2 ИЮНЯ 2026, МОСКВА, ЛОФТ ГОЭЛРО

БЕКОН LUNTRY '26

ЕДИНСТВЕННАЯ КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

Фреймворк JCSF: zero to hero в контейнерах

Дмитрий Селезнев | Инфосистемы Джет

БЕКОН'26

Jet Container Security Framework: from Zero to Hero в контейнерах

Селезнев Дмитрий

Старший инженер DevSecOps, Инфосистемы Джет

О СПИКЕРЕ

СТАРШИЙ ИНЖЕНЕР DEVSECOPS
И, заодно, техлид SecretsManagement и ContainerSecurity решений

АДМИНИСТРАТОР СТЕНДА ПО СРАВНЕНИЮ ВСЕХ РЕШЕНИЙ DSO
Участник комплексных проектов по внедрению/аудиту РБПО и/или СЗСК
Один из контрибьюторов DAF и JCSF

В ИБ – БОЛЕЕ 5 ЛЕТ
Прошел все: от закрытых до облачных систем
Более 2-х лет в K8s

AGENDA

1. Подводные камни масштабирования микросервисов и способы их преодоления
2. Плюсы и минусы существующих подходов к безопасности контейнеров
3. Почему мы решили создать свой фреймворк
4. Из чего состоит фреймворк JCSF, методика оценки
5. Пример использования фреймворка JCSF, получаемые результаты
6. Перспективы развития фреймворка JCSF

КОМУ ПОЛЕЗЕН ДОКЛАД

CTO / TEAM LEAD / TECH LEAD
которые отвечают за архитектурные решения и хотят понять, как стандартизировать подход к безопасности контейнеров на уровне всей команды

DEVOPS / DEVSECOPS / SRE
которые внедряют политики безопасности и хотят заранее выстроить защитные механизмы и централизованный контроль инфраструктуры контейнеров

КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ

	1	2	3	4	5	6
	Initial Access Attacker gains an initial foothold	**Execution** Malicious content is executed	**Privilege Escalation** Attacker gains elevated capabilities	**Discovery** Reconnaissance inside the environment	**Lateral Movement** Move to other parts of the environment	**Impact** Perform malicious activities
SA THEFT **Access to a Pod**	Pod	Compromised Pod uses its ServiceAccount token	Kubernetes API access (with SA permissions)	List resources, secrets, nodes, workloads	Impersonate / create resources / access other namespaces	Data exfiltration, Resource abuse, Persistence

КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ

	1 **Initial Access** Attacker gains an initial foothold	2 **Execution** Malicious content is executed	3 **Privilege Escalation** Attacker gains elevated capabilities	4 **Discovery** Reconnaissance inside the environment	5 **Lateral Movement** Move to other parts of the environment	6 **Impact** Perform malicious activities
SA THEFT Access to a Pod	Pod	Compromised Pod uses its ServiceAccount token	Kubernetes API access (with SA permissions)	List resources, secrets, nodes, workloads	Impersonate / create resources / access other namespaces	Data exfiltration, Resource abuse, Persistence
REACT2SHELL Malicious package in npm registry	npm Repository	Code execution in build/start (via malicious dep)	RCE in container (context of app user)	Enumerate files, configs, secrets	Exploit other services in cluster	Reverse shell, Data exfiltration

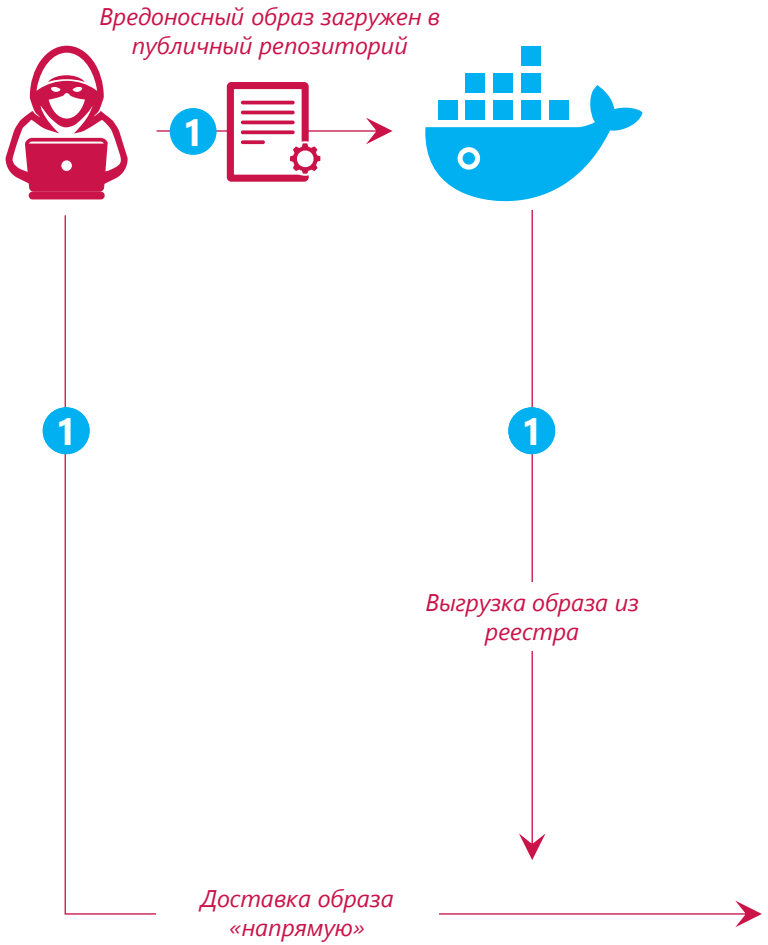
КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ

	1 **Initial Access** Attacker gains an initial foothold	2 **Execution** Malicious content is executed	3 **Privilege Escalation** Attacker gains elevated capabilities	4 **Discovery** Reconnaissance inside the environment	5 **Lateral Movement** Move to other parts of the environment	6 **Impact** Perform malicious activities
SA THEFT Access to a Pod	Pod	Compromised Pod uses its ServiceAccount token	Kubernetes API access (with SA permissions)	List resources, secrets, nodes, workloads	Impersonate / create resources / access other namespaces	Data exfiltration, Resource abuse, Persistence
REACT2SHELL Malicious package in npm registry	npm Repository	Code execution in build/start (via malicious dep)	RCE in container (context of app user)	Enumerate files, configs, secrets	Exploit other services in cluster	Reverse shell, Data exfiltration
LEAKY VESSELS Malicious image in registry	Container Registry	Container Start & script execution	Access to more hosts via Docker API / spread	Scan for exposed APIs / nodes / credentials	Deploy to other nodes via insecure Docker API / new containers	Cryptomining (Deploy XMR miner), DoS, Data exfil

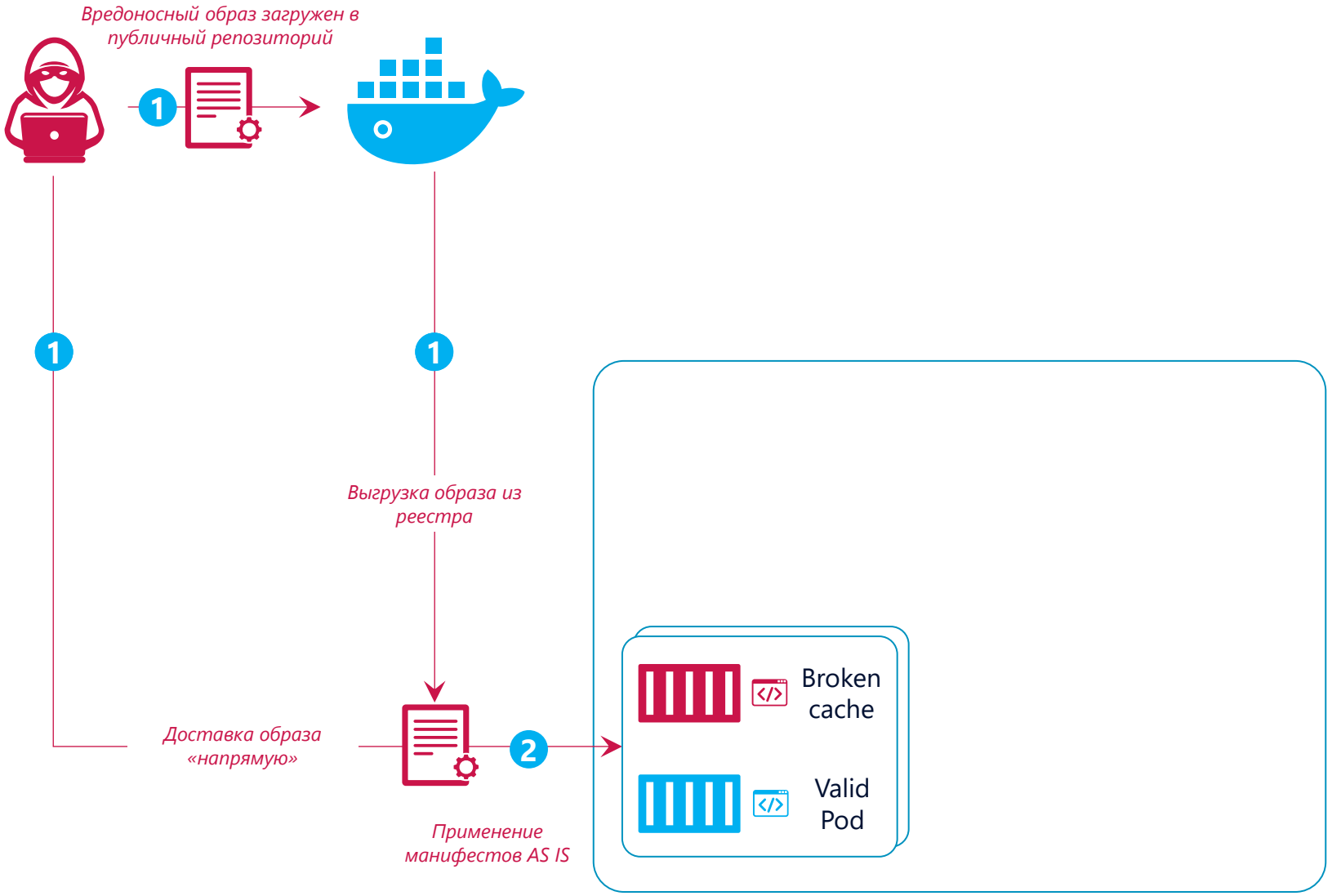
КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ

	1 **Initial Access** Attacker gains an initial foothold	2 **Execution** Malicious content is executed	3 **Privilege Escalation** Attacker gains elevated capabilities	4 **Discovery** Reconnaissance inside the environment	5 **Lateral Movement** Move to other parts of the environment	6 **Impact** Perform malicious activities
SA THEFT Access to a Pod	Pod	Compromised Pod uses its ServiceAccount token	Kubernetes API access (with SA permissions)	List resources, secrets, nodes, workloads	Impersonate / create resources / access other namespaces	Data exfiltration, Resource abuse, Persistence
REACT2SHELL Malicious package in npm registry	npm Repository	Code execution in build/start (via malicious dep)	RCE in container (context of app user)	Enumerate files, configs, secrets	Exploit other services in cluster	Reverse shell, Data exfiltration
LEAKY VESSELS Malicious image in registry	Container Registry	Container Start & script execution	Access to more hosts via Docker API / spread	Scan for exposed APIs / nodes / credentials	Deploy to other nodes via insecure Docker API / new containers	Cryptomining (Deploy XMR miner), DoS, Data exfil
COPY FAIL Broken image in registry	Container Registry	Vulnerable program executes with elevated privileges (copy.fail)	Container -> Host Privilege Escalation (root on host)	Read host files, kernel info, container escape	Move on host pivot to other containers/nodes	Full host compromise, Persistence, Lateral movement

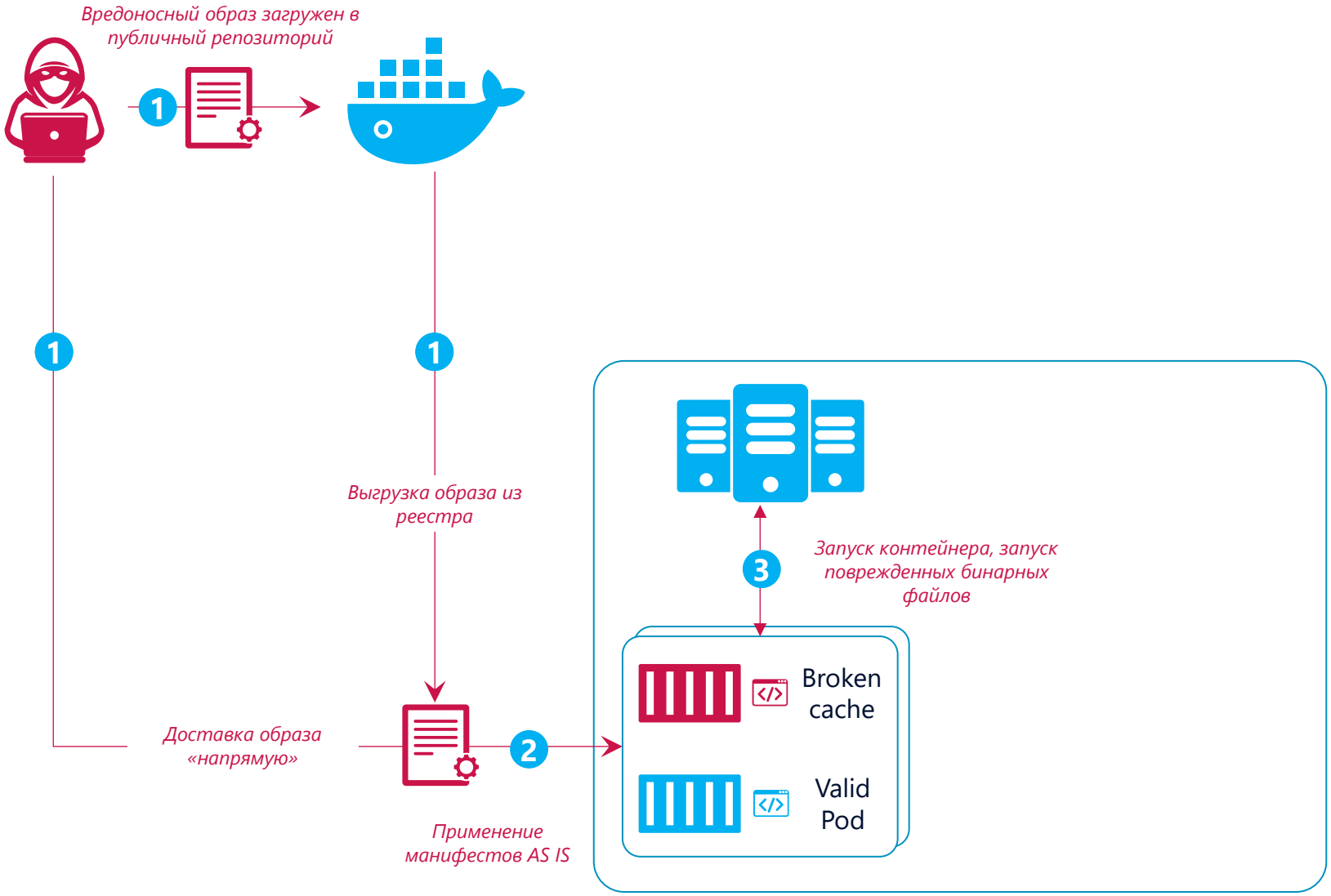
КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ: COPY.FAIL



