

МЕТОДЫ И ИНСТРУМЕНТЫ ДЛЯ ВЫЯВЛЕНИЯ И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ:

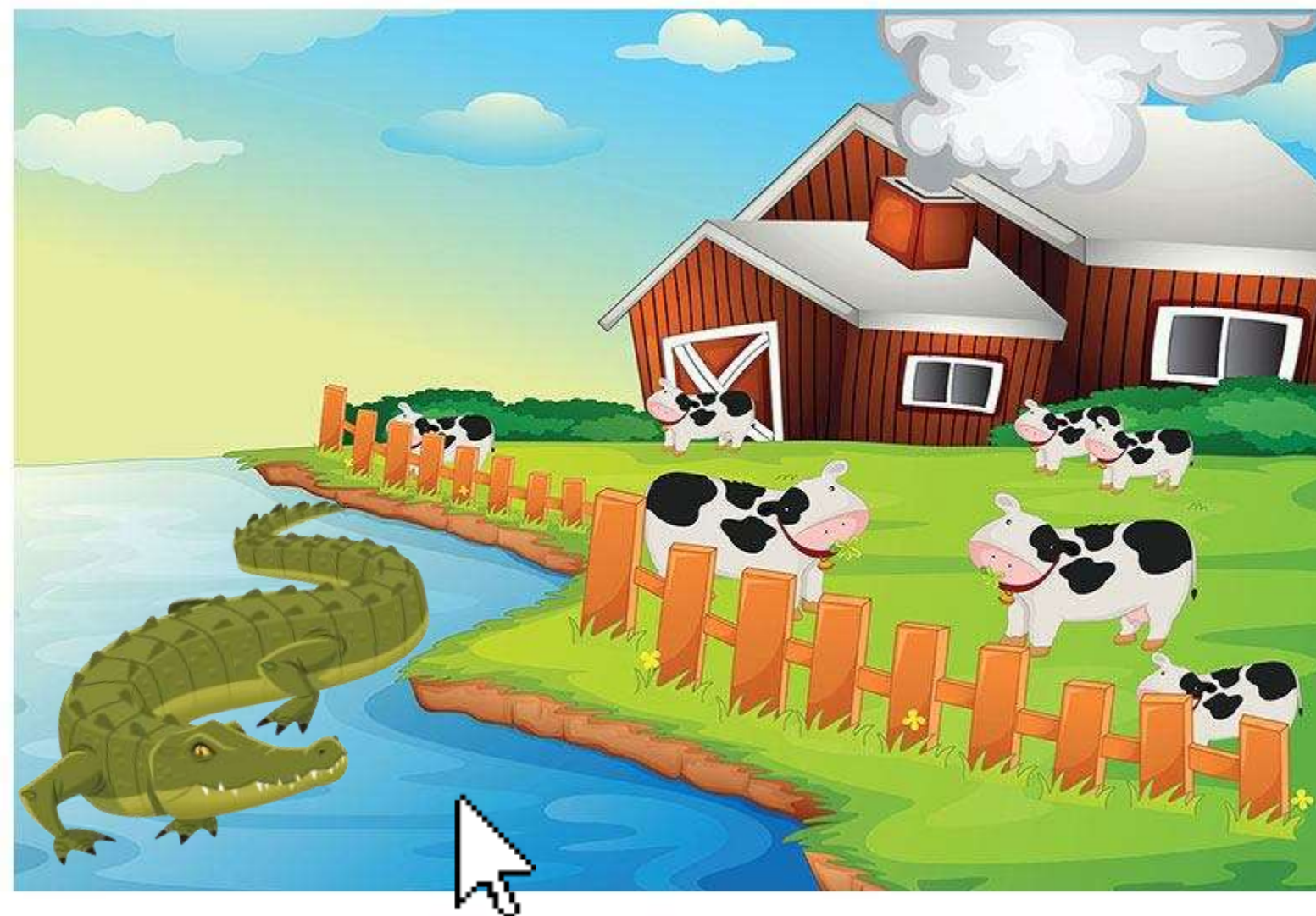
«Устранить нельзя оставить»



BELYAEV



1. MaxPatrol 8
 2. RedCheck
 3. ScanOVAL
 4. XSpider
 5. «Ревизор сети»
 6. «Сканер-ВС»
 7. Nikto
 8. OpenVAS
 9. MaxPatrol VM
 10. AlfaSense
 11. CPT
- И многое другое.



