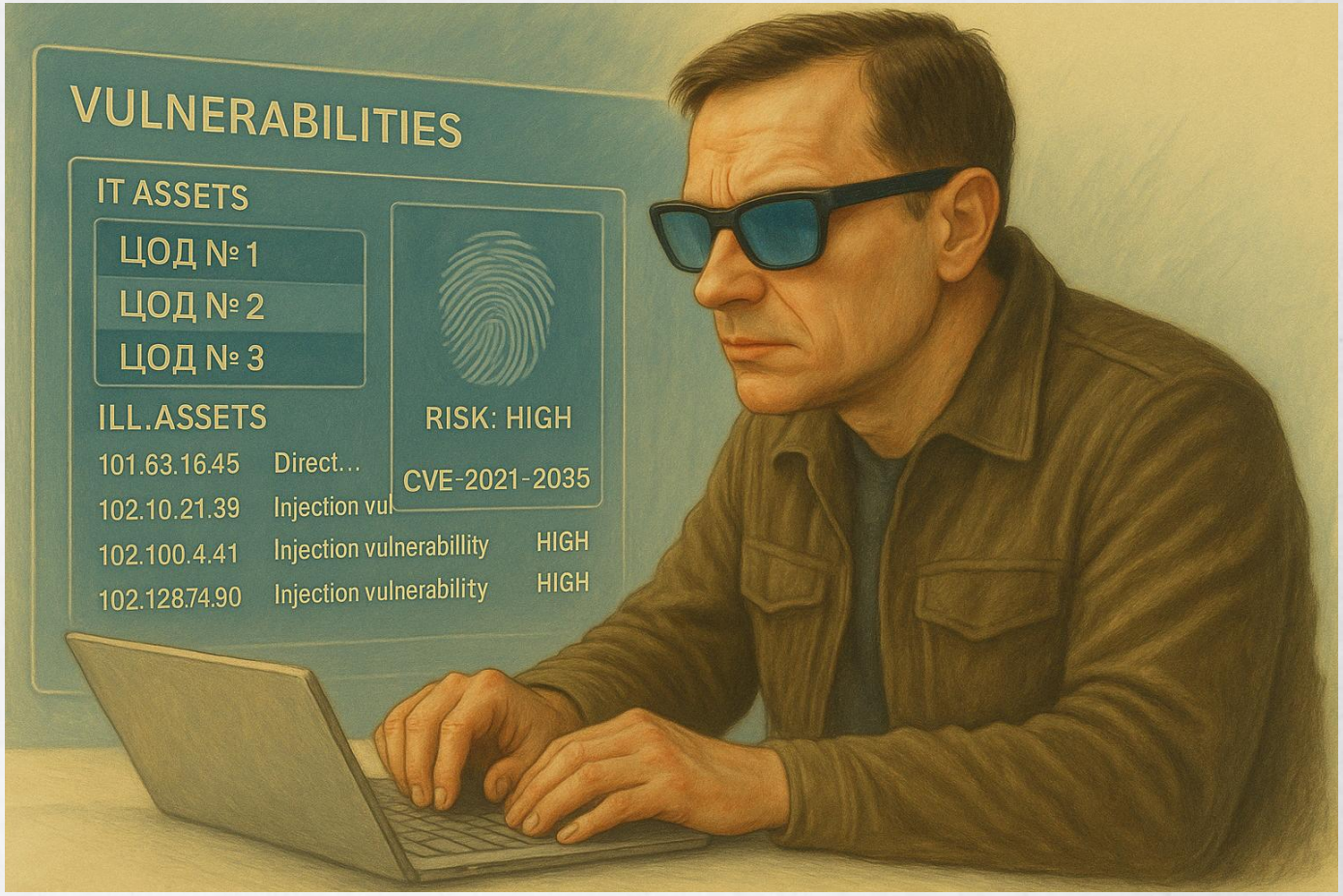
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

ИБ БЕРЁТ ДЕЛО В СВОИ РУКИ:

