КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

31 МАРТА, 2022
КРАСНОЯРСК

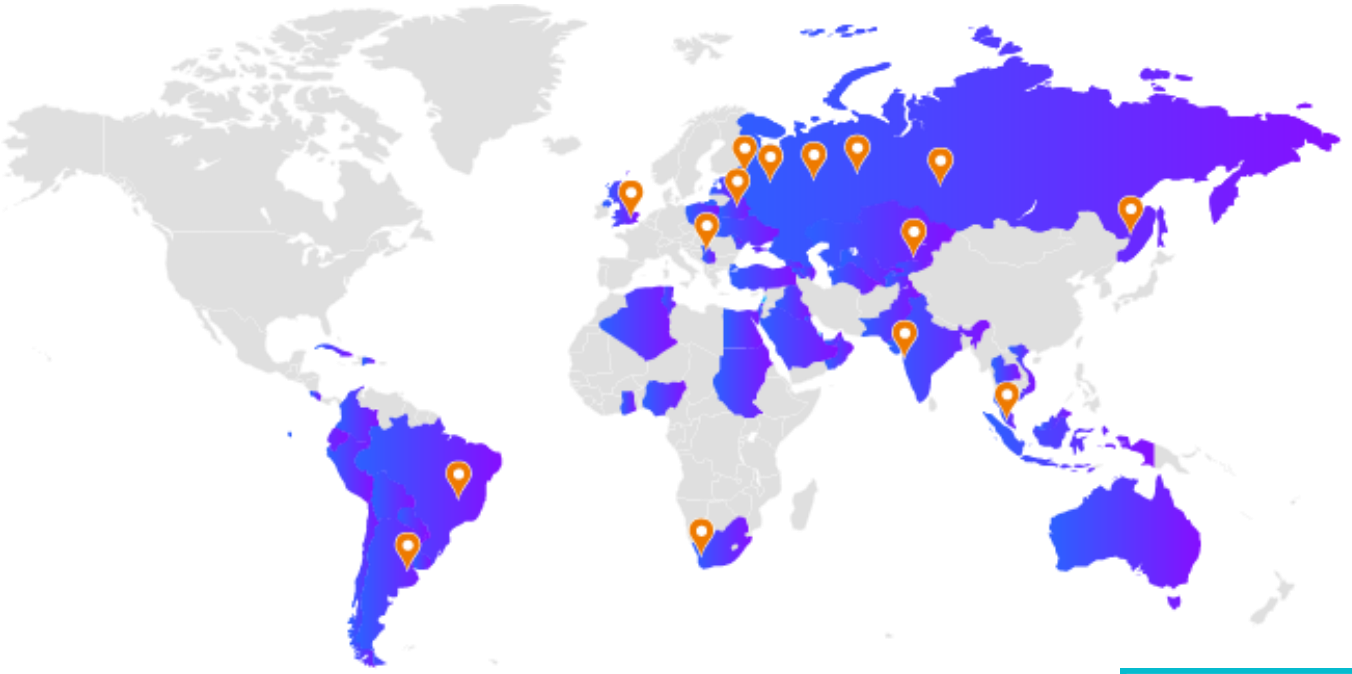
Гибкость и объективность.
Польза симбиоза SIEM и DCAP

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»

Продукты «СёрчИнформ» входят в Реестр отечественного ПО

Решения «СёрчИнформ»

