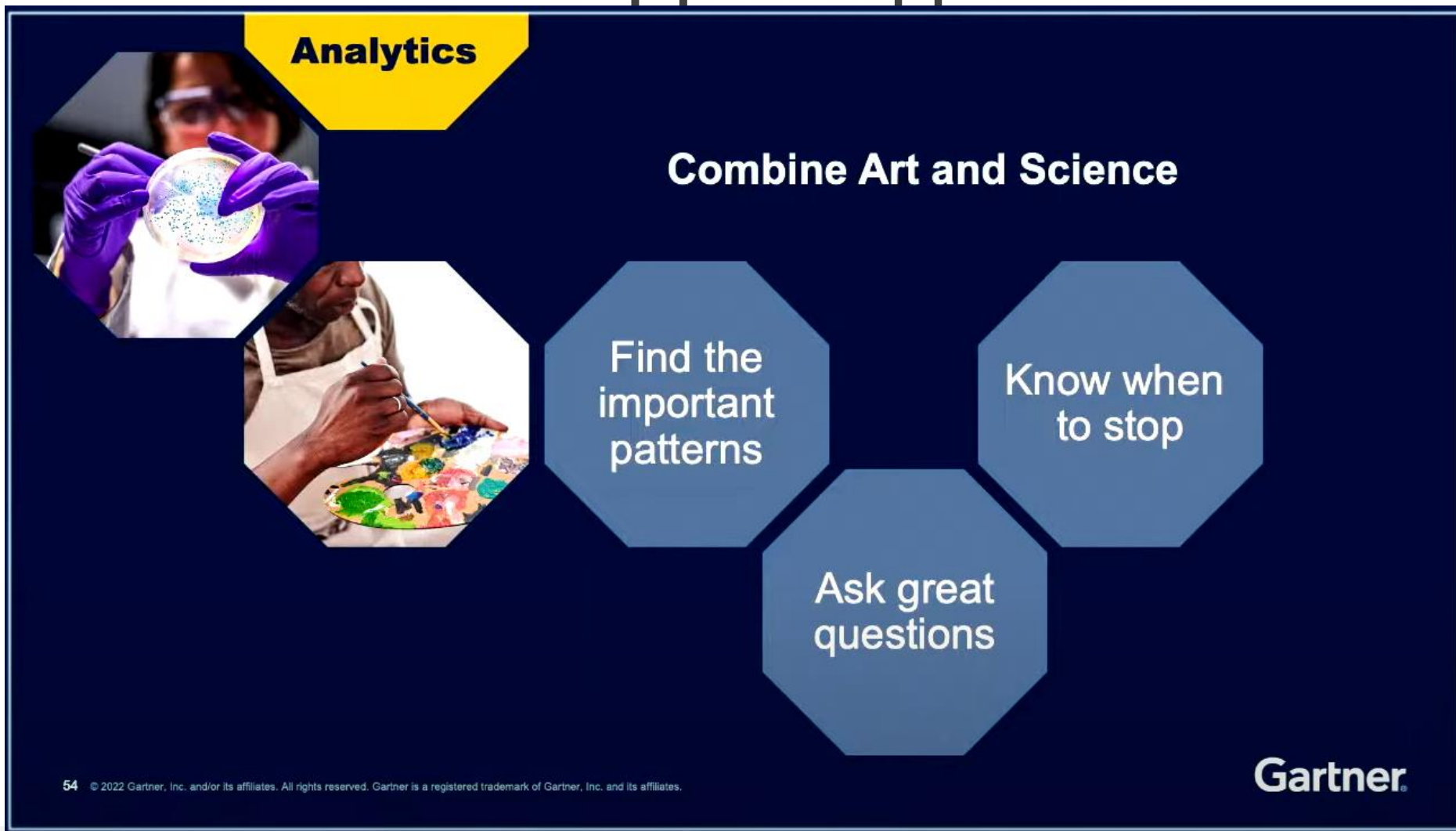
Поделиться

Создать клип

Сохранить



# Почему именно сейчас интересна тема автоматической киберразведки



# Почему именно сейчас интересна тема автоматической киберразведки





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





# Сбор информации



**Requests**  
*http for humans*

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/...](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/></p></a></strong><em>Turritopsis Dohrnii Teo En Mi
... : 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'
```



## **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](#)



## WiFi File Transfer 1.0.8 Cross Site Scripting

Authored by Vulnerability Laboratory | Site [vulnerability-lab.com](https://vulnerability-lab.com)

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

Authored by malvuln | Site [malvuln.com](https://malvuln.com)

## MiniDVBLinux 5.4 Remote Root Command Injection

Authored by Liquidworm | Site [zeroscience.mk](https://zeroscience.mk)

## pfSense pfBlockerNG 2.1.4\_26 Shell Upload

Authored by IT Team, jneysel17 | Site [metasploit.com](https://metasploit.com)

## Spring Cloud Gateway 3.1.0 Remote Code Execution

Authored by Ayan Saha | Site [metasploit.com](https://metasploit.com)

## Webile 1.0.1 Directory Traversal

Authored by Vulnerability Laboratory | Site [vulnerability-lab.com](https://vulnerability-lab.com)

# Обогащение

# packet storm



## WiFi File Transfer 1.0.8 Cross Site Scripting

Authored by Vulnerability Laboratory | Site [vulnerability-lab.com](http://vulnerability-lab.com)