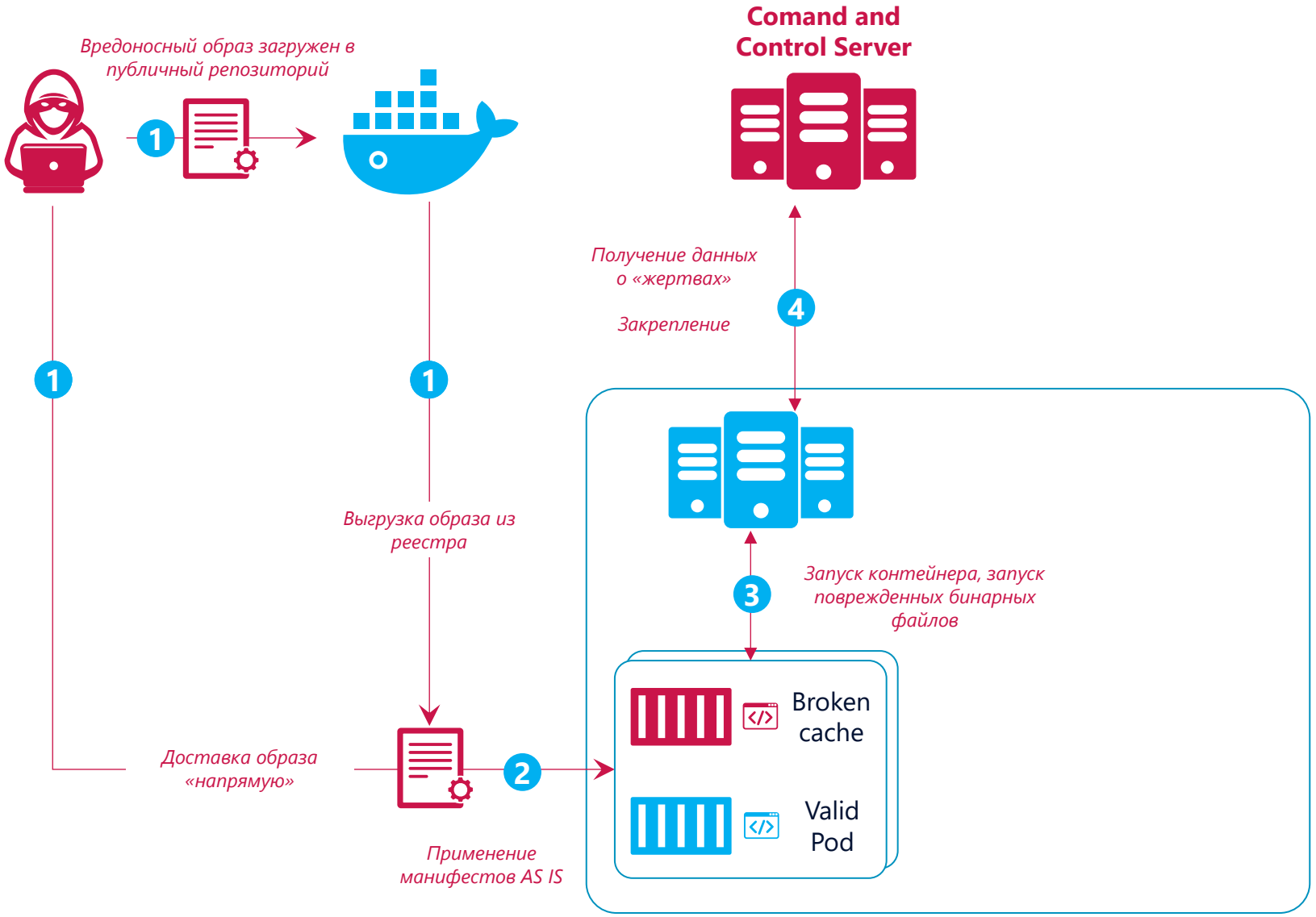
КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ: COPY.FAIL



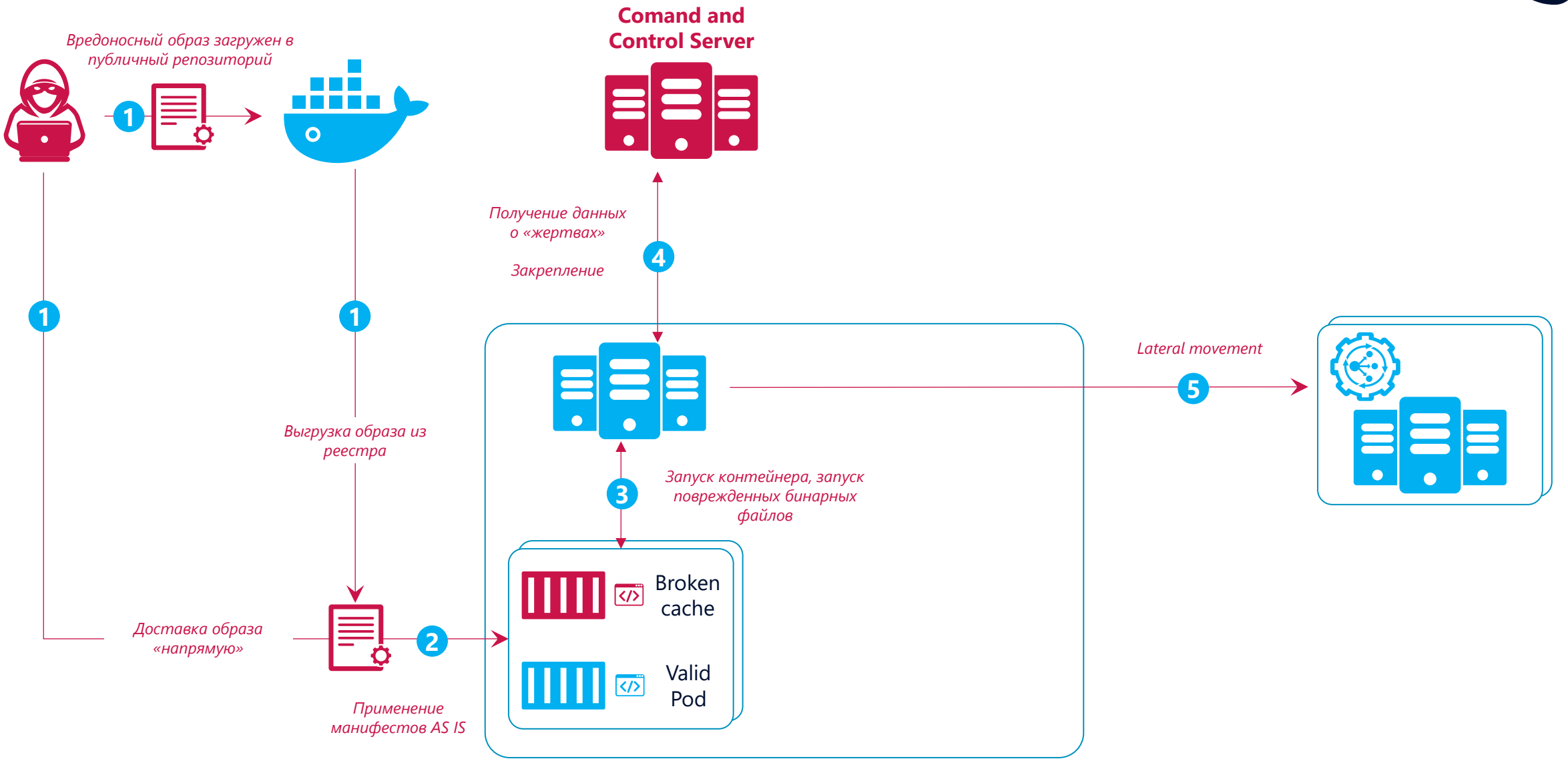
КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ: COPY.FAIL



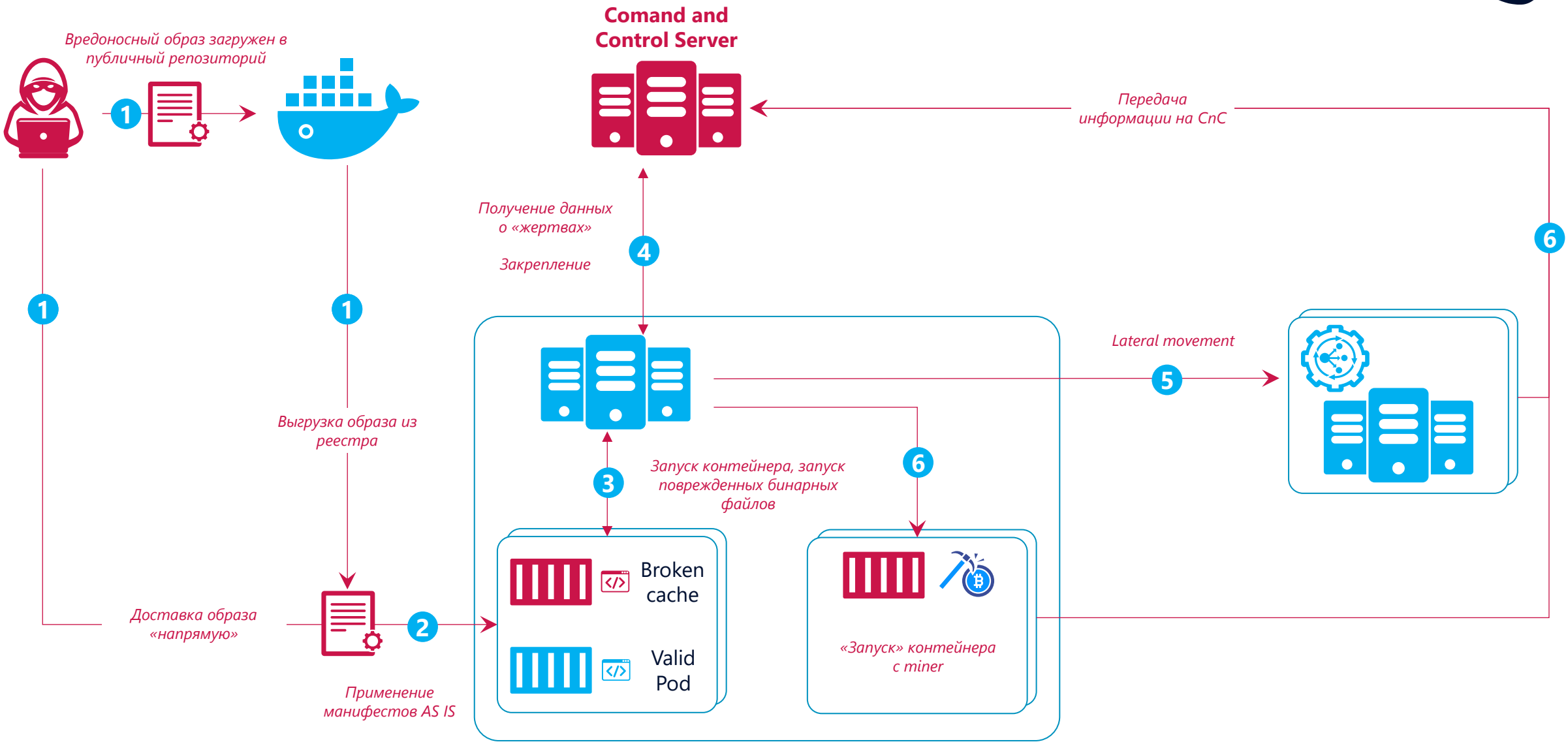
КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ: COPY.FAIL



КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ: COPY.FAIL



КОНТЕЙНЕРИЗАЦИЯ: УГРОЗЫ: COPY.FAIL

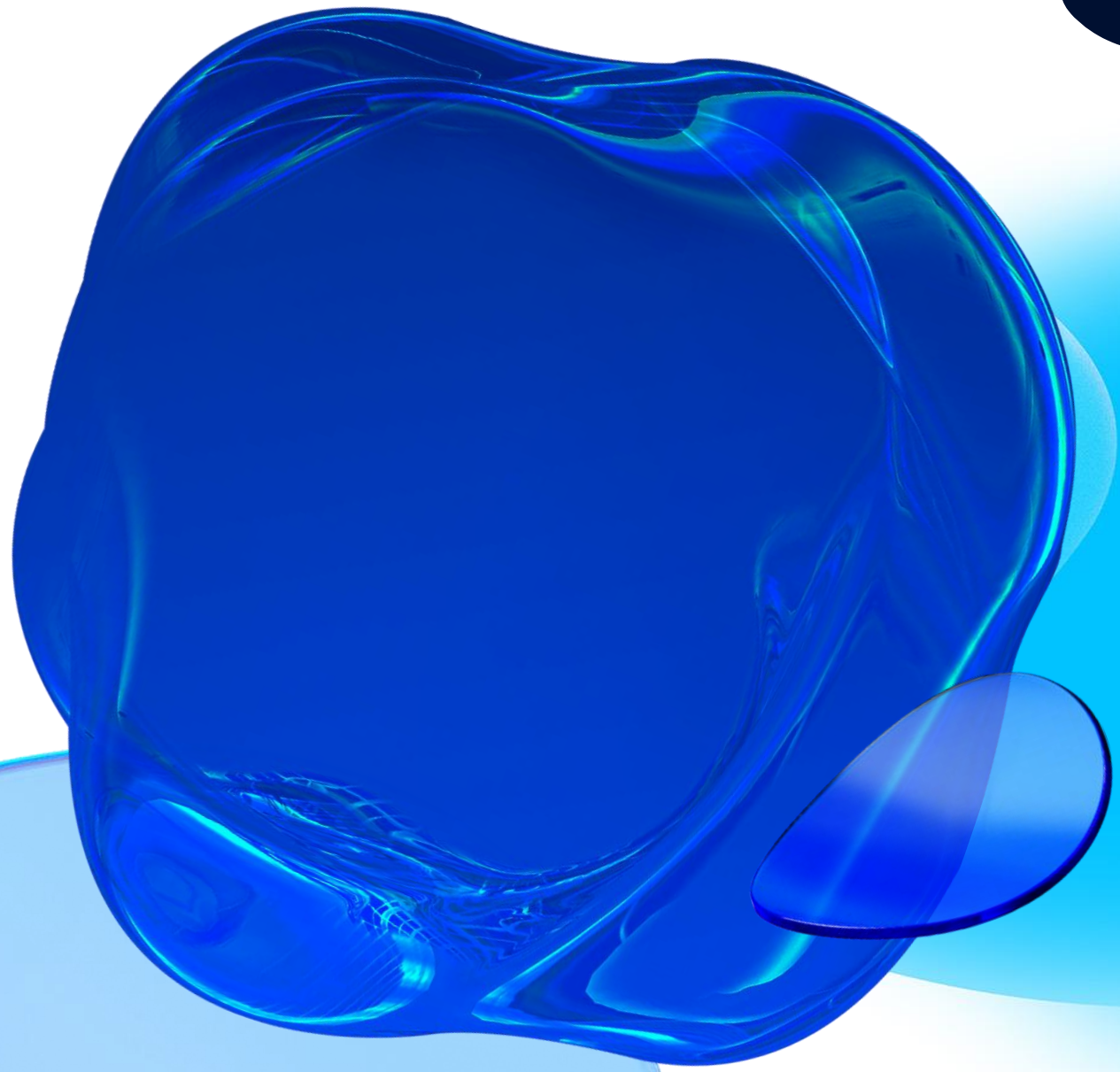


ГЛАВНАЯ ПРОБЛЕМА: С ЧЕГО НАЧАТЬ?

