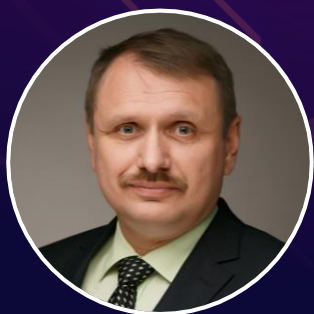




Гибкость и объективность. Полезность симбиоза SIEM и DCAP



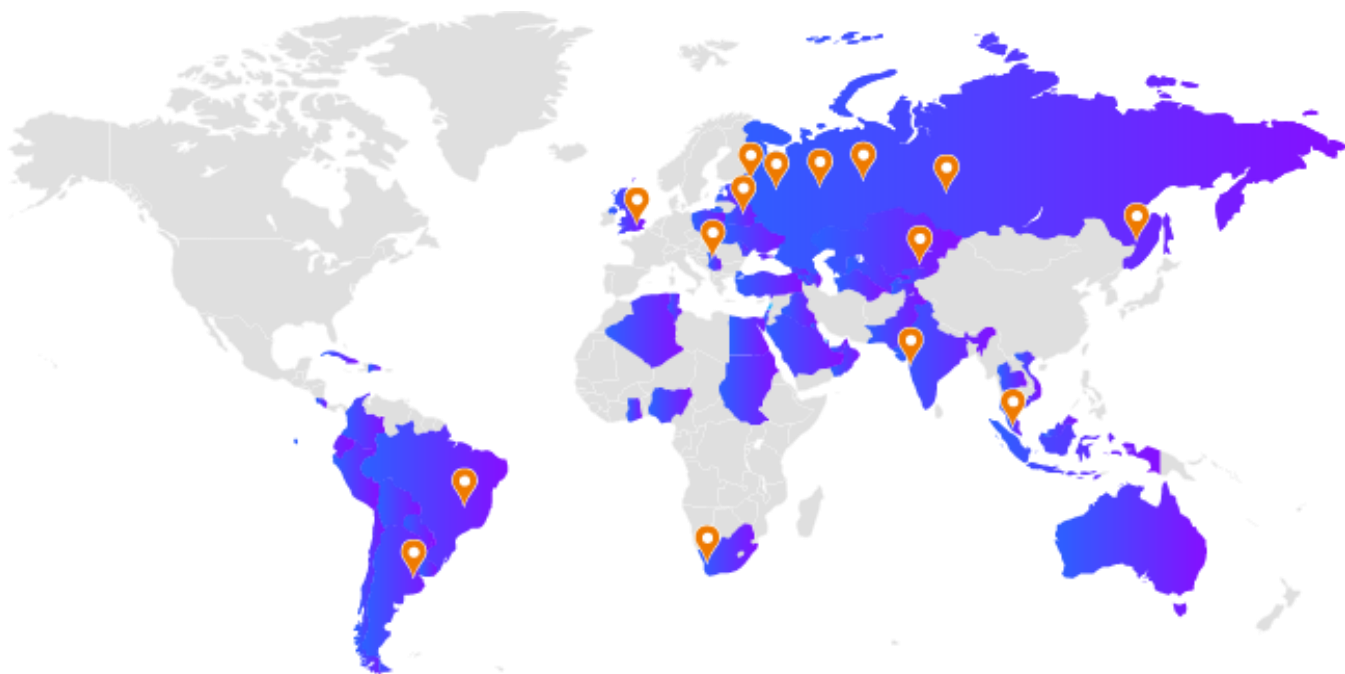
Дмитрий Стельченко

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:

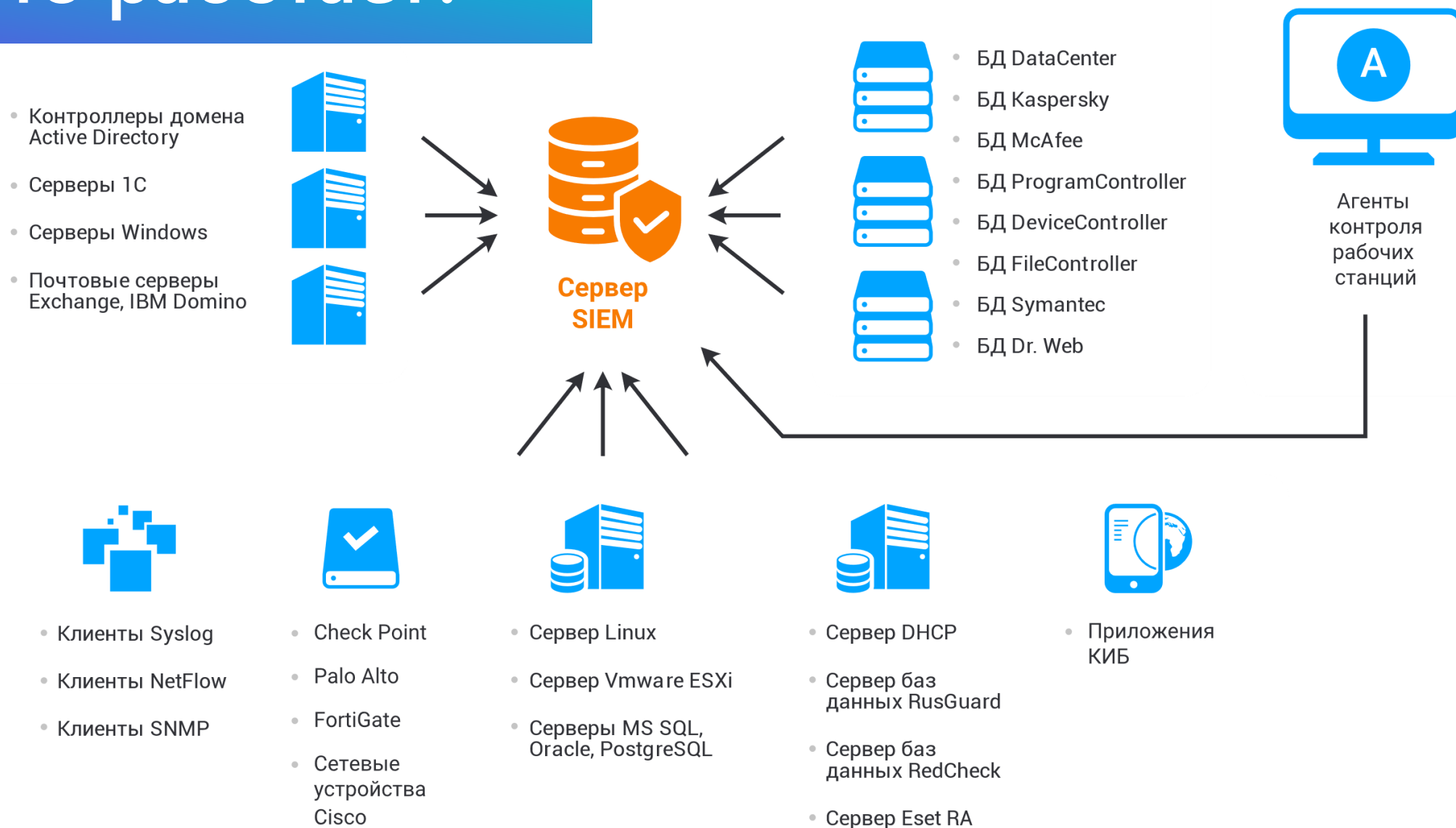
- Скрытые подключения.
- Обход сетевых средств защиты.
- Нетиповую файловую активность пользователей.
- Нетиповую файловую активность процессов.
- Выполнение скриптов и прочие не отражающиеся в классическом логировании инциденты.

#CODEIB

SEARCHINFORM

INFORMATION SECURITY

Как это работает?



Как это работает?

The screenshot displays the SIEM Client console interface. The main window is titled "Rules - SIEM.Client console [1.45.2.1]". The interface is divided into several sections:

- Left Panel (Rules List):** A list of rules with their status and counts. The selected rule is "Большое количество пользователей, работающих с файлом" (56 / 58).
- Right Panel (Rule Configuration):** Shows the rule's description and threat level. The description states: "Инциденты показывают ситуации, когда к одному файлу за короткий промежуток времени подключается аномально большое количество пользователей." The threat level is "Отчет может говорить о статистических аномалиях, когда пользователь слишком часто обращается к определенным файлам."
- Table (Incident Log):** A table listing incidents with columns for ID, Flag, Date, Source, File, File Size, and Device Type. The table shows 10 incidents, all occurring on 09.02.2022 at 13:48:22, involving various files on the local drive (C:\aaa\zaq\...).
- Global Filter:** A section for filtering incidents by date, ranging from 01.02.2022 00:00:00 to 28.02.2022.
- Rule Filter:** A section for filtering the rule by flag (currently "вкл.") and event date.

The bottom status bar shows the current rule name, its status ("Выполняется"), and the total number of records ("Всего записей: 58"). The system tray includes the IP address "192.168.175.50:27017\siem" and a 100% zoom level.

#CODEIB

SEARCHINFORM
INFORMATION SECURITY

Как это работает?

#CODEIB

SEARCHINFORM
INFORMATION SECURITY

The screenshot displays the SIEM Client console interface. On the left, a sidebar lists various rules with their counts. The main area shows the configuration for a rule named 'Активность давно отсутствующего пользователя'. Below this, a table lists several incidents. The selected incident (ID 1) is detailed at the bottom of the screen.

Правила

- 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

Правило: 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.

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

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: : :

1 / 1

Активность давно отсутствующего пользователя

Дата/время инцидента: 17.01.2022 8:42:13

Пользователь: [redacted]

Компьютер: [redacted]

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/)