## Backdoor.Win32.Redkod.d [MVID-2022-0649] Hardcoded Credential

Authored by malvuln | Site [malvuln.com](http://malvuln.com)

## MiniDVBLinux 5.4 Remote Root Command Injection

Authored by LiquidWorm | Site [zeroscience.mk](http://zeroscience.mk)

## pfSense pfBlockerNG 2.1.4\_26 Shell Upload

Authored by iH Team, jneysel17 | Site [metasploit.com](http://metasploit.com)

## Spring Cloud Gateway 3.1.0 Remote Code Execution

Authored by Ayan Saha | Site [metasploit.com](http://metasploit.com)

## Webile 1.0.1 Directory Traversal

Authored by Vulnerability Laboratory | Site [vulnerability-lab.com](http://vulnerability-lab.com)

Вредоносное ПО  
[шаблон именования  
Касперского]

Свободное известное СЗИ!

Известная библиотека!



## 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](#)





WiFi File Transfer 1.0.8 **Cross Site Scripting**

Authored by Vulnerability Laboratory | Site [vulnerability-lab.com](http://vulnerability-lab.com)

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

Authored by malvuln | Site [malvuln.com](http://malvuln.com)

MiniDVBLinux 5.4 **Remote Root Command Injection**

Authored by LiquidWorm | Site [zeroscience.mk](http://zeroscience.mk)

pfSense pfBlockerNG 2.1.4\_26 **Shell Upload**

Authored by IHTeam, jheysel-r7 | Site [metasploit.com](http://metasploit.com)

Spring Cloud Gateway 3.1.0 **Remote Code Execution**

Authored by Ayan Saha | Site [metasploit.com](http://metasploit.com)

Webile 1.0.1 **Directory Traversal**

Authored by Vulnerability Laboratory | Site [vulnerability-lab.com](http://vulnerability-lab.com)

# Обогащение

# packet storm



## WiFi File Transfer 1.0.8 Cross Site Scripting

Authored by Vulnerability Laboratory | Site [vulnerability-lab.com](https://vulnerability-lab.com)

