



# Гибкость и объективность. Польза симбиоза SIEM и DCSAP



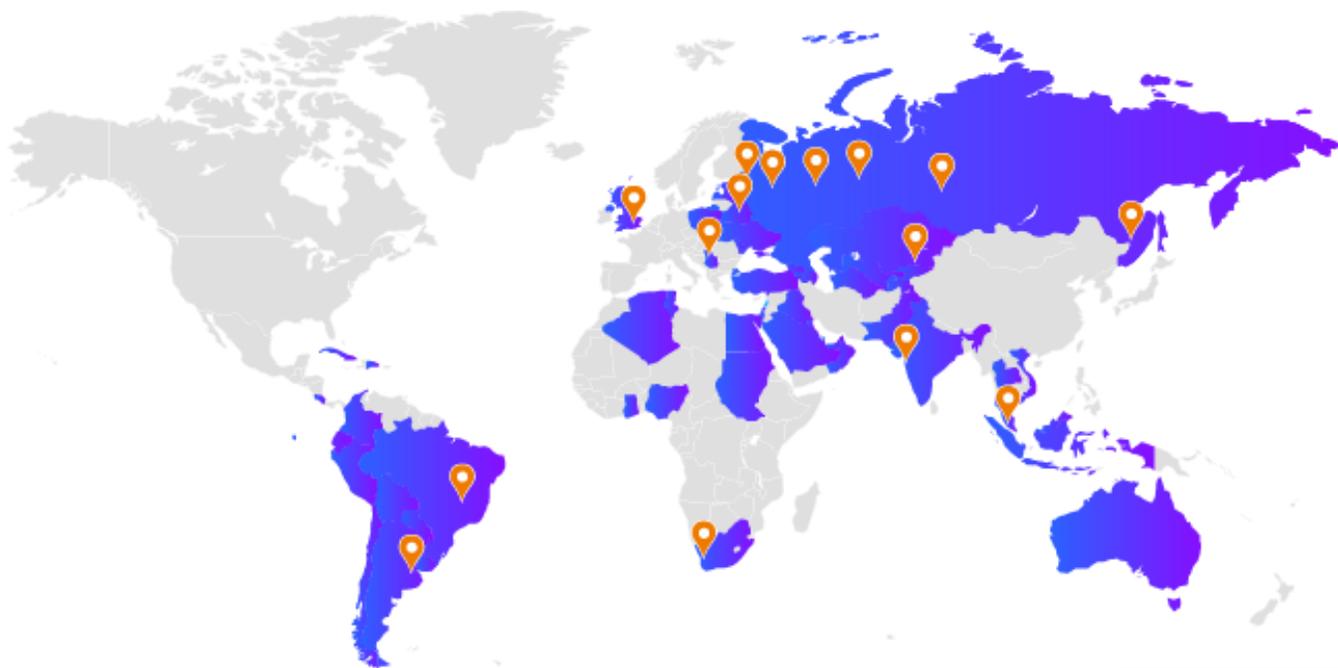
**Дмитрий Стельченко**

Куратор представительства «СёрчИнформ»  
в Сибирском ФО

**SEARCHINFORM**

INFORMATION SECURITY

# «СёрчИнформ» сегодня



**3 000+** клиентов по всей России и в  
**20+** странах мира

**25+** лет в IT

**6** решений для комплексной  
защиты бизнеса

**2 000 000+** ПК  
под защитой продуктов «СёрчИнформ»

## Решения «СёрчИнформ»

рекомендованы к внедрению и тиражированию  
в регионах Минпромторгом РФ, Минцифры РФ,  
Аналитическим центром при Правительстве России

Продукты «СёрчИнформ» входят  
в Реестр отечественного ПО

# Гибкость архитектуры SIEM

- Логирование практически любых систем.
- Опрос по WMI.
- Подключение к СУБД.
- Работа через скрипты.

- Работа со всеми инцидентами в «едином окне».
- Инвентаризация инфраструктуры.
- Аудит безопасности инфраструктуры.

#CODEIB

SEARCHINFORM  
INFORMATION SECURITY

# Нерешенные проблемы современных SIEM

SEARCHINFORM  
INFORMATION SECURITY

#CODEIB

- Нет контроля, если нет логирования.
- Уровень логирования всегда хуже уровня контроля приложений, служб или драйверов.
- Работоспособность зависит от многих факторов.
- Проактивная реакция только посредством скриптов, взаимодействия на AD либо API.
- Слабая связка с уровнем Endpoint`ов.