ОТ ПРОБЛЕМ К РЕШЕНИЮ

1. Практики, которые охватывают жизненный цикл контейнеров с детализацией
2. Только актуальные для рынка РФ практики с учетом требований регуляторов
3. Возможность определить текущий уровень зрелости организации и относящиеся к нему практики
4. Максимальная автоматизация процесса оценки
5. Встроенная визуализация результатов для удобства восприятия
6. Инкрементальный подход к уровням зрелости

Сравнение существующих подходов к безопасности контейнеров



СРАВНЕНИЕ СУЩЕСТВУЮЩИХ ПОДХОДОВ

MITRE ATT&CK™

+ Универсальные практики
- Фокус на модели угроз / атакующего
- Неочевидный уровень критичности
- Отсутствует модель зрелости

SLSA

CIS Center for Internet Security®

СРАВНЕНИЕ СУЩЕСТВУЮЩИХ ПОДХОДОВ

MITRE ATT&CK™

+ Универсальные практики
- Фокус на модели угроз / атакующего
- Неочевидный уровень критичности
- Отсутствует модель зрелости

+ Простой и понятный фреймворк
+ Приоритизация критичности
- Фокус только на Kubernetes
- Минимальное количество практик
- Отсутствует модель зрелости

SLSA

CIS Center for Internet Security®

СРАВНЕНИЕ СУЩЕСТВУЮЩИХ ПОДХОДОВ

MITRE ATT&CK™

+ Универсальные практики
- Фокус на модели угроз / атакующего
- Неочевидный уровень критичности
- Отсутствует модель зрелости

TOP 10 RBAC misconfiguration vulnerable components ... kubernetes OWASP

+ Простой и понятный фреймворк
+ Приоритизация критичности
- Фокус только на Kubernetes
- Минимальное количество практик
- Отсутствует модель зрелости

SLSA

+ Наличие модели зрелости
+ Детальные практики «что надо сделать»
- Фокус на цепочке поставок

CIS Center for Internet Security®

СРАВНЕНИЕ СУЩЕСТВУЮЩИХ ПОДХОДОВ

MITRE ATT&CK™

+ Универсальные практики
- Фокус на модели угроз / атакующего
- Неочевидный уровень критичности
- Отсутствует модель зрелости

TOP 10 RBAC misconfiguration vulnerable components ... kubernetes OWASP

+ Простой и понятный фреймворк
+ Приоритизация критичности
- Фокус только на Kubernetes
- Минимальное количество практик
- Отсутствует модель зрелости

SLSA

+ Наличие модели зрелости
+ Детальные практики «что надо сделать»
- Фокус на цепочке поставок

CIS Center for Internet Security®

+ Детальные практики «что надо сделать»
- Фокус на функциональность конкретного ПО
- Нет приоритизации критичности
- Отсутствует модель зрелости

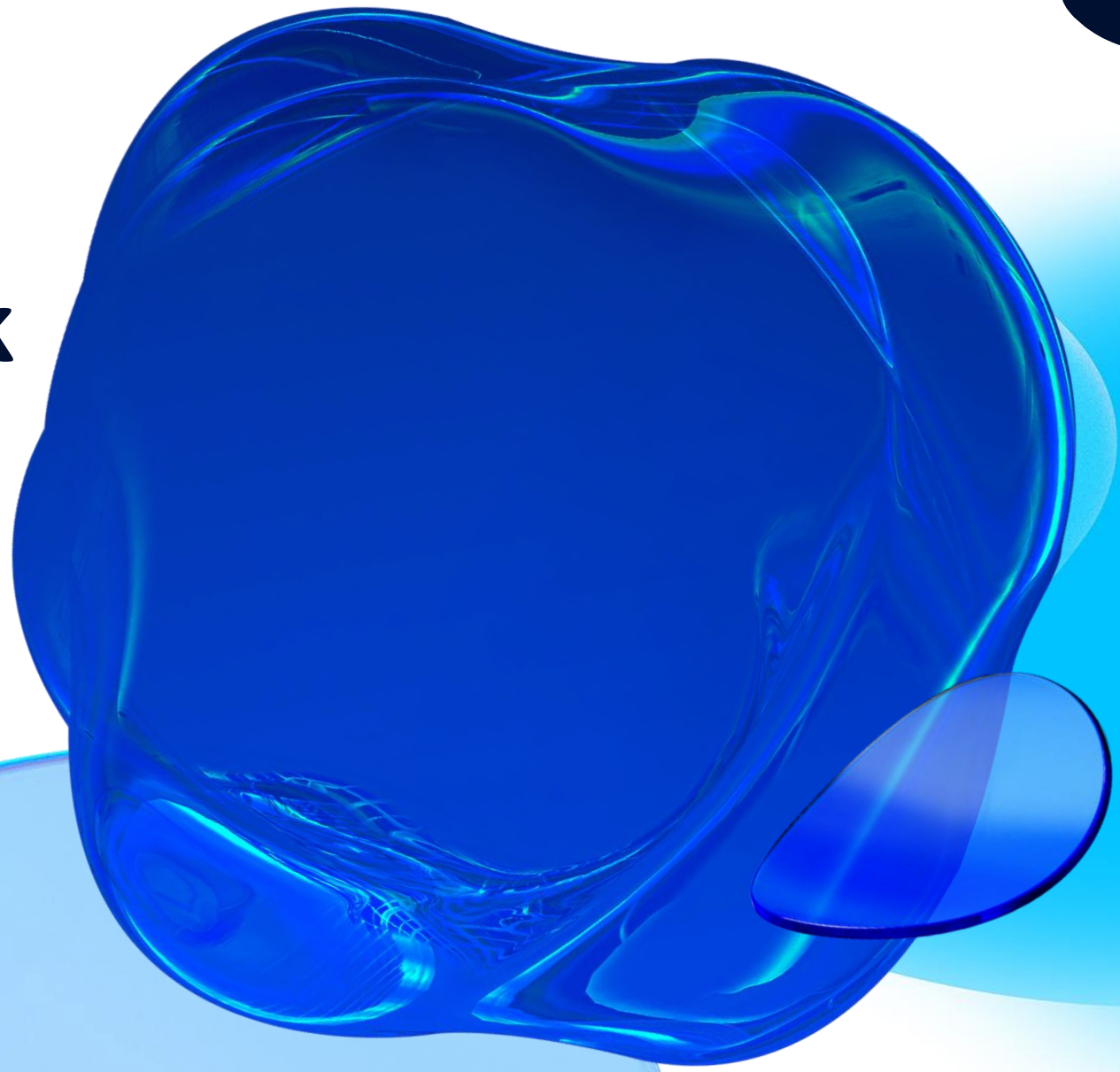
СРАВНЕНИЕ СУЩЕСТВУЮЩИХ ТРЕБОВАНИЙ

ФСТЭК России

- Обязательные к выполнению требования
- Расхождения между БДУ / Пр118 / Пр117
- Неочевидный уровень критичности
- Условная модель зрелости

Jet Container Security Framework

Знакомство



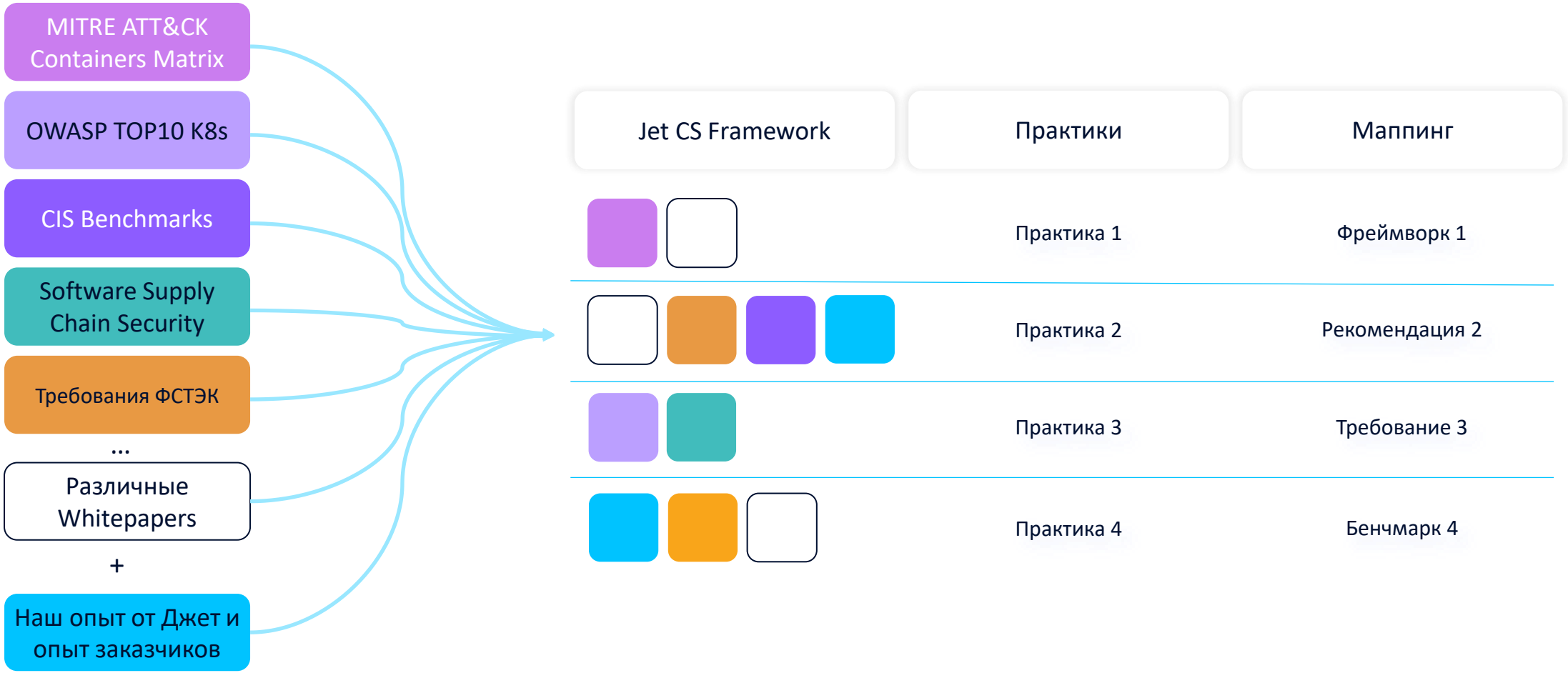
JCSF: РЕШАЕМЫЕ ЗАДАЧИ

- Определение текущего состояния AS IS
- Определение состояния TO BE

JCSF: РЕШАЕМЫЕ ЗАДАЧИ

- Определение текущего состояния AS IS
- Определение инициатив, необходимых для достижения целевого состояния
- Определение состояния TO BE
- Определение вектора развития процесса
- Информация, необходимая для бюджетирования реализации инициатив

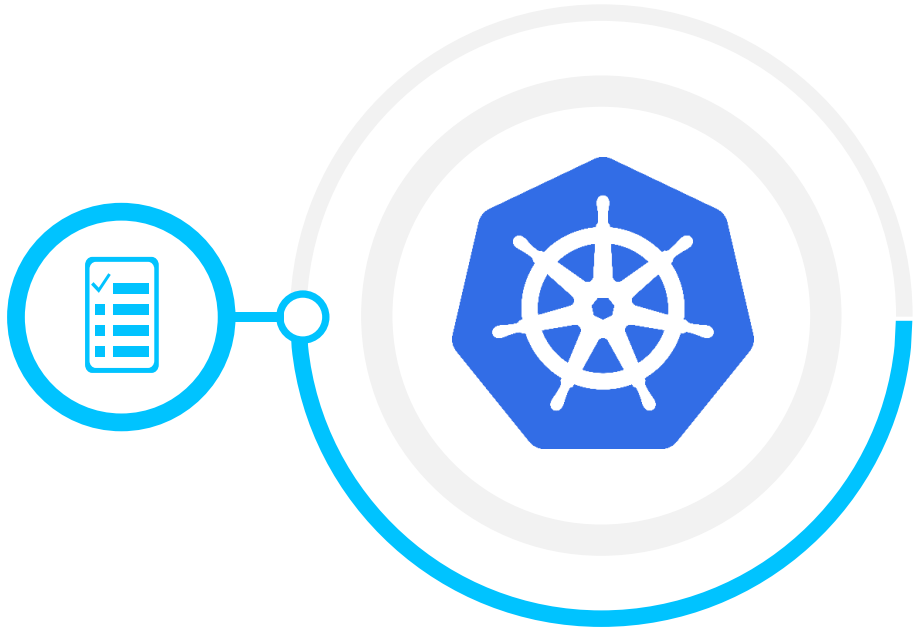
JCSF: ИЗ ЧЕГО СОСТОИТ ФРЕЙМВОРК



JCSF: АБСТРАКЦИИ

BASE 00

Базовые требования
информационной безопасности



JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 00)

Общие требования

ЗАДАЧА РАЗДЕЛА

Интеграция в инфраструктуру

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1 Минимальный	Создаются резервные копии критичных серверов, процесс резервирования является системным	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 00)

Общие требования

ЗАДАЧА РАЗДЕЛА

Интеграция в инфраструктуру

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	**Минимальный**	Создаются резервные копии критичных серверов, процесс резервирования является системным	**Высокая**
2	**Начальный**	Удаленный доступ подрядчиков регламентирован, права минимально необходимы и контролируется	**Высокая**

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 00)

Общие требования

ЗАДАЧА РАЗДЕЛА

Интеграция в инфраструктуру

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	**Минимальный**	Создаются резервные копии критичных серверов, процесс резервирования является системным	**Высокая**
2	**Начальный**	Удаленный доступ подрядчиков регламентирован, права минимально необходимы и контролируется	**Высокая**
3	**Продвинутый**	Тестовая среда располагается в отдельном сетевом сегменте. Доступ к среде ограничен	**Средняя**

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 00)

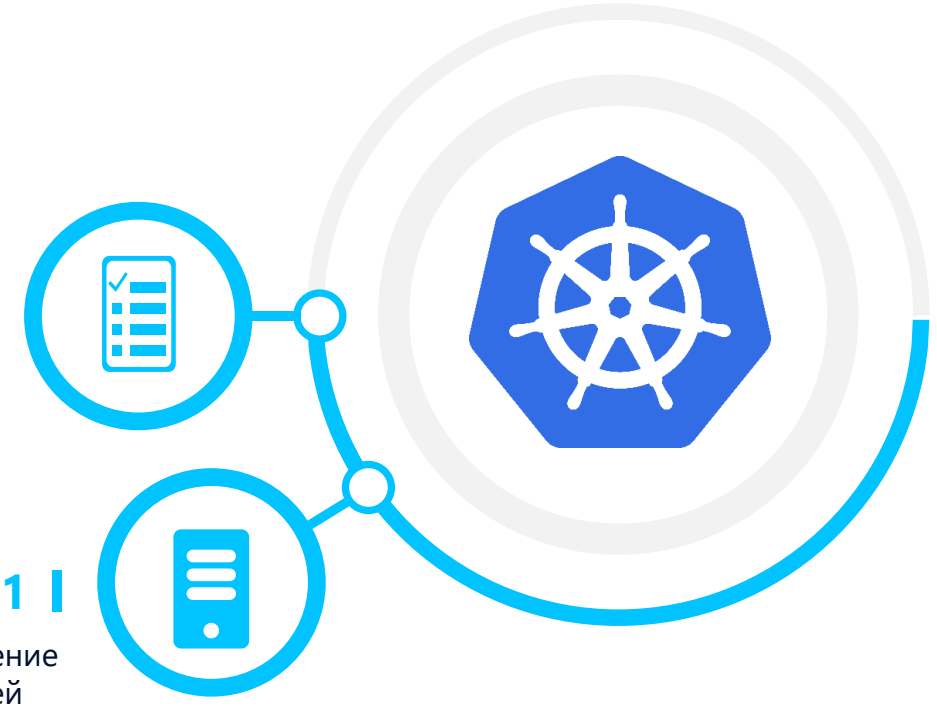
Общие требования

ЗАДАЧА РАЗДЕЛА

Интеграция в инфраструктуру

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ	СТАТУС
1	Минимальный	Создаются резервные копии критичных серверов, процесс резервирования является системным	Высокая	Выполняется
2	Начальный	Удаленный доступ подрядчиков регламентирован, права минимально необходимы и контролируется	Высокая	Не применимо
3	Продвинутый	Тестовая среда располагается в отдельном сетевом сегменте. Доступ к среде ограничен	Средняя	Частично выполняется
4	Экспертный	Обеспечена отказоустойчивость серверной инфраструктуры в рамках нескольких сайтов	Средняя	Не полняется