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

Authored by malvuln | Site [malvuln.com](https://malvuln.com)

## MiniDVBLinux 5.4 Remote Root Command Injection

Authored by LiquidWorm | Site [zeroscience.mk](https://zeroscience.mk)

## pfSense pfBlockerNG 2.1.4\_26 Shell Upload

Authored by IHTeam, jheysel-r7 | Site [metasploit.com](https://metasploit.com)

## Spring Cloud Gateway 3.1.0 Remote Code Execution

Authored by Ayan Saha | Site [metasploit.com](https://metasploit.com)

## Webile 1.0.1 Directory Traversal

Authored by Vulnerability Laboratory | Site [vulnerability-lab.com](https://vulnerability-lab.com)

Отдать человекам в первую очередь

# 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



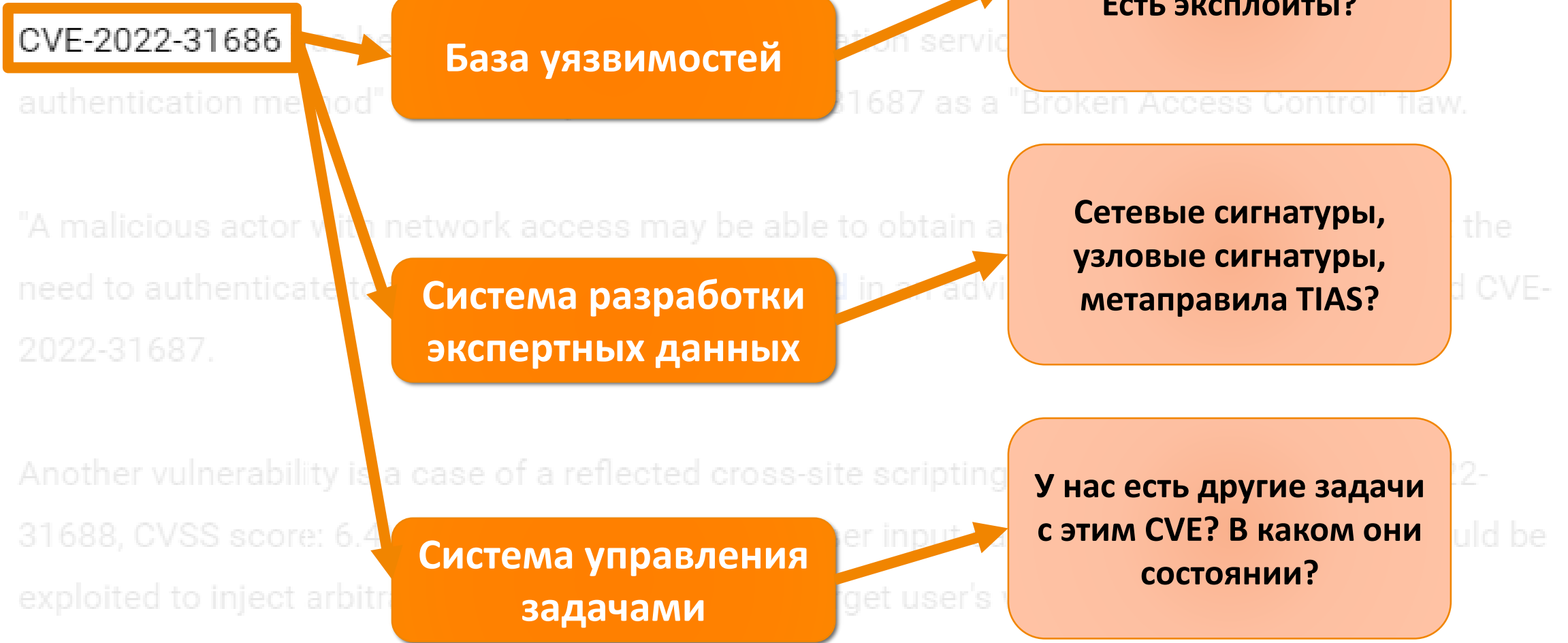
**CVE-2022-31686** has been described by the virtualization services provider as a "broken authentication method" vulnerability, and CVE-2022-31687 as a "Broken Access Control" flaw.

"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



# 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.

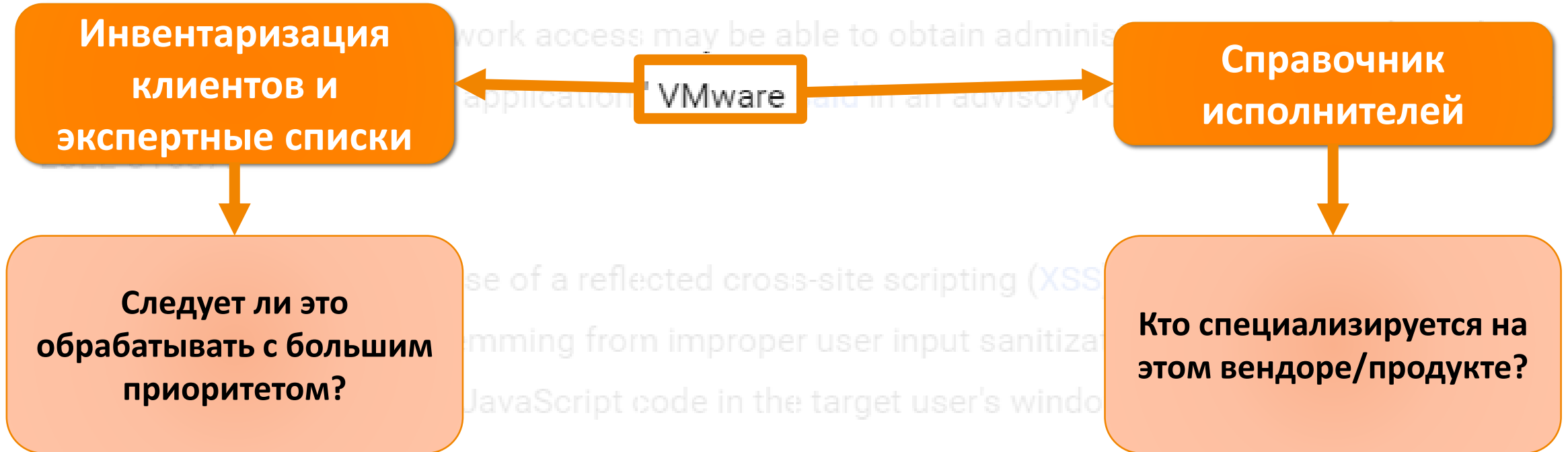
"A malicious actor with network access may be able to obtain administrative access without the need to authenticate to the application." VMware [aid](#) in an advisory for CVE-2022-31686 and CVE-2022-31687.

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.



# 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



- C** ~~CTRТА-19089~~ Threatpost (March 29, 2022): Log4JShell Used to Swarm VMware Servers with Miners, Backdoors 3   
