

DEVOPS/DEVSECOPS.
БЕЗОПАСНАЯ РАЗРАБОТКА
ФРЕЙМВОРКИ ЗРЕЛОСТИ SSDLC



АЛЕКСАНДР БАКИН

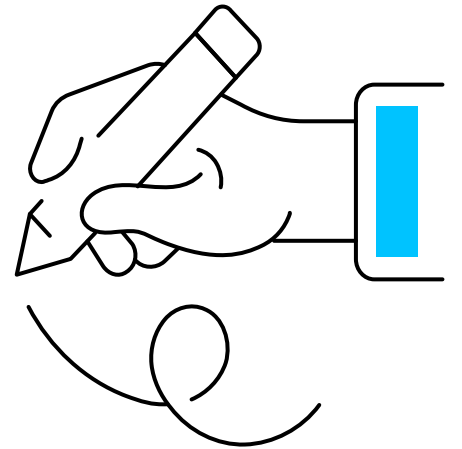
АО «Инфосистемы Джет»

Люблю шоссейный бег и безопасную разработку ПО в любых ее проявлениях.

Отвечаю за консалтинг в направлении безопасной разработки ПО в ЦИБ Джет

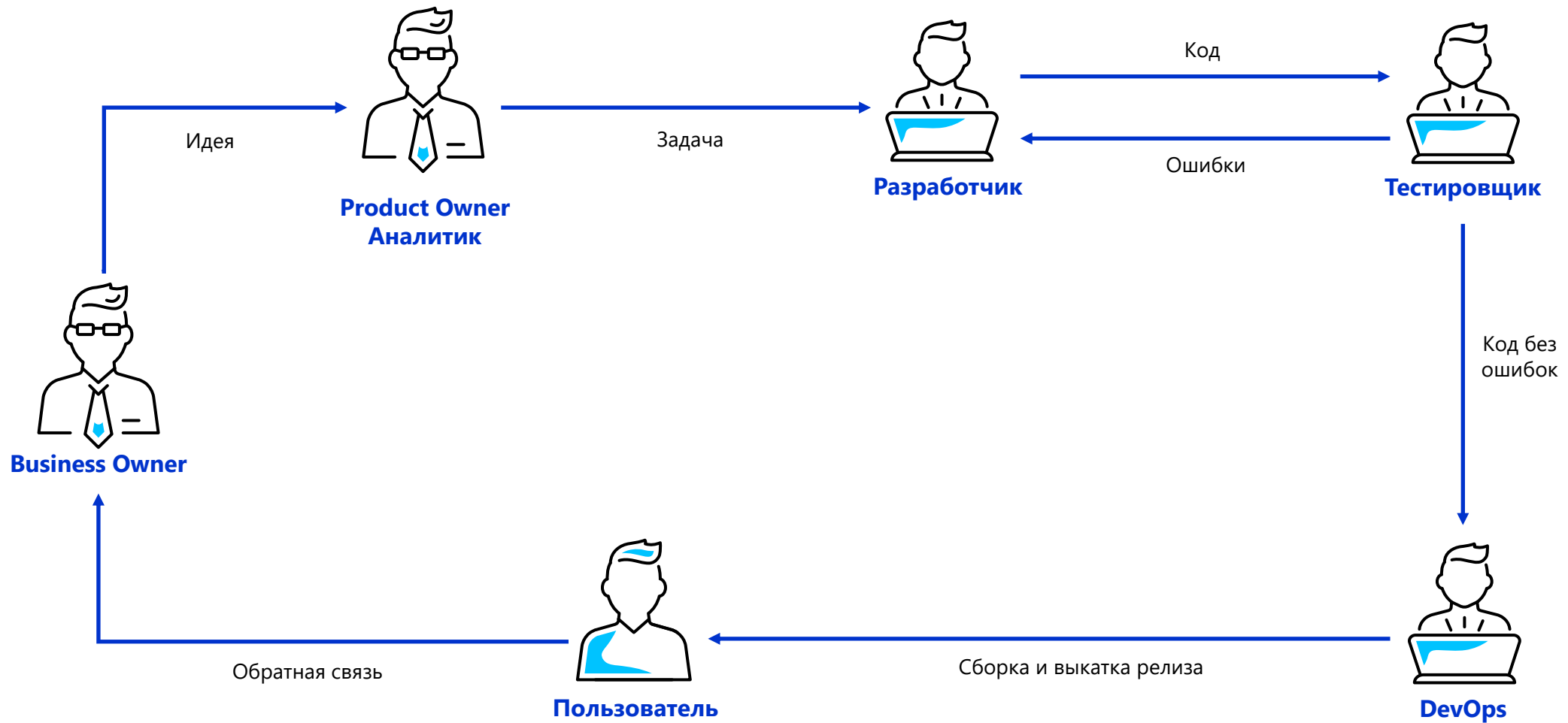
ЦЕЛИ ЗАНЯТИЯ

- ✓ Понять зачем вообще мерить SSDLC
- ✓ Познакомиться с существующими моделями оценки зрелости SSDLC
- ✓ Глубже познакомится с лучшей отечественной моделью оценки зрелости SSDLC/DevSecOps - DevSecOps Assessment Framework (DAF)