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

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

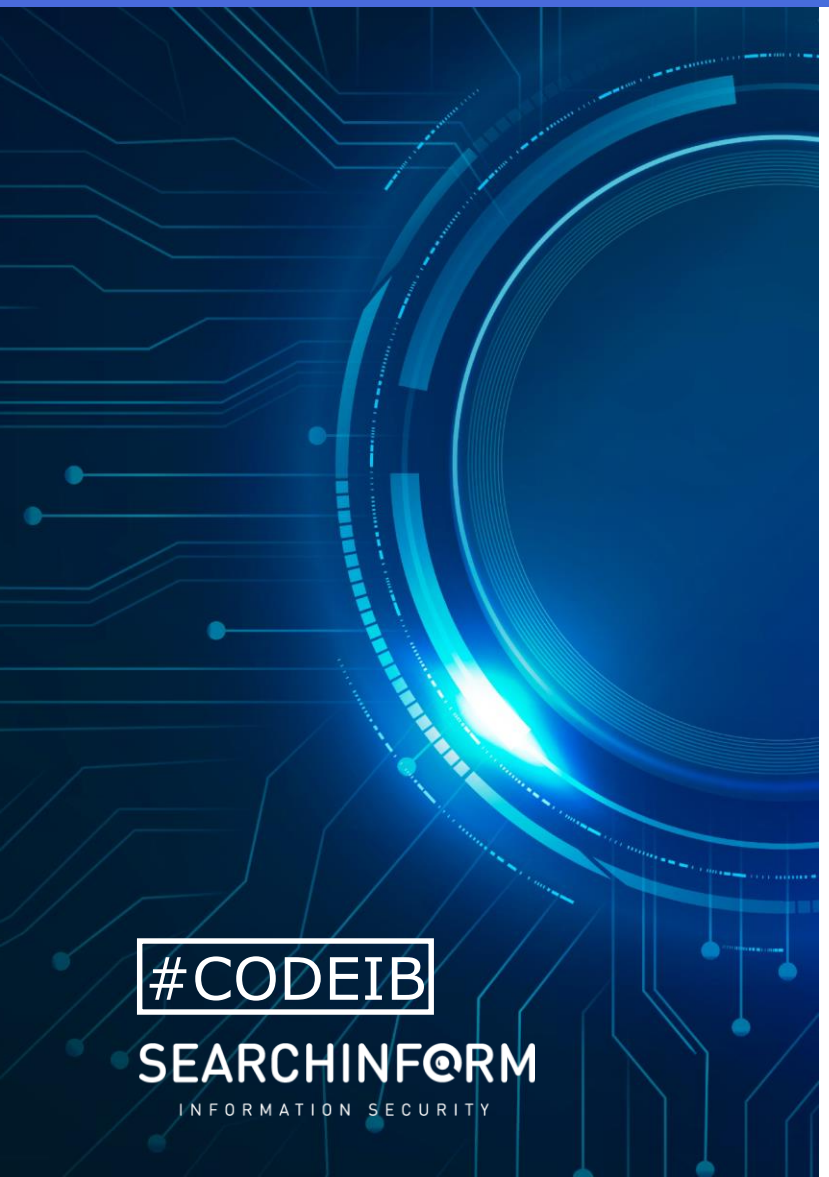
Нерешенные проблемы современных SIEM

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 DCAP одинаковы



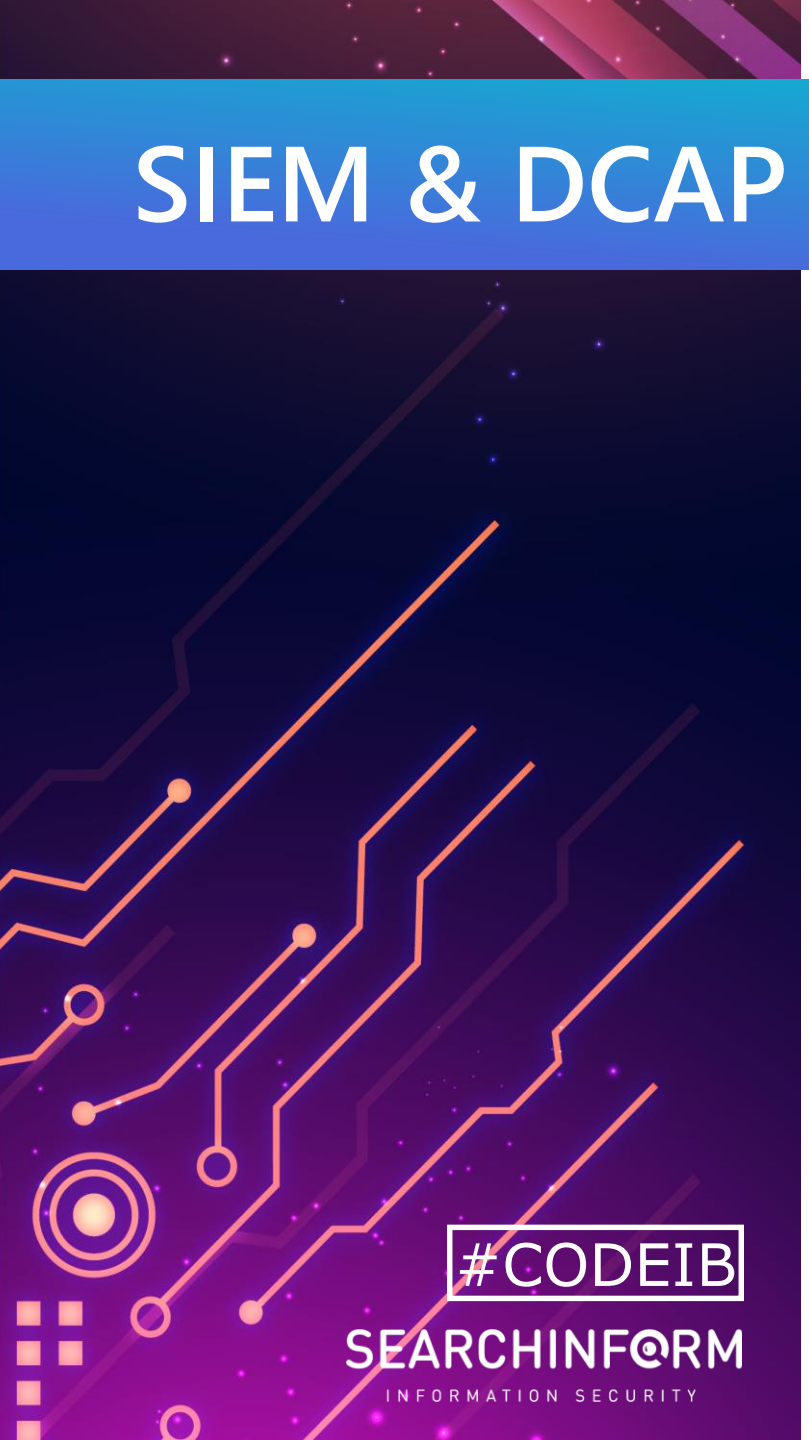