JCSF: АБСТРАКЦИИ



BASE 00

Базовые требования информационной безопасности

NODES 01

Защита узлов кластера – управление уязвимостями и конфигурацией

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 01)

Безопасность Узлов

ЗАДАЧА РАЗДЕЛА

Защита узлов среды контейнеризации

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1 Минимальный	УЗ root не должна использоваться для администрирования ОС	Средняя

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 01)

Безопасность Узлов

ЗАДАЧА РАЗДЕЛА

Защита узлов среды контейнеризации

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	Минимальный	УЗ root не должна использоваться для администрирования ОС	Средняя
2	Начальный	Проводятся периодические сканирования ОС, направленные на выявление уязвимостей	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 01)

Безопасность Узлов

ЗАДАЧА РАЗДЕЛА

Защита узлов среды контейнеризации

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	**Минимальный**	УЗ root не должна использоваться для администрирования ОС	**Средняя**
2	**Начальный**	Проводятся периодические сканирования ОС, направленные на выявление уязвимостей	**Высокая**
3	**Продвинутый**	Проводятся на регулярной основе внутренние аудиты ИБ конфигурационных настроек ОС	**Высокая**

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 01)

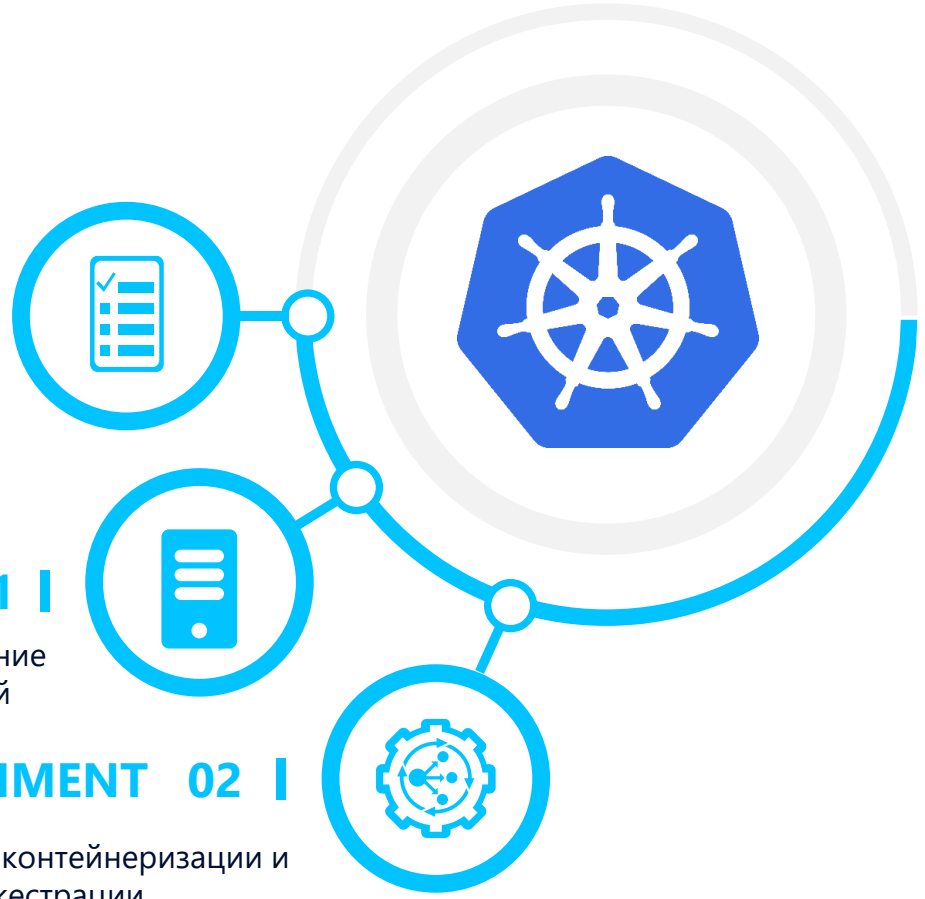
Безопасность Узлов

ЗАДАЧА РАЗДЕЛА

Защита узлов среды контейнеризации

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ	СТАТУС
1 Минимальный	УЗ root не должна использоваться для администрирования ОС	Средняя	Частично выполняется
2 Начальный	Проводятся периодические сканирования ОС, направленные на выявление уязвимостей	Высокая	Выполняется
3 Продвинутый	Проводятся на регулярной основе внутренние аудиты ИБ конфигурационных настроек ОС	Высокая	Частично выполняется
4 Экспертный	Применяется шифрование диска	Низкая	Не выполняется

JCSF: АБСТРАКЦИИ



BASE 00

Базовые требования информационной безопасности

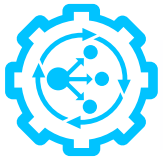
NODES 01

Защита узлов кластера – управление уязвимостями и конфигурацией

ENVIRONMENT 02

Защита сред контейнеризации и оркестрации

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 02)



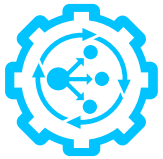
Безопасность Платформы

ЗАДАЧА РАЗДЕЛА

Защита среды контейнеризации

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1 Минимальный	• Read-only доступ к kubelet не используется • Определена единая cgroup (control group) по умолчанию для всех контейнеров	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 02)



Безопасность Платформы

ЗАДАЧА РАЗДЕЛА

Защита среды контейнеризации

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	Минимальный	• Read-only доступ к kubelet не используется • Определена единая cgroup (control group) по умолчанию для всех контейнеров	Высокая
2	Начальный	Используются Policy engine или Admission controller, позволяющие контролировать конфигурацию запускаемых микросервисов	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 02)

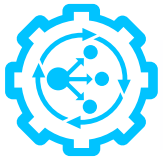
Безопасность Платформы

ЗАДАЧА РАЗДЕЛА

Защита среды контейнеризации

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1 Минимальный	• Read-only доступ к kubelet не используется • Определена единая cgroup (control group) по умолчанию для всех контейнеров	Высокая
2 Начальный	Используются Policy engine или Admission controller, позволяющие контролировать конфигурацию запускаемых микросервисов	Высокая
3 Продвинутый	Используются отдельные решения по хранению секретов	Средняя

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 02)



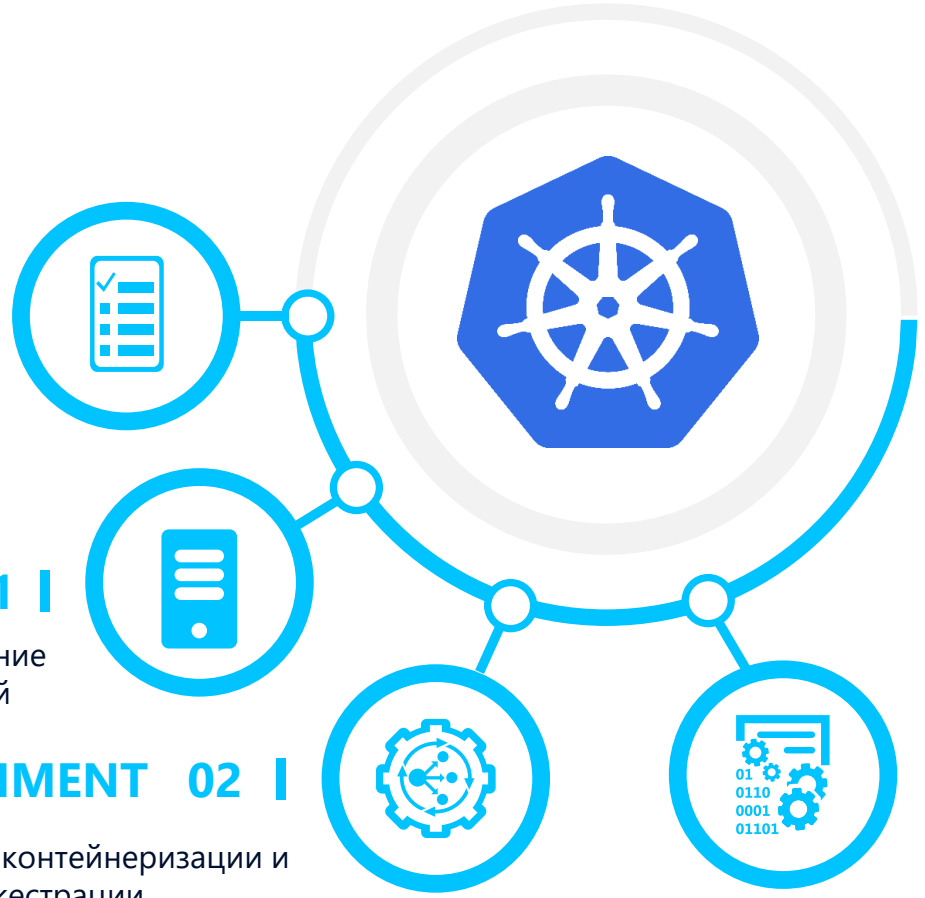
Безопасность Платформы

ЗАДАЧА РАЗДЕЛА

Защита среды контейнеризации

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ	СТАТУС
1 Минимальный	• Read-only доступ к kubelet не используется • Определена единая cgroup (control group) по умолчанию для всех контейнеров	Высокая	Выполняется
2 Начальный	Используются Policy engine или Admission controller, позволяющие контролировать конфигурацию запускаемых микросервисов	Высокая	Не выполняется
3 Продвинутый	Используются отдельные решения по хранению секретов	Средняя	Частично выполняется
4 Экспертный	При хранении настроек и развертывании оркестратора используется подход IaC	Средняя	Выполняется

КОНТЕЙНЕРИЗАЦИЯ: АБСТРАКЦИИ



BASE 00

Базовые требования информационной безопасности

NODES 01

Защита узлов кластера – управление уязвимостями и конфигурацией

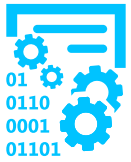
ENVIRONMENT 02

Защита сред контейнеризации и оркестрации

03 IMAGE

Контроль создания, хранения и использования образов контейнеров

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 03)



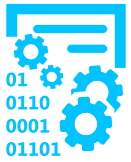
Безопасность Образов

ЗАДАЧА РАЗДЕЛА

Использование безопасных образов контейнеров

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1 Минимальный	Контейнеры запускаются из образов, хранящихся в локальных репозиториях	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 03)



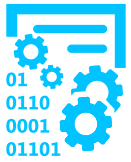
Безопасность Образов

ЗАДАЧА РАЗДЕЛА

Использование безопасных образов контейнеров

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	Минимальный	Контейнеры запускаются из образов, хранящихся в локальных репозиториях	Высокая
2	Начальный	Образы контейнеров не должны содержать уязвимостей, которые возможно проэксплуатировать	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 03)



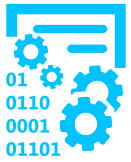
Безопасность Образов

ЗАДАЧА РАЗДЕЛА

Использование безопасных образов контейнеров

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	**Минимальный**	Контейнеры запускаются из образов, хранящихся в локальных репозиториях	**Высокая**
2	**Начальный**	Образы контейнеров не должны содержать уязвимостей, которые возможно проэксплуатировать	**Высокая**
3	**Продвинутый**	Собираемые образы подписываются электронной подписью при сборке, а также осуществляется их проверка	**Средняя**

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 03)



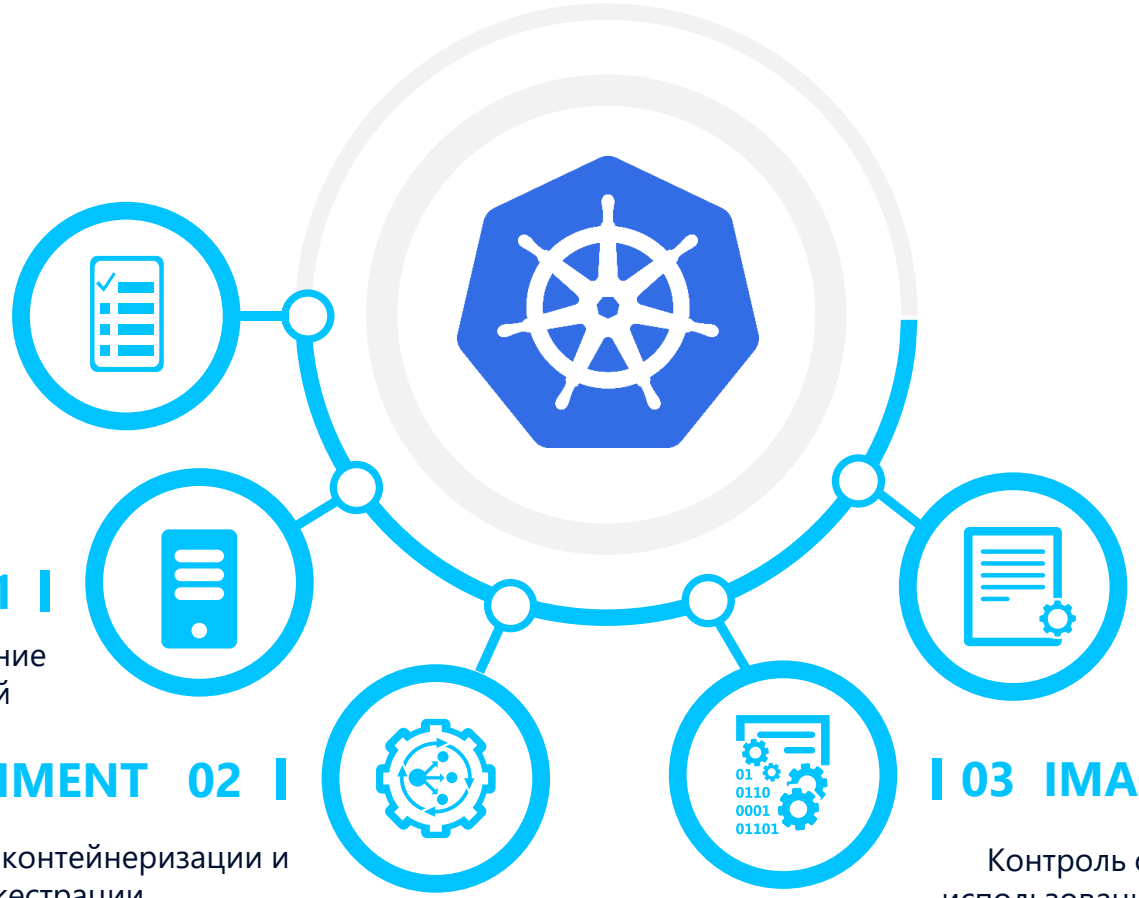
Безопасность Образов

ЗАДАЧА РАЗДЕЛА

Использование безопасных образов контейнеров

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ	СТАТУС
1	Минимальный	Контейнеры запускаются из образов, хранящихся в локальных репозиториях	Высокая	Не выполняется
2	Начальный	Образы контейнеров не должны содержать уязвимостей, которые возможно проэксплуатировать	Высокая	Не выполняется
3	Продвинутый	Собираемые образы подписываются электронной подписью при сборке, а также осуществляется их проверка	Средняя	Не выполняется
4	Экспертный	Должны использоваться образы, содержащие минимальную функциональность (distroless)	Высокая	Частично выполняется