КАК МЫ СОЗДАЛИ ЕДИНОЕ ОКНО ДЛЯ АВТОМАТИЧЕСКОГО СБОРА ДАННЫХ ОБ АКТИВАХ И УЯЗВИМОСТЯХ ИЗ МНОЖЕСТВА ИСТОЧНИКОВ

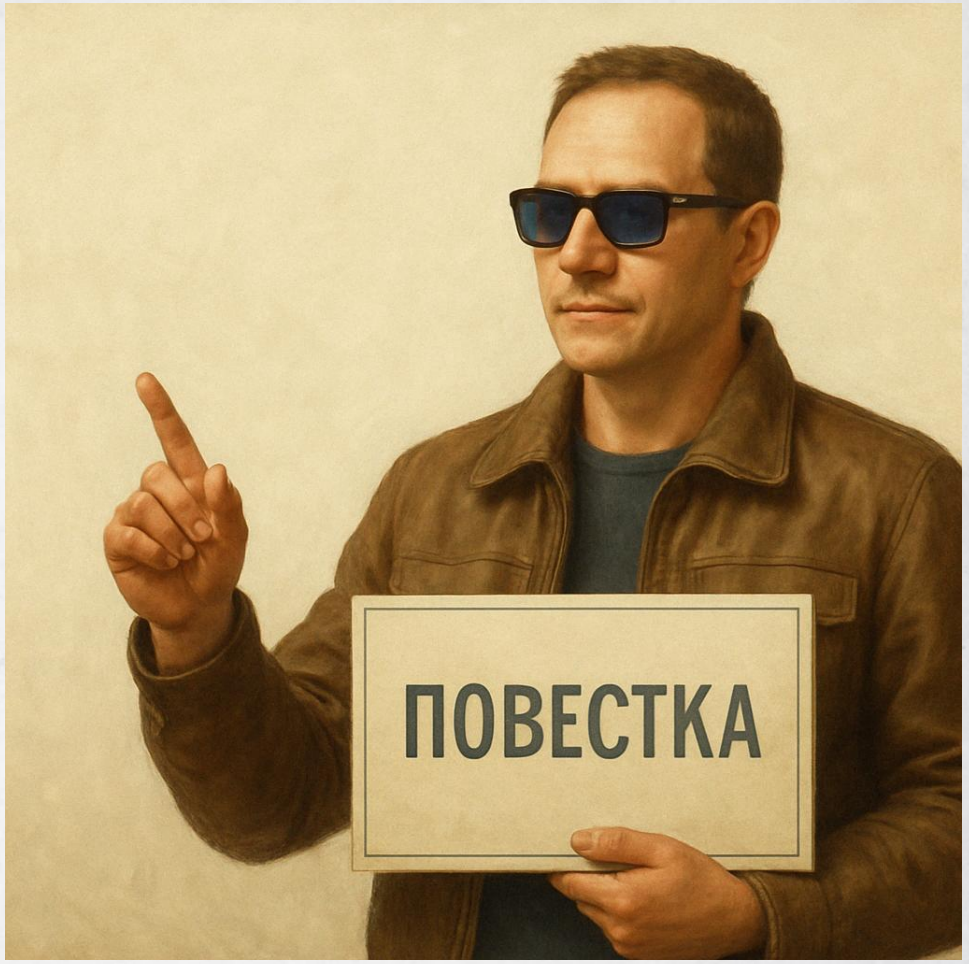


КИРИЛЛ КАРПИЕВИЧ
Специалист по анализу уязвимостей
СберТех

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

О чем поговорим?

- Место VM на поляне ИБ, и что там с управлением ИТ-активами
- ИБ и ИТ в процессе VM: ⚔ или 🤝?
- Как было и что болело ДО
- Как решили и вылечили без плацебо
- Итог и затравка на холивар



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

Место VM на поляне ИБ, и что там с управлением ИТ-активами

Итоги опроса 20 CISO в интересах вебинара:

