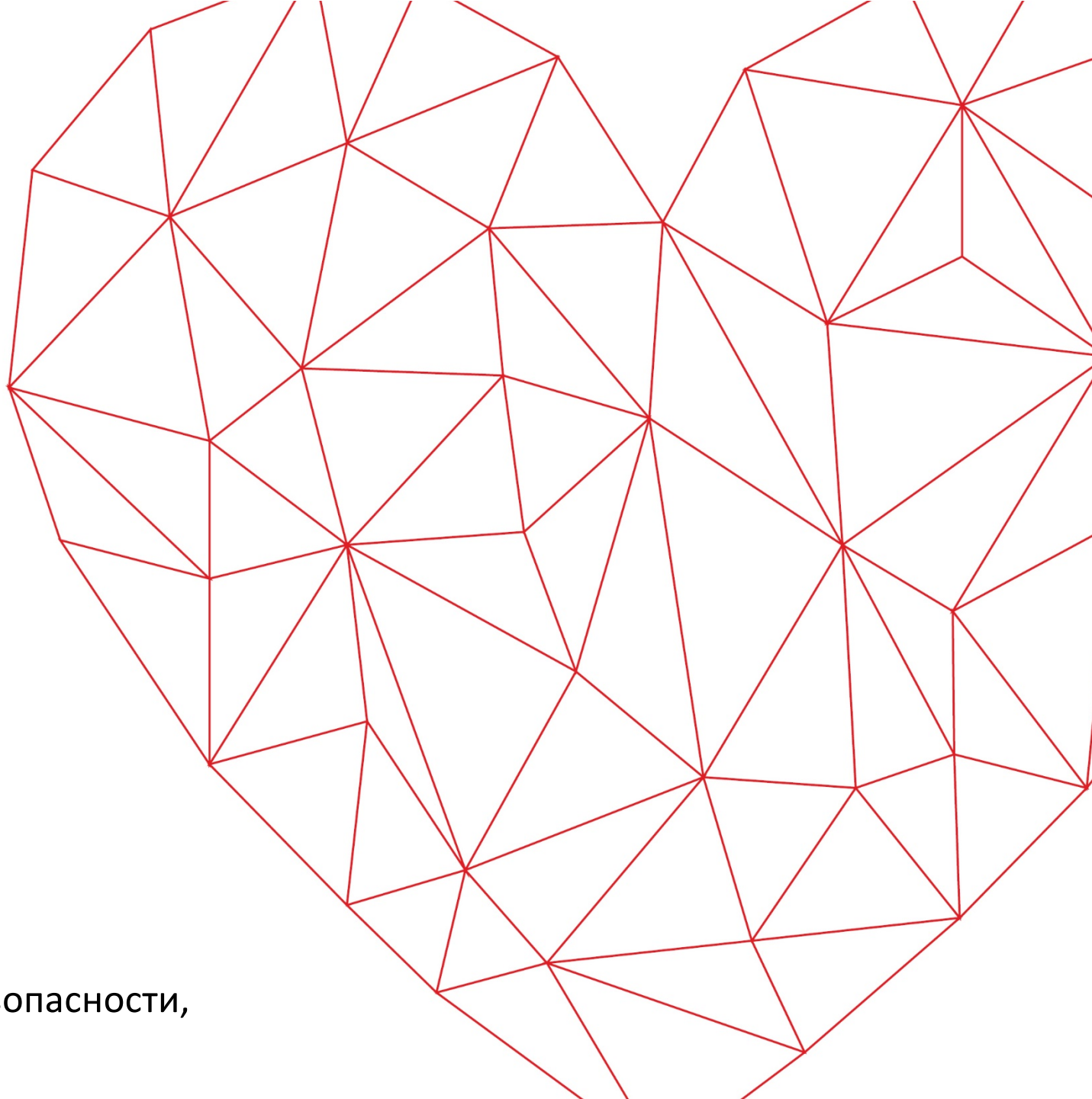
SUNLIGHT

Secure SDLC: инструменты для гибкого внедрения процессов DevSecOps



Подготовил: Шмаков Илья, CISO, AppSec

Заместитель директора по информационной безопасности,

2021, материал для ITSec

Аннотация

- Модель, получившая имя DevSecOps, подразумевает обеспечение безопасности на всех этапах разработки приложений, - контроль безопасности и разработка осуществляются параллельно, где безопасность внедряют в каждую часть процесса разработки.
- Материл рассматривается со стороны коммерческого сектора и самых эффективных форматов безопасной разработки для бесперебойной работы бизнеса.
- DevSecOps может использоваться, при переходе на микросервисы, в процессах Непрерывной интеграции (Continuous Integration, CI) и Непрерывного развертывания (Continuous Deployment, CD), или просто для тестирования инфраструктуры.
- Целью представленног является передача опыта и аналитика инструментов для гибкого внедрения процессов, методов и средств разработки в защищенном исполнении.
- Безопасная разработка критична из-за числа рисков, инцидентов ИБ – которые экспоненциально растут с каждым днем. Прогрессирующие злоумышленники стали понимать принципы разработки модели **win2win** организаций, которые подвергаются атакам, при этом им удается входить в группу доверенных пользователей из-за недостатка компетенций сотрудников.
