ANGARA SECURITY

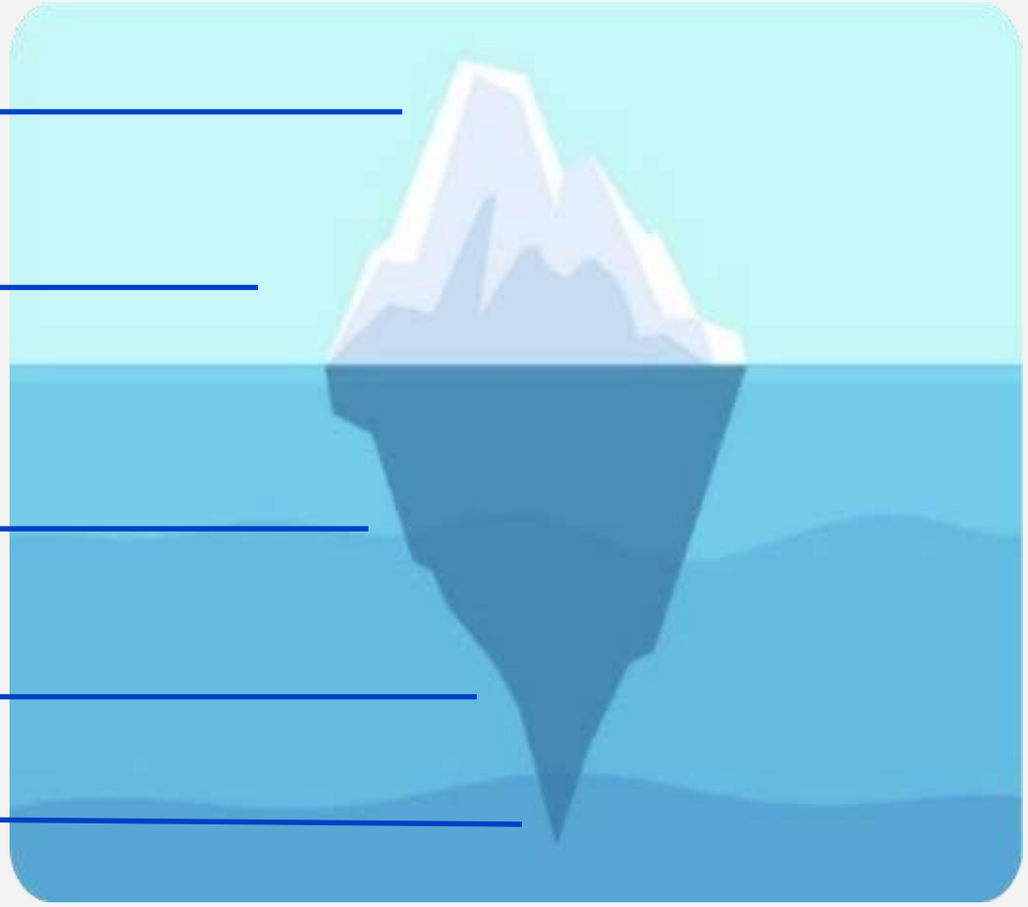
Инструменты обеспечения доверия сторонним компонентам

Илья Поляков, руководитель отдела анализа кода

Специализируемся на защите данных и бизнес-систем,
предотвращаем и расследуем кибератаки

Почему актуально?

- Заимствованные компоненты и транзитивные зависимости
- Тренд на микросервисы
- Требование по использованию отечественного ПО
- Сбои в процессах управления уязвимостями + Zero Day
- Protestware и НДВ



Зачем нужен доверенный репозиторий?

Доверие к opensource коду

Блокировка заимствуемых компонент с недопустимыми уязвимостями и НДВ в парадигме Shift Left

Размещение и хранение прошедшего проверки ПО в виде бинарных артефактов и исходного кода

Регулярное проведение ретроспективного анализа содержимого с учетом свежевыявленных уязвимостей

Доверенный репозиторий

- Создаётся на базе артефактория (Nexus, JFrog)
- Содержит артефакты для сборки приложений
- В том числе – опенсорсные компоненты
- Риски: уязвимости, malware, protestware
- Доверие обеспечивается сканированием на входе
- ...а также – ретроспективным анализом

С точки зрения DevSecOps

- Сокращение сроков разработки бизнес-функций приложения (уменьшение time to market)
- Управляемый и понятный процесс взаимодействия разработчиков и специалистов ИБ, повышение вовлеченности в совместное взаимодействие
- Сокращение ресурсов (человеческих и временных) на исправление допущенных ошибок разработки
- Повышение осведомленности команды разработки в части практик безопасного программирования

SCA/OSS Firewall

- Осуществляет композиционный анализ
- Формирует SBoM
- Выявляет компоненты с известными уязвимостями
- Блокирует на основании политик (как загрузку, так и выгрузку)
- НЕ требует автоматизации ретроспективного анализа

Антивирус

- Выявление ВПО статическим анализом
- В том числе – серверных бэкдоров
- Сканирование образов контейнеров
- Плохо работает против APT

Песочница

Динамический (поведенческий) анализ

- В изолированной виртуальной среде
- PT ML (машинное обучение)
- Анализ ссылок

Статический анализ

- Антивирусное сканирование
- Экспертная оценка (YARA-правила)
- Проверка по индикаторам компрометации