Мониторинг событий и реагирование на инциденты

Назвали 16 человек

Поиск и устранение уязвимостей

Назвали 14 человек

Выполнение требований законодательства или головной организации

Назвали 11 человек

https://forms.yandex.ru/u/680661c250569075b3b1c93f/

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

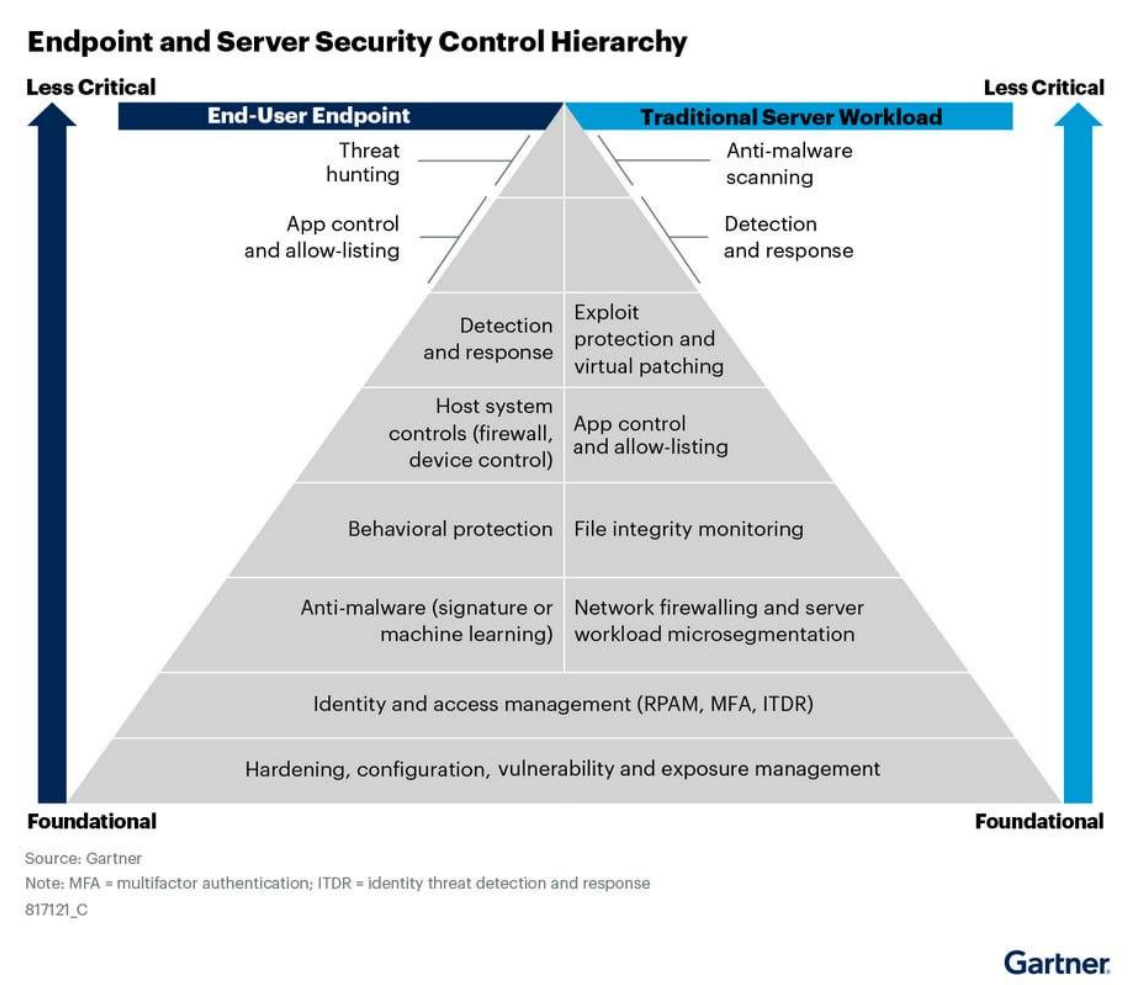
Инвентаризация ИТ-активов и управление ими

Назвали ?? человек

https://forms.yandex.ru/u/680661c250569075b3b1c93f/

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

Место VM на поляне ИБ, и что там с управлением ИТ-активами



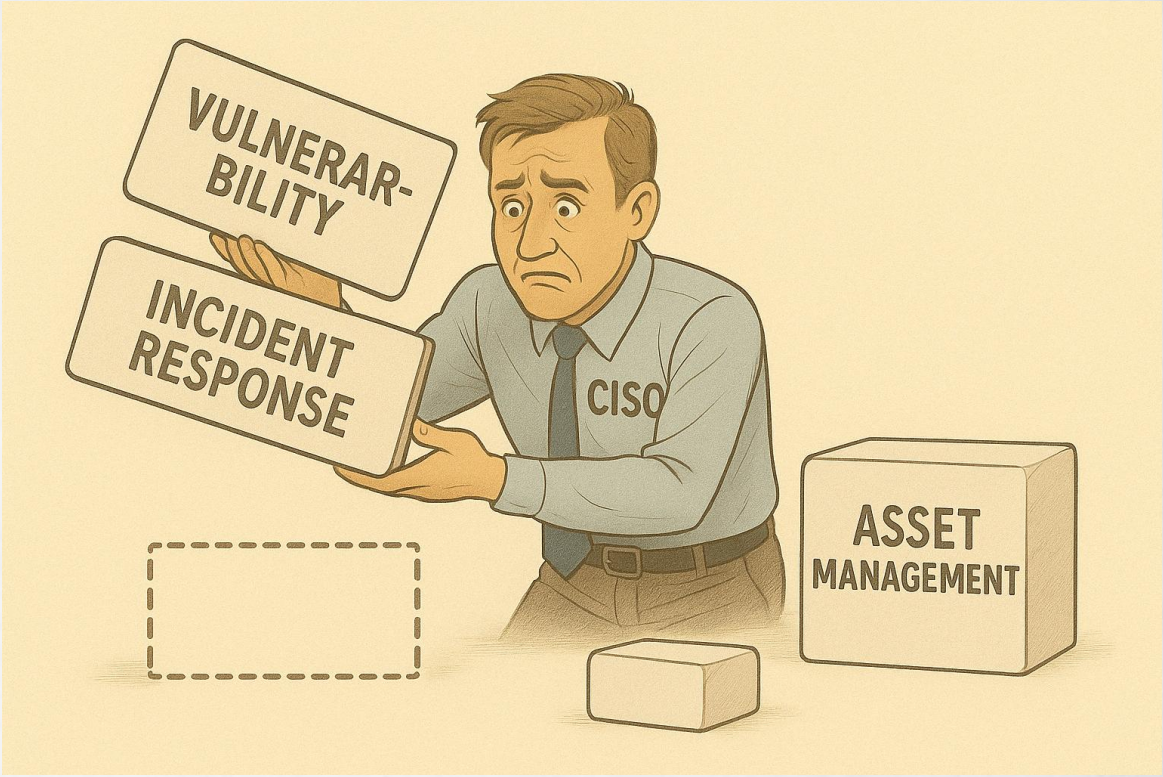
Источник: https://t.me/alexredsec/562

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

Место VM на поляне ИБ, и что там с управлением ИТ-активами

Инвентаризация ИТ-активов и управление ими

Назвал **1** человек



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНФЕРЕНЦИЯ

ИБ и ИТ в процессе VM: ⚔ или 🤝?