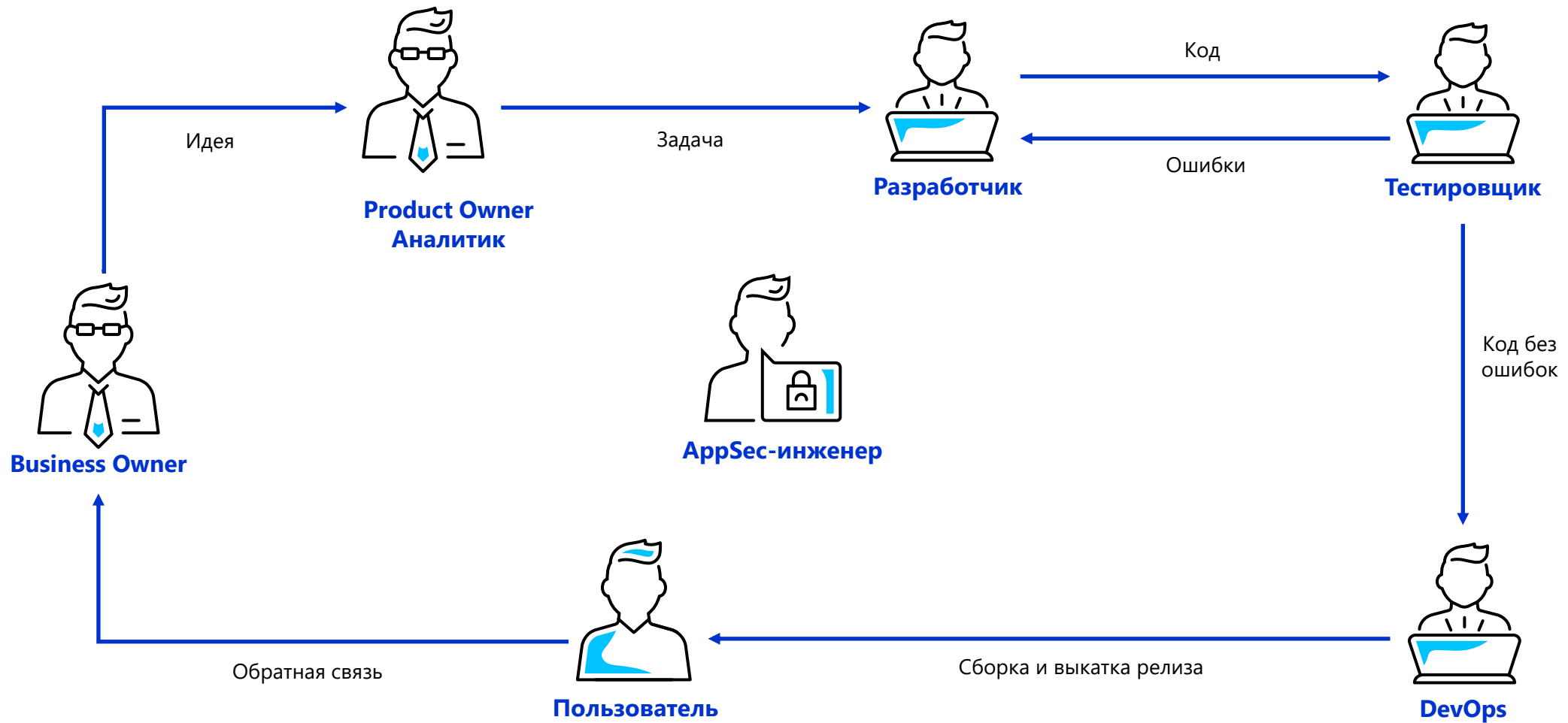


ЗАЧЕМ МЕРИТЬ ЗРЕЛОСТЬ?