- Важнее люди, а не инструменты.

SUNLIGHT

Универсальные характеристики ИС в безопасной разработке

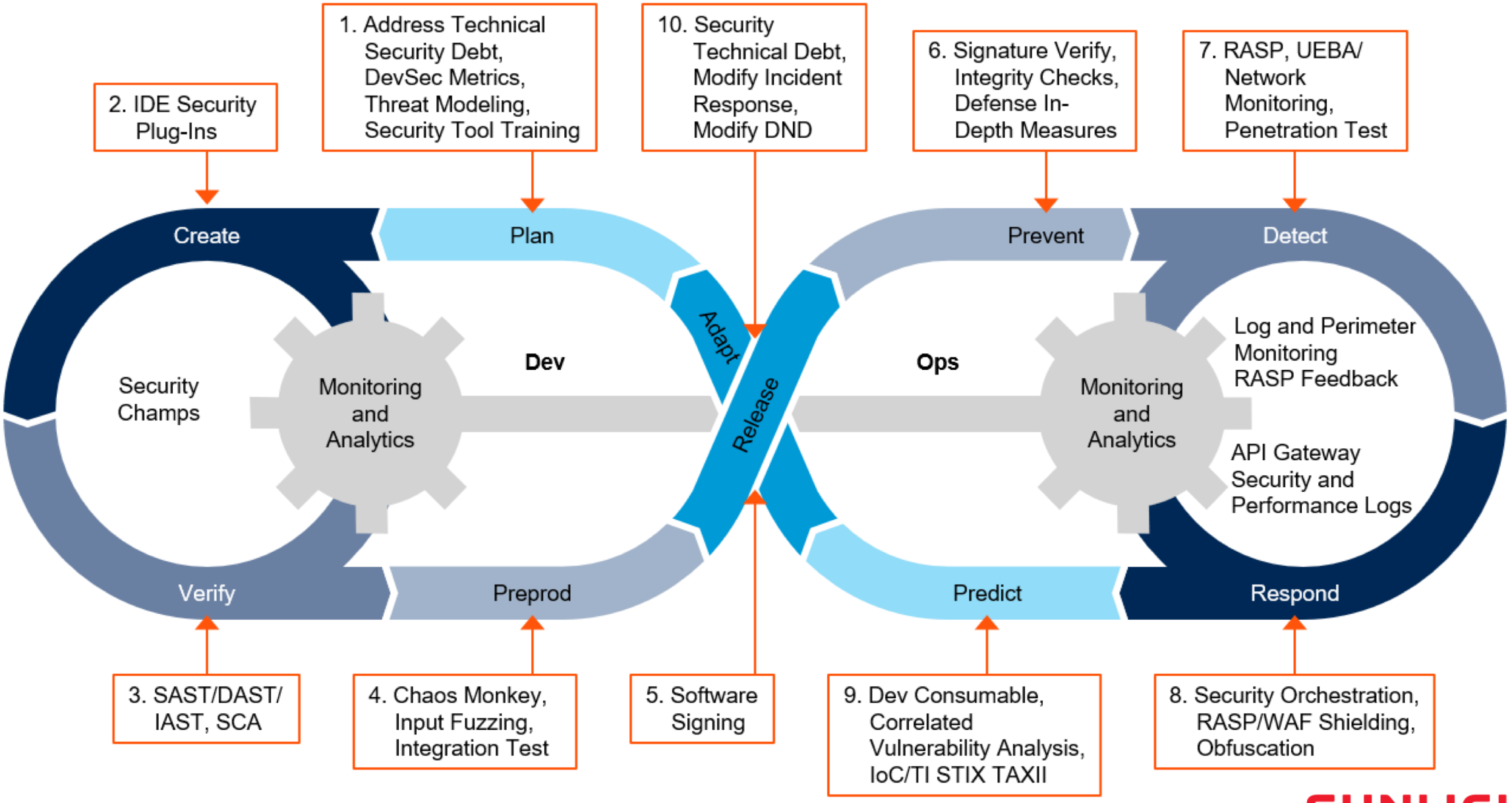
- Определим термин *безопасность информации*, который будем понимать как состояние уровня ее защищенности, которое обеспечивается сохранением качественных и количественных характеристик, а именно — целостности, доступности, конфиденциальности.
- Нацеленность функционирования под потребительские нужны и цели, при необходимости реализации: объединения и распараллеливания функциональных возможностей на подразделения и структуры, непосредственно самой организации;
- В следствии сбора и обработки информационных данных, последующего воссоздания, воздействия и изменения информации — на ней отражается политика взаимодействия процессов анализа, представляемая обобщением организационных, технологических, технических, программно-аппаратных и информационных средств, и методов;
- Представление проектирования интерфейса, в том числе соотношения **UI/UX**, прикладного программно-аппаратного обеспечения, как принцип минимальной содержательной достаточности для представление реализации взаимодействия функционирования с исключением эксплуатационной возможности НДВ, в целом и частном.
- Security Champion — точка входа в команду разработки и евангелист безопасности в одном лице.

