

AppSecAutomation:

как внедрить проверки в жизнь разработчиков и не свести их с ума

Алена Жилина

DevSecOps-инженер

Вячеслав Давыдов

DevSecOps-инженер

О нас

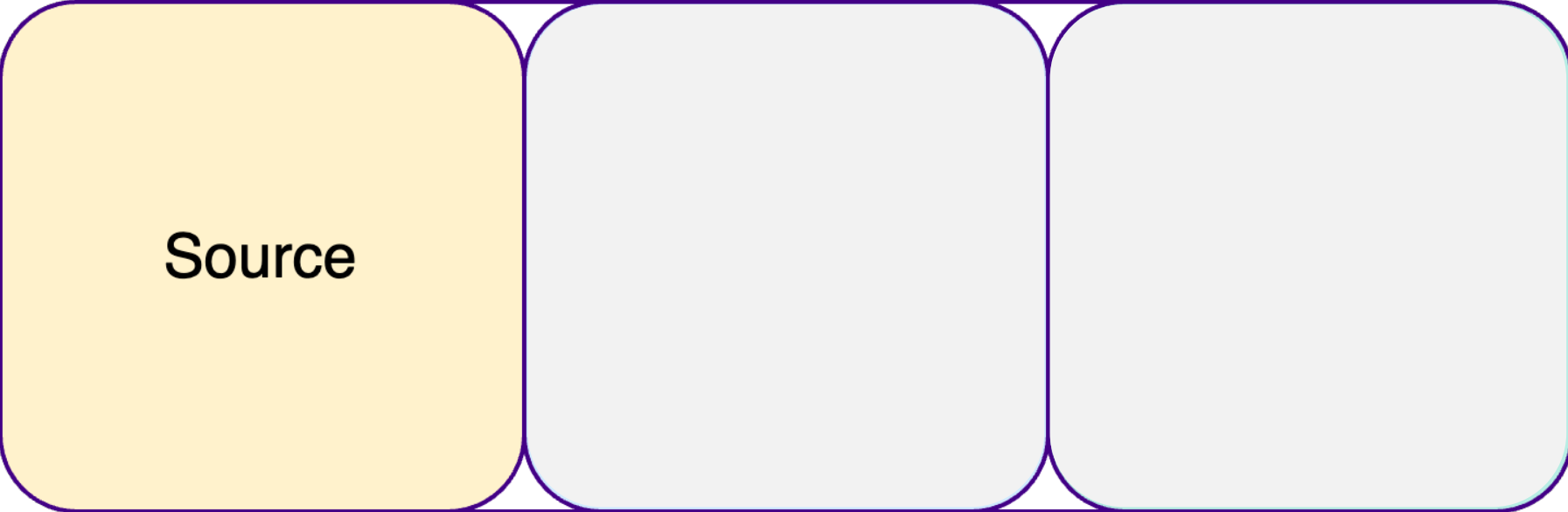


- проектирование и интеграция в AppSec
- безопасность Kubernetes
- data-инжиниринг



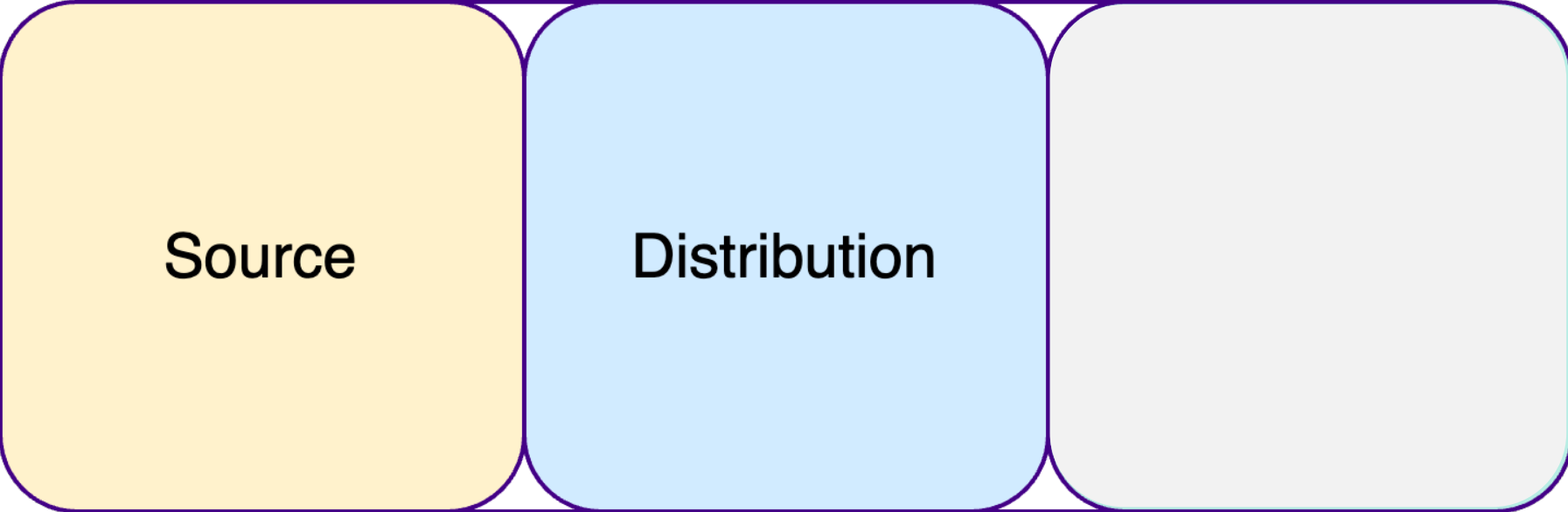
- разработка в AppSec
- CI/CD микросервисов
- геоинформационные системы

