Команда цифровых сервисов ОМК

Кто мы?

- Небольшая численность команды, высокий темп разработки
- Десятки постоянно развиваемых сервисов в основе на LEMP стеке, но не исключительно.
- Гибкие команды, гибкие подходы к управлению проектами и разработкой
- **Скорость поставки функционала и проверки гипотез бизнесом — ключевой приоритет**

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

С чем мы столкнулись

1. Возрастание рисков (внешняя конъюнктура, внутренние риски: растущее количество продуктов и их сложность, объемов критичных данных).

2. Высокая частота релизов. При этом «супер-срочные-релизы» никто не отменял.

3. **Скорость поставки продуктов бизнесу не предмет для торга.**

4. Ограниченные внутренние ресурсы

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

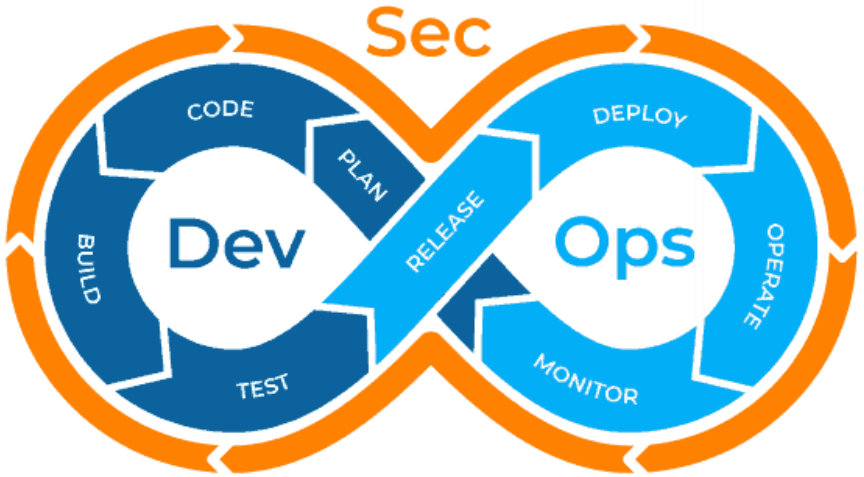
Приоритеты DevSecOps

DevOps

1. Увеличить скорость деплоев
2. Уменьшить время на устранение сбоев
3. Снизить количество проблем при деплоях
4. Увеличить частоту деплоев
5. Вовлекать Безопасность в процесс разработки на более ранних стадиях
6. Ускорить устранение проблем с нормативными требованиями

Security

1. Снизить риски
2. Выполнить нормативные требования



ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

Фреймворки DevSecOps

- DSOMM (DevSecOps Maturity Model);
- BSIMM (Building Security In Maturity Model);
- OWASP SAMM (Software Assurance Maturity Model);
- Microsoft SDL (Security Development Lifecycle);
- NIST SP 800-64 (Security Considerations in the System Development Life Cycle).
- DevSecOps Assessment Framework

Есть также фреймворк известного интегратора, закрывающий полный цикл — DAF (DevSecOps Assessment Framework)

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

Как прийти к DevSecOps? Глобально подхода три, но два

1. Сдаться интегратору который проведёт аудит и поможет внедрить DevSecOps, как стратегию, извне.

2. Сформировать внутреннюю команду и делать то же самое изнутри.

3. Приступить к внутреннему аудиту, начать планировать и внедрять практики внутренним ресурсом, чтобы в итоге прийти к варианту 2 или 1.

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

Мы были не в худшей стартовой позиции

Команда решила пойти по пути поэтапной оценки процесса SDLC для каждого продукта с позиции рисков и возможностей их снижения рекомендуемыми практиками DevSecOps.