× × × ×
× × × ×
× × × ×
× × × ×

1. MaxPatrol 8
 2. RedCheck
 3. ScanOVAL
 4. XSpider
 5. «Ревизор сети»
 6. «Сканер-ВС»
 7. Nikto
 8. OpenVAS
 9. MaxPatrol VM
 10. AlfaSense
 11. CPT
- И многое другое.



× × × ×
× × × ×
× × × ×
× × × ×

Проблемы

- Нехватка кадров в ИТ или ИБ;
- Нехватка времени;
- Попытка закрыть все и сразу;
- Недостаток компетенций в настройке сканеров безопасности;
- Отсутствие реестра и эскалации;
- Отсутствие списка критичных систем;
- Отсутствие бюджета;
- Невозможность заменить иностранное решение;
- И многие другие.



× × ×
× × ×
× × × ×
× × × ×

1. Использование OpenSource или бюджетных коммерческих решений;
2. Прохождение обучений с помощью доступных источников;
3. Разворачивание тестового стенда;
4. Согласование работы сканеров с ИТ и Бизнесом;
5. Обмен опытом с коллегами;
6. Инвентаризация и оценка критичности АС/ИС → формирование собственной методологии оценки на основе cvss 3.0 под конкретные процессы компании
7. Заведение корректных заявок на тестирование обновлений и устранение уязвимости, с описанием уязвимости, рейтингом ее серьезности согласно cvss, внутренним рейтингом, описание способов устранения, SLA, план отката изменений.