С чем работаем



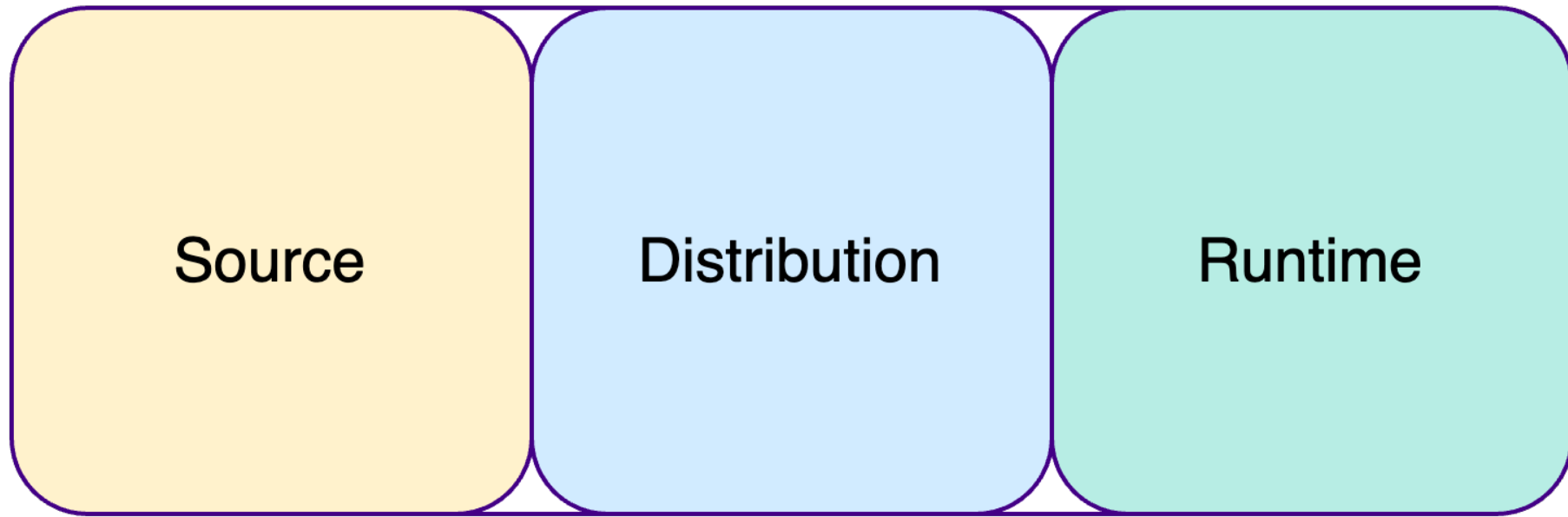
Application

С чем работаем



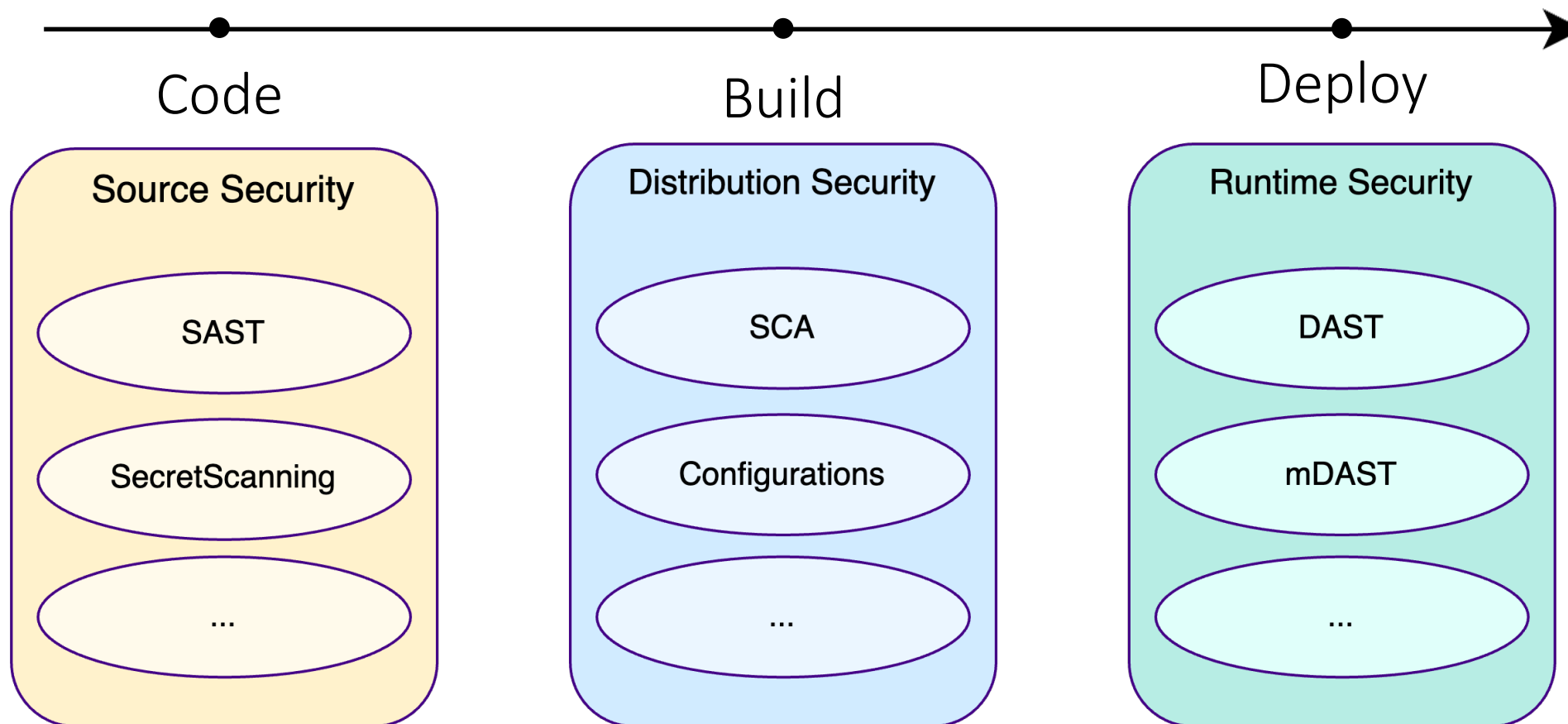
Application

С чем работаем

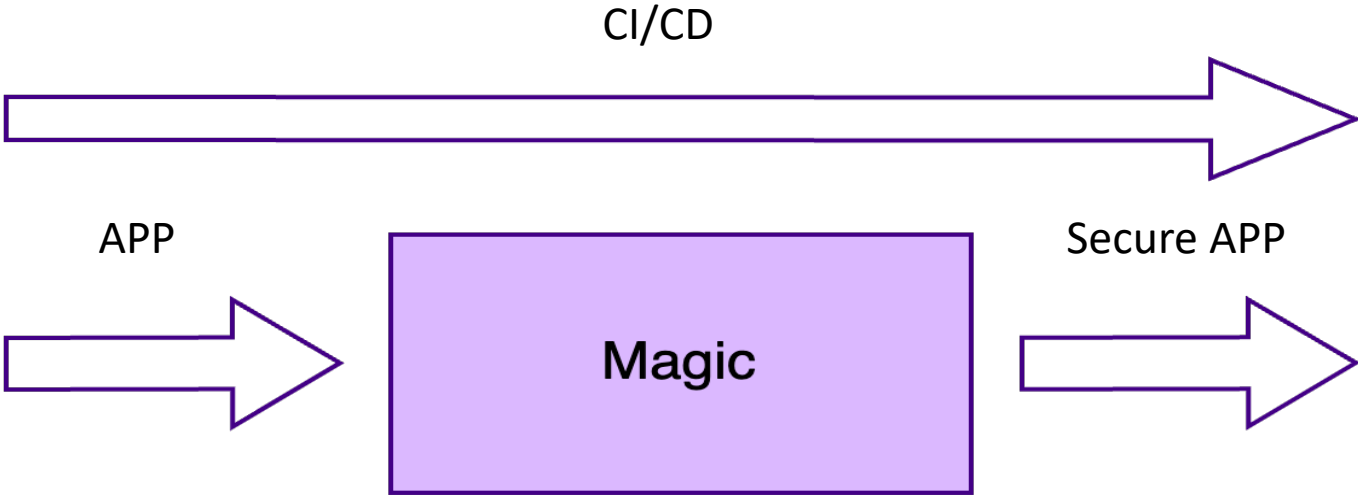


Application