РАЗРАБОТКА ПО



РАЗРАБОТКА ПО



МОДЕЛИ ЗРЕЛОСТИ БЕЗОПАСНОЙ РАЗРАБОТКИ

4
домена

12
практик

122
активности

Практики

GOVERNANCE

1. Стратегия и метрики
2. Соответствие требованиям и политики
3. Обучение

INTELLIGENCE

4. Модели атак
5. Механизмы безопасности и дизайн
6. Стандарты и требования

SSDL TOUCHPOINTS

7. Анализ архитектуры
8. Ревью кода
9. Тестирование безопасности

DEPLOYMENT

10. Тестирование на проникновение
11. Среды функционирования
12. Управление конфигурацией и уязвимостями

OWASP SAMM

GOVERNANCE

Strategy & Metrics

SM1 | SM2 | SM3

- A. Create & Promote
- B. Measure & Improve

Policy & Compliance

PC1 | PC2 | PC3

- A. Policy & Standards
- B. Compliance management

Education & Guidance

EG1 | EG2 | EG3

- A. Training & Awareness
- B. Organization & Culture

DESIGN

Threat Assessment

TA1 | TA2 | TA3

- A. Application risk profile
- B. Threat modeling

Security Requirement

SR1 | SR2 | SR3

- A. Software requirements
- B. Supplier security

Security Architecture

SA1 | SA2 | SA3

- A. Architecture design
- B. Technology management

IMPLEMENTATION

Security Build

SB1 | SB2 | SB3

- A. Build process
- B. Software dependencies

Security Deployment