SUNLIGHT

DevOps против DevSecOps: интеграция

- ИБ-руководителям необходимо придерживаться универсального и гибкого похода к DevOps, позволяющего сохранить прозрачность процесса разработки и уделяющего внимание целостности безопасности.
- Вопрос безопасности редко обсуждается, инфраструктура рассматривается как код. На данный момент существуют два лагеря: одни выбирают DevOps, другие считают DevSecOps единственно правильным подходом.
- Процесс может строиться по-разному — например, при написании кода есть ли у разработчиков инструмент, осуществляющий проверку на уязвимости в процессе локальной сборки или это реализуется внутри CI/CD с использованием Jenkins (Ansible)? Или же эти два подхода применяются одновременно, что помогает убедиться, что в каждом процессе сборки присутствует элемент безопасности, проверяющий степень защищенности кода.
- Майк Берселл из Red Hat подчеркивает, что бизнес редко рассматривает безопасность как отдельную категорию, которой должно быть уделено максимум внимания, ИБ рассматривается, скорее, в разрезе минимизации рисков. Берселл убежден, что безопасность является «ответственностью каждого», следовательно, компаниям стоит распределить соответствующие роли.

The DevSecOps Toolchain



Source: Gartner
ID: 377293

SUNLIGHT

Задачи для обеспечения Secure SDLC

- В условиях трансформации бизнеса и сокращения времени вывода новых цифровых продуктов на рынок основным индустриальным вызовом становится обеспечение информационной безопасности на всех этапах непрерывного производственного процесса.
- Реализация парадигмы кибербезопасности в DevOps представляет собой достаточно сложный процесс, в рамках которого слой Security-практик как бы обволакивает весь производственный инженерный цикл. Сами практики обеспечения информационной безопасности поддерживаются инструментальным стеком, интегрированным во все этапы технологического процесса.
- Отдельно стоит акцентировать внимание на важности практики DevSecOps-оркестрации (Application Security Testing Orchestration, ASTO), реализующей сквозную интеграцию инструментального стека ИБ с инструментами разработки, автоматизированное управление security-конвейером (пайплайнами), а также сбор, консолидацию и анализ всех данных в рамках непрерывного процесса разработки защищенного ПО. Практика оркестрации позволяет значительно сэкономить ресурсы и сократить общее время внедрения инициативы DevSecOps.