Даже известные DCAP имеют критические проблемы:

- 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 связки с Endpoint`ами (безагентские), поэтому не видят активности процессов.

Идеальный DCAP «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



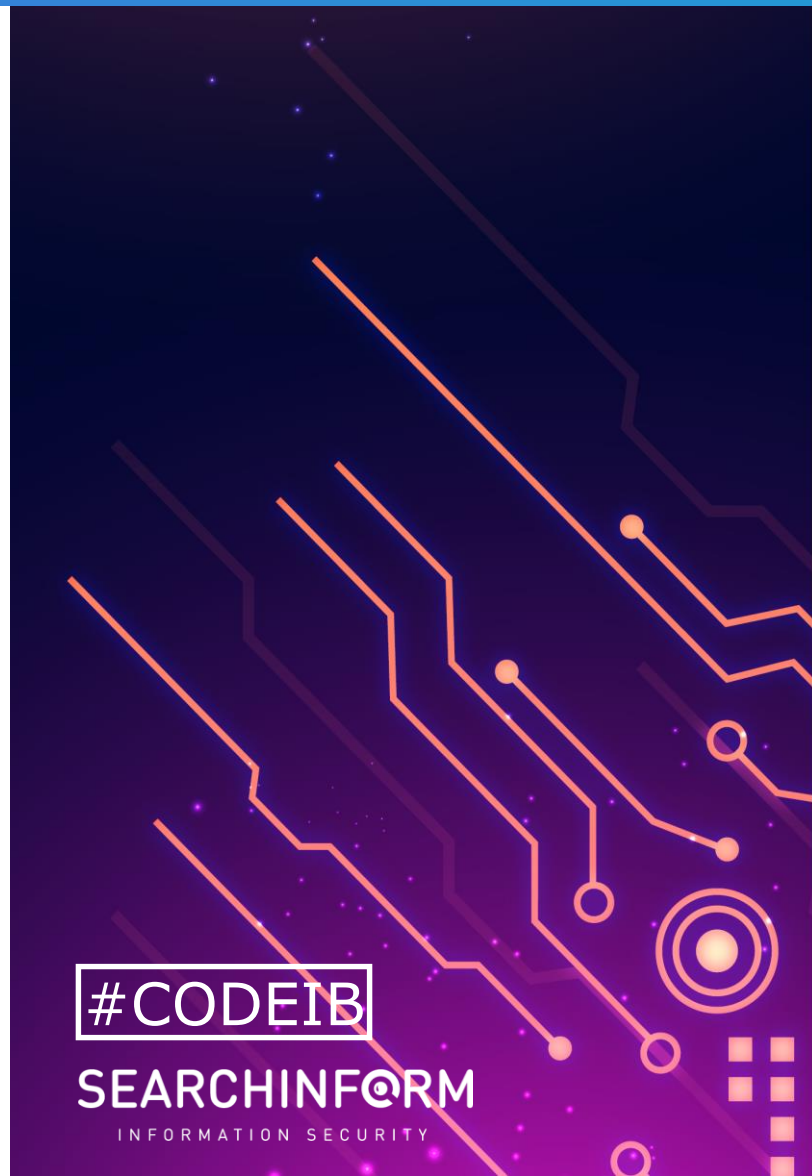
Совместное использование SIEM и DCAP даёт:

- 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.

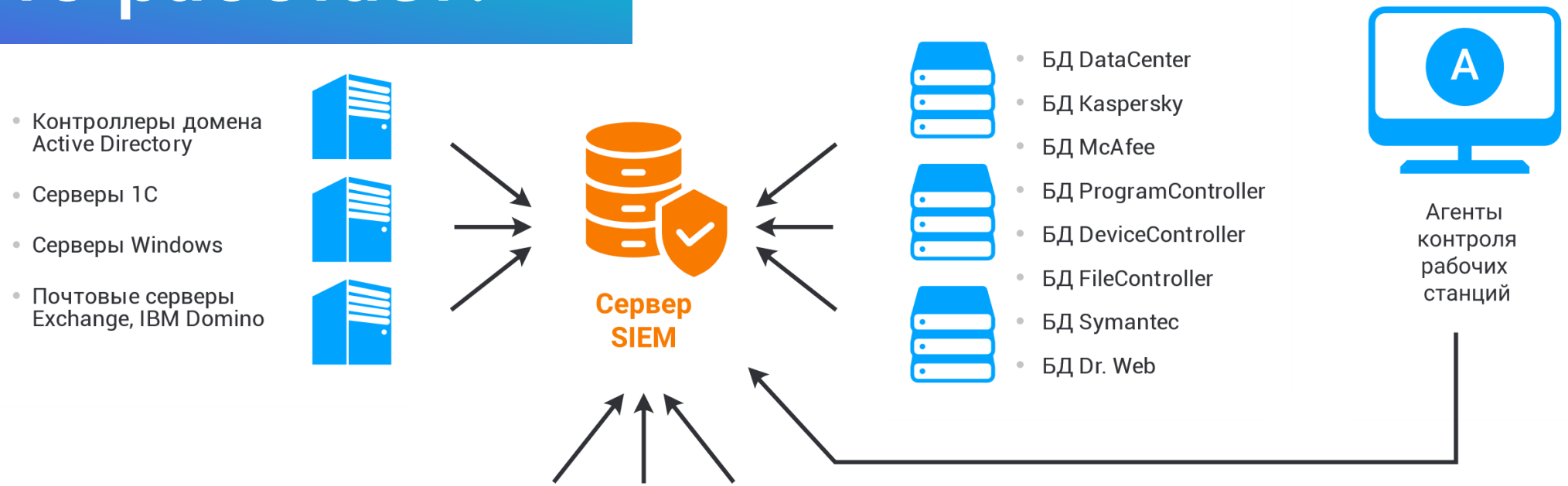
SIEM & DCAP

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.



Как это работает?