- У нас есть реализованные автоматизированные пайплайны CI/CD;
- Наши приложения контейнеризированны и мы научились без шума и пыли деплоить их во все окружения;
- Мы используем централизованный Harbor OMK-IT и свой собственный Nexus и есть также процесс проверки образов и сканирования контейнеров на уязвимости;
- Используем HashiCorp Vault для хранения секретов;
- В конце концов, мы используем CVS и «git-flow like» подход для управления исходным кодом;

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

Как нам видится наш трек

- ✓ Определяем практики, отвечающие нашим потребностям и возможностям;
- ✓ Реализуем пилот охватывающий основные этапы SDLC, внедрив инструментов и артефактов DevSecOps которые приняла команда;
- ✓ Производим устранение рисков, выявленных в ходе эксплуатации пилота;
- ✓ Проводим внешний аудит процесса и тестирование на проникновение продуктов, включенных в пилот, получая от внешних профессионалов рекомендации по текущему состоянию и дорожной карте DevSecOps;
- ❑ Выходим на проект и стратегию внедрения DevSecOps под общим лидерством команды ИБ;
- ❑ На финальном этапе внедрения и с заданной в стратегии регулярности проводим аудит процесса безопасной разработки и повторное тестирование на проникновение продуктов;
- ❑ Вносим коррективы в процесс и решения, мониторим целевые метрики DevSecOps.

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

Как нам видится наш трек

- ✓ Определяем практики, отвечающие нашим потребностям и возможностям;
- ✓ Реализуем пилот охватывающий основные этапы SDLC, внедрив инструментов и артефактов DevSecOps которые приняла команда;
- ✓ Производим устранение рисков, выявленных в ходе эксплуатации пилота;
- ✓ Проводим внешний аудит процесса и тестирование на проникновение продуктов, включенных в пилот, получая от внешних профессионалов рекомендации по текущему состоянию и дорожной карте DevSecOps;
- ❑ Выходим на проект и стратегию внедрения DevSecOps под общим лидерством команды ИБ;
- ❑ На финальном этапе внедрения и с заданной в стратегии регулярности проводим аудит процесса безопасной разработки и повторное тестирование на проникновение продуктов;
- ❑ Вносим коррективы в процесс и решения, мониторим целевые метрики DevSecOps.

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

Основные этапы цикла безопасной разработки в пилоте в развернутом виде

Дизайн и разработка

Процесс планирования архитектуры с ИБ

Security-плагин в среде IDE

Проверка соответствия стандартам кодирования

Коммит в репозиторий

SAST анализ

Автоматические тесты

Защита системы контроля версий

Сборка и тестирование

DAST, IAST анализ

Проверка инфраструктуры и конфигурации контейнеров,

Проверка зависимостей

Идентификация секретов

Деплой приложений

Анализ контейнеров

IaC Scanning CheckMarx KICS SAST

Kubesec анализ манифестов

Эксплуатация в промышленном контуре

Защита и фильтрация L7 трафика

Мониторинг и подсчет метрик

DAST, IAST анализ приложений

Мониторинг инфраструктуры и окружений

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

Важные замечания

- Все системы на этапе runtime формируют и высылают автоматизированные отчеты. Часть отчетов интегрирована в SIEM, остальные в процессе интеграции.
- Артефакты и алерты, возникающие в процессе CI/CD/CT на текущий текущий момент хранятся в Gitlab, а также передаются во внешние сервисе алертинга и трекинга инцидентов.
- На стороне CVS ОМК происходит дополнительное security-code-review, обязательное перед релизом изменений чувствительных к безопасности
- Процесс сборки доставки приложения в любое из внутренних окружений инициирует сканирование приложения (**SAST** + **DAST** + **IAST**) на стенде сборки перед деплоем в любые окружения. В случае найденной уязвимости процесс доставки прерывается, формируется артефакт с отчетом

ОБЪЕДИНЕННАЯ МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

Основные элементы этапы пайплайна

Дополнительно и независимо и асинхронно от цикла SDLC происходит:

- **Система контроля защищенности и соответствия стандартам —** сканирование происходит по расписанию и независимо от процесса сборки приложений. Проверяется конфигурация окружений, контейнеров, инфраструктуры.
- Сканирование извне сети ОМК инструментами DAST, IAST. С активным WAF и поднятой ширмой WAF
- В рамках управления процессом безопасной разработки, команда использует регулярную встречу комитета по вопросам безопасности продуктов, в которых обязательно участвует Lead разработки, архитектор, DevOps-инженеры и офицер ИБ.