С чем работаем

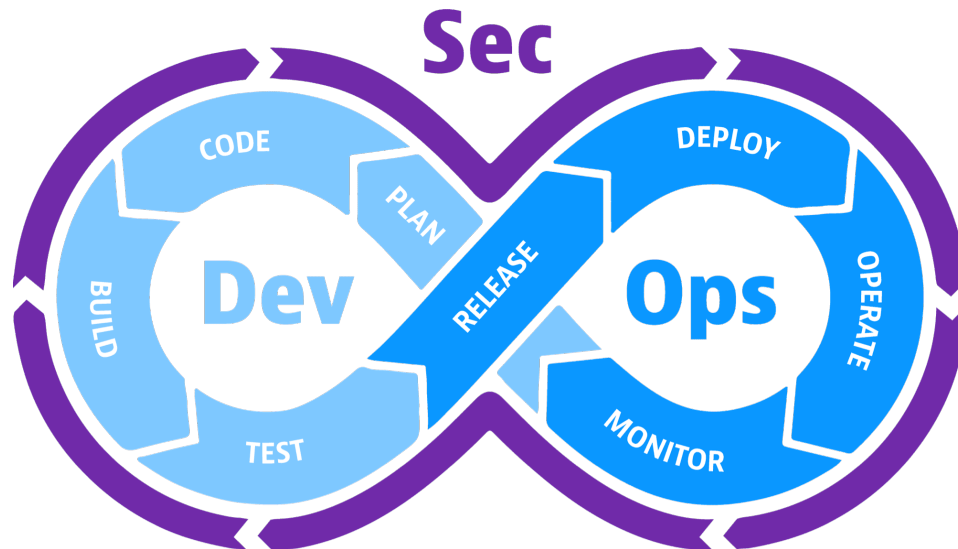


Дивный новый мир



Дивный новый мир

- OnDemand
- Shift left
- триаж и исправление дефектов кода сразу
- перед релизом все баги уже исправлены



