

Форум ITSEC 2025

08.09.2025

УЯЗВИМОСТИ РЕШЕНИЙ ПО СЕТЕВОЙ БЕЗОПАСНОСТИ

ЧТО ИЗМЕНИЛОСЬ ЗА ГОД (С СЕНТЯБРЯ 2024)

НАТАЛЬЯ ОНИЩЕНКО

НЕЗАВИСИМЫЙ ЭКСПЕРТ ПО КИБЕРБЕЗОПАСНОСТИ

АКТУАЛЬНЫЙ ВОПРОС

Каким должен быть процесс публикации уязвимостей?

+

уязвимости
оперативно
обнаруживаются
и публикуются

-

есть PoC, нет
патча или
workaround



ПУБЛИКАЦИЯ НЕ ДОЛЖНА СОЗДАВАТЬ РЕАЛЬНЫЕ РИСКИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМ

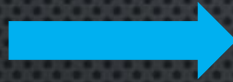
ПУБЛИКАЦИЯ УЯЗВИМОСТЕЙ И ТЕОРИЯ ПОЛЯ КУРТА ЛЕВИНА

Способствующие силы

заказчики

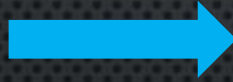


интеграторы



вендоры

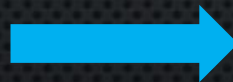
(в части других решений)



злоумышленники



государство



Публикация
уязвимостей

Сдерживающие силы

вендоры

(в части своих решений)



законопроекты



злоумышленники



для полноценного запуска процесса способствующие силы должны перевесить

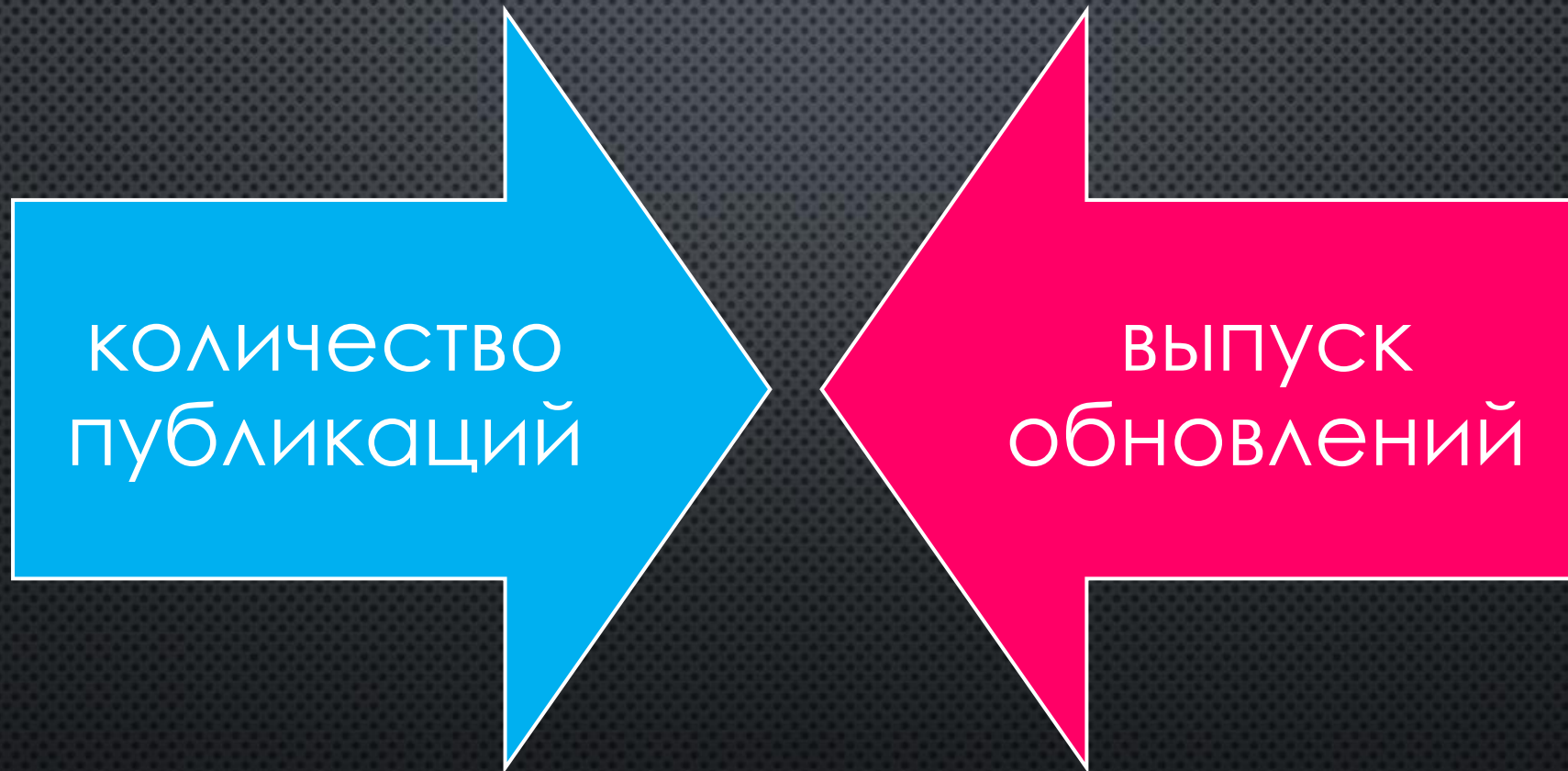
КТО ОБНАРУЖИВАЕТ УЯЗВИМОСТИ

идентификатор	угроза	Дата публикации	Кто обнаружил
SUM-16541	Перехват удаленного помощника	05.05.2025 портал вендора	
SUM-17063	Выполнение произвольной команды в CLI	портал вендора	
BDU:2025-08181	Уязвимость кода	09.07.2025 BDU ФСТЭК	Positive Technologies
BDU:2025-02934	Уязвимость веб-интерфейса	24.03.2025 BDU ФСТЭК	АО «СберТех»
BDU:2025-04720	выполнение команды удаленным пользователем с max привилегиями	05.05.2025 BDU ФСТЭК	Иванов Кирилл, исследователь



