

МОДЕЛЬ ЗРЕЛОСТИ КОМАНД РАЗРАБОТЧИКОВ:

практические рекомендации для выстраивания процесса безопасной разработки

АНДРЕЙ БИРЮКОВ

Технический директор • InfoW

Год назад я рассказывал...

Security Development Lifecycle



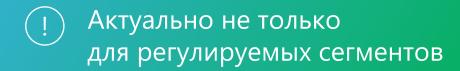
является описанием того, какие практики разработки надо использовать, чтобы сделать качественный продукт



CVE-2023-22518 - Improper Authorization Vulnerability In Confluence Data Center and Server

CVE-2023-22518 - Improper Authorization Vulnerability in Confluence Data Center and Server

Summary	CVE-2023-22518 - Improper Authorization Vulnerability in Confluence Data Center and Server
Advisory Release Date	Tues, Oct 31 2023 00:00 ET
Products	Confluence Data Center Confluence Server
CVE ID	CVE-2023-22518
Related Jira Ticket(s)	CONFSERVER-93142



Посредством этой уязвимости можно сбросить систему

Решение от вендора — отключение части функциональности



Что это означает?



SDL - это инженерные практики, актуальные для любого продукта



Необходимо выстроить процесс, а не разово пройти сертификацию



Нужно внедрять, как любые другие подходы



Продуктовая линейка из 6 продуктов

13 продуктовых команд

Сервисные команды

- Флагманские имеют сертификацию ФСТЭК
- Сертификация в Казахстане и Белоруссии
 - № Разные уровни внедрения SDL

- 🌣 Команда НИОКР
- ★ Командам с разным уровнем развития сложно взаимодействовать



МОДЕЛЬ ЗРЕЛОСТИ

Описание ожиданий от команд по набору критериев Оценка каждого критерия Определение точек развития команды

Использовали данный подход в других областях





ЦЕЛЬ ВНЕДРЕНИЯ МОДЕЛИ ЗРЕЛОСТИ



Оценить и вырастить инженерные команды



Определить правильный вектор развития команд



Поднять все команды на базовый уровень или выше



Не копить технический долг



КРИТЕРИИ МОДЕЛИ ЗРЕЛОСТИ

Моделирование угроз и анализ рисков

Работа с 3rdparty

SAST

Паттерны безопасного проектирования

Анализ CVE на 3rdparty

Практики безопасного кодирования

DAST. Санитайзеры

DAST. Фаззинг

Тестирование изменений

Хранение исходного кода

Реакция на дефекты



Как проводить оценку







Есть выделенный эксперт, отвечающий за процесс

Регулярные встречи раз в квартал

Смотрим текущие показатели и изменения





Берем задачи на улучшение

Команда сама выбирает направление развития

Скоринг команды разработки



ВЫУЧЕННЫЕ **УРОКИ**





Несмотря на описание уровней, будет нужно их пояснение от эксперта



2. Нужен организатор процесса, сама команда может не справится с оценкой Нужна хорошая модерация встречи

3. Самооценка должна валидироваться экспертом

4. Отслеживание взятых на себя задач и результатов



КАК НЕЛЬЗЯ ИСПОЛЬЗОВАТЬ МОДЕЛЬ ЗРЕЛОСТИ

НЕ ОЦЕНИВАЕМ, КТО ЛУЧШЕ

НЕ НАКАЗЫВАЕМ ОТСТАЮЩИХ



КОНЕЧНАЯ ЦЕЛЬ

СИЛЬНАЯ ИНЖЕНЕРНАЯ КУЛЬТУРА

цель внедрения инструмента

прозрачность

знаем, что у нас происходит на самом деле

ВСЕМ НРАВИТСЯ

делать хорошие продукты







ЖДЁМ ВАС НА СТЕНДЕ

D30



и в наших соцсетях



/InfoWatchOut



W /InfoWatch