КОНТЕЙНЕРИЗАЦИЯ: АБСТРАКЦИИ



BASE 00

Базовые требования информационной безопасности

NODES 01

Защита узлов кластера – управление уязвимостями и конфигурацией

ENVIRONMENT 02

Защита сред контейнеризации и оркестрации

03 IMAGE

Контроль создания, хранения и использования образов контейнеров

04 MANIFEST

Контроль написания и использования манифестов приложений

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 04)

Безопасность Манифестов

ЗАДАЧА РАЗДЕЛА

Контроль написания и применения манифестов

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1 Минимальный	В манифестах не используются секреты в открытом виде	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 04)

Безопасность Манифестов

ЗАДАЧА РАЗДЕЛА

Контроль написания и применения манифестов

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	Минимальный	В манифестах не используются секреты в открытом виде	Высокая
2	Начальный	В манифестах настроены ограничения ресурсов для контейнеров	Средняя

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 04)

Безопасность Манифестов

ЗАДАЧА РАЗДЕЛА

Контроль написания и применения манифестов

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	Минимальный	В манифестах не используются секреты в открытом виде	Высокая
2	Начальный	В манифестах настроены ограничения ресурсов для контейнеров	Средняя
3	Продвинутый	Осуществляется контроль за выполнением команд внутри контейнера от пользователя root	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 04)

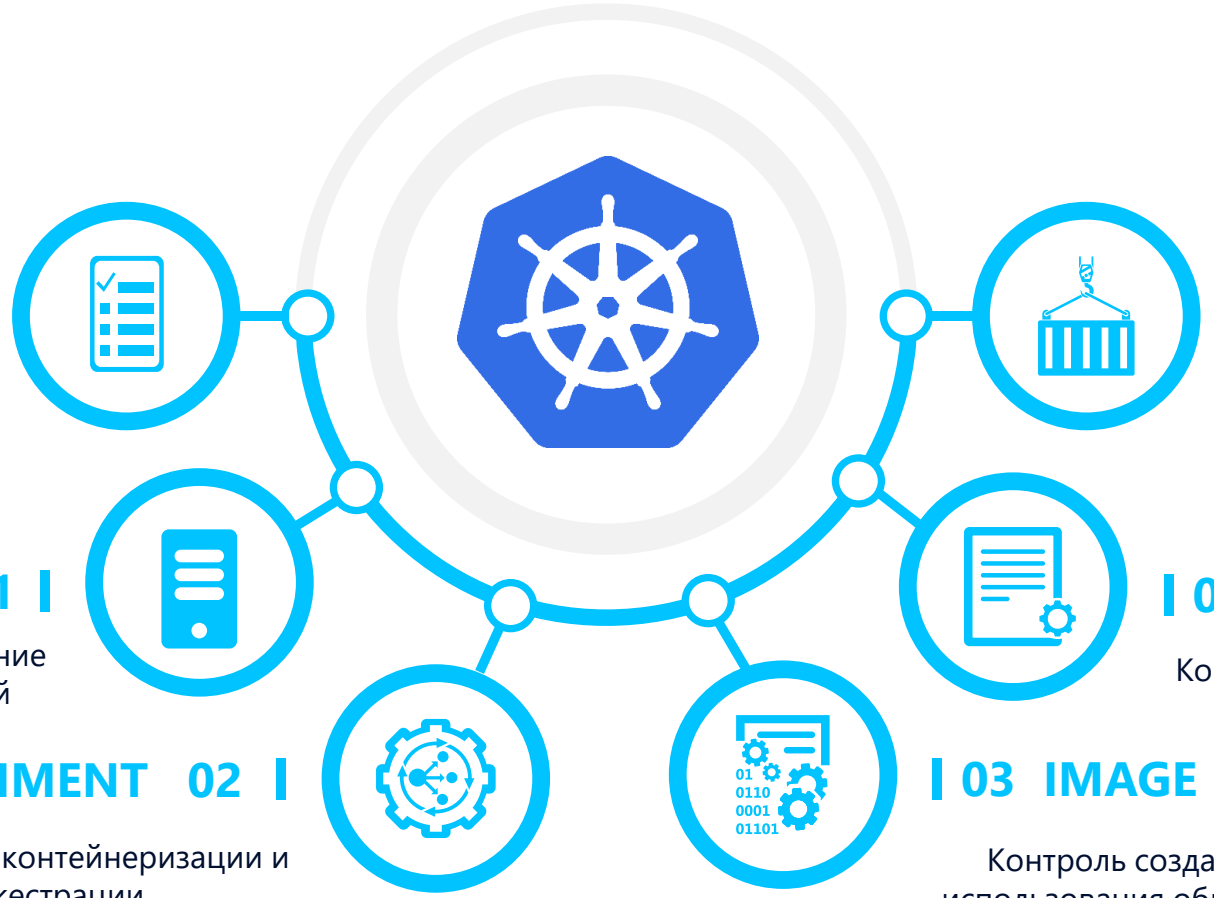
Безопасность Манифестов

ЗАДАЧА РАЗДЕЛА

Контроль написания и применения манифестов

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ	СТАТУС
1	Минимальный	В манифестах не используются секреты в открытом виде	Высокая	Не выполняется
2	Начальный	В манифестах настроены ограничения ресурсов для контейнеров	Средняя	Выполняется
3	Продвинутый	Осуществляется контроль за выполнением команд внутри контейнера от пользователя root	Высокая	Частично выполняется
4	Экспертный	Для групп контейнеров используются отдельные AppArmor-профили	Средняя	Не выполняется

КОНТЕЙНЕРИЗАЦИЯ: АБСТРАКЦИИ



BASE 00

Базовые требования информационной безопасности

NODES 01

Защита узлов кластера – управление уязвимостями и конфигурацией

ENVIRONMENT 02

Защита сред контейнеризации и оркестрации

03 IMAGE

Контроль создания, хранения и использования образов контейнеров

04 MANIFEST

Контроль написания и использования манифестов приложений

05 CONTAINER

Контроль активности контейнера в режиме runtime

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 05)

Безопасность Среды выполнения

ЗАДАЧА РАЗДЕЛА

Защита запущенных контейнеров

УРОВЕНЬ	ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1 Минимальный	В контейнерах не запущен демон sshd	Высокая

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 05)

Безопасность Среды выполнения

ЗАДАЧА РАЗДЕЛА

Защита запущенных контейнеров

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	**Минимальный**	В контейнерах не запущен демон sshd	**Высокая**
2	**Начальный**	Настроены и используются сетевые политики в режиме мониторинга	**Средняя**

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 05)

Безопасность Среды выполнения

ЗАДАЧА РАЗДЕЛА

Защита запущенных контейнеров

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ
1	**Минимальный**	В контейнерах не запущен демон sshd	**Высокая**
2	**Начальный**	Настроены и используются сетевые политики в режиме мониторинга	**Средняя**
3	**Продвинутый**	Используется мониторинг аномалий для запущенных контейнеров	**Средняя**

JCSF: ДЕТАЛИЗАЦИЯ (ДОМЕН 05)

Безопасность Среды выполнения

ЗАДАЧА РАЗДЕЛА

Защита запущенных контейнеров

УРОВЕНЬ		ПРИМЕРЫ ПРАКТИК	КРИТИЧНОСТЬ	СТАТУС
1	Минимальный	В контейнерах не запущен демон sshd	Высокая	Частично выполняется
2	Начальный	Настроены и используются сетевые политики в режиме мониторинга	Средняя	Не выполняется
3	Продвинутый	Используется мониторинг аномалий для запущенных контейнеров	Средняя	Не выполняется
4	Экспертный	Настроены и используются кастомизированные Runtime политики в режиме блокирования	Средняя	Не выполняется

Что получилось?

ID практики	Требование	Уровень зрелости	Статус	Соответствие уровню зрелости	Классификация	Уровень критичности	Вес критерия	Выполняется	Итоговый балл	CIS Kubernetes	CIS Docker	CIS Linux (Debian)	CIS Linux (RHEL)	118 Приказ	УБИ ФСТЭК	Примечание
Dock-4-6	В кластере SWARM используется режим auto-lock. Для запуска узлов необходимо ввести ключ разблокировки доступа к ключам шифрования	4	Не заполнено		Харденинг	Низкий	1	0	0	-	7.5	-	-			docker info --format 'Swarm Autolock: {{ .Swarm.Cluster.Spec.EncryptionConfig.AutoLockManagers }}'
Dock-4-7	Для ключей разблокировки режима auto-lock используется ротация	4	Не заполнено		Харденинг	Низкий	1	0	0	-	7.6	-	-			Docker SWARM Процессный контроль. Выясняется в процессе интервью
						Максимальный балл	**143**	**Итоговый общий балл**	**0**							
Безопасность используемых образов (Images)																
IMG-1-1	В собранных образах не должны храниться секреты	1	Не заполнено		Защита секретов	Высокий	5	0	0	-	4.10	-	-		УБИ.226	trivy trufflehog
IMG-1-2	Контейнеры запускаются из образов, хранящихся в локальных репозиториях	1	Не заполнено	0%	Контроль репозиториев	Высокий	5	0	0	5.5.1	4.2	-	-		УБИ.224 УБИ.226 УБИ.227	Полностью выполняется, если настроена политика, контролирующая корректность конфигурации. Если выполняется для всех образов контейнеров, но не настроена контролирующая политика - частично выполняется (0.5 балла)
IMG-1-3	Выполняется сканирование образов контейнеров. Запуск сканирования происходит в ручном режиме.				Сканирование образов						4.4	-	-		УБИ.225 УБИ.226 УБИ.227	
IMG-1-4	Осуществляется мультиуровневая сборка для минимизации размера образа и его функционала										4.3; 4.7; 4.9; 4.11	-	-			
IMG-1-5	Осуществляется сканирование Docker файлов на недостатки конфигурации ИБ										4.4	-	-		УБИ.223 УБИ.226	
IMG-2-1	Образы контейнеров не должны содержать уязвимостей, которые возможно проэксплуатировать										4.4; 4.11	-	-	10.1	УБИ.225 УБИ.226	
IMG-2-2	Выполняется сканирование образов контейнеров в CI/CD на наличие уязвимостей										4.4	-	-	10.1	УБИ.226	trivy
IMG-2-3	При обнаружении дефектов ИБ в образах контейнеров автоматизированно создаются задачи на их устранение в тикет-системе										-	-	-			
IMG-3-1	Для собираемых образов генерируется SBOM										-	-	-		УБИ.226	trivy syft cdxgen
IMG-3-2	На образы регулярно устанавливаются обновления (обновляются базовые образы)	3	Не заполнено	0%	Обновление ПО	Высокий	5	0	0	-	4.4; 4.7	-	-	10.1	УБИ.226	
IMG-3-3	Собираемые образы подписываются электронной подписью при сборке, а также осуществляется их проверка	3	Не заполнено		Харденинг	Средний	3	0	0	5.5.1	4.5; 4.12	-	-	12.1 13.2	УБИ.224 УБИ.227	Cosign В случае, если запуск контейнера из некорректно подписанного образа блокируется на уровне оркестратора - контроль выполняется полностью. Если осуществляется проверка без блокировки - данный контроль выполняется частично (0.5 балла)
IMG-3-4	Выполняется периодическое сканирование образов контейнеров, размещенных во внутренних репозиториях, на наличие уязвимостей	3	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	4.4	-	-	10.2 13.2	УБИ.227	
IMG-4-1	Должны использоваться образы, содержащие минимальный функционал (distroless)	4	Не заполнено	0%	Харденинг	Высокий	5	0	0	-	4.3; 4.8	-	-		УБИ.223 УБИ.226	
IMG-4-2	Сборки в CI/CD блокируются при найденных уязвимостях в образах контейнеров по договоренности между ИБ и разработчиками	4	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	-	-	-	10.2	УБИ.227	
						Максимальный балл	**60**	**Итоговый общий балл**	**0**							
Безопасность манифестов (Manifests)																
MAN-1-1	В манифестах не используются секреты в открытом виде	1	Не заполнено		Защита секретов	Высокий	5	0	0	5.1.2; 5.4.1	4.10	-	-		УБИ.223 УБИ.224	Полностью выполняется, если используется инструмент контроля. Иначе - частично выполняется (0.5 балла)
																Полностью выполняется, если применимо как для манифестов, так и настроена политика

1 Практики, которые охватывают жизненный цикл контейнеров с детализацией

Что получилось?

ID практики	Требование	Уровень зрелости	Статус	Соответствие уровню зрелости	Классификация	Уровень критичности	Вес критерия	Выполняется	Итоговый балл	CIS Kubernetes	CIS Docker	CIS Linux (Debian)	CIS Linux (RHEL)	118 Приказ	УБИ ФСТЭК	Примечание
Dock-4-6	В кластере SWARM используется режим auto-lock. Для запуска узлов необходимо ввести ключ разблокировки доступа к ключам шифрования	4	Не заполнено		Харденинг	Низкий	1	0	0	-	7.5	-	-			ocker info --format 'Swarm Autolock: {{ warm.Cluster.Spec.EncryptionConfig.AutoLock anagers }}'
Dock-4-7	Для ключей разблокировки режима auto-lock используется ротация	4	Не заполнено		Харденинг	Низкий	1	0	0	-	7.6	-	-			ocker SWARM роцессный контроль. Выясняется в процессе нтервью
						Максимальный балл	143	Итоговый общий балл	0							
Безопасность используемых образов (Images)																
IMG-1-1	В собранных образах не должны храниться секреты	1	Не заполнено		Защита секретов	Высокий	5	0	0	-	4.10	-	-		УБИ.226	ivy ufflehog
IMG-1-2	Контейнеры запускаются из образов, хранящихся в локальных репозиториях	1	Не заполнено	0%	Контроль репозиториев	Высокий	5	0	0	5.5.1	4.2	-	-		УБИ.224 УБИ.226 УБИ.227	олностью выполняется, если настроена олитика, контролирующая корректность онфигурации. Если выполняется для всех разов контейнеров, но не настроена онтролирующая политика - частично ыполняется (0.5 балла)
IMG-1-3	Выполняется сканирование образов контейнеров. Запуск сканирования происходит в ручном режиме.	1	Не заполнено		Сканирование образов	Высокий	5	0	0	-	4.4	-	-		УБИ.225 УБИ.226 УБИ.227	
IMG-1-4	Осуществляется мультиуровневая сборка для минимизации размера образа и его функционала	1	Не заполнено		Харденинг	Средний	3	0	0	-	4.3; 4.7; 4.9; 4.11	-	-			
IMG-1-5	Осуществляется сканирование Docker файлов на недостатки конфигурации ИБ	1	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	4.4	-	-		УБИ.223 УБИ.226	
IMG-2-1	Образы контейнеров не должны содержать уязвимостей, которые возможно проэксплуатировать	2	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	4.4; 4.11	-	-	10.1	УБИ.225 УБИ.226	
IMG-2-2	Выполняется сканирование образов контейнеров в CI/CD на наличие уязвимостей	2	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	4.4	-	-	10.1	УБИ.226	ivy
IMG-2-3	При обнаружении дефектов ИБ в образах контейнеров автоматизированно создаются задачи на их устранение в тикет-системе	2	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	-	-	-			
IMG-3-1	Для собираемых образов генерируется SBOM	3	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	-	-	-		УБИ.226	ivy ft xgen
IMG-3-2	На образы регулярно устанавливаются обновления (обновляются базовые образы)	3	Не заполнено		Обновление ПО	Высокий	5	0	0	-	4.4; 4.7	-	-	10.1	УБИ.226	
IMG-3-3	Собираемые образы подписываются электронной подписью при сборке, а также осуществляется их проверка	3	Не заполнено	0%	Харденинг	Средний	3	0	0	5.5.1	4.5; 4.12	-	-	12.1 13.2	УБИ.224 УБИ.227	osign случае, если запуск контейнера из корректно подписанного образа локируется на уровне оркестратора - онтроль выполняется полностью. Если уществляется проверка без блокировки - анный контроль выполняется частично (0.5 алла)
IMG-3-4	Выполняется периодическое сканирование образов контейнеров, размещенных во внутренних репозиториях, на наличие уязвимостей	3	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	4.4	-	-	10.2 13.2	УБИ.227	
IMG-4-1	Должны использоваться образы, содержащие минимальный функционал (distroless)	4	Не заполнено	0%	Харденинг	Высокий	5	0	0	-	4.3; 4.8	-	-		УБИ.223 УБИ.226	
IMG-4-2	Сборки в CI/CD блокируются при найденных уязвимостях в образах контейнеров по договоренности между ИБ и разработчиками	4	Не заполнено		Сканирование образов контейнеров	Средний	3	0	0	-	-	-	-	10.2	УБИ.227	
						Максимальный балл	60	Итоговый общий балл	0							
Безопасность манифестов (Manifests)																
MAN-1-1	В манифестах не используются секреты в открытом виде	1	Не заполнено		Защита секретов	Высокий	5	0	0	5.1.2; 5.4.1	4.10	-	-		УБИ.223 УБИ.224	олностью выполняется, если используется струмент контроля. Иначе - частично ыполняется (0.5 балла)
																олностью выполняется, если применимо как я манифестов, так и настроена политика

2

Только актуальные для рынка РФ практики с учетом требований регуляторов

Что получилось?