Обобщенные инструменты в формате этапов DevSecOps

Этап компоновки:

- Статический анализ исходного кода на наличие слабых мест
- Автоматическое тестирование безопасности (AST)
- Анализ состава ПО
- Брандмауэр веб-приложений (WAF)

Этап тестирования:

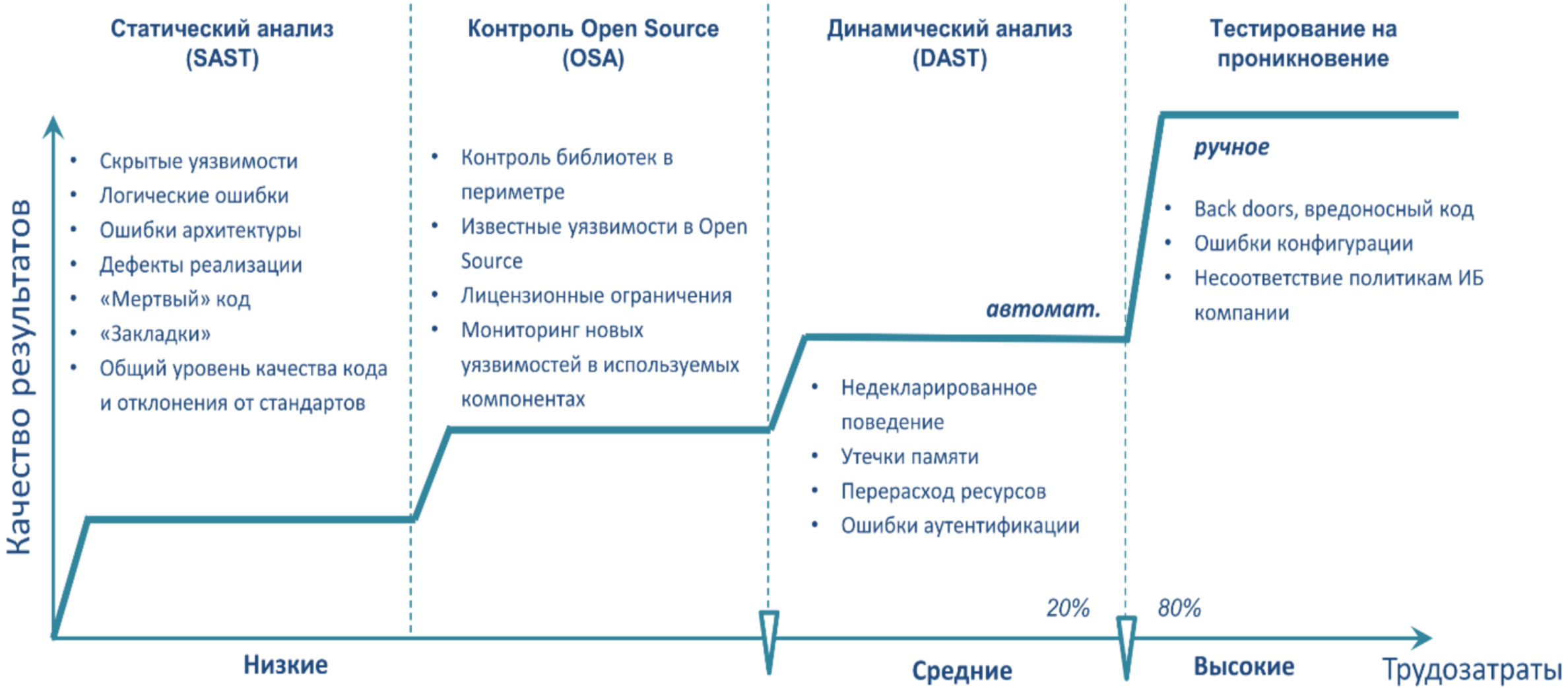
- Динамическое тестирование безопасности (DAST)
- Интерактивное тестирование безопасности (IAST)
- Брандмауэр веб-приложений (WAF)

Этап выполнения:

- Брандмауэр веб-приложений (WAF)
- Динамическое тестирование безопасности (DAST)
- Программа вознаграждения за нахождение ошибок
- Анализ угроз

SUNLIGHT

Этапы тестирования



SUNLIGHT

Необходимые инструменты для обеспечения Secure SDLC, Часть 1

- Контроль компонент с открытым исходным кодом при попадании в периметр разработки (Open Source Analysis, OSA);
- Статический анализ кода (Static Application Security Testing, SAST);
- Контроль состава компонент ПО (Software Composition Analysis, SCA);
- Все виды динамического анализа (Dynamic Application Security Testing, DAST / Interactive Application Security Testing, IAST / Behavioral Application Security Testing, BAST);
- Анализ бинарного кода и контроль состава контейнеров (Bytecode and Container Analysis, BCA);
- Реализация WAF (Web Application Firewall).