Проблематика

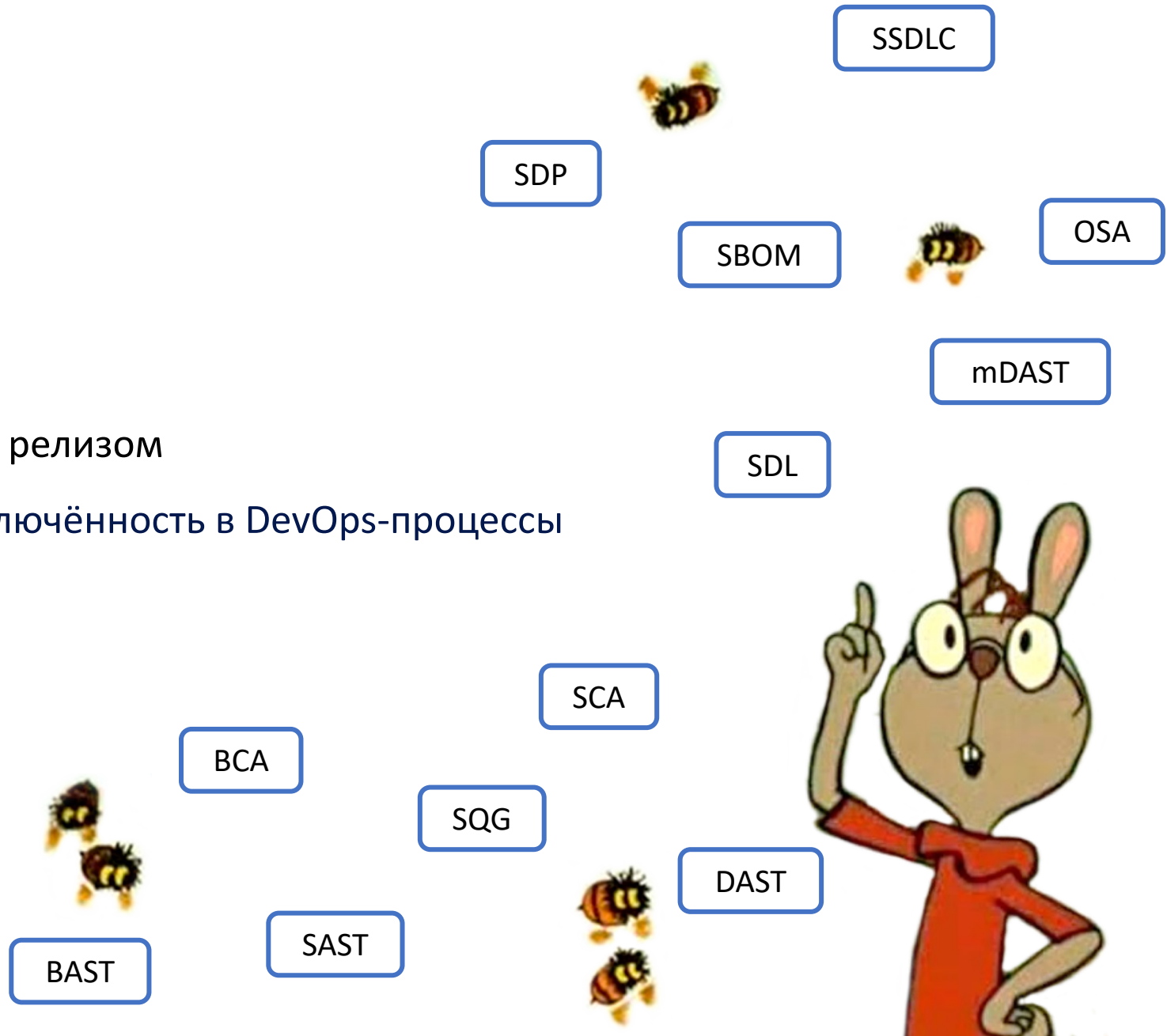


команды разработки



→ сложные абстракции

- много срочных консультаций перед релизом
- AppSec-инженерам необходима включённость в DevOps-процессы