НЕТ формализованного процесса или он не соответствует реальности

НЕТ владельца процесса VM

НЕТ приоритизации уязвимостей

НЕТ согласованных с ИТ SLA

НЕТ четких зон ответственности: кто, что и как обновляет / чинит

=

ИБ ⚔ ИТ

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

ИБ и ИТ в процессе VM: ⚔ или 🤝?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНФЕРЕНЦИЯ

ИБ и ИТ в процессе VM: ⚔ или 🤝?

ЕСТЬ договоренности с ИТ по SLA

ЕСТЬ владельцы ИТ-активов и ответственные за обновление

ЕСТЬ перечень недопустимых событий, смапленных на группы активов → известны критичности активов

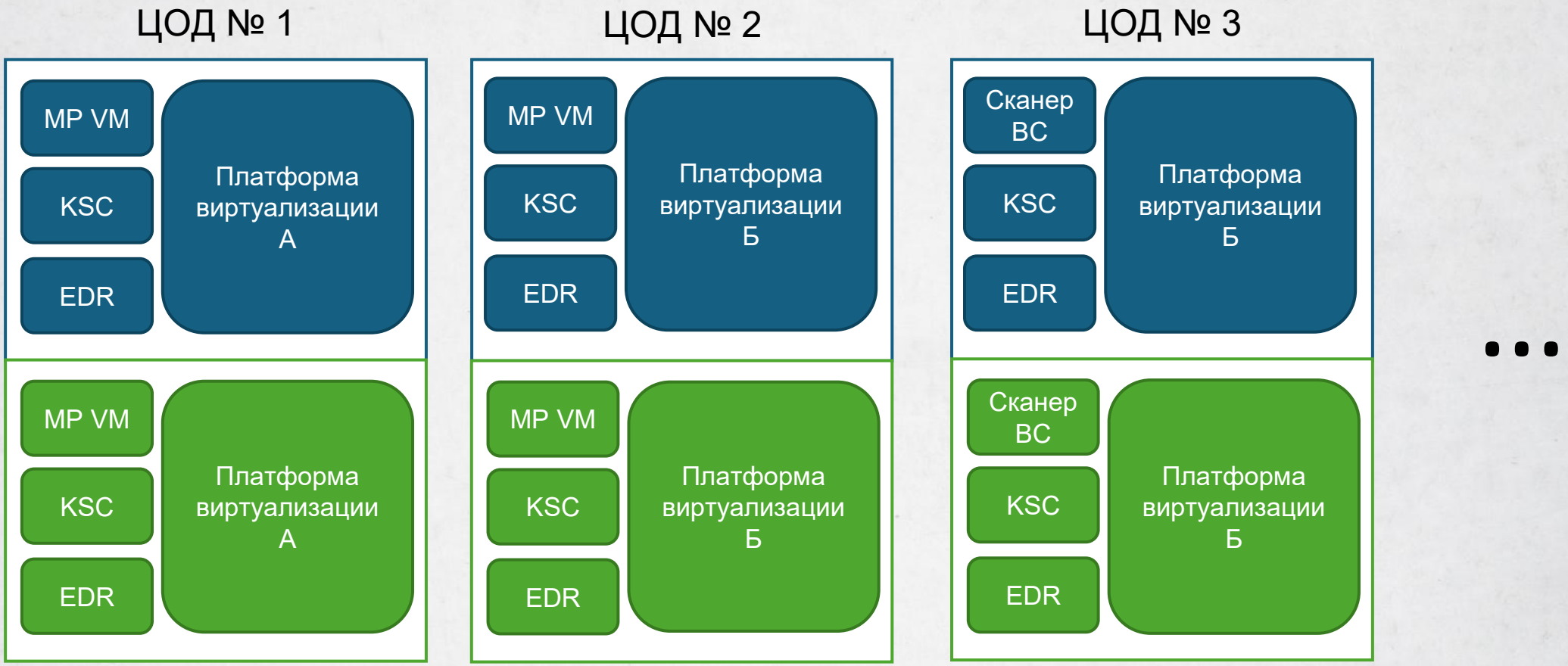
ЕСТЬ понятный и прозрачный для всех стейкхолдеров процесс

