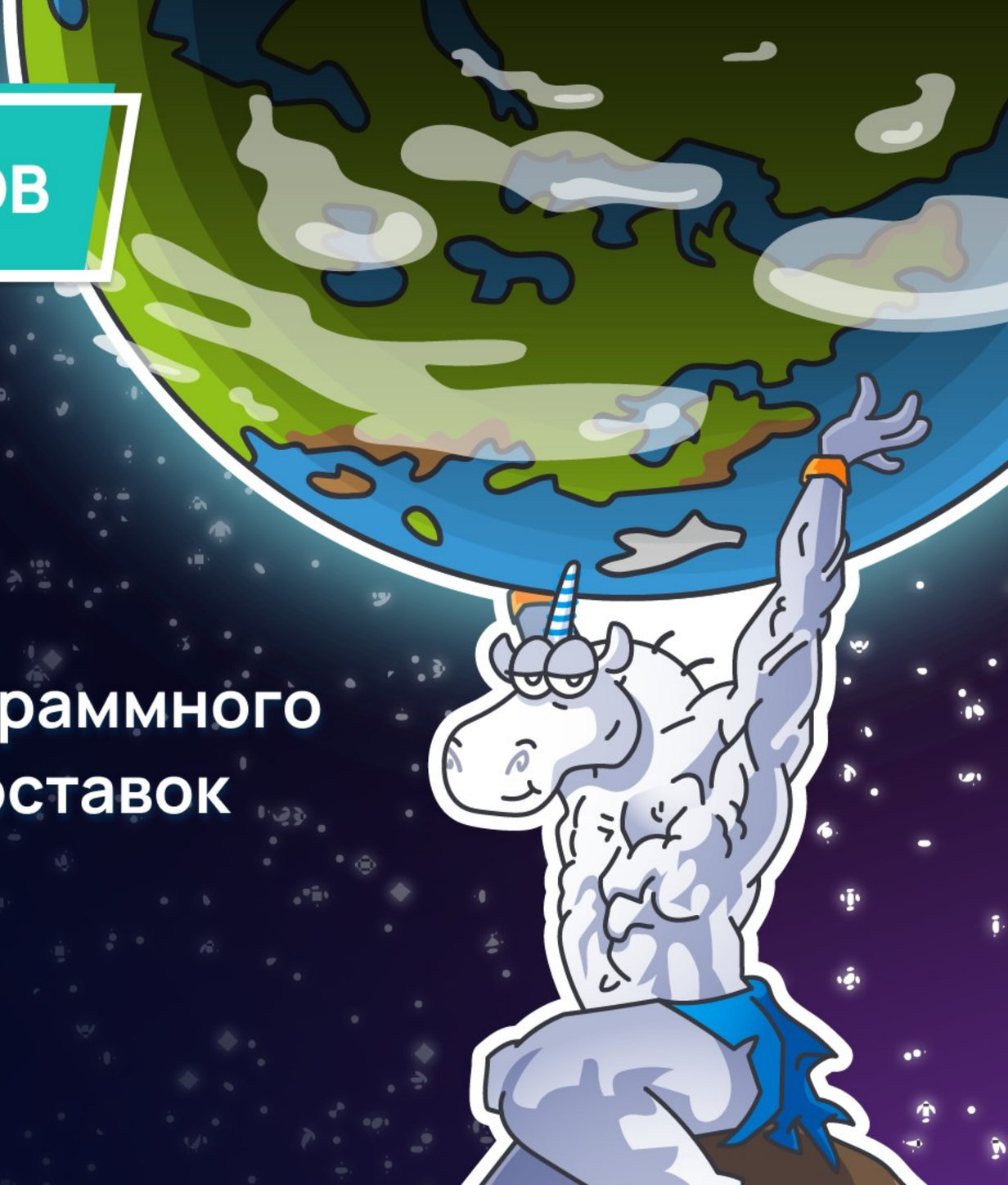
ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

Вебинар 17.
Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок



PVS-Studio

УЧЕБНЫЙ ЦЕНТР МАСКОМ

Представимся!

Спикеры и гости вебинара



Владислав Богданов

Developer Advocate, Java Developer

- Разрабатываю ядро статического анализатора PVS-Studio для языка Java.
- Рассказываю про технологии статического анализа в статьях и на различных IT мероприятиях.