SD1 | SD2 | SD3

- A. Deployment process
- B. Secret management

Defect Management

DM1 | DM2 | DM3

- A. Defect tracking
- B. Metrics & feedback

VERIFICATION

Architecture Assessment

AA1 | AA2 | AA3

- A. Architecture validation
- B. Architecture mitigation

Requirements-driven Testing

RT1 | RT2 | RT3

- A. Control verification
- B. Misuse/abuse testing

Security Testing

ST1 | ST2 | ST3

- A. Scalable baseline
- B. Deep understanding

OPERATION

Incident Management

IM1 | IM2 | IM3

- A. Incident detection
- B. Incident response

Environment Management

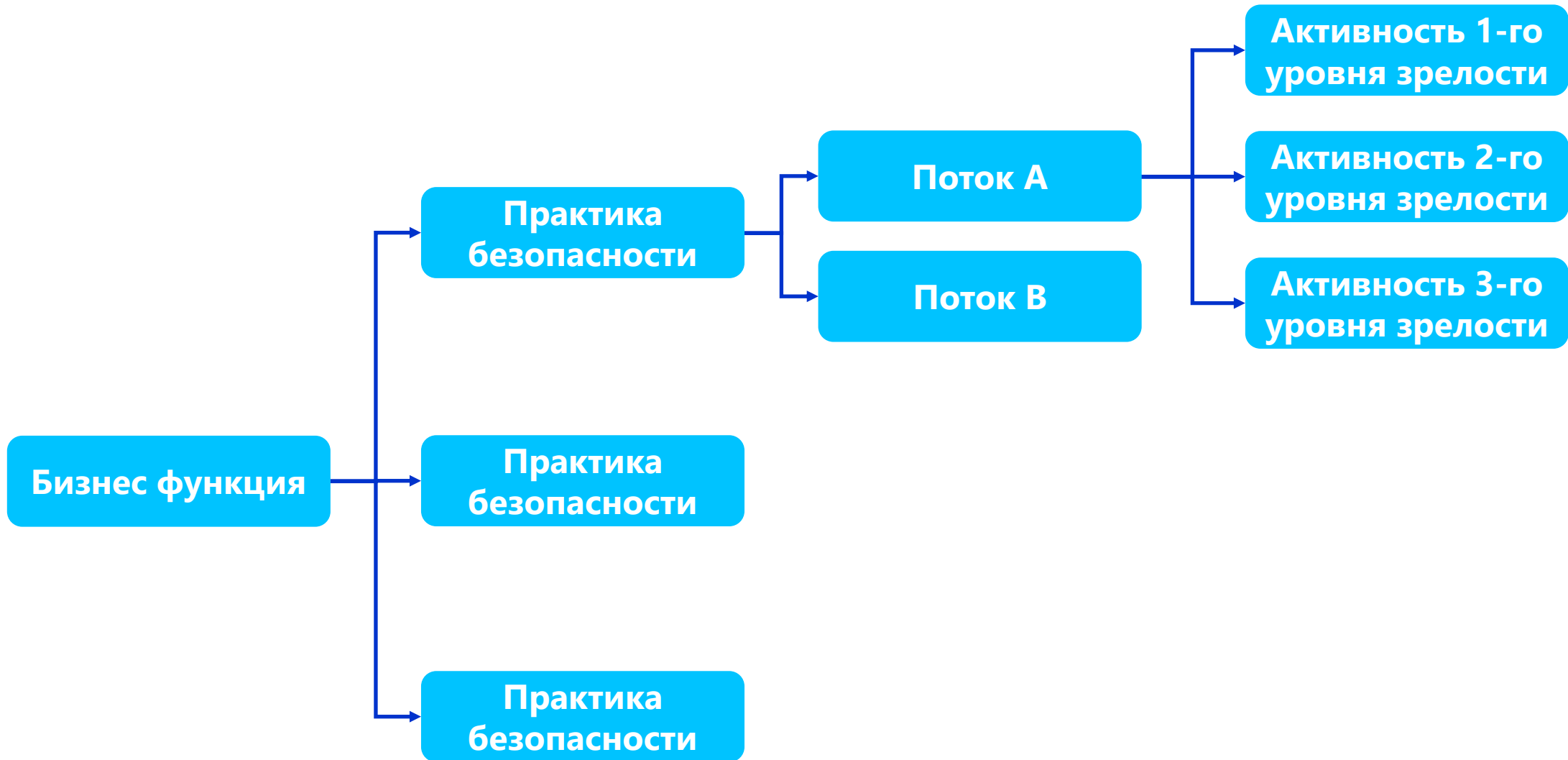
EM1 | EM2 | EM3

- A. Configuration hardening
- B. Patching & Updating

Operational Management

OM1 | OM2 | OM3

- A. Data protection
- B. System decommissioning / legacy management





SubDimension Filter

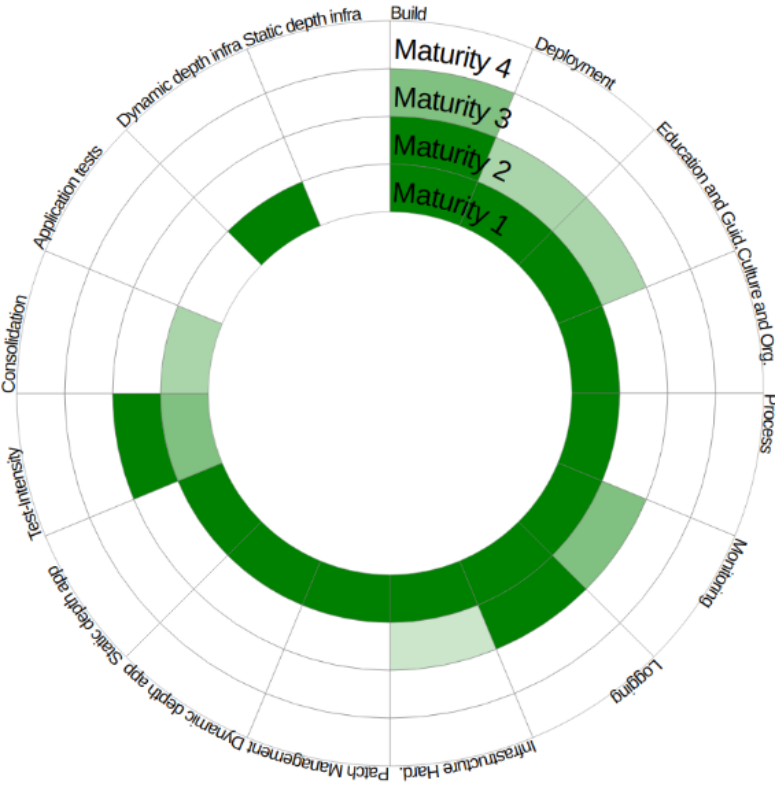
BuildDeploymentPatch ManagementDesignEducation and GuidanceProcessApplication HardeningDevelopment and Source ControlInfrastructure HardeningLoggingMonitoringApplication testsConsolidationDynamic depth for applicationsDynamic depth for infrastructureStatic depth for applicationsStatic depth for infrastructureTest-Intensity