# Не все DСАР одинаковы

## Даже известные DСАР имеют критические проблемы:

- Ряд систем отслеживает действия с файлами на базе системного логирования, а не файловых потоков.
- Ряд систем мониторит действия пользователей на основании логов AD либо локальных логов.
- Ряд систем регулирует права доступа через атрибуты NFS\DFS.
- Многие системы вообще не имеют прямой связи с Endpoint`ами (безагентские), поэтому не видят активности процессов.

#CODEIB

SEARCHINFORM

INFORMATION SECURITY

# Идеальный DCSAR

## «из палаты мер и весов»

- В результате категоризации ставит неудаляемую метку в файле\файловом потоке, а не в свойствах файла.
- Работает как на конечных точках, так и по сети.
- Логирует файловые операции на драйверном уровне.
- Знает, какой процесс обращался к файлу.
- Является средством построения модели ABAC на основе контентного анализа файлов, а не «поисковиком» или анализатором статистики.

# SIEM & DCAP

## Совместное использование SIEM и DCAP даёт:

- Агент для Endpoint как часть архитектуры SIEM.
- Объективную ситуацию с действиями с файлами.
- Информацию об активности процессов и служб.
- Контроль состава оборудования и ПО (непосредственно с хоста).
- Контроль сетевых подключений и браузерной активности.
- Объективную ситуацию по работе пользователей.
- «Двойное» логирование, несовпадения могут быть выявлены кросс-корреляциями.

#CODEIB

SEARCHINFORM  
INFORMATION SECURITY

# SIEM & DCAP

## Совместное использование SIEM и DCAP позволяет выявить:

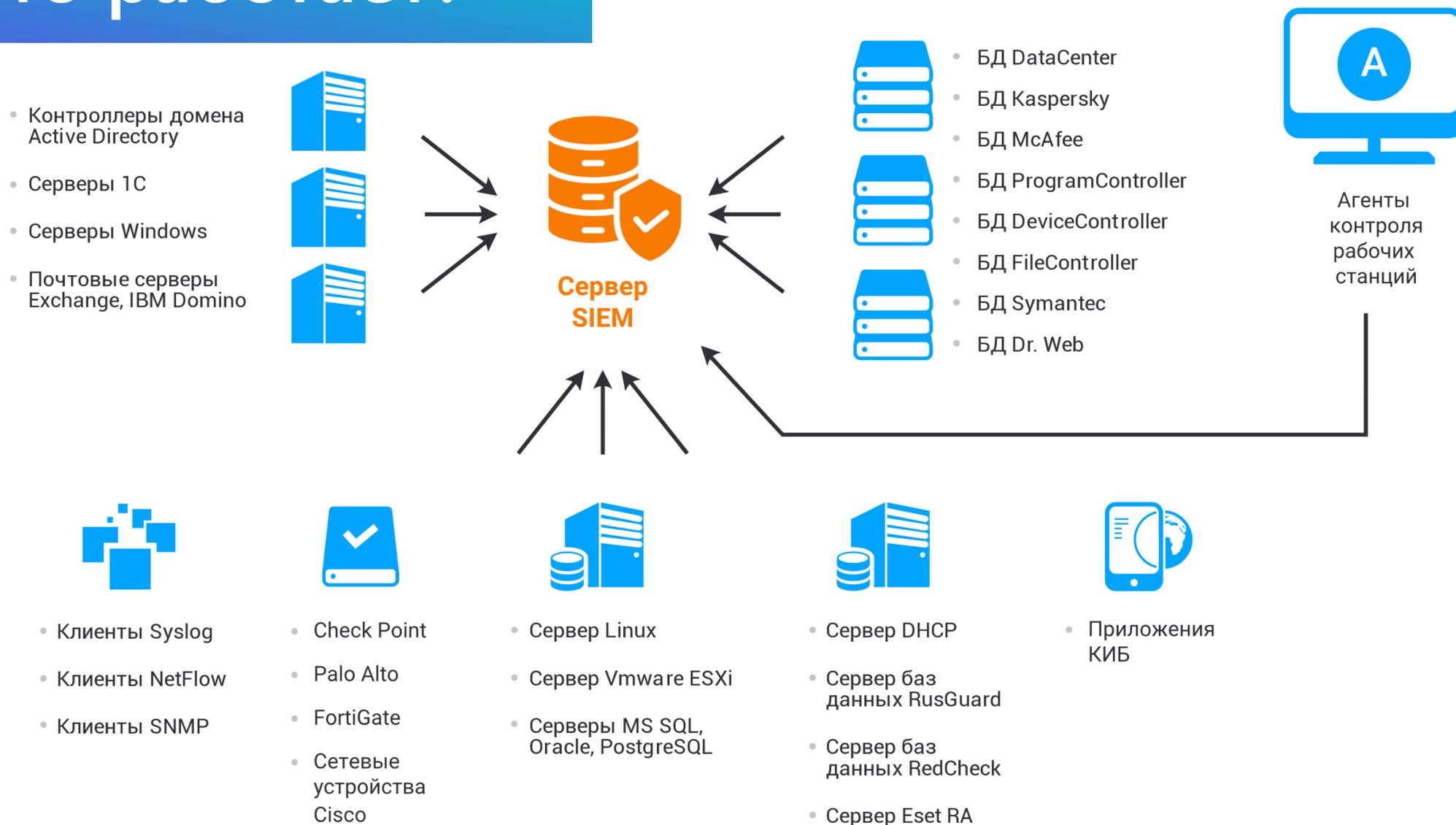
- Скрытые подключения.
- Обход сетевых средств защиты.
- Нетиповую файловую активность пользователей.
- Нетиповую файловую активность процессов.
- Выполнение скриптов и прочие не отражающиеся в классическом логировании инциденты.

