Международный ТБ ФОРУМ Технологии Безо

infotecs

VII конференция
Актуальные вопросы защиты информации

Практика внедрения процедур безопасной разработки программного обеспечения

Дмитрий Гусев
ОАО «ИнфоТеКС»

Ретроспектива внедрения

ГОСТ Р 56939-2016

Эксперты внедряют SDL в Инфотекс

Разработчики сами осваивают SDL

Системный подход с адаптацией SDL к процессам компании

НЕМНОГО ПРО SDL

- SDL – Security Development Lifecycle
- На каждом этапе жизненного цикла ПО добавляются дополнительные практики безопасности
- Концепция SDL впервые предложена Microsoft и опубликована в 2004 году
- По оценкам Microsoft внедрение SDL в разработку ее продуктов позволило сократить число выявленных уязвимостей на 50-70%

ВОСПРИЯТИЕ ТРЕБОВАНИЙ/СТАНДАРТОВ ГЛАЗАМИ РАЗРАБОТЧИКА

Как велено	Человеческий фактор
ГОСТ 19.ххх-77/78/79	Уберите это старье с глаз, мы равняемся на лучшие практики зарубежных компаний!
Требования ФАПСИ/Гостехкомиссии	Это понятно, это хлеб!
ГОСТ ИСО/МЭК 15408	Мы не теоретики, мы практики, объясните что эти ученые тут написали!
Требования ФСБ/ФСТЭК	Так бы и сразу, работаем!
ГОСТ Р 56939-2016	А где же вы раньше были…?! А мы вам говорили - следуйте ГОСТ 19.ххх!

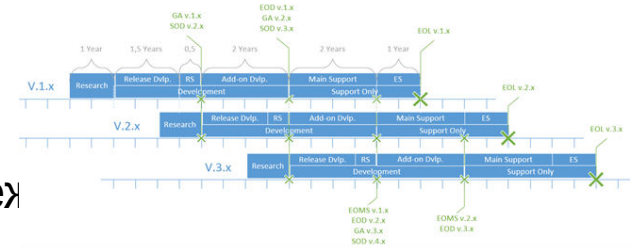
ТЕКУЩИЕ ДОСТИЖЕНИЯ

- Разработка более 20 продуктов компании ведется с применением практик безопасной разработки:
  - ViPNet Coordinator/Coordinator HW
  - ViPNet Client
  - ViPNet CSP
  - ViPNet Administrator
  - ViPNet IDS
- создан и развивается внутренний стандарт безопасной разработки **Infotecs Security Development Lifecycle** (ISDL) на основе Microsoft SDL и ГОСТ Р 56939
- разработаны практики первичного внедрения ISDL в продуктовые проекты - **ISDL Quick Start Model**
- разработаны и апробированы процедуры обработки выявленных уязвимостей: анализ, устранение, обновление
- автоматизирован процесс контроля выявления уязвимостей в сторонних компонентах