@vlade1
k

Виталий Пиков

Эксперт в области ИТ, ИБ, преподаватель



- Стаж преподавательской работы более 10 лет
- Заслуженный доцент Российского нового университета, преподаватель высшей школы
- Microsoft Certifications Earned: MCT, MCPS, MCSA, MCTS
- Автор более 30 научных публикаций

MACKOM
УЧЕБНЫЙ ЦЕНТР

Смирнов Алексей Алексеевич



Основатель и генеральный директор CodeScoring

- Занимается вопросами экспертного анализа исходных кодов на качество и безопасность с 2011 года
- Регулярно выступает на конференциях по вопросам применения композиционного анализа, состояния мирового open source и методическим аспектам внедрения процессов безопасной разработки

Доклад: Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок

О цикле вебинаров



Вокруг РБПО за 25 вебинаров: ГОСТ Р 56939-2024

- Организуют УЦ МАСКОМ и ООО «ПВС» (PVS-Studio)
- ГОСТ Р 56939-2024 описывает 25 процессов, необходимых для реализации разработки безопасного ПО, поэтому и 25 вебинаров
- Также, цикл включает в себя бонусные вебинары
- Мы открыты к сотрудничеству по разбору тем, пишите нам!

Записи предыдущих вебинаров



pvs-studio.ru/ru/webinar/rbpo/

Процесс 17

Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок



PVS-Studio

5.17.1 Цели

- Создание условий для снижения рисков внедрения вредоносного ПО посредством воздействий на ПО или механизмы его доставки до получения ПО конечными пользователями и недопущение компрометации данных (информации) или информационной системы, использующей такое ПО



5.17.2 Требования к реализации

- Осуществлять контроль зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков; компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков).
- Осуществлять контроль договорных обязательств со сторонними поставщиками

5.17.2 Требования к реализации

- Осуществлять выявление элементов инфраструктуры разработчика, воздействие на которые может повлиять на возникновение недекларированных возможностей в ПО.
- Осуществлять контроль использования предсобранного поставщиком ПО (кода, для которого отсутствуют исходные тексты)
- Осуществлять анализ кода ПО, полученного через цепочки поставок, на предмет внедрения вредоносного программного обеспечения.

5.17.3 Артефакты реализации требований

- Перечень процессов, компонентов инфраструктуры, частей разрабатываемого ПО, зависящих от сторонних поставщиков, должен содержать следующие сведения:
  - описание внутренних процессов, зависящих от сторонних поставщиков;
  - описание компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков;
  - описание компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков.

5.17.3 Артефакты реализации требований

- Сведения о договорных обязательствах со сторонними поставщиками могут включать следующую информацию:
  - перечень поставщиков с указанием поставляемых продуктов (услуг);
  - сведения о заключенных договорах со сторонними поставщиками, включающие информацию о поставляемых продуктах (услугах), сроках начала и окончания договоров, иную информацию.

5.17.3 Артефакты реализации требований

- Сведения о критичных и вероятных с точки зрения внедрения недекларированных возможностей элементах инфраструктуры (компонентах инфраструктуры разработки ПО, зависящих от сторонних поставщиков) должны содержать следующую информацию:
  - перечень элементов инфраструктуры разработчика, воздействие на которые может повлиять на возникновение недекларированных возможностей в ПО;
  - информацию о поставщиках продуктов (услуг) для указанных в перечне элементов инфраструктуры разработчика.

5.17.3 Артефакты реализации требований

- Результаты контроля использования предсобранного поставщиком ПО должны содержать информацию, позволяющую определить наличие предсобранных поставщиком ПО компонентов и осуществить их идентификацию (по свойствам файлов, контрольным суммам файлов и т. п.).

5.17.3 Артефакты реализации требований

- Результаты анализа кода ПО, полученного через цепочки поставок, на предмет внедрения вредоносного программного обеспечения должны содержать, как минимум, отчеты сканирования средств антивирусной защиты.

Дополнительные материалы

- **ИНФАРС:** Атаки на цепочки поставок: как защитить своё програм мное обеспечение?
- **Security Vision:** Open software supply chain attack reference
- **CNews:** Впервые цепочки поставок ПО были атакованы с использ ованием открытого кода

- Телеграм канал «Бестиарий программирования»:
  - Опубликован цикл постов, посвящённых РБПО
  - Пост «РБПО-061. Процесс 17 – Проверка кода на предмет внедрени вредоносного программного обеспечения через цепочки поставо

@PROGRAMMING_TALES

Передаю слово следующему спикеру



Сделай свой проект
чистым и безопасным
вместе с PVS-Studio

PVS-Studio

Telegram-канал
CodeScoring

Сайт CodeScoring

CODE SCORING

Получи 10% скидку
на курсы «М БРПО»
в Учебном Центре
«МАСКОМ»

УЧЕБНЫЙ ЦЕНТР
МАСКОМ