Ремарка событийности:

— А вы кто? Я вас вижу в первый раз. У меня все хорошо — мне старший товарищ на code review поставил «apply», мы идем дальше!

SUNLIGHT

Необходимые инструменты для обеспечения Secure SDLC, Часть 2

В то же время важнейшими аспектами при масштабировании и трансформации DevOps процессов в производную парадигму DevSecOps являются:

- Использование безопасных по умолчанию библиотек, фреймворков и компонент ПО в процессе разработки (Secure-by-Default);
- Интеграция технологических практик ИБ в самое начало конвейера CI/CD (Shift-Left подход);
- Автоматизация всех процессов в концепции Everything-as-a-Code;
- Формирование сообщества security-чемпионов, которые отвечают за задачи информационной безопасности в производственных командах и являются проводниками инженерной security-культуры;
- Применение модели зрелости DevSecOps как для оценки существующего процесса, так и для постоянного совершенствования;
- Обеспечение прозрачности всех security активностей для всех участников инженерного производственного процесса.

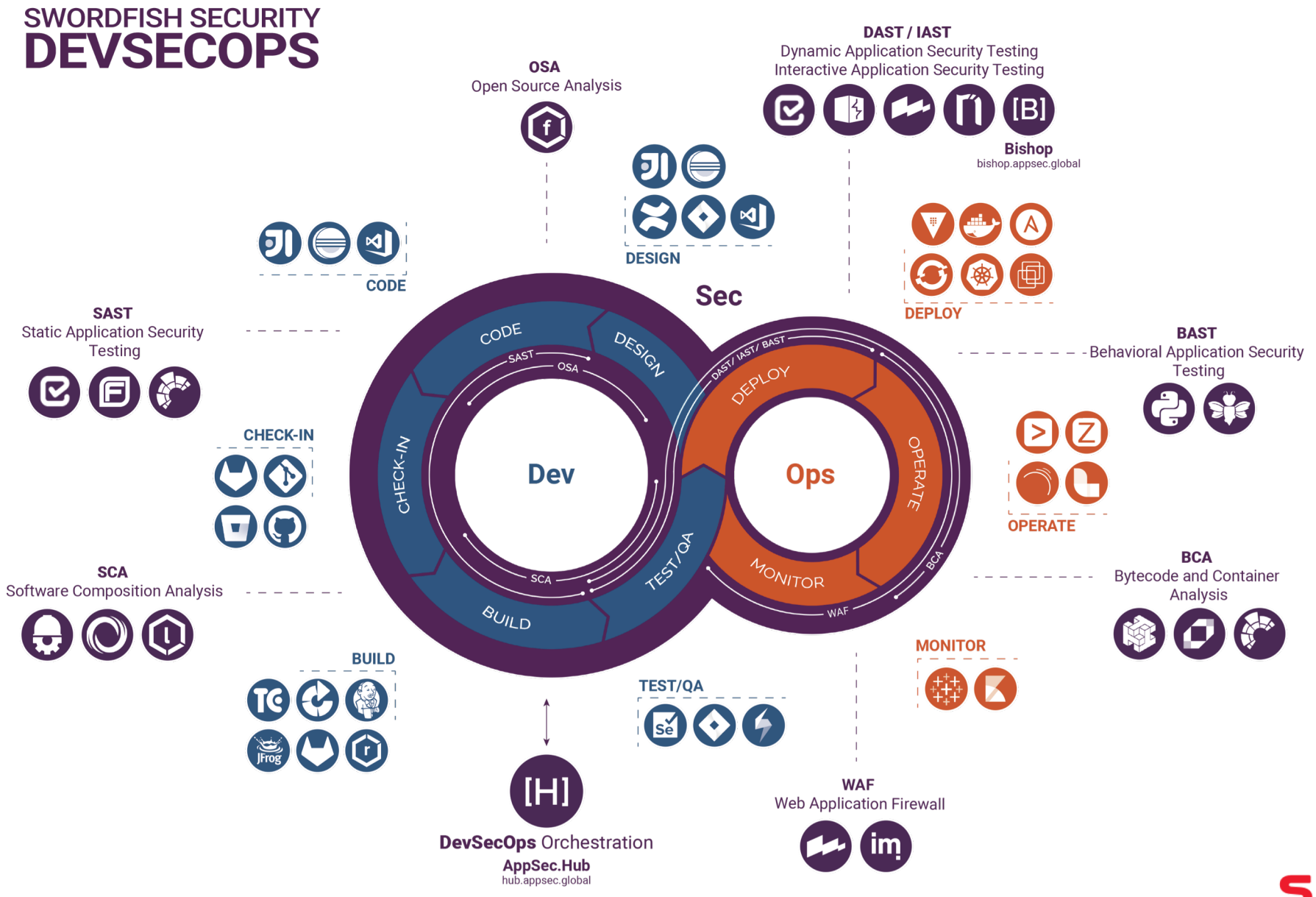
SUNLIGHT

Ключевые факторы внедрения инструментов DevSecOps

- Внедрение отдельного инструмента или элемента процесса кибербезопасности, безусловно, является важным шагом, но ни в коем случае не является серебряной пулей для решения вопросов защищенности разрабатываемого ПО в промышленных масштабах. Ключом к успеху является только комплексное применение всего пула практик обеспечения ИБ.