ЧТО ДЛЯ ЭТОГО ПОТРЕБОВАЛОСЬ

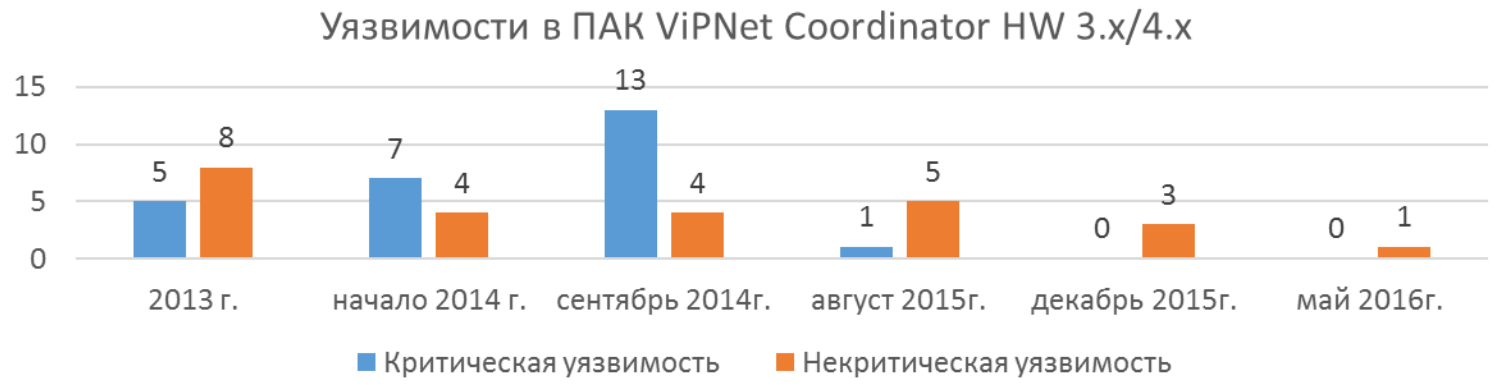
- Принять решение о выделении постоянного ресурса на внедрение ISDL:
  - До 30% на ISDL от общих затрат на проект
  - По факту имеем 10-15%
- Выделить явные роли **главного ответственного** за безопасность продуктов и **ответственных за безопасность конкретных продуктов**
- Разработать и начать внедрять типовой жизненный цикл продукта
- Начать регулярные тренинги проектных команд (разработчиков, аналитиков, архитекторов, менеджеров) по практикам ISDL
- Модернизировать инфраструктуру системы автоматизированной разработки
- Согласовать новые процессы взаимодействия меж подразделениями разработки, производства, реализации и поддержки продуктов

Команда ISDL



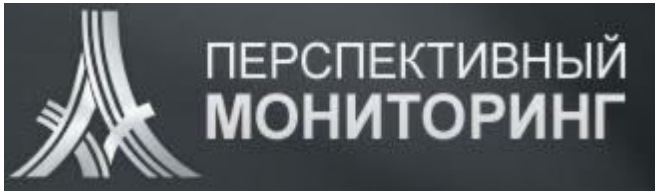
ЧТО ПОЛЕЗНОГО ПОЛУЧИЛИ

- Фиксируется, обсуждается, актуализируется архитектура продуктов
- Проводится тщательное ревью кода ПО
- Расширилось число используемых инструментальных средств сборки и анализа программного кода
- Затраты на продуктовые проекты стали более прозрачными (улучшился анализ проблем в проектах, выросло качество бизнес-аналитики по продуктам)
- Отслеживаются и исправляются уязвимости (в т.ч. в сторонних компонентах):



НО МЫ НИЧЕГО НЕ СМОГЛИ БЫ ДОБИТЬСЯ, ЕСЛИ БЫ…

Не организовали в 2007 году команду экспертов по практической безопасности – компанию «Перспективный мониторинг»



«ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ» И ГОСТ Р 56939

Услуги	Требования ГОСТ Р 56939-2016
Построение модели угроз и нарушителя	5.1, 5.2
Анализ продуктов на проникновение ("черный ящик")	5.4
Рецензирование спроектированных решений с точки зрения безопасности	5.1, 5.2
Фаззинг-тестирование, написание автотестов	5.4
Анализ исходного кода программных продуктов на предмет безопасности	5.3, 5.4
Аудит процесса эксплуатации ИС, аудит безопасности системы обновлений	5.5, 5.6
Тестирование на проникновение среды разработки и обновлений ПО	5.8

ОСНОВНЫЕ ВЫВОДЫ

- Внедрение практик безопасной разработки требует дополнительных инвестиций, но уже в среднесрочной перспективе (3-4 года) может окупиться:
  - Повышение качества продуктов в целом, а не только в части безопасности
  - Повышение прозрачности процессов разработки и их прогнозируемость – сокращение незапланированных расходов на исправление ошибок/уязвимостей
  - Повышение компетентности команд разработчиков в области ИБ
  - Повышение лояльности заказчиков
- Текущему стандарту ГОСТ Р 56939-2016 не хватает гибкости по уровням требований – их, в принципе, не предусмотрено, в отличие от ГОСТ 15408 (уровни доверия) и Microsoft SDL (4 уровня зрелости):
  - высокий порог вхождения,
  - снижается порог понимания требований безопасности, по сравнению с тем же ГОСТ 15408

Спасибо за внимание!