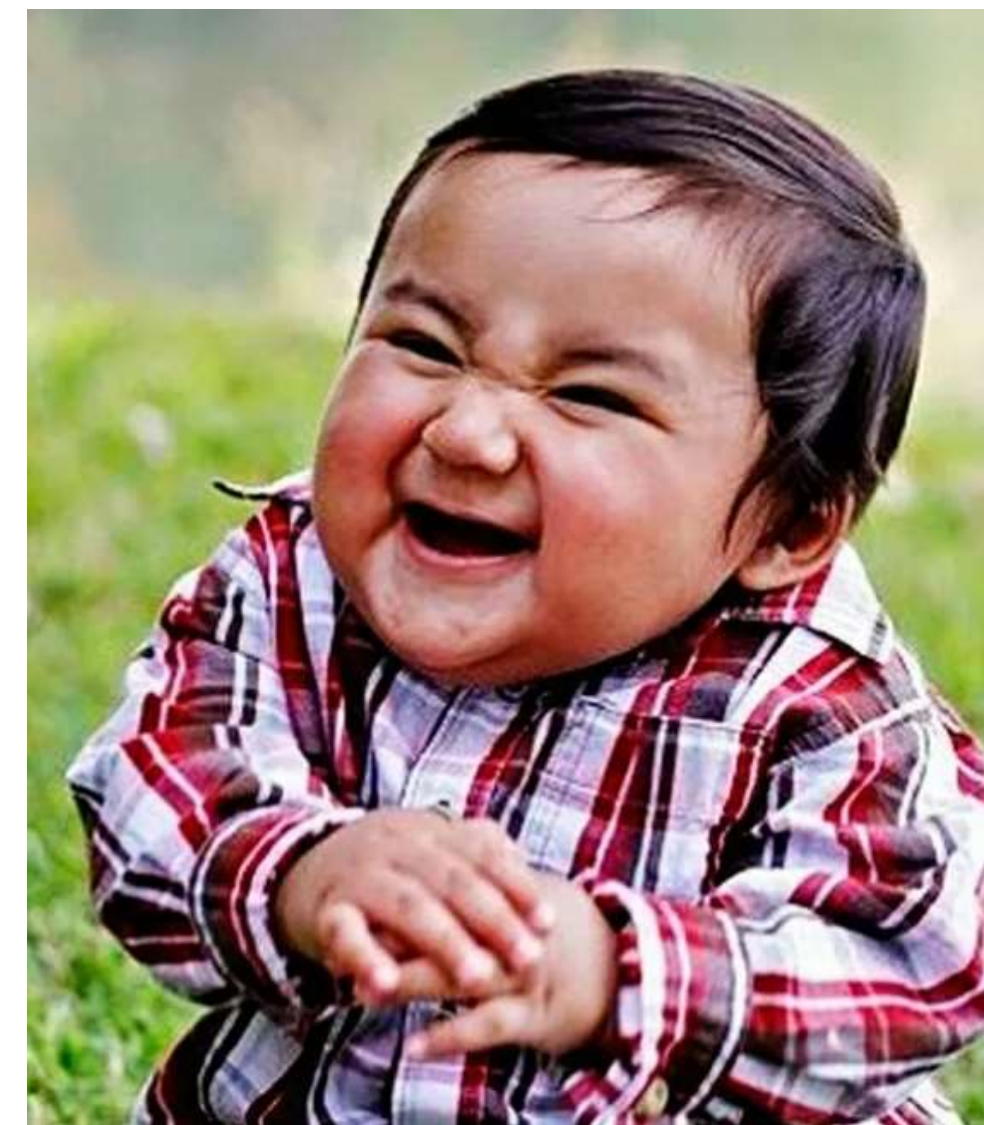
× × ×
× × ×
× × × ×
× × × ×



Системы оценки уязвимостей

06

CVSS (Common Vulnerability Scoring System) — это система оценки уязвимостей, которая позволяет количественно оценить влияние обнаруженной уязвимости на информационную систему. Она была разработана для того, чтобы дать возможность организациям определить приоритетность устранения найденных уязвимостей. Существует две версии этой системы: CVSS v2.0 и CVSS v3.0.





ОСНОВНЫЕ ОТЛИЧИЯ CVSS 2.0 ОТ CVSS 3.0

07



1. Введение новых векторов атаки:

CVSS v3.0 добавляет новые векторы атаки: network, adjacent network, local, physical и jailbreak. Это позволило расширить возможности моделирования угроз и лучше учитывать специфику различных сценариев атак.

2. Оценка сложности эксплуатации:

В CVSS v2.0 оценка сложности эксплуатации уязвимости основывалась исключительно на уровне технических знаний атакующего. В CVSS v3.0 этот параметр был разбит на два компонента: access complexity (сложность доступа к уязвимости) и authentication (требование аутентификации). Таким образом, стало возможным более точно оценивать сложность эксплуатации уязвимости.

3. Учет временного окна атаки:

В CVSS v3.0 было введено понятие временного окна атаки (exploit code maturity), которое отражает зрелость эксплоита. Этот параметр помогает учитывать скорость разработки и распространения эксплоитов, что особенно важно при оценке актуальности уязвимости.

4. Обновление компонентов метрик:

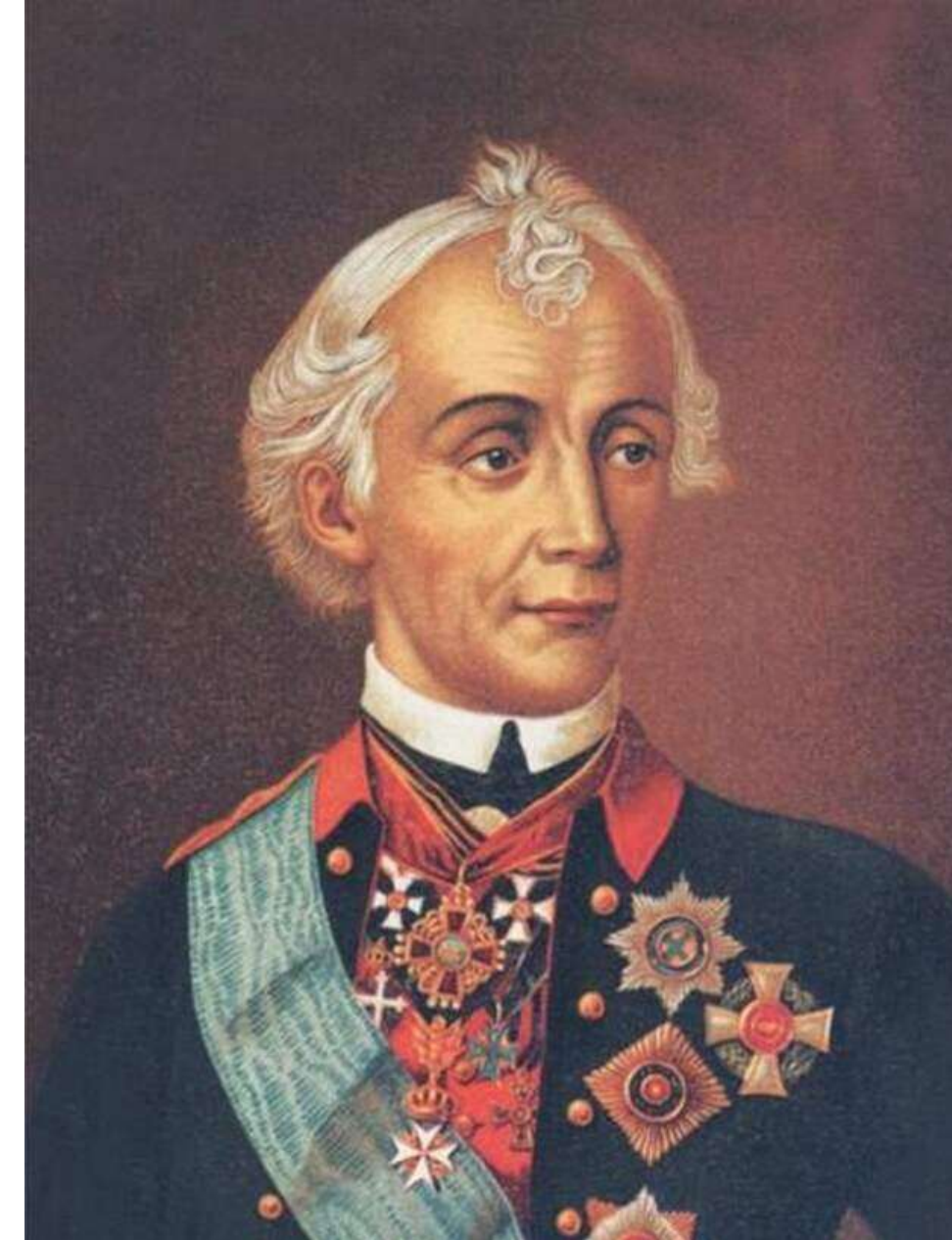
Метрики CVSS v3.0 были пересмотрены и обновлены для учета современных реалий информационной безопасности. Например, в CVSS v3.0 используется метрика collateral damage potential, которая учитывает возможный ущерб для третьих лиц, вызванный эксплуатацией уязвимости.

5. Улучшение масштабируемости и точности оценки:

В CVSS v3.0 были внесены изменения, направленные на улучшение масштабируемости и точности оценки. В частности, была изменена шкала оценки (от 0 до 10 вместо 0 до 10), что делает результаты более понятными и легко интерпретируемыми.



Ученье — свет, а неученье — тьма.



А.В.Суворов.

× × ×
× × ×
× × × ×
× × × ×

Обо мне:

- 10 лет в ИБ;
- В 23 года стал Начальником СИБ;
- Действующий Директор КБ в одной из ИТ компаний;
- Имею 2 образования (ИБ и Юриспруденция);
- Имею более 130 сертификатов/дипломов и благодарностей по тематике ИБ;
- Руководил 5-ю стартапами и командой из более 100 человек;
- Имею за плечами более 60 выступлений.
- Вхожу в ТОП-100 лучших руководителей ИТ по версии GlobalCIO 2023.



ОБО МНЕ



Мобильный номер

8-905-486-49-11



Почта

da.belyaev@mail.ru



Аккаунт в телеграме

da_belyaev



Telegram-канал

Пожалуйста, подпишитесь
и поддержите канал



Спасибо за внимание!