ID практики	Требование	Уровень зрелости	Статус	Соответствие уровню зрелости	Классификация	Уровень критичности	Вес критерия	Выполняется	Итоговый балл	CIS Kubernetes	CIS Docker	CIS Linux (Debian)	CIS Linux (RHEL)	118 Приказ	УБИ ФСТЭК	Примечание
Dock-4-6	В кластере SWARM используется режим auto-lock. Для запуска узлов необходимо ввести ключ разблокировки доступа к ключам шифрования	4	Не заполнено		Харденинг	Низкий	1	0	0	-	7.5	-	-			docker info --format 'Swarm Autolock: {{ .Swarm.Cluster.Spec.EncryptionConfig.AutoLockManagers }}'
Dock-4-7	Для ключей разблокировки режима auto-lock используется ротация	4	Не заполнено		Харденинг	Низкий	1	0	0	-	7.6	-	-			Docker SWARM Процессный контроль. Выясняется в процессе интервью
						Максимальный балл	143	Итоговый общий балл	0							
Безопасность используемых образов (Images)																
IMG-1-1	В собранных образах не должны храниться секреты	1	Не заполнено		Защита секретов	Высокий	5	0	0	-	4.10	-	-		УБИ.226	trivy trufflehog
IMG-1-2	Контейнеры запускаются из образов, хранящихся в локальных репозиториях	1	Не заполнено	0%	Контроль репозиториев	Высокий	5	0	0	5.5.1	4.2	-	-		УБИ.224 УБИ.226 УБИ.227	Полностью выполняется, если настроена политика, контролирующая корректность конфигурации. Если выполняется для всех образов контейнеров, но не настроена контролирующая политика - частично выполняется (0.5 балла)
IMG-1-3	Выполняется сканирование образов контейнеров. Запуск сканирования происходит в ручном режиме.				анирование образов						4.4	-	-		УБИ.225 УБИ.226 УБИ.227	
IMG-1-4	Осуществляется мультиуровневая сборка для минимизации размера образа и его функционала										4.3; 4.7; 4.9; 4.11	-	-			
IMG-1-5	Осуществляется сканирование Docker файлов на недостатки конфигурации ИБ										4.4	-	-		УБИ.223 УБИ.226	
IMG-2-1	Образы контейнеров не должны содержать уязвимостей, которые возможно проэксплуатировать										4.4; 4.11	-	-	10.1	УБИ.225 УБИ.226	
IMG-2-2	Выполняется сканирование образов контейнеров в CI/CD на наличие уязвимостей										4.4	-	-	10.1	УБИ.226	trivy
IMG-2-3	При обнаружении дефектов ИБ в образах контейнеров автоматизированно создаются задачи на их устранение в тикет-системе										-	-	-			
IMG-3-1	Для собираемых образов генерируется SBOM										-	-	-		УБИ.226	trivy syft cdxgen
IMG-3-2	На образы регулярно устанавливаются обновления (обновляются базовые образы)	3	Не заполнено		Обновление ПО	Высокий	5	0	0	-	4.4; 4.7	-	-	10.1	УБИ.226	
IMG-3-3	Собираемые образы подписываются электронной подписью при сборке, а также осуществляется их проверка	3	Не заполнено	0%	Харденинг	Средний	3	0	0	5.5.1	4.5; 4.12	-	-	12.1 13.2	УБИ.224 УБИ.227	Cosign В случае, если запуск контейнера из некорректно подписанного образа блокируется на уровне оркестратора - контроль выполняется полностью. Если осуществляется проверка без блокировки - данный контроль выполняется частично (0.5 балла)
IMG-3-4	Выполняется периодическое сканирование образов контейнеров, размещенных во внутренних репозиториях, на наличие уязвимостей	3	Не заполнено		анирование образов контейнеров	Средний	3	0	0	-	4.4	-	-	10.2 13.2	УБИ.227	
IMG-4-1	Должны использоваться образы, содержащие минимальный функционал (distroless)	4	Не заполнено	0%	Харденинг	Высокий	5	0	0	-	4.3; 4.8	-	-		УБИ.223 УБИ.226	
IMG-4-2	Сборки в CI/CD блокируются при найденных уязвимостях в образах контейнеров по договоренности между ИБ и разработчиками	4	Не заполнено		анирование образов контейнеров	Средний	3	0	0	-	-	-	-	10.2	УБИ.227	
						Максимальный балл	60	Итоговый общий балл	0							
Безопасность манифестов (Manifests)																
MAN-1-1	В манифестах не используются секреты в открытом виде	1	Не заполнено		Защита секретов	Высокий	5	0	0	5.1.2; 5.4.1	4.10	-	-		УБИ.223 УБИ.224	Полностью выполняется, если используется инструмент контроля. Иначе - частично выполняется (0.5 балла)
																Полностью выполняется, если применимо как для манифестов, так и настроена политика,

3

Возможность определить текущий уровень зрелости организации и относящиеся к нему практики

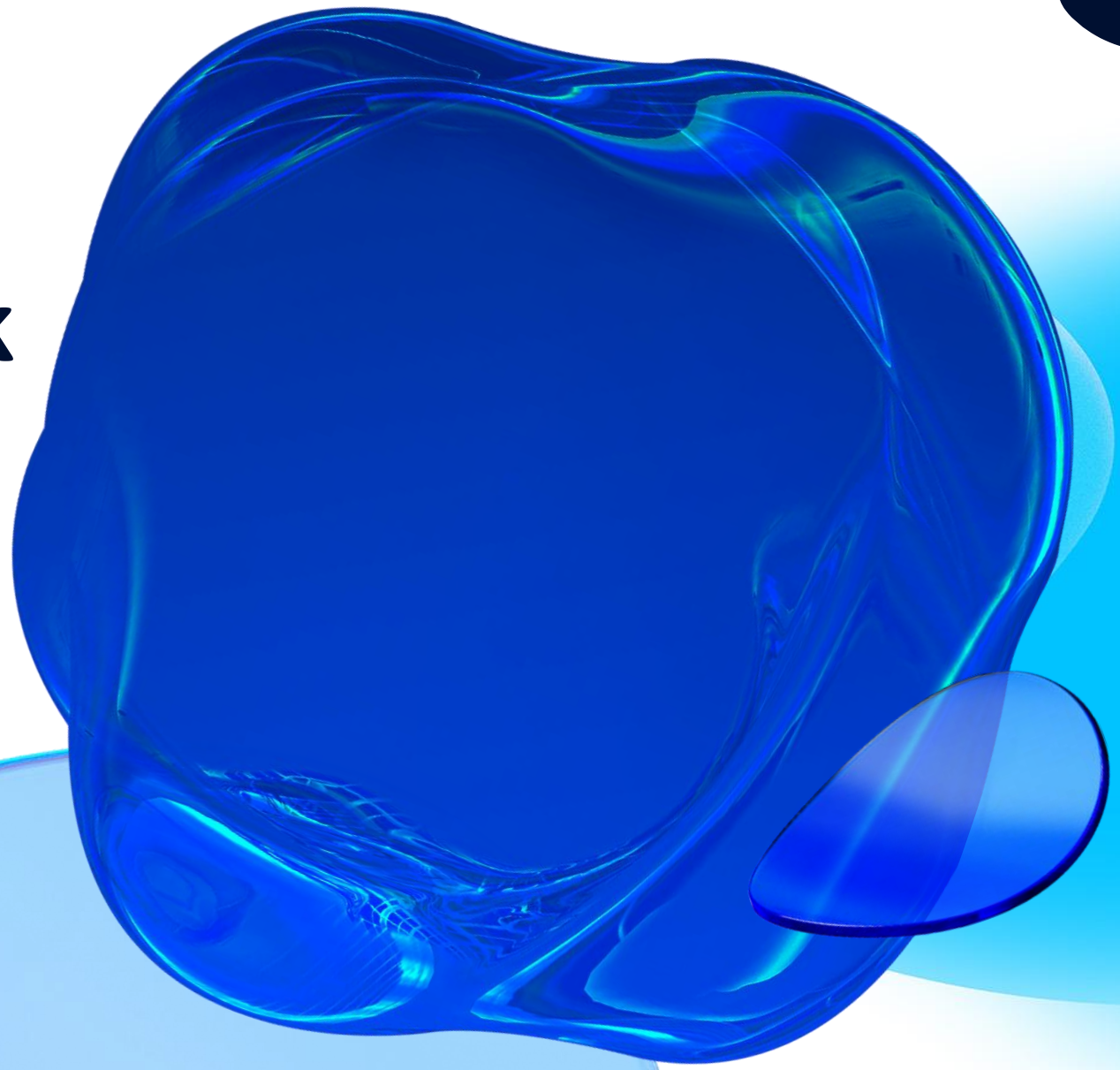
Что получилось?

ID практики	Требование	Уровень зрелости	Статус	Соответствие уровню зрелости	Классификация	Уровень критичности	Вес критерия	Выполняется	Итоговый балл	CIS Kubernetes	CIS Docker	CIS Linux (Debian)	CIS Linux (RHEL)	118 Приказ	УБИ ФСТЭК	Примечание
Dock-4-6	В кластере SWARM используется режим auto-lock. Для запуска узлов необходимо ввести ключ разблокировки доступа к ключам шифрования	4	Не заполнено		Харденинг	Низкий	1	0	0	-	7.5	-	-			docker info --format 'Swarm Autolock: {{ .Swarm.Cluster.Spec.EncryptionConfig.AutoLock Managers }}'
Dock-4-7	Для ключей разблокировки режима auto-lock используется ротация	4	Не заполнено		Харденинг	Низкий	1	0	0	-	7.6	-	-			Docker SWARM Процессный контроль. Выясняется в процессе интервью
						Максимальный балл	143	Итоговый общий балл	0							
Безопасность используемых образов (Images)																
IMG-1-1	В собранных образах не должны храниться секреты	1	Не заполнено		Защита секретов	Высокий	5	0	0	-	4.10	-	-		УБИ.226	trivy trufflehog
IMG-1-2	Контейнеры запускаются из образов, хранящихся в локальных репозиториях	1	Не заполнено	0%	Контроль репозиториев	Высокий	5	0	0	5.5.1	4.2	-	-		УБИ.224 УБИ.226 УБИ.227	Полностью выполняется, если настроена политика, контролирующая корректность конфигурации. Если выполняется для всех образов контейнеров, но не настроена контролирующая политика - частично выполняется (0.5 балла)
IMG-1-3	Выполняется сканирование образов контейнеров. Запуск сканирования происходит в ручном режиме.	1			канирование образов						4.4	-	-		УБИ.225 УБИ.226 УБИ.227	
IMG-1-4	Осуществляется мультиуровневая сборка для минимизации размера образа и его функционала										4.3; 4.7; 4.9; 4.11	-	-			
IMG-1-5	Осуществляется сканирование Docker файлов на недостатки конфигурации ИБ										4.4	-	-		УБИ.223 УБИ.226	
IMG-2-1	Образы контейнеров не должны содержать уязвимостей, которые возможно проэксплуатировать										4.4; 4.11	-	-	10.1	УБИ.225 УБИ.226	
IMG-2-2	Выполняется сканирование образов контейнеров в CI/CD на наличие уязвимостей										4.4	-	-	10.1	УБИ.226	trivy
IMG-2-3	При обнаружении дефектов ИБ в образах контейнеров автоматизированно создаются задачи на их устранение в тикет-системе										-	-	-			
IMG-3-1	Для собираемых образов генерируется SBOM										-	-	-		УБИ.226	trivy syft cdxgen
IMG-3-2	На образы регулярно устанавливаются обновления (обновляются базовые образы)	3	Не заполнено		Обновление ПО	Высокий	5	0	0	-	4.4; 4.7	-	-	10.1	УБИ.226	
IMG-3-3	Собираемые образы подписываются электронной подписью при сборке, а также осуществляется их проверка	3	Не заполнено		Харденинг	Средний	3	0	0	5.5.1	4.5; 4.12	-	-	12.1 13.2	УБИ.224 УБИ.227	Cosign В случае, если запуск контейнера из некорректно подписанного образа блокируется на уровне оркестратора - контроль выполняется полностью. Если осуществляется проверка без блокировки - данный контроль выполняется частично (0.5 балла)
IMG-3-4	Выполняется периодическое сканирование образов контейнеров, размещенных во внутренних репозиториях, на наличие уязвимостей	3	Не заполнено		канирование образов контейнеров	Средний	3	0	0	-	4.4	-	-	10.2 13.2	УБИ.227	
IMG-4-1	Должны использоваться образы, содержащие минимальный функционал (distroless)	4	Не заполнено	0%	Харденинг	Высокий	5	0	0	-	4.3; 4.8	-	-		УБИ.223 УБИ.226	
IMG-4-2	Сборки в CI/CD блокируются при найденных уязвимостях в образах контейнеров по договоренности между ИБ и разработчиками	4	Не заполнено		канирование образов контейнеров	Средний	3	0	0	-	-	-	-	10.2	УБИ.227	
						Максимальный балл	60	Итоговый общий балл	0							
Безопасность манифестов (Manifests)																
MAN-1-1	В манифестах не используются секреты в открытом виде	1	Не заполнено		Защита секретов	Высокий	5	0	0	5.1.2; 5.4.1	4.10	-	-		УБИ.223 УБИ.224	Полностью выполняется, если используется инструмент контроля. Иначе - частично выполняется (0.5 балла)
																Полностью выполняется, если применимо как для манифестов, так и настроена политика.

4 Максимальная автоматизация процесса оценки

Jet Container Security Framework

Пример использования



DEVSECOPS ASSESSMENT FRAMEWORK

Технологии

Контроль ИБ артефактов, зависимостей и образов

- Управление артефактами
- Контроль использования сторонних компонентов-зависимостей (библиотеки, образы и т.д.)

Защита окружения разработки

- Защита рабочих мест разработчика
- Защита секретов
- Защита Build-среды
- Защита реестра артефактов
- Контроль внесения изменений в исходный код
- Защита конвейера сборки

Контроль разрабатываемого ПО в части ИБ

Анализ ПО (development)

- Статический анализ
- Композиционный анализ
- Анализ образов контейнеров
- Идентификация секретов
- Контроль безопасности Dockerfile'ов

Анализ ПО в режиме Runtime-Preprod

- Динамический анализ приложений
- Тестирование на проникновение перед внедрением приложений в продуктив
- Функциональное ИБ-тестирование
- Контроль конфигураций - Контроль безопасности манифестов (k8s, terraform и т.д.)