Activity Tag Filter

nonepatching

RESET

Dimension	Sub-Dimension	Level 1: Basic understanding of security practices	Level 2: Adoption of basic security practices	Level 3: High adoption of security practices	Level 4: Very high adoption of security practices	Level 5: Advanced deployment of security practices at scale
 Build and Deployment	Build	<div>▶ Defined build process [none]</div>	<div>▶ Building and testing of artifacts in virtual environments [none]</div> <div>▶ Pinning of artifacts [none]</div> <div>▶ SBOM of components [none]</div>	<div>▶ Signing of code [none]</div>		<div>▶ Signing of artifacts [none]</div>
 Build and Deployment	Deployment	<div>▶ Defined deployment process [none]</div>	<div>▶ Defined decommissioning process [none]</div> <div>▶ Environment depending configuration parameters (secrets) [none]</div> <div>▶ Evaluation of the trust of used components [none]</div>	<div>▶ Handover of confidential parameters [none]</div> <div>▶ Inventory of dependencies [none]</div> <div>▶ Inventory of running artifacts [none]</div> <div>▶ Rolling update on deployment [none]</div>	<div>▶ Same artifact for environments [none]</div> <div>▶ Usage of feature toggles [none]</div>	<div>▶ Blue/Green Deployment [none]</div>



<https://dsomm.owasp.org/>

DEVSECOPS ASSESSMENT FRAMEWORK (DAF)

ТЕХНОЛОГИИ

Контроль ИБ артефактов, зависимостей и образов

Контроль использования сторонних компонентов

Управление артефактами

Защита окружения разработки

Защита рабочих мест разработчика

Защита секретов

Защита Build-среды

Защита source code management (SCM)

Контроль внесения изменений в исходный код

Защита конвейера сборки

Контроль кода, ИБ артефактов, зависимостей и образов

Статический анализ (SAST)

Композиционный анализ (SCA)

Анализ образов контейнеров

Идентификация секретов

Контроль безопасности Dockerfile'ов

Анализ ПО в режиме runtime - Preprod

Динамический анализ приложений (DAST) в PREPROD среде

Тестирование на проникновение перед внедрением приложений в продуктив

Функциональное ИБ-тестирование

Контроль безопасности манифестов (k8s, terraform)

Анализ инфраструктуры PREPROD среды на уязвимости

Защита ПО и инфраструктуры в режиме runtime

Управление секретами

Динамический анализ приложений (DAST) в продуктивной среде

Тестирование на проникновение продуктивной среды

Управление изменениями инфраструктуры и доступом к ней

Контроль сетевого трафика (L4-L7)