- Применение практики оркестрации убережет инженерные команды и команду информационной безопасности от технологического хаоса «наколеночной» интеграции инструментов и неуправляемой «лоскутной» автоматизации.
- Сбор данных и последующая визуализация метрик позволит управлять сквозным процессом, реализовать полную прозрачность, а также создать необходимый базис для применения практик машинного обучения в будущем.
- Часто планирование процесса безопасной разработки начинается с выбора и покупки инструмента, а заканчивается — попытками интегрировать инструмент в текущий процесс, которые так и остаются попытками.
- Распространенный случай, когда отдел безопасности выбрал хороший, дорогой инструмент, с широкими возможностями, и пришел к разработчикам — встраивать в процесс. Но не выходит — процесс построен так, что ограничения уже купленного инструмента не ложатся в текущую парадигму.

SUNLIGHT

Пример: Swordfish Security DevSecOps



SUNLIGHT

Алгоритм действий внедрения DevSecOps

- Назначьте экспертов по безопасности
- Учитывайте безопасность на стадии проектирования
- Добавляйте в пайплайн авто-тесты на безопасность
- Заручитесь помощью экспертов
- Проверяйте зависимости
- Зовите красную команду
- Уязвимости — это те же ошибки
- Следите за продакшеном

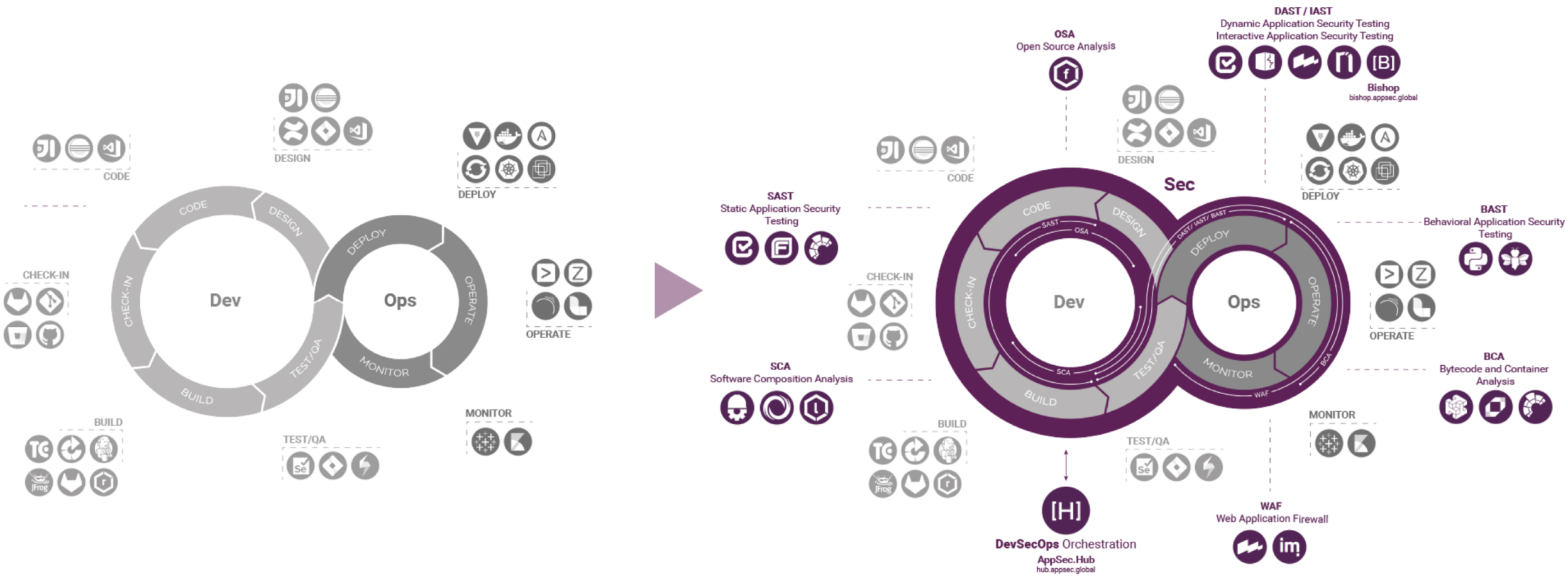
Результаты: технологический процесс – практики ИБ – метрики – масштабируемость – полное покрытие.