Защита ПО и инфраструктуры в режиме Runtime

- Управление секретами
- Управление контролем доступа к средам работы приложений
- Контроль сетевого трафика (L4-L7)
- Контроль выполняемых процессов и их прав доступа
- Анализ инфраструктуры и приложений на уязвимости
- Тестирование на проникновение продуктивной среды
- Анализ событий информационной безопасности

Процессы и методология

Обучение и Onboarding

- Обучение специалистов
- Управление базой знаний DSO
- Процесс «подключения» команд

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

Управление ИБ-дефектами

- Обработка дефектов ИБ
- Консолидация дефектов ИБ

Оценка эффективности процессов DSO

- Управление набором метрик ИБ
- Контроль исполнения метрик (как собираем и что с ними делаем)

Функциональные роли

- Security Champions
- Разграничение ролей процесса DSO

JCSF: ПРОЦЕССЫ

Технологии

Контроль ИБ артефактов, зависимостей и образов

- Управление артефактами
- Контроль использования сторонних компонентов-зависимостей (библиотеки, образы и т.д.)

Защита окружения разработки

- Защита рабочих мест разработчика
- Защита секретов
- Защита Build-среды
- Защита реестра артефактов
- Контроль внесения изменений в исходный код
- Защита конвейера сборки

Контроль разрабатываемого ПО в части ИБ

Анализ ПО (development)

- Статический анализ
- Композиционный анализ
- Анализ образов контейнеров
- Идентификация секретов
- Контроль безопасности Dockerfile'ов

Анализ ПО в режиме Runtime-Preprod

- Динамический анализ приложений
- Тестирование на проникновение перед внедрением приложений в продуктив
- Функциональное ИБ-тестирование
- Контроль конфигураций - Контроль безопасности манифестов (k8s, terraform и т.д.)

Защита ПО и инфраструктуры в режиме Runtime

- Управление секретами
- Управление контролем доступа к средам работы приложений
- Контроль сетевого трафика (L4-L7)
- Контроль выполняемых процессов и их прав доступа
- Анализ инфраструктуры и приложений на уязвимости
- Тестирование на проникновение продуктивной среды
- Анализ событий информационной безопасности

Процессы и методология

Обучение и Onboarding

- Обучение специалистов
- Управление базой знаний DSO
- Процесс «подключения» команд

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

Управление ИБ-дефектами

- Обработка дефектов ИБ
- Консолидация дефектов ИБ

Оценка эффективности процессов DSO

- Управление набором метрик ИБ
- Контроль исполнения метрик (как собираем и что с ними делаем)

Функциональные роли

- Security Champions
- Разграничение ролей процесса DSO

JCSF: ТЕПЛОВАЯ МАТРИЦА

Домены	УРОВЕНЬ 1 МИНИМАЛЬНЫЙ	УРОВЕНЬ 2 НАЧАЛЬНЫЙ	УРОВЕНЬ 3 ПРОДВИНУТЫЙ	УРОВЕНЬ 4 ЭКСПЕРТНЫЙ
Общие практики безопасности	100%	100%	100%	Не применимо
Безопасность Узлов	93%	79%	14%	38%
Безопасность Платформы	78%	38%	50%	50%
Безопасность Образов контейнеров	80%	33%	25%	0%
Безопасность Манифестов	38%	50%	13%	0%
Безопасность среды выполнения контейнеров	25%	0%	0%	0%
Итого, процент достижения каждого уровня зрелости по всем доменам JCSF	69%	50%	29%	18%

JCSF: РЕЗУЛЬТАТ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ

1

Понимание,
где вы сейчас

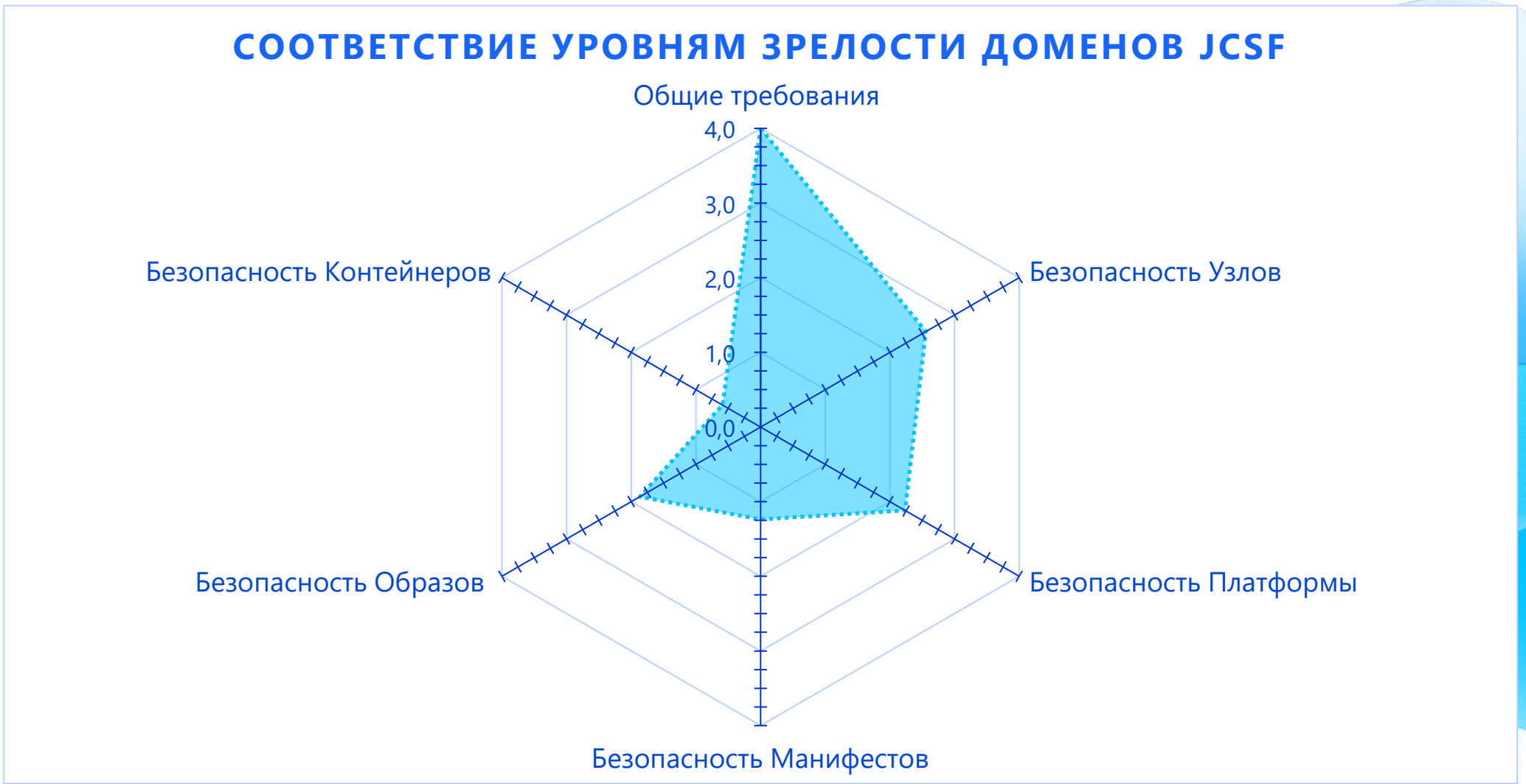
2

Понимание, что надо сделать
прямо сейчас
и куда двигаться, в том числе в
долгосрочной перспективе

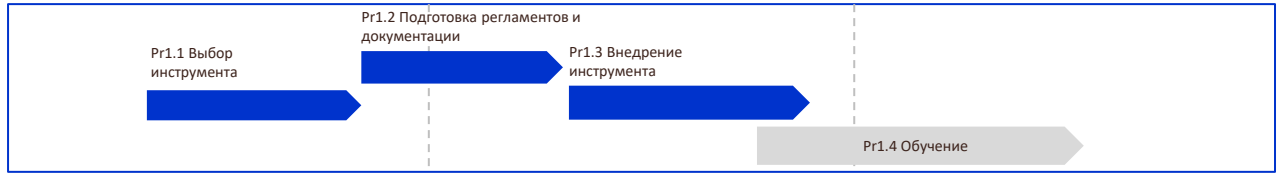
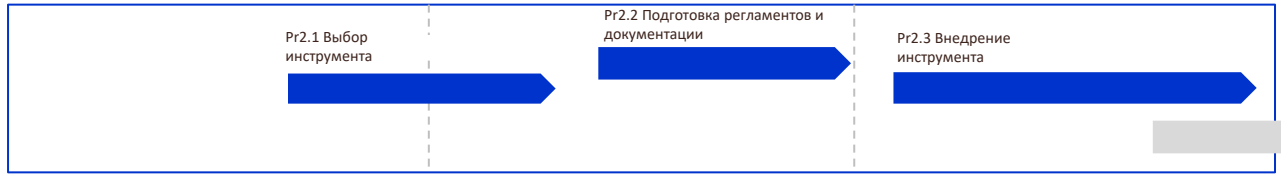
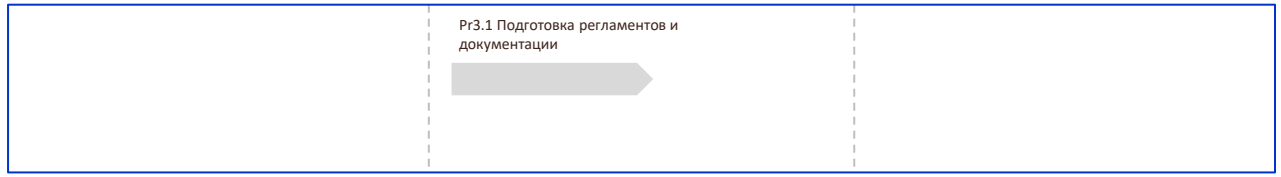
3

Какие инвестиции необходимы
сейчас
и в дальнейшем

JCSF: ПЛАН РАЗВИТИЯ



JCSF: ПРИМЕР ДОРОЖНОЙ КАРТЫ РАЗВИТИЯ

Процесс	План-график реализации	Стоимость развития, ₽	Выгоды от реализации активностей (верхнеуровневое описание)
Pr1 Внедрение инструмента Secrets Management		₽ ₽	Реализация практики управления секретами
Pr2 Внедрение инструмента Container Security		₽ ₽ ₽	Внедрение инструмента контроля безопасности среды контейнеризации и оркестрации
Pr3 Разработка регламентов безопасной настройки		Реализуется внутренними силами компании	Описание процесса безопасной настройки

JCSF+DAF: ПРИМЕР ДОРОЖНОЙ КАРТЫ РАЗВИТИЯ

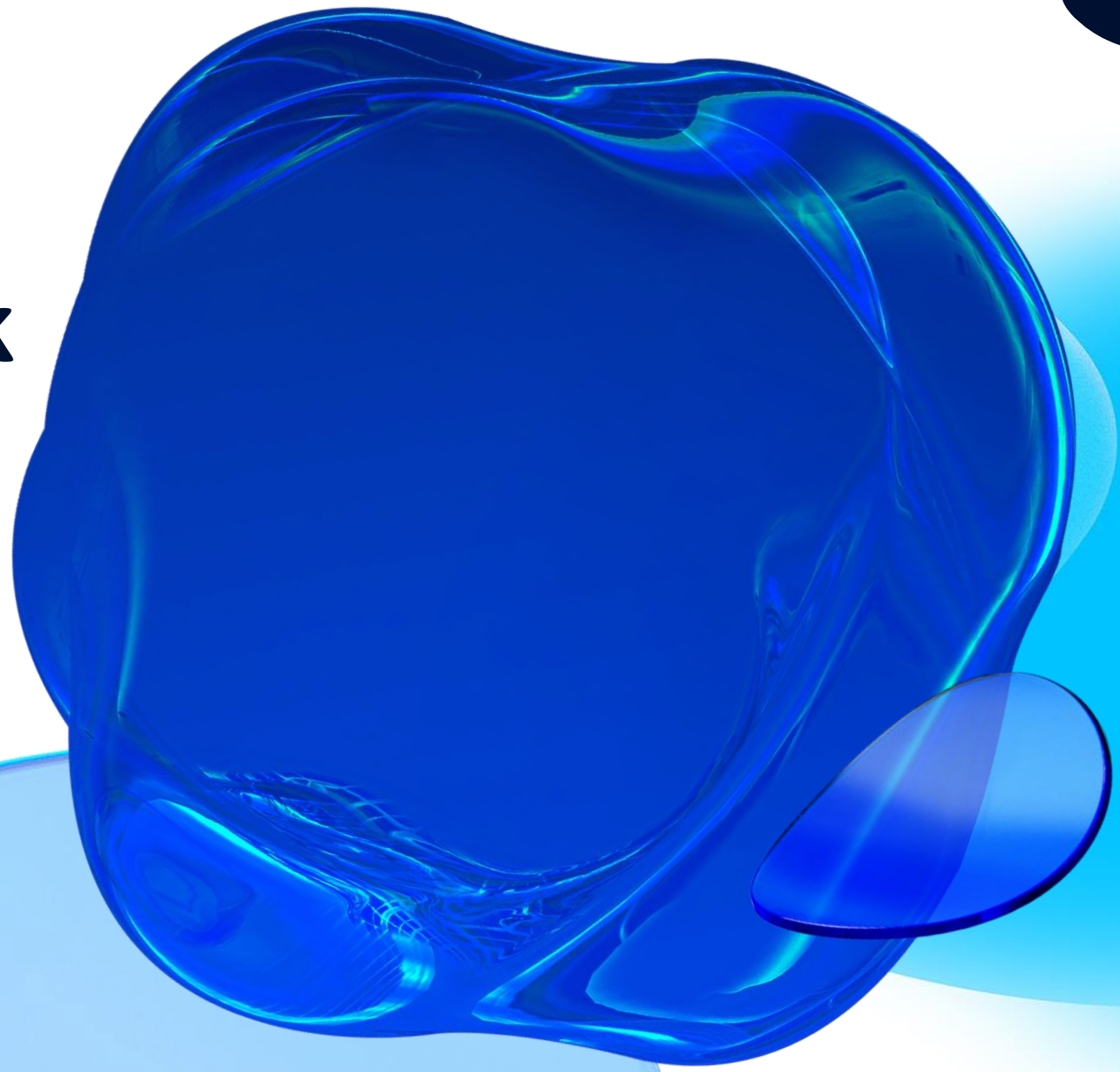
Процесс	План-график реализации (2026: 2 квартал, 3 квартал, 4 квартал)	Стоимость развития, ₽	Выгоды от реализации активностей (верхнеуровневое описание)
Pr1 Внедрение инструмента Secrets Detection	Pr1.1 Выбор инструмента; Pr1.2 Подготовка регламентов и документации; Pr1.3 Внедрение инструмента; Pr1.4 Обучение	₽ ₽	Реализация практики детектирования секретов
Pr2 Внедрение инструмента Container Security	Pr2.1 Выбор инструмента; Pr2.2 Подготовка регламентов и документации; Pr2.3 Внедрение инструмента; Pr2.4 Обучение	₽ ₽ ₽	Внедрение инструмента контроля безопасности среды контейнеризации и оркестрации
Pr3 Разработка регламентов безопасной настройки	Pr3.1 Подготовка регламентов и документации	Реализуется внутренними силами компании	Описание процесса безопасной настройки
Pr4 Внедрение инструмента контроля Dockerfiles	Pr4.1 Выбор инструмента; Pr4.2 Подготовка регламентов и документации; Pr4.3 Внедрение инструмента; Pr.4.4 Обучение	₽	Внедрение инструмента контроля образов контейнеров
Pr5 Разработка регламента управления уязвимостями	Pr5.1 Подготовка регламентов и документации	Реализуется внутренними силами компании	Описание процесса управления уязвимостями