Контроль выполняемых и процессов и их прав доступа

Анализ инфраструктуры PROD среды на уязвимости

Анализ событий ИБ

ПРОЦЕССЫ

Обучение и база знаний

Обучение специалистов

Управление базой знаний DSO

Контроль и формирование требований ИБ к ПО

Оценка критичности
приложений и
моделирование угроз

Определение требований
ИБ, предъявляемых к ПО

Контроль выполнения
требований ИБ

Разработка стандартов конфигураций
разрабатываемого ПО

Разработка стандартов конфигураций
для компонентов инфраструктуры

Управление ИБ дефектами

Обработка дефектов ИБ

Консолидация дефектов ИБ

Управление набором метрик ИБ

Контроль исполнения метрик

Функциональные роли

Security Champions

Разграничение ролей процесса DSO

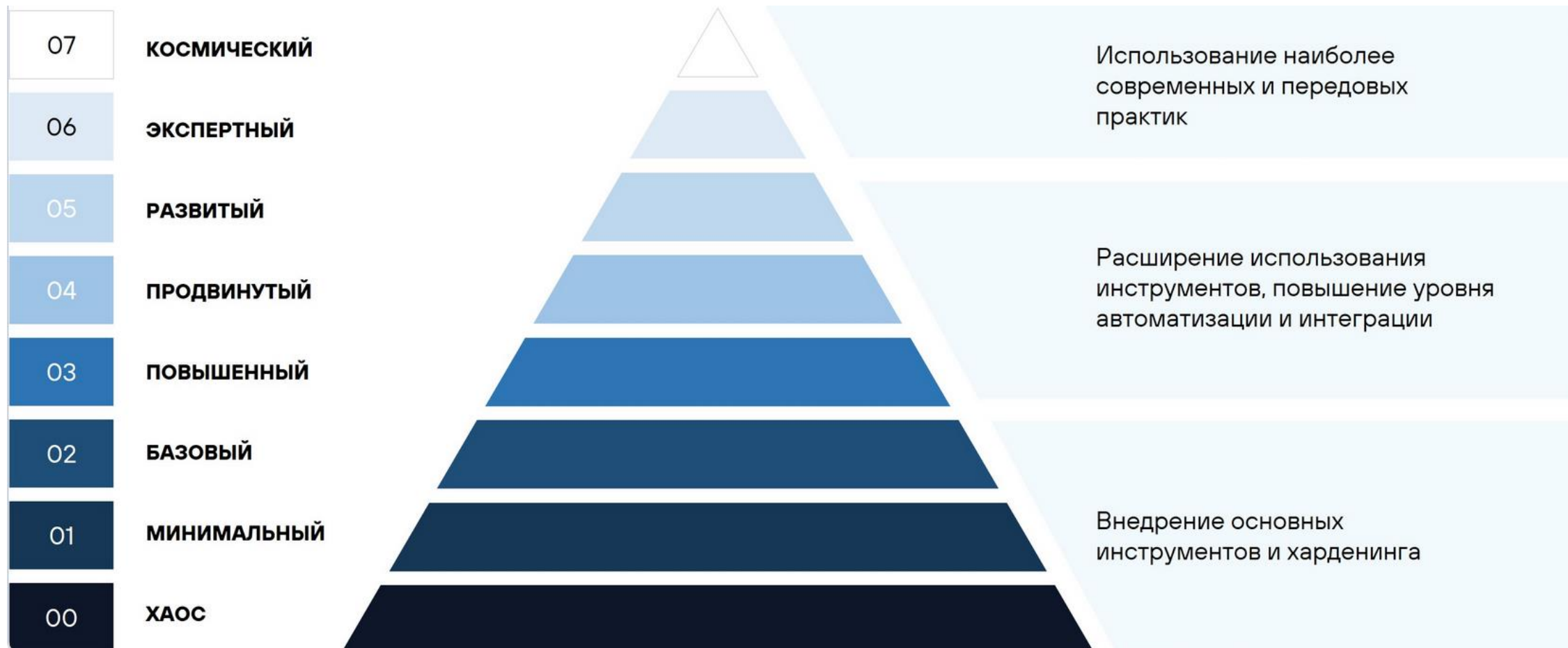
DAF – МАППИНГ СО СТАНДАРТАМИ

Поддомен	ID	Практики и их требования	Оценка	Уровень сложности практики	Соответствие уровню сложности	% выполнения группы практик	Уровень Пирамиды зрелости	BSIMM	OWASP SAM
Домен "Контроль ИБ артефактов, зависимостей и образов"									
Контроль использования сторонних компонентов	T-ADI-DEP-0-1	Управление зависимостями (Dependencies) в исходном коде осуществляется в каком-либо виде	Неверно	0			0		
	T-ADI-DEP-1-1	Существуют (формализованы) единые правила, определяющие возможность использования тех или иных зависимостей в коде. Например, есть утвержденный документ, и/или страница в базе знаний, описывающие порядок использования зависимостей в коде.	Не выполняется				2		
	T-ADI-DEP-1-2	Обновление существующих зависимостей выполняется вручную. Например, если возникла необходимость использовать новую версию библиотеки в коде, то ее вручную выгружают и добавляют в проект	Не выполняется	1	0%		2		
	T-ADI-DEP-1-3	Существует (описан, формализован) план реагирования на события ИБ, связанных с зависимостями.	Не выполняется				2	SR2.7	
	T-ADI-DEP-1-4	Выполняется харденинг (безопасная настройка) файлов конфигураций используемых пакетов open source software - OSS (например, nuget.config, .npmrc, pip.conf, pom.xml, etc.).	Не выполняется				2		
	T-ADI-DEP-1-5	Зависимости с тэгом "latest" не применяются	Не выполняется				2		
	T-ADI-DEP-2-1	Разработчики получают и используют OSS компоненты, применяя только стандартизованные (формализованные и утвержденные) методы	Не выполняется				3	SR2.7	
	T-ADI-DEP-2-2	Контролируется и регулируется использование новых (молже 60 дней) и старых (неактуальных, заброшенных, старше 365 дней) OSS. Например, настроен OSS firewall на предупреждение (или запрет) использования OSS, выпущенных\актуализированных более 365 дней назад и менее чем 60 дней	Не выполняется	2	0%		3		
	T-ADI-DEP-3-1	Выполняется инвентаризация используемых зависимостей. Например, создан внутренний репозиторий.	Не выполняется				4	SR1.5	
	T-ADI-DEP-3-2	При выполнении Pull/Merge request предоставляется список всех уязвимостей используемых зависимостей. Это может быть реализовано с помощью SCA системы.	Не выполняется	3	0%		4		
	T-ADI-DEP-3-3	Выполняется верификация цифровой подписи SBOM перед использованием зависимостей в сборке. Это может быть реализовано с помощью SCA системы.	Не выполняется				4		
	T-ADI-DEP-3-4	Выполняется автоматическое обновление используемых зависимостей. Это может быть реализовано с помощью специальных утилит для обновления зависимостей.	Не выполняется				4		
	T-ADI-DEP-4-1	Выполняется самостоятельная сборка необходимых зависимостей в доверенной среде	Не выполняется				6		
	T-ADI-DEP-4-2	Выполняется создание и проверка цифровой подписи собранных зависимостей Например, с помощью Cosign	Не выполняется	4	0%		6	SE2.4	
	T-ADI-DEP-4-3	Выполняется создание и проверка цифровой подписи на SBOM для собранных зависимостей Например, с помощью Cosign	Не выполняется				6		
	T-ADI-ART-0-1	Управление артефактами разработки присутствует в каком-либо виде	Неверно	0			0		