=

ИБ 🤝 ИТ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

Как было и что болело ДО



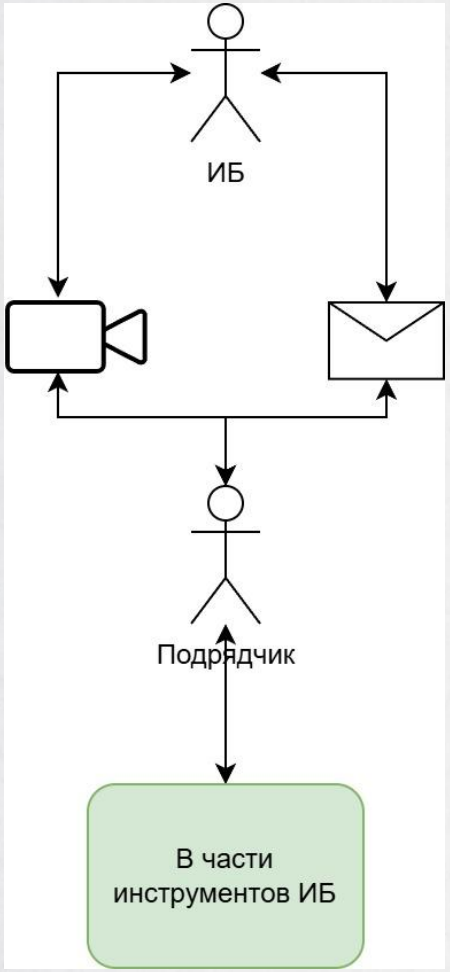
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНФЕРЕНЦИЯ

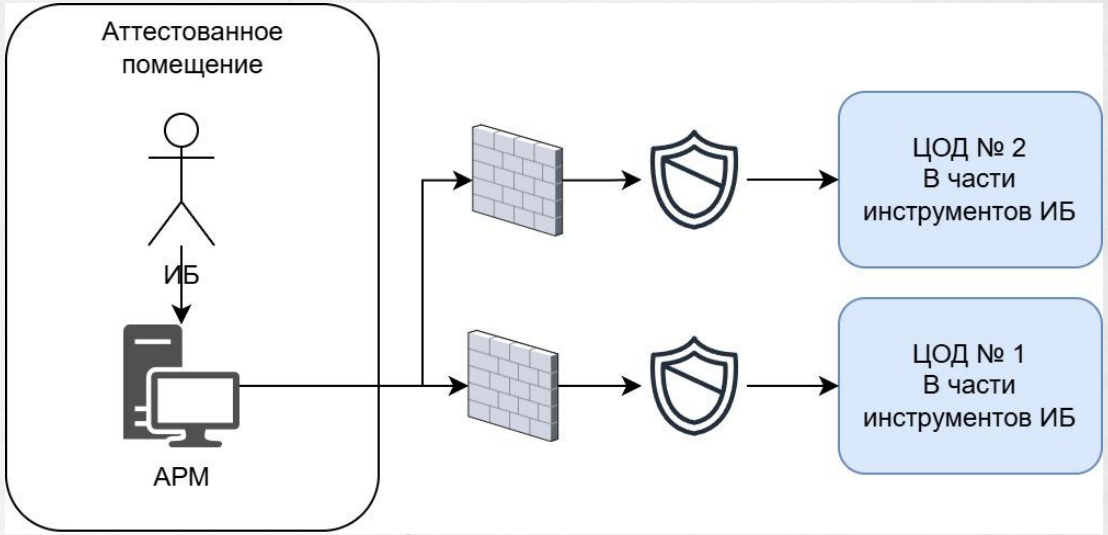
Как было и что болело ДО

...