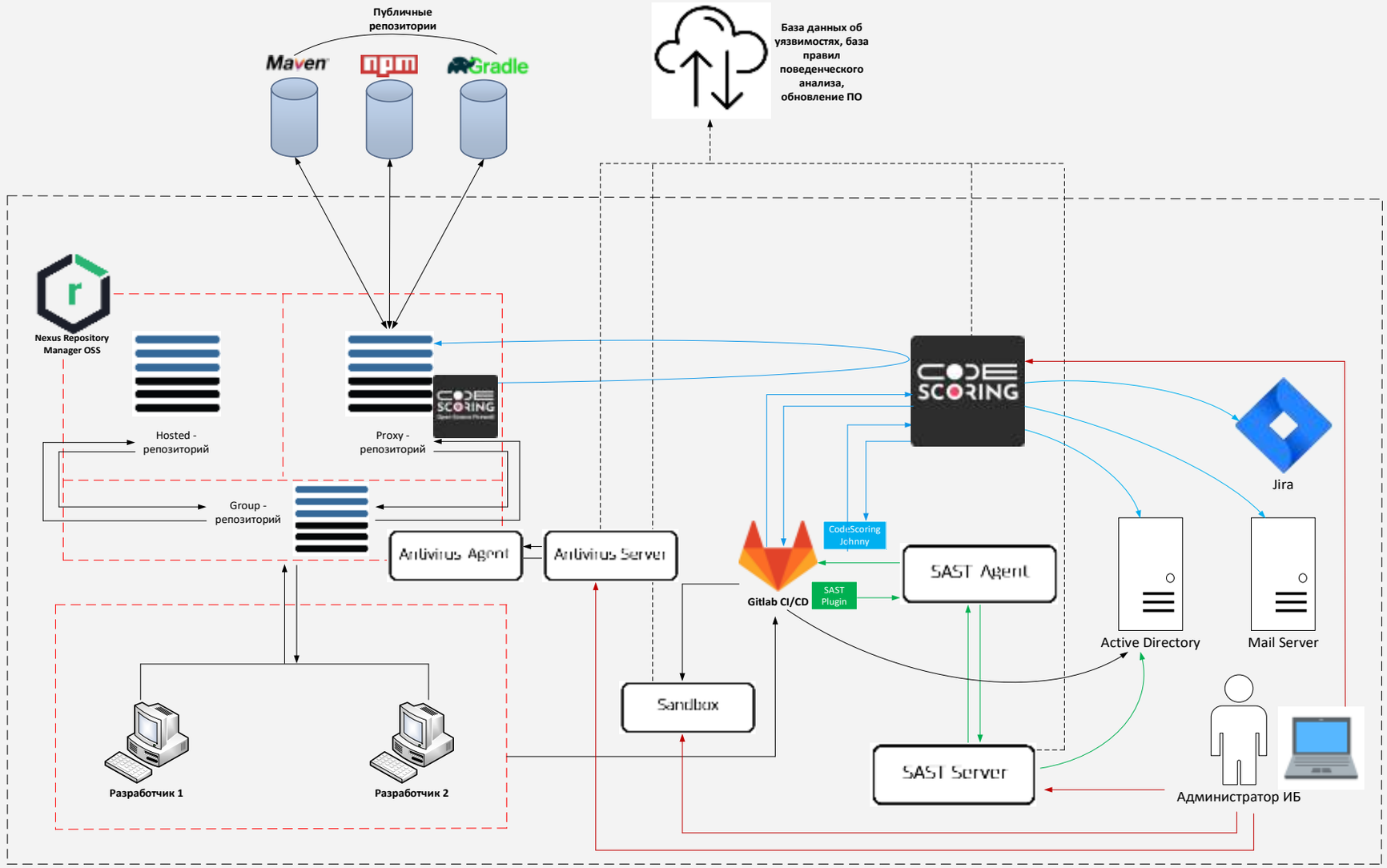
SAST (статический анализатор кода)

- Опенсорсные компоненты – это архивы с иходным кодом (.jar, .tgz, .whl)
- Анализ кода позволяет выявить даже неизвестные уязвимости
- Настраиваемые правила могут выявлять protestware
- Также зачастую в комплекте идёт SCA

Контейнеризированный микросервис оркестрации

- Входной контроль
- Ретроспективный анализ (по расписанию)
- Сканирование всеми инструментами
- Распараллеливание
- Интеграция с Jira

Пример архитектуры



Результат

Функционирование инфраструктуры разработки ПО с применением отечественных средств защиты, сертифицированных ФСТЭК

Защита от выявленных уязвимостей на самых ранних стадиях процесса разработки

Централизованное управление политиками безопасности

Обеспечение лицензионной чистоты для заимствуемых компонентов

ANGARA SECURITY

СПАСИБО ЗА ВНИМАНИЕ!

Адрес офиса
БЦ «Парк Победы», Москва,
ул. Василисы Кожиной, д.1 к.1

Общий телефон
+7 495 269 26 06

Общий адрес электронной почты
info@angarasecurity.ru

Сайт
angarasecurity.ru

НАШИ УСЛУГИ

Анализ защищенности и пентест

Внешний и внутренний тест на проникновение, анализ защищенности мобильных и веб-приложений, выявление нестойких паролей, имитация хакерской атаки на инфраструктуру в режиме 24/7 (Red Team Operations)

Мониторинг и управление инцидентами ИБ (SOC)

Услуги по управлению инцидентами ИБ — от выявления инцидентов и расследования до реагирования и устранения последствий, по цифровой криминалистике, OSINT и защите бренда

Выстраивание процесса безопасной разработки

Анализ исходного кода, создание доверенного репозитория, построение безопасных процессов DevOps

Аудит, консалтинг и оценка рисков в области ИБ

Оценка рисков в области информационной безопасности, комплексный аудит информационной безопасности, категорирование объектов КИИ и их защита

9
Лет проектного опыта на рынке информационной безопасности

470+
Заказчиков

280+
Экспертов в команде

60+
Вендоров, с которыми мы сотрудничаем в качестве Платинового, Премиум, Золотого или Авторизованного партнера