ВЫСТРАИВАНИЕ БЕЗОПАСНОГО КОНВЕЙЕРА РАЗРАБОТКИ

Сергей Грачев
Заместитель директора по кибербезопасности

Артур Галеев
Начальник отдела DevOps

28 марта 2024 г., Москва

Обеспечение безопасности в эпицентре инноваций*

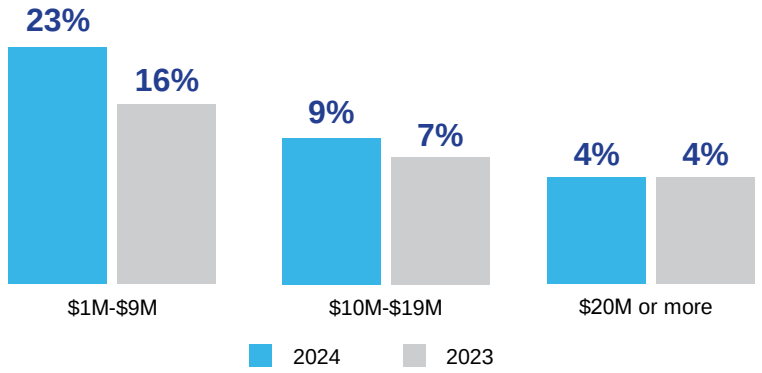
Информационная безопасность – приоритетное направление, которое всегда в тренде

Нарушения становятся все более дорогостоящими – любой изъян в системе безопасности стоит дорого, а цена ошибки и количество попыток нарушить работу систем продолжают расти

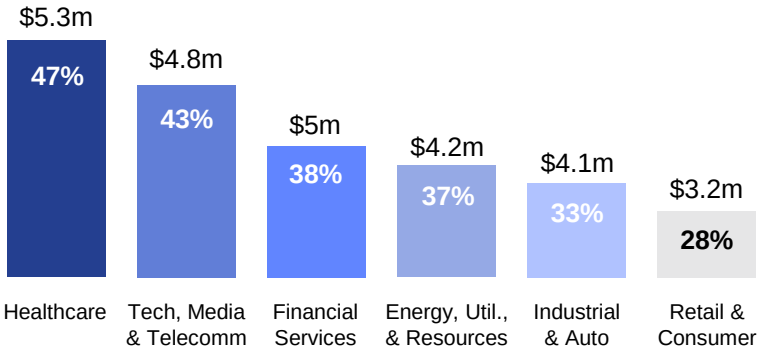
Снижение киберрисков – главный приоритет на 2024 год

Кибербезопасность – неотъемлемая часть работы компаний, которая помогает стимулировать инновации, экономить средства и расти бизнесу

Оценочные затраты организаций на самую масштабную утечку данных за последние 3 года



Средняя стоимость взлома и процент наиболее опасных взломов, стоимость которых составляет 1 млн долл. и более, в разбивке по секторам



* На основе данных исследования PwC Global Digital Trust Insights, 2024 г.

Обеспечение безопасности в эпицентре инноваций* (2)

Мировые приоритеты в сфере информационной безопасности:

Модернизация технологий, включая киберинфраструктуру

Использование искусственного интеллекта для киберзащиты

Создание новой операционной модели, ориентированной на поддержку бизнеса

~50%

Опрошенных считают использование облачных технологий главной киберугрозой

Приоритеты инвестиций в кибербезопасность для лидеров бизнеса на ближайшие 12 месяцев

* На основе данных исследования PwC Global Digital Trust Insights, 2024 г.

Вызовы российского рынка кибербезопасности

- Взрывной рост количества сложных кибератак, в том числе с применением методов социальной инженерии, и утечек конфиденциальной информации
- Появление нового типа угроз, связанного с применением искусственного интеллекта и машинного обучения
- Активизация госрегулирования в области информационной безопасности, издание целого ряда новых нормативных документов, ужесточение ответственности за нарушения
- Санкции, уход из России ряда крупных вендоров, переход на отечественные сертифицированные решения, импортозамещение
- Тенденция к росту рынка информационной безопасности, количества ИТ-стартапов, расходов на ИБ: например, закупки защищенных ОС*, СЗИ**, сопутствующих услуг

* ОС – операционная система
** СЗИ – средства защиты информации

Тренды (1)

Обеспечение безопасности на всех этапах жизненного цикла

Глобальные

DevOps	Dev**Sec**Ops
MLOps	ML**Sec**Ops

Российские

ГОСТ Р 56939 *	ГОСТ Р XXXXX 2024 г.
ГОСТ Р 58412 **	ГОСТ Р XXXXX

* Защита информации. Разработка безопасного ПО. Общие требования
** Защита информации. Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО

Тренды (2)

Рост запроса рынка на безопасную разработку по следующим направлениям:

- Выстраивание процессов DevSecOps/ГОСТ 56939 и построение безопасной архитектуры/инфраструктуры Заказчика
- Учет требований безопасности DevSecOps/ГОСТ 56939 в рамках заказной разработки программных продуктов, адаптации существующих программных решений и платформ Заказчика
- Собственные разработки программных решений с учетом требований DevSecOps/ГОСТ 56939

Неочевидные плюсы

Процесс безопасной разработки имеет множество пересечений с подготовкой к сертификации ПО и соответствующим оценочным процедурам по требованиям федеральных регуляторов – ФСТЭК, ФСБ. Чем выше зрелость процесса, степень его оптимизации и автоматизации, тем проще будет осуществляться подготовка к оценочным и сертификационным процедурам и их прохождение

Подход IBS на основе ГОСТ Р 56939/58412

Классический SDLC-подход к разработке, применяемый в IBS

Менеджмент инфраструктуры среды разработки ПО – защита от несанкционированного доступа, резервное копирование, регистрация событий

Управление человеческими ресурсами – программы обучения

ГОСТ Р 584129 – угрозы безопасности информации при разработке ПО

Инструменты DevSecOps

SAST-инструменты
Solar appScreener, PT Application Inspector

Поиск уязвимостей
Solar appScreener, PT Application Inspector, CodeScoring, Trivy

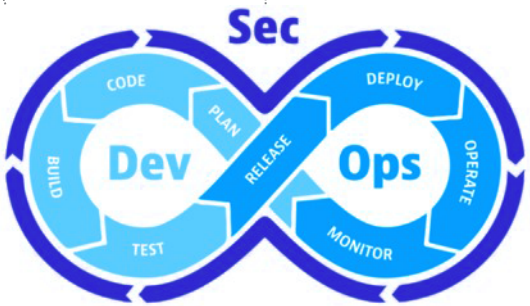
Поиск уязвимостей в ОС
Solar appScreener, PT Application Inspector, CodeScoring, Trivy

Управление конфигурациями
Ansible

Управление артефактами
Sonatype Nexus, Harbor, «РТК-Феникс»

Системы мониторинга
Zabbix, Prometheus, Grafana, Initi

Системы виртуализации
Альт Виртуализация, РЕД Виртуализация, zVirt, QEMU



Инструменты информационной безопасности (DAST) и фаззинга
Solar appScreener, PT Application Inspector, Nikto, ZAP, OSS-Fuzz

Инструменты SCM
Gitea, GitFlic, MosHub

Безопасность оркестрации
Luntry, Kube-Hunter

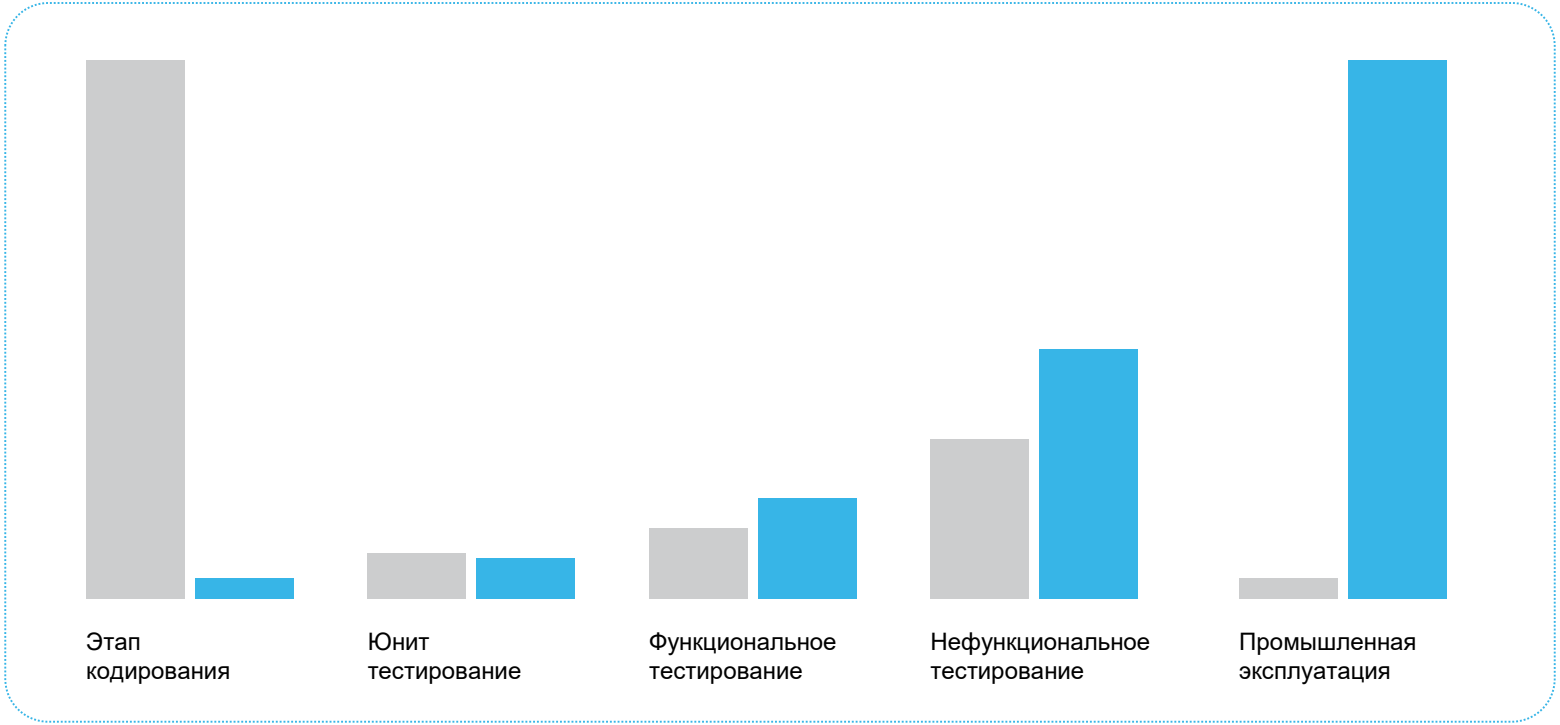
Мониторинг и отслеживание
Telegram, Grafana