Проблематика



команды разработки

- сложные абстракции

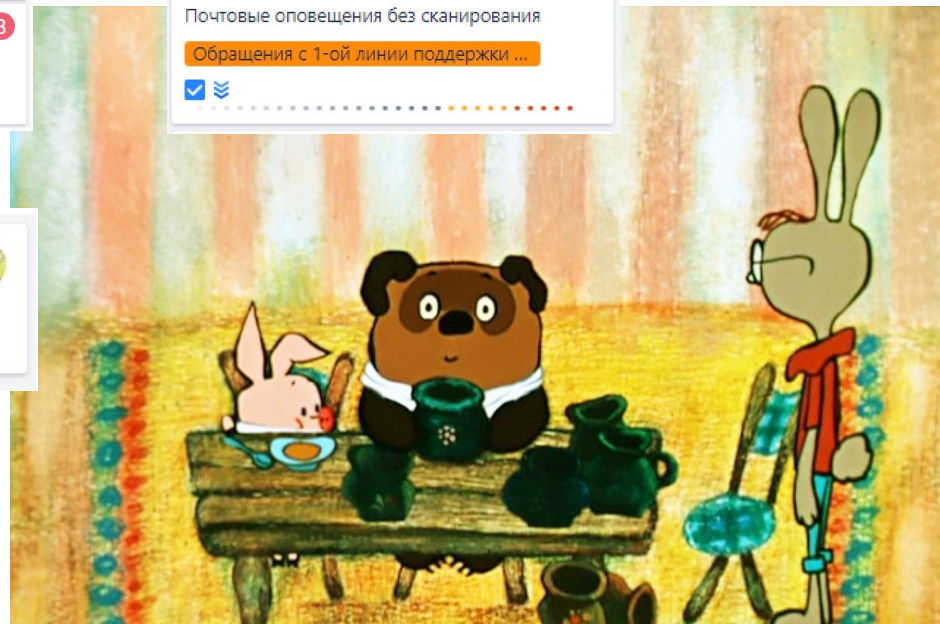
 → много срочных консультаций перед релизом

- AppSec-инженерам необходима включённость в DevOps-процессы

DSOR-1154
Заявка на консультацию по уязвимостям в исходном коде
SALM реагирует на библиотеки, котор...
✓

DSOR-1015
Почтовые оповещения без сканирования
Обращения с 1-ой линии поддержки ...
✓

DSOR-1134
Консультация (false positive)
✓



DSOR-1168
Исключение репозитория из проверок SAST/OSS
Исключение репозитория по практик...
✓

DSOR-1131
Исключение репозитория из проверок SAST/OSS
Исключение репо...
✓

DSOR-1140
Заявка на консультацию по уязвимостям в исходном коде
Обращения с первой линии
✓

DSOR-747
Ошибка входа пользователя в интерфейс
Обращения со 2-...
✓

DSOR-1157
Заявка на консультацию по уязвимостям в исходном коде
Проблема при сборке в SALM (OSS)
✓

Проблематика



команды разработки

- сложные абстракции
- много срочных консультаций перед релизом

 ...→ AppSec-инженерам необходима включённость в DevOps-процессы



Проблематика



реализация проверок



…► нужны релевантные инструменты

- автоматизация запуска требует ресурсов
- непонятные отчёты
- onDemand сканирования создают доп нагрузку на ресурсы
- длительные согласования доступов

A screenshot of three GitHub repository cards. The first card is for 'OWASP/CheatSheetSeries', described as 'The OWASP Cheat Sheet Series was created to provide a concise collection of high value information on specific application security topics.' It has 27.6k stars and was updated 3 days ago. The second card is for 'zaproxy/zaproxy', described as 'The ZAP core project'. It has 12.5k stars and was updated yesterday. The third card is for 'chaitin/SafeLine', described as 'serve as a reverse proxy to protect your web services from attacks and exploits.' It has 11.9k stars and was updated 5 days ago. Each card includes tags for related topics and 'Star' and 'Sponsor' buttons.

1.9k results (163 ms)



Проблематика



реализация проверок

- нужны релевантные инструменты
- …▶ автоматизация запуска требует ресурсов
- непонятные отчёты
- onDemand сканирования создают доп нагрузку на ресурсы
- длительные согласования доступов



затраты на обучение

место на диске

время на тестирование

время на интеграцию

время на обучение

мотивация

ОЗУ

сетевые ресурсы

CPU

затраты на инструменты



Проблематика



реализация проверок

- нужны релевантные инструменты
- автоматизация запуска требует ресурсов



…► непонятные отчёты

- onDemand сканирования создают доп нагрузку на ресурсы
- длительные согласования доступов

```
3      "runs": [
4        {
48102          "tool": {
48103            "driver": {
48231              "rules": [
49084                {
49085                  },
49086                  "defaultConfiguration": {
49087                    "enabled": true,
49088                    "level": "warning"
49089                  },
49090                  "fullDescription": {
49091                    "text": "Using broken or weak cryptographic algorithms can allow an attacker to compromise
49092                  },
49093                  "id": "java/weak-cryptographic-algorithm",
49094                  "name": "java/weak-cryptographic-algorithm",
49095                  "properties": {
49096                    "description": "Using broken or weak cryptographic algorithms can allow an attacker to compromise",
49097                    "id": "java/weak-cryptographic-algorithm",
49098                    "kind": "path-problem",
49099                    "name": "Use of a broken or risky cryptographic algorithm",
49100                    "precision": "high",
49101                    "problem.severity": "warning",
49102                    "security-severity": "7.5",
49103                    "tags": [
49104                      "security",
49105                      "external/cwe/cwe-327",
49106                      "external/cwe/cwe-328"
49107                    ]
49108                  },
49109                  "shortDescription": {
49110                    "text": "Use of a broken or risky cryptographic algorithm"
49111                  }
                }
              ]
            }
          }
        }
      ]
    }
  }
}
```