#CODEIB

SEARCHINFORM

INFORMATION SECURITY

# Как это работает?



# Как это работает?

The screenshot displays the 'Rules - SIEM.Client console [1.45.2.1]' interface. The main window shows a rule configuration for 'Большое количество пользователей, работающих с файлом'. The rule description states that incidents indicate situations where an anomalously large number of users connect to a file in a short period. The threat level is 'Warning' (Угроза), noting that reports can indicate statistical anomalies.

The left sidebar lists various event categories, with 'События FileControl...' selected, showing 28697 / 28704 events. The 'Глобальный фильтр' (Global filter) is set to 'Дата инцидента: 01.02.2022 00:00:00 - 28.02.2022'. The 'Фильтр правила' (Rule filter) is currently empty.

The main content area shows a table of incidents:

* №	Флаги	Дата инцидента	Источник	Файл	Размер файла	Тип устройства	...	...
4		09.02.2022 13:48:22		C:\aaa\Файл2.xls	28 KB	Жесткий	...	...
5		09.02.2022 13:48:22		C:\aaa\zaq\Ошибки_маршрутизации.xls	53 KB	Жесткий	...	...
6		09.02.2022 13:48:22		C:\aaa\zaq\Изменения_конфигурации.xls	84,5 KB	Жесткий	...	...
7		09.02.2022 13:48:22		C:\Users\b.beavis\Desktop\йцццц — копия (2) — копия.xls	28 KB	Жесткий	...	...
8		09.02.2022 13:48:22		C:\Users\b.beavis\Desktop\щцшмщцлващзвлщцааяцслыждслфьждсфоджсфьждсф.xls	28 KB	Жесткий	...	...
9		09.02.2022 13:48:22		C:\Users\b.beavis\Desktop\йцццц.xls	28 KB	Жесткий	...	...
10		09.02.2022 13:48:22		C:\Users\b.beavis\Desktop\Файл10000.xls	28 KB	Жесткий	...	...

Below the incident table, there is a detailed view of the rule configuration and a table of related events:

Дата инцидента	Операции с файлом	Домен	Имя пользователя	Имя компьютера	Имя конечного файла
06.11.2020 17:54:30	Чтение файла	T04	b.beavis	kvc21.t04.local	C:\aaa\zaq\Ошибки_мар
27.02.2020 18:43:00	Файл скопирован	T04	user1504	kvc21.t04.local	C:\aaa\zaq\Ошибки_мар
28.02.2020 11:23:50	Чтение файла	T04	user1507	kvc21.t04.local	C:\aaa\zaq\Ошибки_мар

The bottom status bar shows the rule name, its status ('Выполняется'), the total number of records ('Всего записей: 58'), the IP address (192.168.175.50:27017/siem), and the system tray icons.