eBPF
Cillium

Системы оркестрации
Deckhouse, Platform V, «Штурвал», Vanilla Kubernetes

Системы сбора и обработки логов
Arenadata LogSearch, OpenSearch

Метрики DevSecOps



Стандарты безопасности для систем контейнеризации

Для российской розничной торговой компании

Цели и задачи

- Разработать стандарт безопасности для систем контейнеризации на основе Kubernetes, а также рекомендаций вендора и сообщества
- Создать рекомендации для разработчиков с целью повышения безопасности конвейеризированных приложений
- Составить инструкции по настройке аудита безопасности систем контейнеризации на основе Kubernetes

Результаты

- Разработаны стандарты безопасности для Kubernetes и Red Hat OpenShift Cloud Platform с учетом рекомендаций вендора и в полном соответствии с CIS – Center for Internet Security
- Создан документ, включающий лучшие мировые практики, обеспечивающие повышенную безопасность контейнеризированных приложений
- Разработаны инструкции по настройке аудита безопасности систем контейнеризации для Kubernetes и Red Hat OpenShift Cloud Platform

Технологии

- Docker
- Kubernetes
- Red Hat OpenShift Cloud Platform
- Trivy
- Trivy UI
- Clair operator

Управление локальными репозиториями

Для российской телекоммуникационной компании

Цели и задачи

- Организация локальной копии общедоступных репозиториев программных компонентов
- Мониторинг используемых программных компонентов
- Выявление уязвимых компонентов
- Предоставление ресурса для размещения разрабатываемых компонентов

Результаты

- Разработан прототип системы управления репозитория исходного кода и различных видов артефактов: Maven, NPM, Nugget, RPM, Deb, Docker и др.
- Система позволяет сканировать артефакты не только на уязвимости, но и на возможные правовые риски
- Все вносимые в код изменения имели цифровую подпись

Технологии

- GitLab
- Sonatype Nexus 3 Pro
- Sonatype Nexus Firewall
- Sonatype Nexus Lifecycle
- Trivy
- Trivy UI

Управление релизами для группы проектов

Для российской нефтяной компании

Цели и задачи

- Организация сборки и доставки программных компонентов от нескольких команд разработки
- Осуществление мониторинга используемых программных компонентов на соответствие политикам безопасности
- Следование DevSecOps-политикам в компании во время заказной разработки

Результаты

- Разработана автоматизация процессов сборки, сканирования на уязвимости, доставки программных компонентов
- Система позволяет сканировать артефакты не только на уязвимости, но и на возможные правовые риски
- Процесс выявления уязвимых компонентов оповещает о выявленных проблемах на стадии разработки

Технологии

- Red Hat OpenShift
- Jenkins
- Sonatype Nexus 3 OSS
- Helm
- Dtrack
- Clair
- CodeScoring
- PT AI

ВЫСТРАИВАНИЕ БЕЗОПАСНОГО КОНВЕЙЕРА РАЗРАБОТКИ

Сергей Грачев
Заместитель директора по кибербезопасности

Артур Галеев
Начальник отдела DevOps

28 марта 2024 г., Москва

+7 (495) 967 80 80
SGrachev@IBS.RU
AGaleev@IBS.RU