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

Как было и что болело ДО





КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

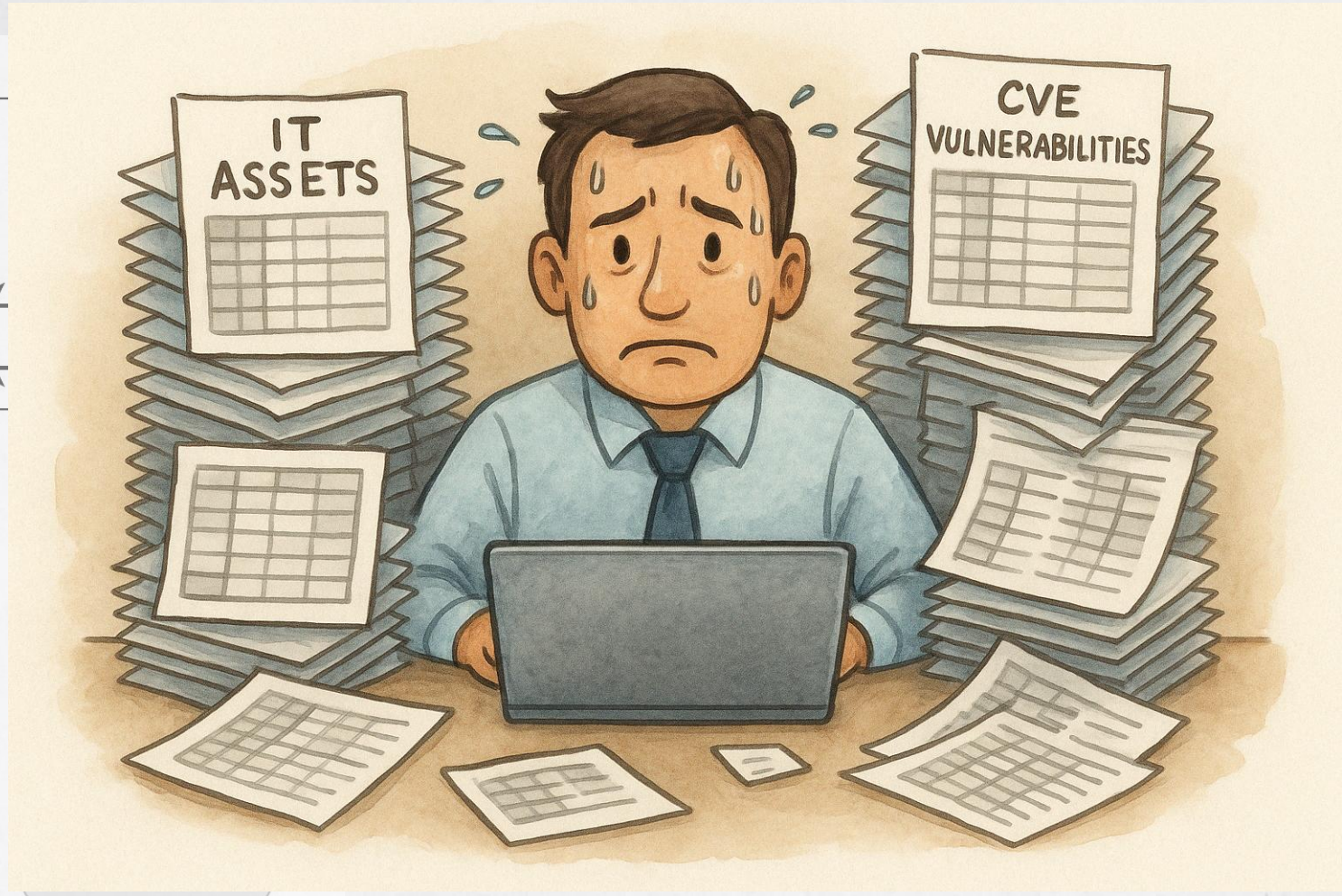
Как было и что болело ДО

ЦОД № 2
В части
инструментов ИБ

ЦОД № 1
В части
инструментов ИБ

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

Как было и что болело ДО



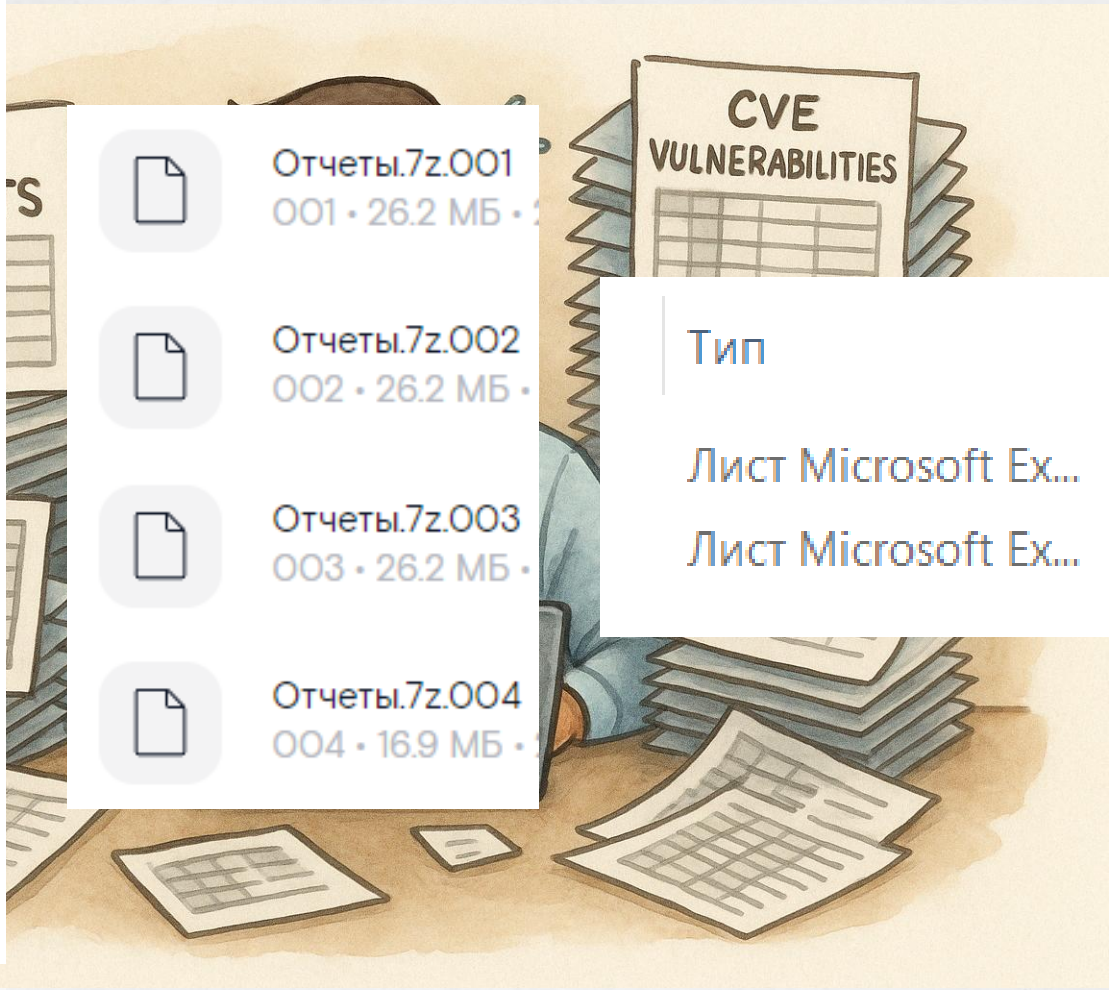
ЦОД № 2
В части
инструментов ИБ

ЦОД № 1
В части
инструментов ИБ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

Как было и что болело ДО

- Overcloud.xlsx
- Undercloud.xlsx
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...
- Дополнение к BDU_Unix_...