CWE-327


```
3      "runs": [
4        {
282          "tool": {
283            "driver": {
284              "name": "semgrep ubo",
285              "rules": [
286                {
287                  "defaultConfiguration": {
288                    "level": "note"
289                  },
290                  "fullDescription": {
291                    "text": "Use of RC4 was detected. RC4 is vulnerable to several attacks, including stream cipher a
292                  },
293                  "help": {
294                    "markdown": "Use of RC4 was detected. RC4 is vulnerable to several attacks, including stream cipher a
295                    "text": "Use of RC4 was detected. RC4 is vulnerable to several attacks, including stream cipher a
296                  },
297                  "id": "tmp.tmp.rules_4085e1a9-aff6-41ee-9a50-e6163468bd45.java.lang.security.audit.crypto.use-of-rc
298                  "name": "tmp.tmp.rules_4085e1a9-aff6-41ee-9a50-e6163468bd45.java.lang.security.audit.crypto.use-of-rc
299                  "properties": {
300                    "precision": "yes-high",
301                    "tags": [
302                      "CWE-327: Use of a Broken or Risky Cryptographic Algorithm",
303                      "HIGH CONFIDENCE",
304                      "OWASP-A02:2021 - Cryptographic Failures",
305                      "OWASP-A03:2017 - Sensitive Data Exposure",
306                      "Security"
307                    ]
308                  },
309                  "shortDescription": {
310                    "text": "Semgrep Finding: tmp.tmp.rules_4085e1a9-aff6-41ee-9a50-e6163468bd45.java.lang.security.a
311                  }
312                }
              ]
            }
          }
        }
      ]
    }
  }
}
```

Проблематика



реализация проверок

- нужны релевантные инструменты
- автоматизация запуска требует ресурсов
- непонятные отчёты

 ...→ onDemand сканирования создают доп нагрузку на ресурсы

- длительные согласования доступов



Проблематика



реализация проверок

- нужны релевантные инструменты
- автоматизация запуска требует ресурсов
- непонятные отчёты
- onDemand сканирования создают доп нагрузку на ресурсы



…→ длительные согласования доступов



О чём расскажем?

1

Сканирование
как ресурс

Управление
сканированиями через
YAML-интерфейсы

2

Что нужно
знать о
приложении?

Анализ характеристик
артефакта

3

Запуск
инструментов

Сценарии запуска
сканеров для
оптимизации процесса

4

Что дальше?

Работа с отчётом и
SecurityQualityGate



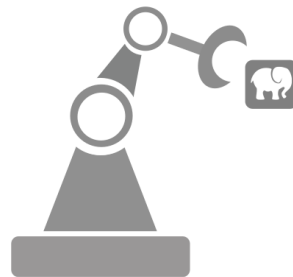
Абстракции:
Kubernetes всюду

Kubernetes-оператор

Software SRE

Программа с навыками опытного администратора

Контроллер, который автоматизирует управление сложными приложениями на кластере, заменяя ручные действия по развертыванию и поддержке.



```
yaml Copy code  
  
apiVersion: postgres-operator.crunchydata.com/v1beta1  
kind: PostgresCluster  
metadata:  
  name: hippo  
spec:  
  image: registry.developers.crunchydata.com/crunchydata/crunchy-postgres:ubi8-13.4-0  
  
  postgresVersion: 13  
  instances:  
    - name: instance1  
      replicas: 3  
      dataVolumeClaimSpec:  
        accessModes:  
          - "ReadWriteOnce"  
        resources:  
          requests:  
            storage: 1Gi  
  
  backups:  
    pgbackrest:  
      image: registry.developers.crunchydata.com/crunchydata/crunchy-pgbackrest:ubi8-2.33-0  
  
  repos:  
    - name: repo1  
      volume:  
        volumeClaimSpec:  
          accessModes:  
            - "ReadWriteOnce"  
          resources:  
            requests:  
              storage: 1Gi
```

AppSecTool custom resource

Минимально и достаточно:

...► **что может сканировать**

- где расположен

Кастомизация поведения:

- необходимые ресурсы
- набор правил
- типизация артефакта

```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecTool
metadata:
  name: semgrep
spec:
  name: semgrep
  toolConfiguration:
  - state: injob
    tag: "mini-python"
    artifactType: "code"
    languages: ["python"]
    size: 200Mi
    image: "my-registry:5000/semgrep:0.1"
    rulesPath:
    - "/etc/semgrep/python"
    cpuRequest: 100m
    memoryRequest: 200Mi

  - state: standAlone
    tag: "custom-secrets"
    artifactType: "code"
    languages: ["java", "python", "yaml"]
    size: 200Mi
    image: "my-registry:5000/semgrep:agent"
    rulesPath:
    - "/etc/semgrep/test/rules"
  host:
    url: "localhost"
    port: 8080
```

AppSecTool custom resource

Минимально и достаточно:

- что может сканировать

...► **где расположен**

Кастомизация поведения:

- необходимые ресурсы
- набор правил
- типизация артефакта

```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecTool
metadata:
  name: semgrep
spec:
  name: semgrep
  toolConfiguration:
  - state: injob
    tag: "mini-python"
    artifactType: "code"
    languages: ["python"]
    size: 200Mi
    image: "my-registry:5000/semgrep:0.1"
    rulesPath:
    - "/etc/semgrep/python"
    cpuRequest: 100m
    memoryRequest: 200Mi

  - state: standAlone
    tag: "custom-secrets"
    artifactType: "code"
    languages: ["java", "python", "yaml"]
    size: 200Mi
    image: "my-registry:5000/semgrep:agent"
    rulesPath:
    - "/etc/semgrep/test/rules"
  host:
    url: "localhost"
    port: 8080
```