Серьёзная | Потенциальная | Завершено | | Нет | Только IOC | ? | Нет: дата оконч | Пелл... | 11 нояб. 2022 19:26
- O** CTRТА-25423 Trend Micro Blog (Tue, 8 Nov 2022 ): DeimosC2: What SOC Analysts and Incident Responders Need to Know About This C&C Framework   
Обычная | Потенциальная угроза | Зарегистрирована | Нет исполнителя | ? | Нет: дата окончания | Пелло... | 8 нояб. 2022 16:45
- O** CTRТА-25422 NVD CVE JSON Feed (2022-11-08): Net-snmp: CVE-2022-44793 [6.5]   
Обычная | Подтверждённая угроза | Зарегистрирована | Нет исполнителя | ? | Нет: дата окончания | Пелло... | 8 нояб. 2022 16:45

# Заводим задачи в YouTrack



ETRTA-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	<a href="https://www.openssl.org/news/secadv/20220315.txt">https://www.openssl.org/news/secadv/20220315.txt</a>	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](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/>

Project: Автомониторинг киберугроз  
Priority: Серьёзная  
Type: Подтверждённая угроза  
Status: Завершено  
Assignee: [User avatars]

Наблюдатели 2 > ☆ Наблюдать за задачей

Доски > + Добавить на доску

# Заводим задачи в YouTrack



ETRTA-21207 Создал(а) Пеллония 2 июн. 2022, 14:44 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	<a href="https://www.openssl.org/news/secadv/20220315.txt">https://www.openssl.org/news/secadv/20220315.txt</a>	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](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



3204672 "AM EXPLOIT Microsoft Windows NFSv4 Buffer Overflow (CVE-2022-34715)" 27 сентября 2022 г. 16:26 ✔ Поставщик: AM Автор:

Группа  Автор правила

Группа TIAS  Classify ?

CVE ? 2022-34715

Исходный текст