- Клиенты Syslog
- Клиенты NetFlow
- Клиенты SNMP

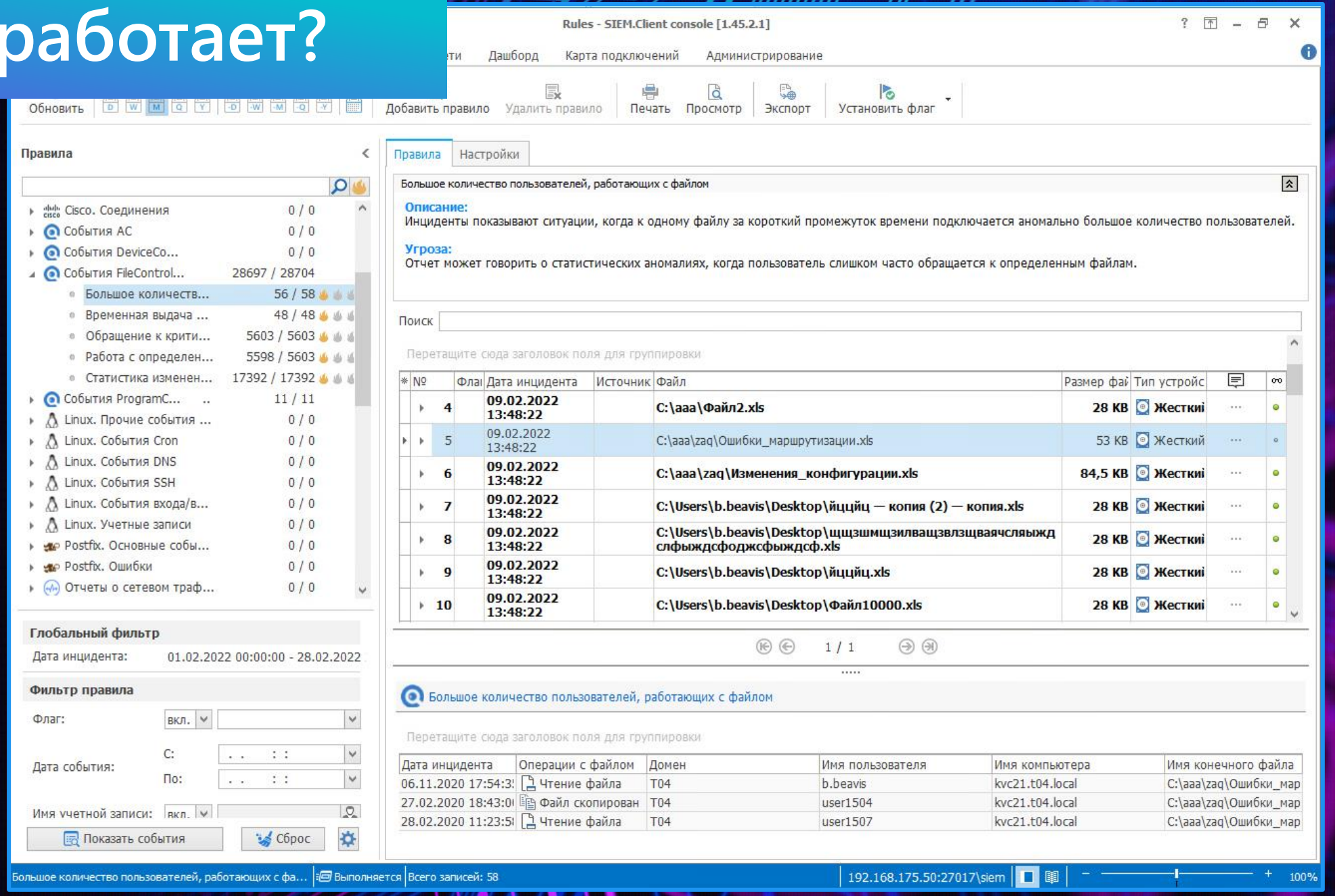
- Check Point
- Palo Alto
- FortiGate
- Сетевые устройства Cisco

- Сервер Linux
- Сервер Vmware ESXi
- Серверы MS SQL, Oracle, PostgreSQL

- Сервер DHCP
- Сервер баз данных RusGuard
- Сервер баз данных RedCheck
- Сервер Eset RA

- Приложения КИБ

Как это работает?