AppSecTool custom resource

Минимально и достаточно:

- что может сканировать
- где расположен

Кастомизация поведения:

…► **необходимые ресурсы**

- набор правил
- типизация артефакта

```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecTool
metadata:
  name: semgrep
spec:
  name: semgrep
  toolConfiguration:
  - state: injob
    tag: "mini-python"
    artifactType: "code"
    languages: ["python"]
    size: 200Mi
    image: "my-registry:5000/semgrep:0.1"
    rulesPath:
    - "/etc/semgrep/python"
    cpuRequest: 100m
    memoryRequest: 200Mi

  - state: standAlone
    tag: "custom-secrets"
    artifactType: "code"
    languages: ["java", "python", "yaml"]
    size: 200Mi
    image: "my-registry:5000/semgrep:agent"
    rulesPath:
    - "/etc/semgrep/test/rules"
  host:
    url: "localhost"
    port: 8080
```


AppSecTool custom resource

Минимально и достаточно:

- что может сканировать
- где расположен

Кастомизация поведения:

- необходимые ресурсы

…› набор правил

- типизация артефакта

```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecTool
metadata:
  name: semgrep
spec:
  name: semgrep
  toolConfiguration:
  - state: injob
    tag: "mini-python"
    artifactType: "code"
    languages: ["python"]
    size: 200Mi
    image: "my-registry:5000/semgrep:0.1"
    rulesPath:
    - "/etc/semgrep/python"
    cpuRequest: 100m
    memoryRequest: 200Mi

  - state: standAlone
    tag: "custom-secrets"
    artifactType: "code"
    languages: ["java", "python", "yaml"]
    size: 200Mi
    image: "my-registry:5000/semgrep:agent"
    rulesPath:
    - "/etc/semgrep/test/rules"
  host:
    url: "localhost"
    port: 8080
```

AppSecTool custom resource

Минимально и достаточно:

- что может сканировать
- где расположен

Кастомизация поведения:

- необходимые ресурсы
- набор правил

…► типизация артефакта

```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecTool
metadata:
  name: semgrep
spec:
  name: semgrep
  toolConfiguration:
  - state: injob
    tag: "mini-python"
    artifactType: "code"
    languages: ["python"]
    size: 200Mi
    image: "my-registry:5000/semgrep:0.1"
    rulesPath:
    - "/etc/semgrep/python"
    cpuRequest: 100m
    memoryRequest: 200Mi

  - state: standAlone
    tag: "custom-secrets"
    artifactType: "code"
    languages: ["java", "python", "yaml"]
    size: 200Mi
    image: "my-registry:5000/semgrep:agent"
    rulesPath:
    - "/etc/semgrep/test/rules"
  host:
    url: "localhost"
    port: 8080
```

AppSecJob custom resource

Минимально и достаточно:

...» **объект сканирования**

Кастомизация поведения:

- доступ к объекту сканирования
- менеджер секретов
- представление результата

```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecJob
metadata:
  name: appsecjob-3
spec:
  artifact:
    code:
      url: ssh://git@bb.mycompany.ru:project/repo.git
      commithash: c8410457c23b57cf04910548d099c28bb39f3c3f
      source:
        secretName: bitbucket
        secretKeys:
          - sshkey
    distribution:
      hash: 541bc8e0cf501c53f8eeae08c3fc8b22b4212cdc
  secretManager:
    type: vault
    namespace: APPSEC
    path: ddd
  host:
    name: secman.mycompany.ru
    port: 443
  resultDesination:
    type: s3
    host:
      name: minio.mycompany.ru
      port: 443
      bucket: appsec-results
```

AppSecJob custom resource

Минимально и достаточно:

- объект сканирования

Кастомизация поведения:

...» **доступ к объекту сканирования**

- менеджер секретов
- представление результата

```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecJob
metadata:
  name: appsecjob-3
spec:
  artifact:
    code:
      url: ssh://git@bb.mycompany.ru:project/repo.git
      commithash: c8410457c23b57cf04910548d099c28bb39f3c3f
      source:
        secretName: bitbucket
        secretKeys:
          - sshkey
    distribution:
      hash: 541bc8e0cf501c53f8eeae08c3fc8b22b4212cdc
  secretManager:
    type: vault
    namespace: APPSEC
    path: ddd
  host:
    name: secman.mycompany.ru
    port: 443
  resultDesination:
    type: s3
    host:
      name: minio.mycompany.ru
      port: 443
      bucket: appsec-results
```

AppSecJob custom resource

Минимално и достаточо:

- обект сканирования

Кастомизация поведения:

- доступ к объекту сканирования

...► **менеджер секретов**

- представление результата

```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecJob
metadata:
  name: appsecjob-3
spec:
  artifact:
    code:
      url: ssh://git@bb.mycompany.ru:project/repo.git
      commithash: c8410457c23b57cf04910548d099c28bb39f3c3f
      source:
        secretName: bitbucket
        secretKeys:
          - sshkey
    distribution:
      hash: 541bc8e0cf501c53f8eeae08c3fc8b22b4212cdc
  secretManager:
    type: vault
    namespace: APPSEC
    path: ddd
  host:
    name: secman.mycompany.ru
    port: 443
  resultDesination:
    type: s3
    host:
      name: minio.mycompany.ru
      port: 443
      bucket: appsec-results
```