```
alert tcp any any -> $HOME_NET 2049 (msg:"AM EXPLOIT Microsoft Windows NFSv4 Buffer Overflow (CVE-2022-34715)";
flow:established,to_server; content:"|00 01 86 a3|"; content:"|00 00 00 04|"; within:4; distance:0; content:"|00 00 00 01|";
within:4; distance:0; content:"|00 00 00 22|"; distance:0; content:"|00 00 10 00|"; distance:0; content:"|80 00 00 01|"; distance:0;
reference:cve,2022-34715; reference:url,github.com/Starssgo/CVE-2022-34715-POC;
reference:url,zerodayinitiative.com/blog/2022/8/31/cve-2022-34715-more-microsoft-windows-nfs-v4-remote-code-execution;
classtype:rpc-portmap-decode; sid:3204672; rev:1; metadata: affected_asset dst, affected_os Windows, affected_product
microsoft:windows_server, affected_vendor microsoft, attack_target File_Server, attack_target Server, tag T1190, tag T1210,
tias_category Exploitation;)
```

Исходный текст (suricata)

```
alert nfs any any -> $HOME_NET 2049 (msg:"AM EXPLOIT Microsoft Windows NFSv4 Buffer Overflow (CVE-2022-34715)";
flow:established,to_server; content:"|00 01 86 a3|"; content:"|00 00 00 04|"; within:4; distance:0; content:"|00 00 00 01|";
within:4; distance:0; content:"|00 00 00 22|"; distance:0; content:"|00 00 10 00|"; distance:0; content:"|80 00 00 01|"; distance:0;
reference:cve,2022-34715; reference:url,github.com/Starssgo/CVE-2022-34715-POC;
reference:url,zerodayinitiative.com/blog/2022/8/31/cve-2022-34715-more-microsoft-windows-nfs-v4-remote-code-execution;
classtype:rpc-portmap-decode; sid:3204672; rev:2; metadata: affected_asset dst, affected_os Windows, affected_product
microsoft:windows_server, affected_vendor microsoft, attack_target File_Server, attack_target Server, tag T1190, tag T1210,
tias_category Exploitation;)
```

Ключ Значение

affected_asset	<input type="text" value="dst"/>	<input type="button" value="x"/>	<input type="button" value="trash"/>
affected_os	<input type="text" value="Windows"/>	<input type="button" value="x"/>	<input type="button" value="trash"/>
affected_product	<input type="text" value="microsoft:windows_server"/>	<input type="button" value="x"/>	<input type="button" value="trash"/>
affected_vendor	<input type="text" value="microsoft"/>	<input type="button" value="x"/>	<input type="button" value="trash"/>
attack_target	<input type="text" value="File_Server"/> <input type="text" value="Server"/>	<input type="button" value="x"/>	<input type="button" value="trash"/>
tag	<input type="text" value="T1190"/> <input type="text" value="T1210"/>	<input type="button" value="x"/>	<input type="button" value="trash"/>
tias_category	<input type="text" value="Exploitation"/>	<input type="button" value="x"/>	<input type="button" value="trash"/>

Рсар

CVE-2022-34715.рсар

Включено  DROP-правило

Короткое описание  
Microsoft Windows NFS версии 4 уязвим к переполнению буфера

Описание правила  
Microsoft Windows NFS версии 4 уязвим к переполнению буфера. Уязвимость связана с некорректной проверкой поля ACE\_Count при обработке данных для атрибута ACL в файлах Nfs4SrvAcBuildWindowsAcIsFromNfsAcI. Данная функция уязвима только при использовании атрибутов ACL с использованием кодов операций 6, 18, 34. Если передать в ACE\_Count значение больше 0x80000000, то произойдет переполнение буфера \0x000186a3 - отвечает за поле "Программа" для протокола RPC. В случае с NFS, оно должно иметь данное значение \0x00000004 - версия протокола NFS \0x00000001 - номер процедуры, обозначающий команду COMPOUND - необходимо для эксплуатации уязвимости \0x00000022 - orcode 34, один из уязвимых кодов операции \0x00001000 - атрибут ACL \0x80000001 - значение ACE\_Count

Критичность  Тип атаки  Название платформы

Дополнительная информация  
Смещение, через которое ACE\_Count встречается после атрибута ACL нельзя контролировать, т.к. пакет NFS не всегда имеет четкую длину, поэтому отслеживаем передачу данного значения. 2049 - стандартный порт для NFS. nfs-protocol для Suricata не имеет специальных ключевых слов, он лишь контролирует потоки принадлежащие данному протоколу.

# 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 доуточнить
- 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](mailto:Aleksandr.Gusev@amonitoring.ru)