Отчеты.7z.001
001 • 26.2 МБ •

Отчеты.7z.002
002 • 26.2 МБ •

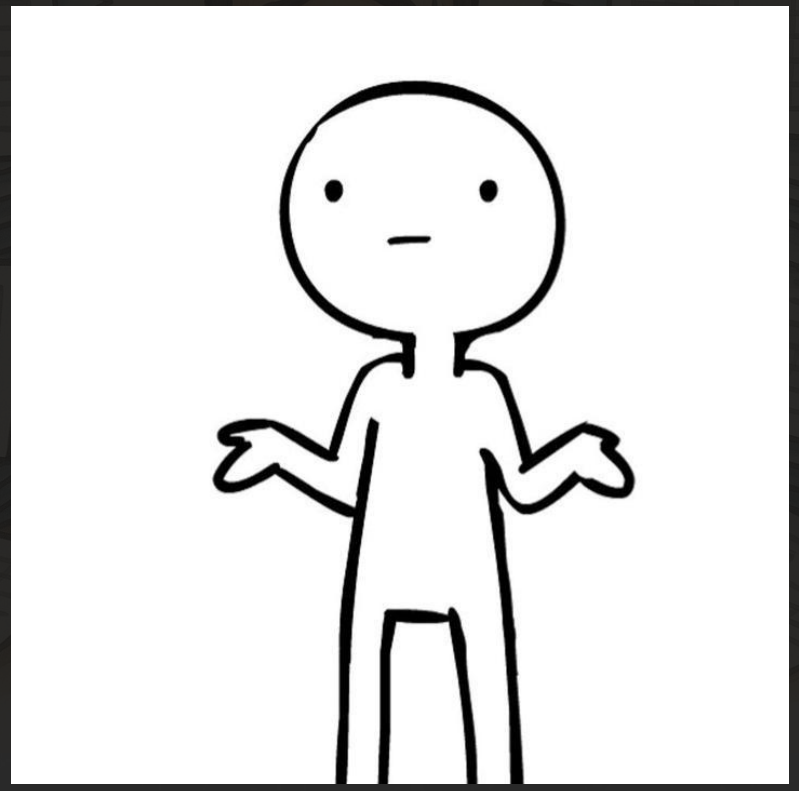
Отчеты.7z.003
003 • 26.2 МБ •

Отчеты.7z.004
004 • 16.9 МБ •

Тип	Размер
Лист Microsoft Ex...	111 921 КБ
Лист Microsoft Ex...	5 863 КБ

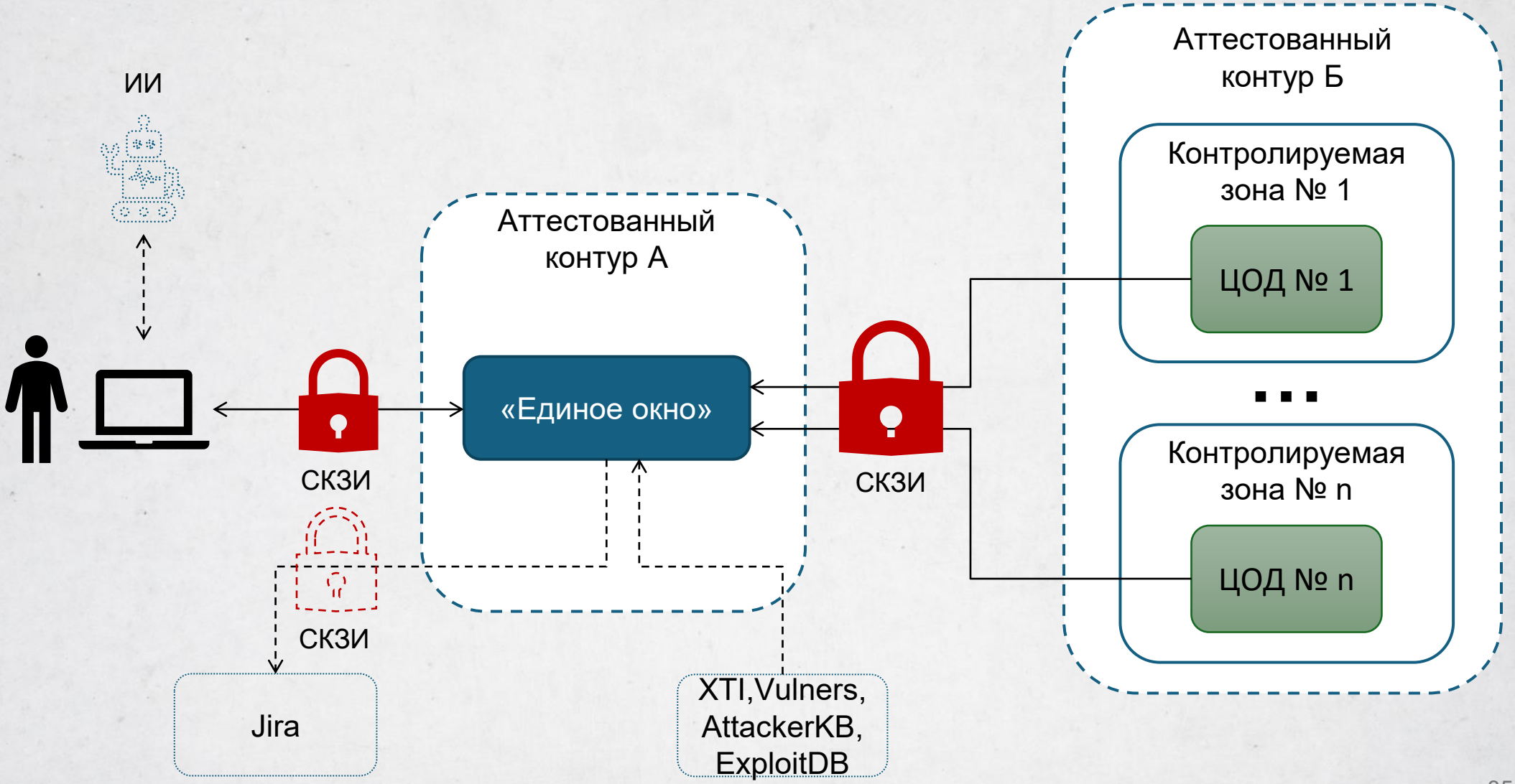
инструментов ИБ

Как дальше работать?
И вообще — как же резбез?



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНФЕРЕНЦИЯ

Как решили и вылечили без плацебо



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

Как решили и вылечили без плацебо

ДОГОВОРИЛИСЬ со всеми подрядчиками о предоставлении необходимых доступов

ДОГОВОРИЛИСЬ о форматах и периодичности предоставления артефактов

ДОГОВОРИЛИСЬ о дальнейшем построении процесса VM учетом внедрения новой системы

Порядок управления уязвимостями приведен в соответствие реальности и **СОГЛАСОВАН** со всеми заинтересованными сторонами

Так почему же «берем в СВОИ руки»?

1. «Доверяй, но проверяй!»
2. Нам было проще.
3. Заточили под цели ИБ.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНФЕРЕНЦИЯ

Итоги и затравка на «холивар»

Кейс: на каждый ИТ-актив установлен определенный приклад (PostgreSQL, elk, ClickHouse и др.)
Активов > 10k.

Сотрудники, ответственные за приклад, не соглашаются обновлять пакеты и ядро ОС, перенаправляя задачи на команду Linux / Инфраструктура.

Хоть и редко, но обновления вызывают проблемы именно в работе приклада: в итоге, команды сопровождения приклада все равно участвуют в АВР.

ВОПРОС: кто должен обновлять ОС?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНФЕРЕНЦИЯ

Итоги и затравка на «холивар»

Добились существенного снижения трудозатрат за счет **централизации** данных

Получаем информацию об активах в полном объеме из первоисточников

С помощью встроенных инструментов визуализации (метрики) строим дашборды **сразу по всем** площадкам

За счет автоматизации информация **актуальна всегда**

Сроки устранения уязвимостей снизились

Покрыли потребности подразделений управления уязвимостями и инцидентами ИБ, аудита ИБ (в части контроля покрытия СЗИ)

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
КОНФЕРЕНЦИЯ

СПАСИБО ЗА ВНИМАНИЕ!