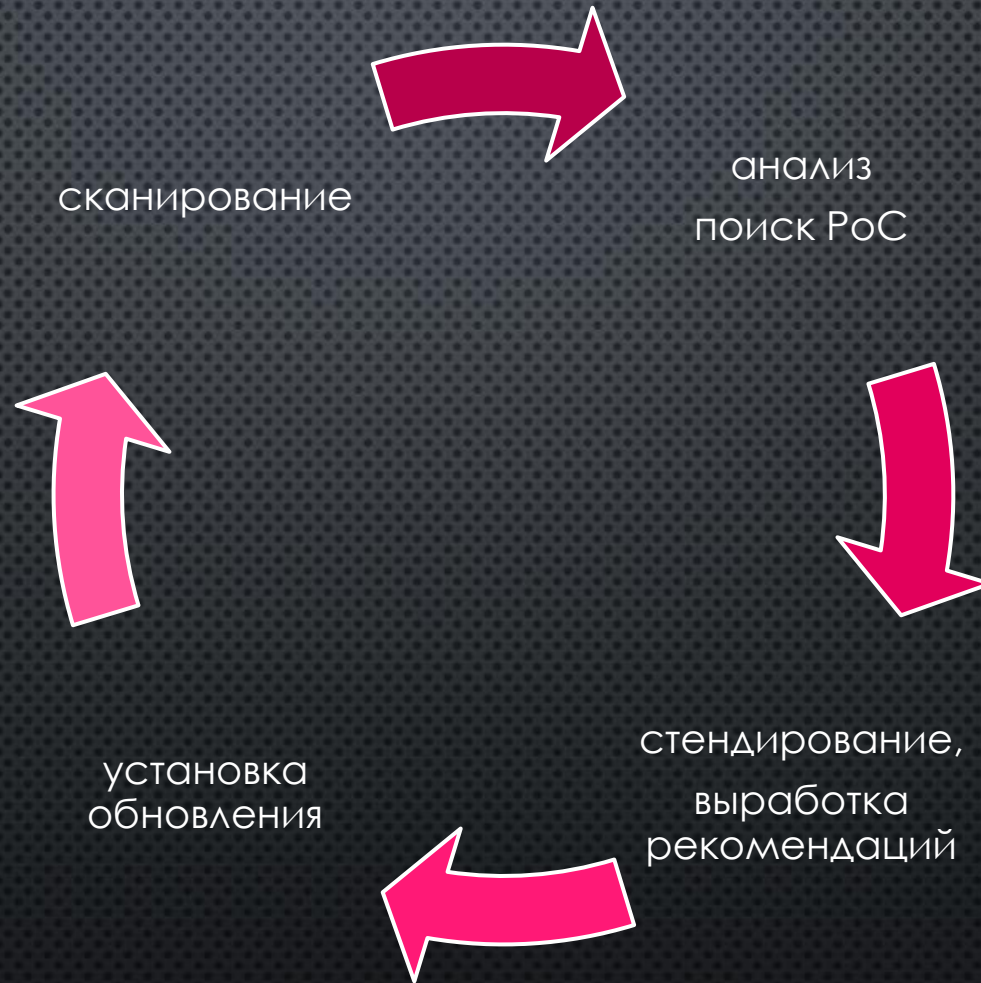
ИНОГДА ВЕНДОРЫ ЛУЧШЕ СЛЕДЯТ ЗА КОНКУРЕНТАМИ, ЧЕМ ЗА СВОИМИ ПРОДУКТАМИ

АКТУАЛЬНЫЕ ТЕНДЕНЦИИ



ВЕНДОРЫ БОЛЕЕ ТЩАТЕЛЬНО ТЕСТИРУЮТ ПО, ЧТО СДВИГАЕТ СРОКИ РЕЛИЗОВ ЛИБО ВЫЗЫВАЕТ ОТЗЫВЫ ПАКЕТОВ

ПРОЦЕСС ЗАКРЫТИЯ УЯЗВИМОСТЕЙ (ВНУТРИ КОМПАНИИ)



УЯЗВИМОСТИ ПРОДУКТОВ ТРЕБУЮТ ПРИСТАЛЬНОГО ВНИМАНИЯ ЭКСПЛУАТИРУЮЩИХ ПОДРАЗДЕЛЕНИЙ

КРАТКИЕ ИТОГИ



- курс на оповещение об уязвимостях
- независимые эксперты, бюллетени НКЦКИ, BDU ФСТЭК и сканеры помогают быть в курсе событий
- случаи отзыва обновлений создают проблемы, но не являются плохим знаком
- увеличились сроки выдачи релизов



НАМЕТИЛСЯ СЕРЬЕЗНЫЙ ПОЗИТИВНЫЙ ТРЕНД, ЕСТЬ ОПАСЕНИЯ ПОЯВЛЕНИЯ «ЧЕРНЫХ ЛЕБЕДЕЙ»



**СПАСИБО
ЗА ВАШЕ ВНИМАНИЕ
ДАВАЙТЕ ОБСУДИМ!**