DAF – ТЕПЛОВАЯ КАРТА

Модель	Домен	Поддомен	Описание поддомена	Этап зрелости					Итого по блоку
				0. Uninitiated	1. Beginners	2. Intermediate	3. Advanced	4. Experts	
Технологии	Контроль ИБ артефактов, зависимостей и образов	T-ADI-DEP	Контроль использования сторонних компонентов	Не реализуется	0%	0%	0%	0%	0%
		T-ADI-ART	Управление артефактами	Не реализуется	0%	0%	0%	0%	0%
	Защита окружения разработки	T-DEV-COMP	Защита рабочих мест разработчика	Не реализуется	0%	0%			0%
		T-DEV-SM	Защита секретов	Не реализуется	0%	0%	0%	0%	0%
		T-DEV-BLD	Защита Build-среды	Не реализуется	0%	0%	0%	0%	0%
		T-DEV-SCM	Защита source code management (SCM)	Не реализуется	0%	0%	0%	0%	0%
		T-DEV-SRC	Контроль внесения изменений в исходный код	Не реализуется	0%	0%	0%	0%	0%
		T-DEV-CICD	Защита конвейера сборки	Не реализуется	0%	0%	0%	0%	0%
	Контроль кода, ИБ артефактов, зависимостей и образов	T-CODE-SST	Статический анализ (SAST)	Не реализуется	0%	0%	0%	0%	0%
		T-CODE-SC	Композиционный анализ (SCA)	Не реализуется	0%	0%	0%	0%	0%
		T-CODE-IMG	Анализ образов контейнеров	Не реализуется	0%	0%	0%	0%	0%
		T-CODE-SECDN	Идентификация секретов	Не реализуется	0%	0%	0%	0%	0%
	Анализ ПО в режиме runtime - Preprod	T-CODE-DOCKERFS	Контроль безопасности Dockerfile'ов	Не реализуется	0%	0%			0%
		T-PREPROD-DAST	Динамический анализ приложений (DAST) в PREPROD среде	Не реализуется	0%	0%	0%	0%	0%
		T-PREPROD-PENTEST	Тестирование на проникновение перед внедрением приложений в продуктив	Не реализуется	0%	0%		0%	0%
		T-PREPROD-SECTEST	Функциональное ИБ-тестирование	Не реализуется	0%	0%	0%		0%
		T-PREPROD-MANSEC	Контроль безопасности манифестов (k8s, terraform и т.д.)	Не реализуется	0%	0%			0%
		T-PREPROD-VULN	Анализ инфраструктуры PREPROD среды на уязвимости	Не реализуется	0%	0%	0%	0%	0%
	Защита ПО и инфраструктуры в режиме runtime	T-PROD-SM	Управление секретами	Не реализуется	0%	0%	0%	0%	0%
		T-PROD-DAST	Динамический анализ приложений (DAST) в продуктивной среде	Не реализуется	0%	0%	0%	0%	0%
		T-PROD-PENTEST	Тестирование на проникновение продуктивной среды	Не реализуется	0%	0%		0%	0%
		T-PROD-ACCESS	Управление изменениями инфраструктуры и доступом к ней	Не реализуется	0%	0%	0%	0%	0%
		T-PROD-NETWORK	Контроль сетевого трафика (L4-L7)	Не реализуется	0%	0%	0%		0%
		T-PROD-RUN	Контроль выполняемых и процессов и их прав доступа	Не реализуется	0%	0%	0%		0%
		T-PROD-VULN	Анализ инфраструктуры PROD среды на уязвимости	Не реализуется	0%	0%	0%	0%	0%
		T-PROD-EVENTS	Анализ событий информационной безопасности	Не реализуется		0%	0%		0%
Процессы	Обучение и база знаний	P-EDU-AWR	Обучение специалистов	Не реализуется	0%	0%	0%	0%	0%
		P-EDU-KB	Управление базой знаний DSO	Не реализуется	0%	0%	0%	0%	0%
	Контроль и формирование требований ИБ к ПО	P-REQ-TM	Оценка критичности приложений и моделирование угроз	Не реализуется	0%	0%	0%	0%	0%
		P-REQ-RD	Определение требований ИБ, предъявляемых к ПО	Не реализуется	0%	0%	0%		0%
		P-REQ-CR	Контроль выполнения требований ИБ	Не реализуется	0%	0%	0%	0%	0%
		P-REQ-STDR-App	Разработка стандартов конфигураций разрабатываемого ПО	Не реализуется	0%	0%	0%	0%	0%
		P-REQ-STDR-Infr	Разработка стандартов конфигураций для компонентов инфраструктуры	Не реализуется	0%	0%	0%	0%	0%
	Управление ИБ дефектами	P-DEFECT-MNG	Обработка дефектов ИБ	Не реализуется	0%	0%	0%	0%	0%
		P-DEFECT-CNS	Консолидация дефектов ИБ	Не реализуется	0%	0%	0%	0%	0%
		P-MET-SET	Управление набором метрик ИБ	Не реализуется		0%	0%		0%
		P-MET-EX	Контроль исполнения метрик	Не реализуется		0%	0%	0%	0%
	Функциональные роли	P-ROLE-SC	Security Champions	Не реализуется	0%	0%	0%	0%	0%
		P-ROLE-RESP	Разграничение ролей процесса DSO	Не реализуется	0%	0%	0%		0%