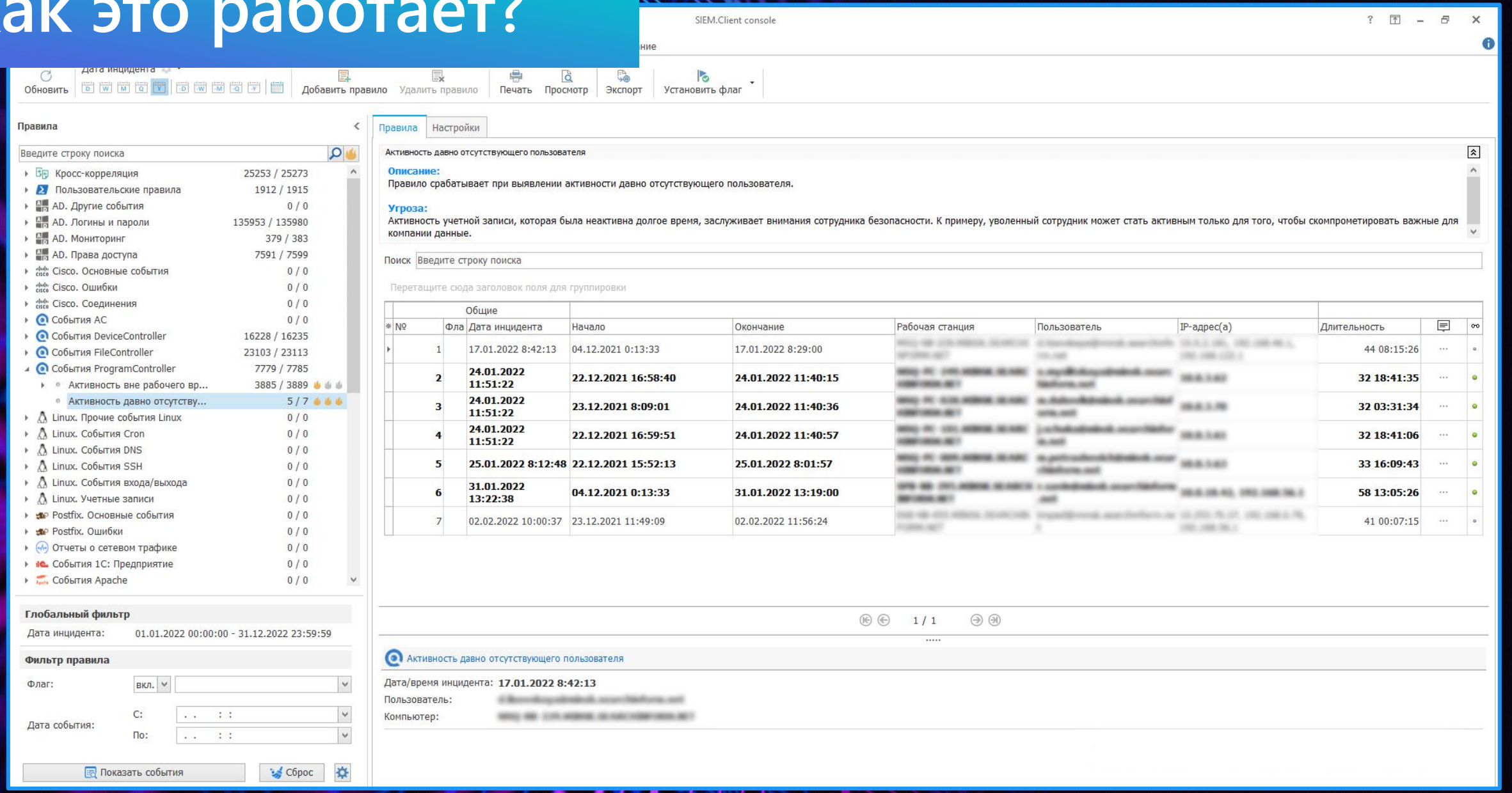
#CODEIB

SEARCHINFORM

INFORMATION SECURITY

Как это работает?

#CODEIB SEARCHINFORM INFORMATION SECURITY



Спасибо за внимание!
Вопросы?

https://t.me/
searchinform

https://vk.com/sec
urityinform

https://www.youtube.
com/user/SearchInform

Практика и аналитика

https://searchinform.ru/
practice-and-analytics/

SEARCHINFORM
INFORMATION SECURITY