SUNLIGHT

Выводы, Часть 1

- Сдвиг безопасности влево предполагает, что вопросы безопасности рассматриваются всей командой на каждой стадии цикла разработки.
- Внедрение аспектов безопасности в ваш пайплайн подразумевает, что вы регулярно получаете обратную связь по безопасности вашего приложения и можете вводить необходимые улучшения точно так же, как вводите другую функциональность.
- Относясь к каждой найденной уязвимости как к обычной ошибке, которую нужно отследить, исправить и протестировать, вы со временем сделаете ваше ПО более устойчивым.
- В конце концов, DevOps (а значит и DevSecOps) — это не только инструменты и процессы, позволяющие осуществлять быструю и частую доставку ПО, но и особая культура. Все это возможно только благодаря людям.
- У каждого члена команды должна быть возможность поднять вопрос безопасности и быть услышанным — будь то во время планирования спринта, код-ревью, ручного тестирования или уже после запуска системы в продакшне. И каждый может сыграть свою роль в оценке важности безопасности и в ее реализации.

Выводы, Часть 2



SUNLIGHT

Sunlight SDLC и продуктовые решения

SUNLIGHT — БОЛЬШЕ ЧЕМ ЮВЕЛИРНАЯ КОМПАНИЯ

5 500	156	120
СОТРУДНИКОВ	ГОРОДОВ	ПРОИЗВОДИТЕЛЕЙ
70 000	400	25млн
ЮВЕЛИРНЫХ УКРАШЕНИЙ	МАГАЗИНОВ	ПОКУПАТЕЛЕЙ

E-commerce
Разработка высоконагру-женных систем с миллионами пользователей и сотнями тысяч заказов в месяц

Supply Chain
Управление IT-системами, которые обеспечивают непрерывные поставки и быструю доставку

Мобильная разработка
Мобильные приложения для IOS и Android: первые места в сторах и миллионы уникальных пользователей

BI&Big Data
Десятки миллионов событий каждый день, современные продукты для аналитики

Marketplace и портал поставщиков
Крупнейший ювелирный маркетплейс и платформа для работы с поставщиками

Retail-платформа
Платформа для магазинов на базе 1С, в которой ежедневно совершаются миллионы операций

SUNLIGHT — это:

- сайт и мобильное приложение, которые посещают более 30 миллионов раз в месяц;
- приложение для продавцов, которым пользуются 4000 продавцов ежедневно - SUNRETAIL — собственная разработка отдела IT & DIGITAL.
- WMS, в котором собираются десятки тысяч заказов каждый день;
- розничная платформа, обрабатывающая миллионы событий каждый день, а также развитая отказоустойчивая IT инфраструктура с сотнями физических и виртуальных серверов.

За 20 лет мы выросли из ювелирного бренда в технологическую компанию!

Сайт и мобильное приложение SUNLIGHT — мощная IT-структура, с сотнями физических и виртуальных серверов.
Это уникальное приложение, которое уже несколько лет успешно оптимизирует работу более 4 тыс. человек в розничном секторе компании.

SUNLIGHT

Спасибо за внимание ;)
Вопросы?