Реализуется силами компании

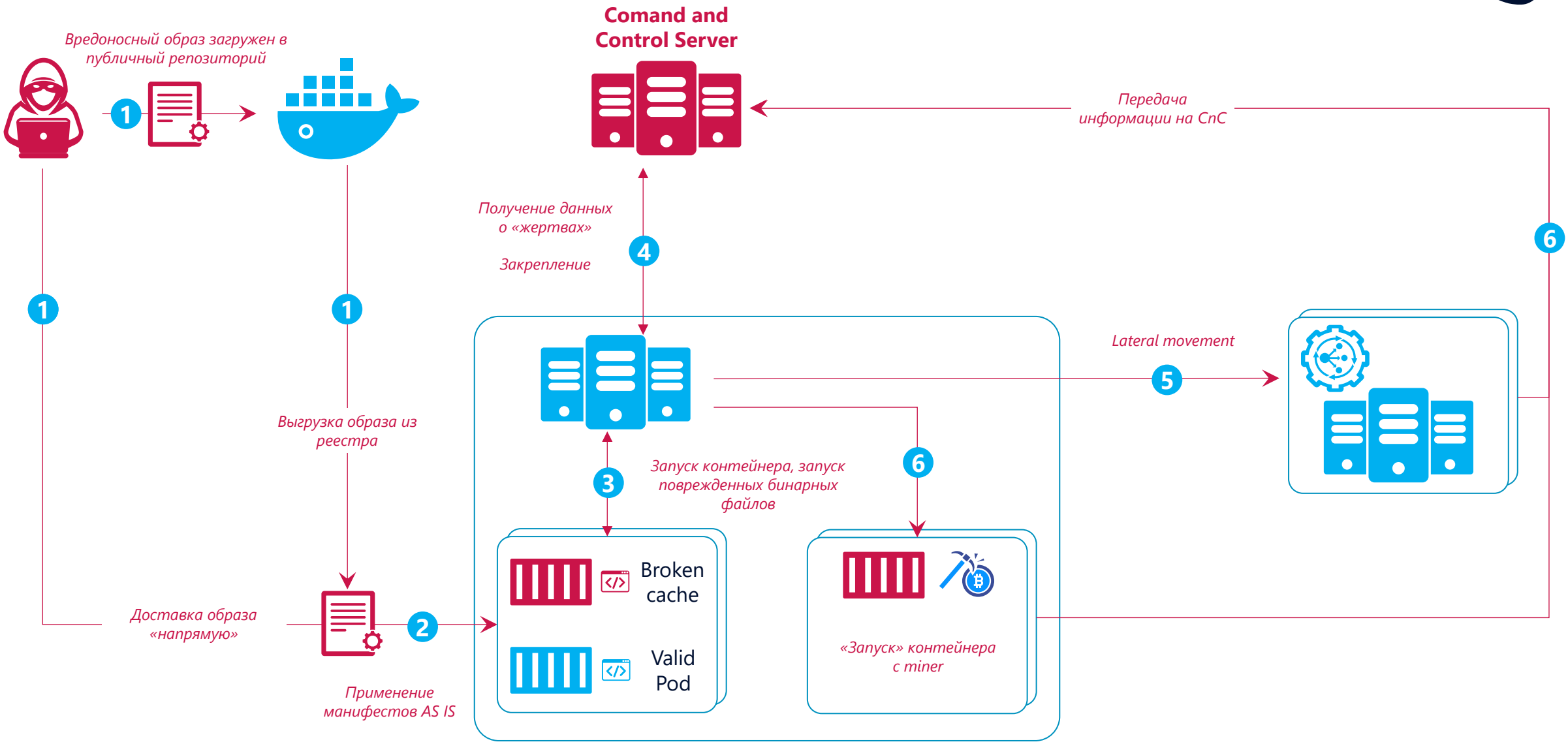
Реализуется с привлечением подрядчика

Jet Container Security Framework

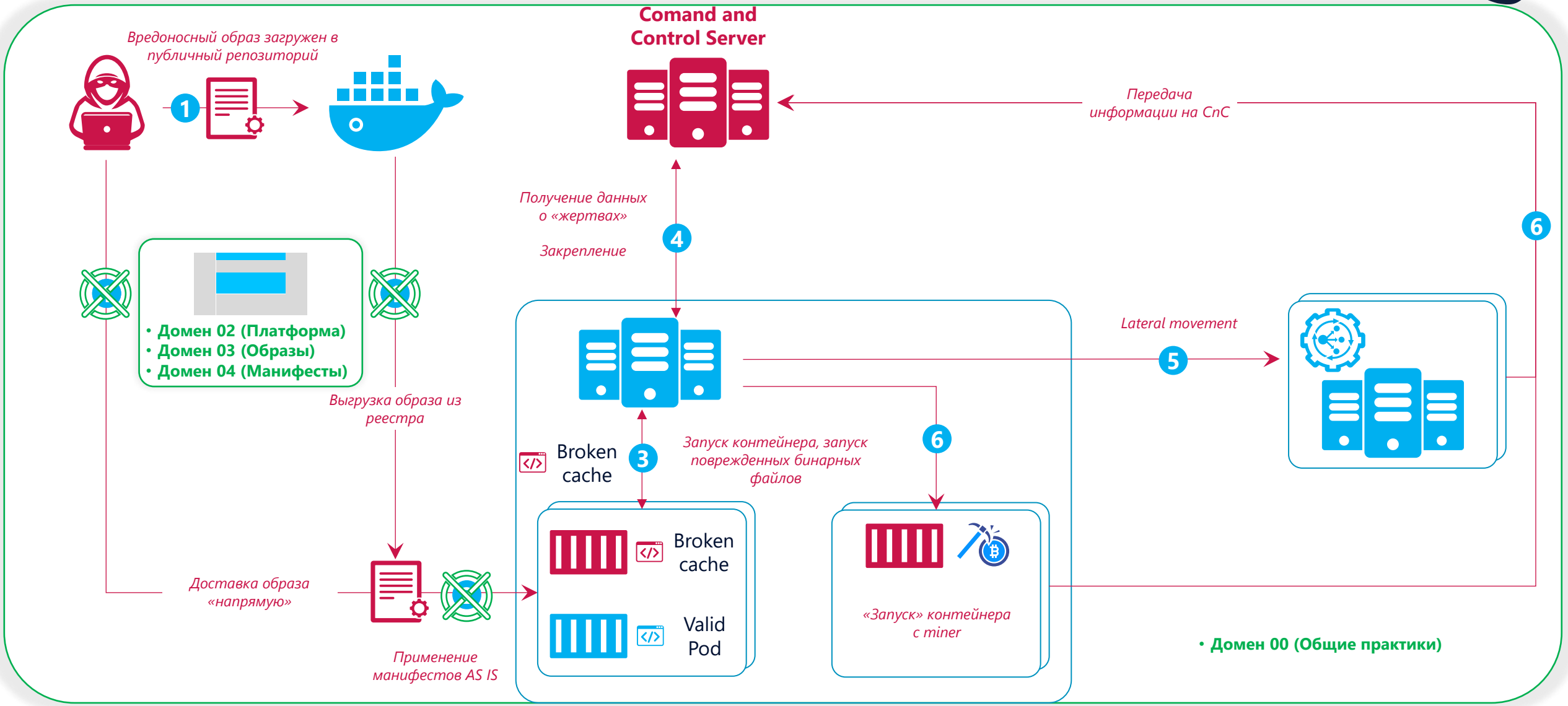
Всё есть процесс!



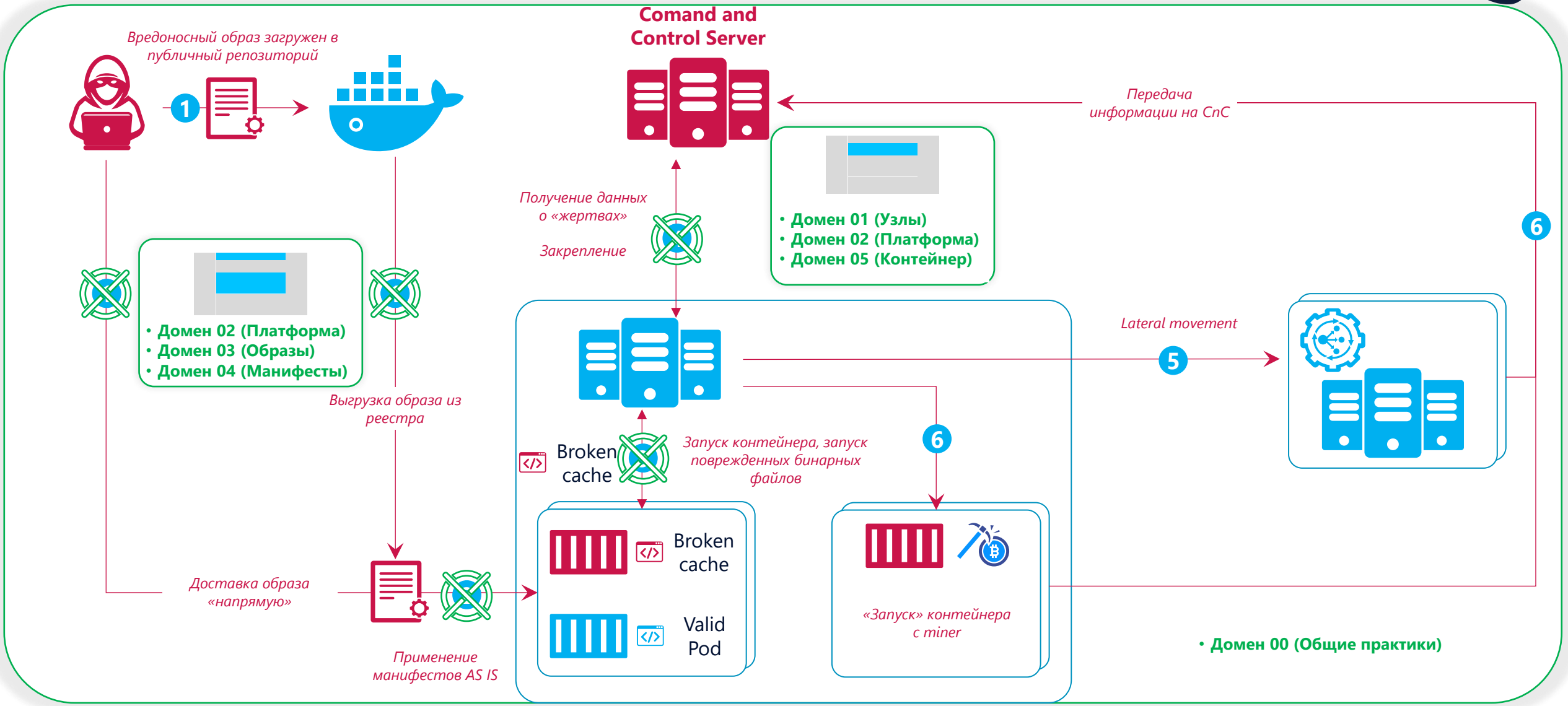
JCSF: РЕЗУЛЬТАТ ПРИМЕНЕНИЯ



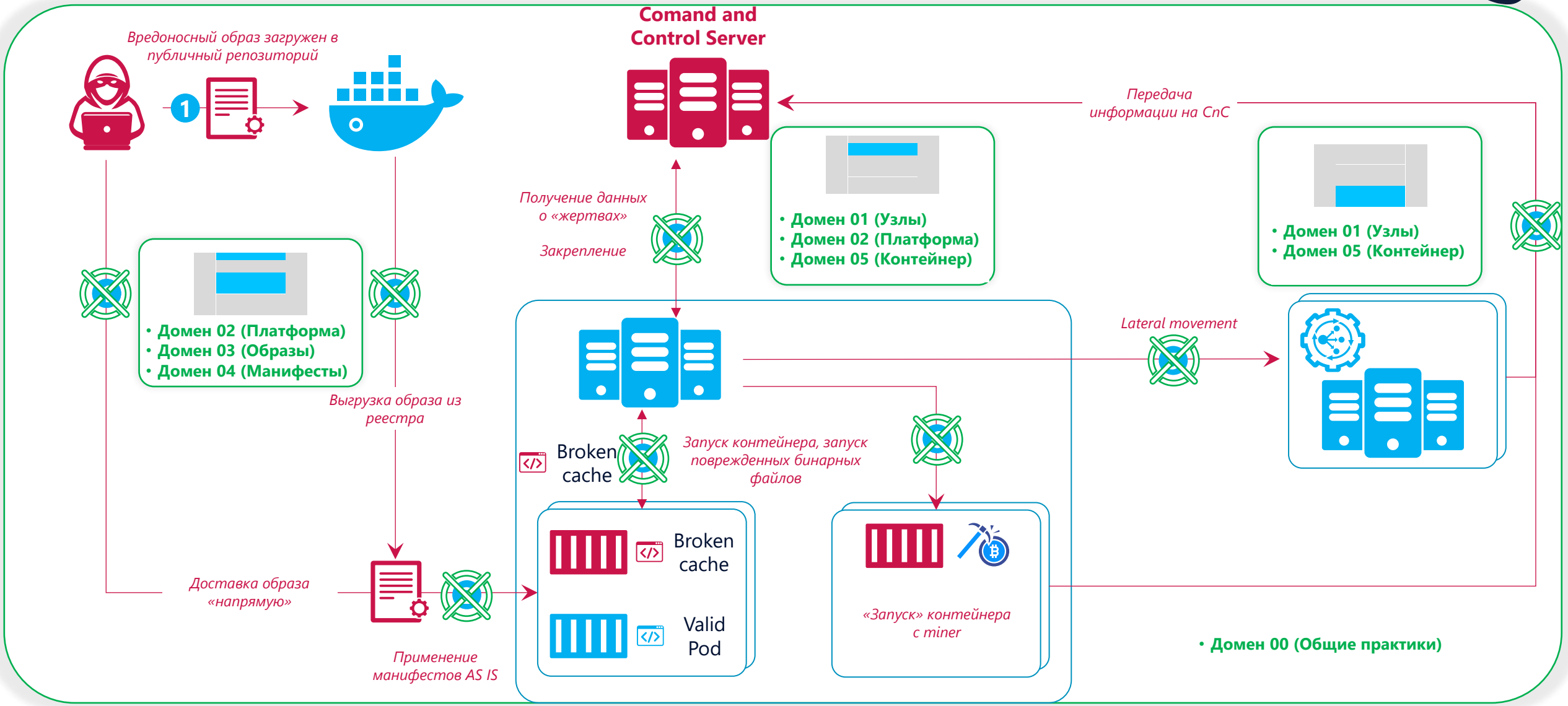
JCSF: РЕЗУЛЬТАТ ПРИМЕНЕНИЯ



JCSF: РЕЗУЛЬТАТ ПРИМЕНЕНИЯ



JCSF: РЕЗУЛЬТАТ ПРИМЕНЕНИЯ



JCSF: ПЕРСПЕКТИВЫ РАЗВИТИЯ

1

Веб-интерфейс с полной автоматизацией процесса оценки уровня зрелости

2

Расширение перечня доступных маппингов на фреймворки, стандарты и требования

3

Учет обратной связи

БЕКОН'26

КОНФЕРЕНЦИЯ ПО БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И КОНТЕЙНЕРНЫХ СРЕД

JCSF

DAF