DAF – ПИРАМИДА ЗРЕЛОСТИ



Что скрыто:

- Подробный план задач на доработку
- Аудиторская часть: как проверить, что требование выполняется; ОЛ аудитора; план интервью
- Автоматизация построения Кирилламиды для Отчетов
- Примеры полноценных RoadMap (открытая часть содержит только обобщенный RoadMap)
- Примеры RACI-матриц
- Матрица компетенций, расчет FTE
- MVP страниц, которые пока не готовы для публикаций (например маппинг с DSOMM и ПЗ ЦБ)



License

"THE BEER-WARE LICENSE" (Revision 42):

* Jet Infosystems DevSecOps Team <daf@jet.su> made this Framework. As long as you retain this notice *
* you can do whatever you want with it, even use it some day, and you think this Framework is worth it, *
* you can buy us a beer. *

A small and optional request:

> If you use our Framework in your local or government development regulations, <
> for marketing or other public relations, please let us know about this Framework in articles or <
> at conferences, please let us know. <
> Telegram: DevSecOps_Assessment <
> Mail: daf@jet.su <

"ЛИЦЕНЗИЯ BEER-WARE" (Версия 42):

* создала этот Фреймворк. До тех пор, пока вы *
* можете делать с ним что угодно, даже использовать его в будущем, *
* если вы считаете, что этот Фреймворк полезен, можете купить нам пиво. *

Небольшая и необязательная просьба:

> Фреймворк в разработке локальных или государственных <
> систем, если рассказываете об этом Фреймворке <
> сообщайте, пожалуйста, по адресу: <
> daf@jet.su <
> Mail: daf@jet.su <

DAF



<https://github.com/Jet-Security-Team/DevSecOps-Assessment-Framework>

Сегодня мы поговорили о...

- Зачем мерить SSDLC
- Существующие модели оценки зрелости SSDLC
- Подробнее остановились на DevSecOps Assessment Framework (DAF)
- Агитировали стать контрибьюторами и помочь улучшить фреймворк ;-)

ДОМАШНЕЕ ЗАДАНИЕ

ДОМАШНЕЕ ЗАДАНИЕ

Цель: самостоятельное углубленное изучение моделей зрелости

Инструмент: любой текстовый редактор, или программы для работы с таблицами

Формат выполнения: doc.google, проверьте настройки доступа к документу, ссылку на работу присылать на pokprobaks@gmail.com

Результат: пощупаете руками модели зрелости

Контекст/описание: сделать сопоставление практик любого поддомена DAF с активностями OWASP SAMM

Сроки выполнения: до 29 августа 2024 включительно

1. OWASP SAMM 2.0.x доступен по [ссылке](#) или можно [загрузить pdf-версию](#).
2. Скачайте [DAF из репозитория](#)
3. Выберите любой поддомен в DAF и найдите (или не найдите) его аналог в SAMM.

Следует отметить, что текущий мэппинг DAF-SAMM может содержать ошибки. Помогите нам их найти!

СПАСИБО ЗА
ВНИМАНИЕ !