#CODEIB

SEARCHINFORM  
INFORMATION SECURITY

# Как это работает?

#CODEIB

SEARCHINFORM  
INFORMATION SECURITY

The screenshot shows the SIEM Client console interface. On the left, there is a 'Правила' (Rules) sidebar with a search bar and a list of rules. The main area displays the details for a specific rule, 'Активность давно отсутствующего пользователя' (Activity of long-absent user). Below the rule details is a table of incidents.

**Правила**

Введите строку поиска

- Кросс-корреляция 25253 / 25273
- Пользовательские правила 1912 / 1915
- AD. Другие события 0 / 0
- AD. Логины и пароли 135953 / 135980
- AD. Мониторинг 379 / 383
- AD. Права доступа 7591 / 7599
- Cisco. Основные события 0 / 0
- Cisco. Ошибки 0 / 0
- Cisco. Соединения 0 / 0
- События AC 0 / 0
- События DeviceController 16228 / 16235
- События FileController 23103 / 23113
- События ProgramController 7779 / 7785
  - Активность вне рабочего вр... 3885 / 3889
  - Активность давно отсутству... 5 / 7**
- Linux. Прочие события Linux 0 / 0
- Linux. События Cron 0 / 0
- Linux. События DNS 0 / 0
- Linux. События SSH 0 / 0
- Linux. События входа/выхода 0 / 0
- Linux. Учетные записи 0 / 0
- Postfix. Основные события 0 / 0
- Postfix. Ошибки 0 / 0
- Отчеты о сетевом трафике 0 / 0
- События 1С: Предприятие 0 / 0
- События Apache 0 / 0

**Глобальный фильтр**  
Дата инцидента: 01.01.2022 00:00:00 - 31.12.2022 23:59:59

**Фильтр правила**  
Флаг:  Вкл.  Выкл.

Дата события: С: . . : : По: . . : :

**Активность давно отсутствующего пользователя**

**Описание:**  
Правило срабатывает при выявлении активности давно отсутствующего пользователя.

**Угроза:**  
Активность учетной записи, которая была неактивна долгое время, заслуживает внимания сотрудника безопасности. К примеру, уволенный сотрудник может стать активным только для того, чтобы скомпрометировать важные для компании данные.

Поиск: Введите строку поиска

Перетащите сюда заголовок поля для группировки

Общие											
* №	Фла	Дата инцидента	Начало	Окончание	Рабочая станция	Пользователь	IP-адрес(а)	Длительность			
1		17.01.2022 8:42:13	04.12.2021 0:13:33	17.01.2022 8:29:00				44 08:15:26			
2		<b>24.01.2022 11:51:22</b>	<b>22.12.2021 16:58:40</b>	<b>24.01.2022 11:40:15</b>				<b>32 18:41:35</b>			
3		<b>24.01.2022 11:51:22</b>	<b>23.12.2021 8:09:01</b>	<b>24.01.2022 11:40:36</b>				<b>32 03:31:34</b>			
4		<b>24.01.2022 11:51:22</b>	<b>22.12.2021 16:59:51</b>	<b>24.01.2022 11:40:57</b>				<b>32 18:41:06</b>			
5		<b>25.01.2022 8:12:48</b>	<b>22.12.2021 15:52:13</b>	<b>25.01.2022 8:01:57</b>				<b>33 16:09:43</b>			
6		<b>31.01.2022 13:22:38</b>	<b>04.12.2021 0:13:33</b>	<b>31.01.2022 13:19:00</b>				<b>58 13:05:26</b>			
7		02.02.2022 10:00:37	23.12.2021 11:49:09	02.02.2022 11:56:24				41 00:07:15			

1 / 1

**Активность давно отсутствующего пользователя**

Дата/время инцидента: **17.01.2022 8:42:13**

Пользователь: [redacted]

Компьютер: [redacted]

Показать события Сброс

# Спасибо за внимание!

## Вопросы?



[https://t.me/  
searchinform](https://t.me/searchinform)



[https://vk.com/sec  
urityinform](https://vk.com/securityinform)



[https://www.youtube.  
com/user/SearchInform](https://www.youtube.com/user/SearchInform)

Практика и аналитика



[https://searchinform.ru/  
practice-and-analytics/](https://searchinform.ru/practice-and-analytics/)