AppSecJob custom resource

Минимално и достаточо:

- обект сканирования

Кастомизация поведения:

- доступ к обекту сканирования
- менеджер секретов

...▶ **представление резултата**

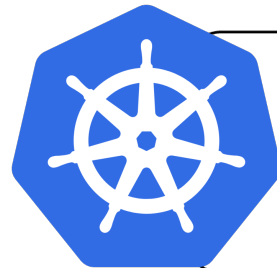
```
---
apiVersion: cache.appsec.ru/v1alpha1
kind: AppSecJob
metadata:
  name: appsecjob-3
spec:
  artifact:
    code:
      url: ssh://git@bb.mycompany.ru:project/repo.git
      commithash: c8410457c23b57cf04910548d099c28bb39f3c3f
      source:
        secretName: bitbucket
        secretKeys:
          - sshkey
    distribution:
      hash: 541bc8e0cf501c53f8eeae08c3fc8b22b4212cdc
  secretManager:
    type: vault
    namespace: APPSEC
    path: ddd
  host:
    name: secman.mycompany.ru
    port: 443
  resultDesination:
    type: s3
    host:
      name: minio.mycompany.ru
      port: 443
    bucket: appsec-results
```


AppSecJob custom resource

```
yaml  
kind: AppSecJob
```



```
yaml  
kind: AppSecTool
```



ASJ Controller

Magic again!

AST Controller

Job

Pod

Отчёт по артефакту

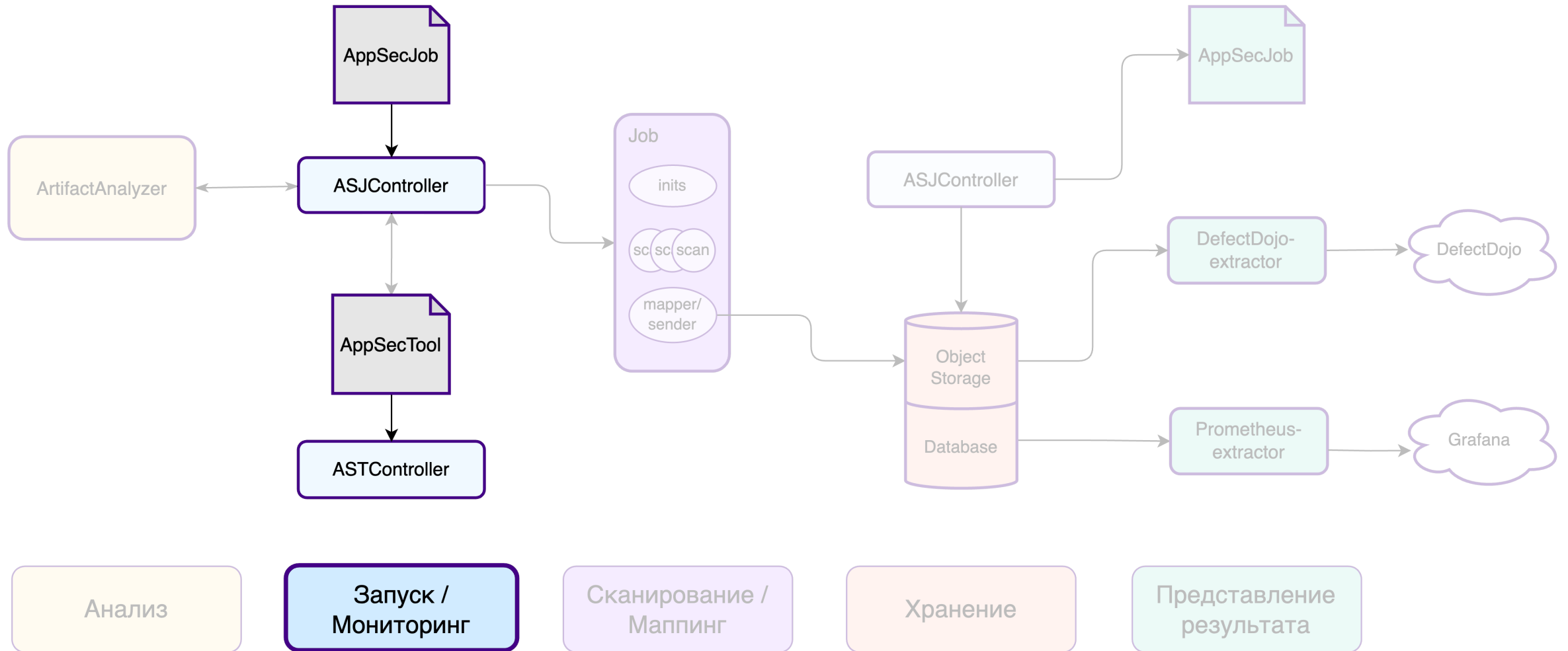




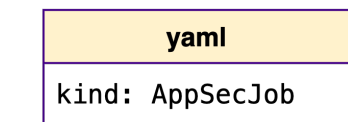
Оркестрация:

управление выбором конфигурацией и запуском
AppSec инструментов для получения отчета
безопасности

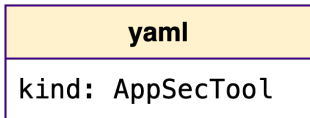
Запуск



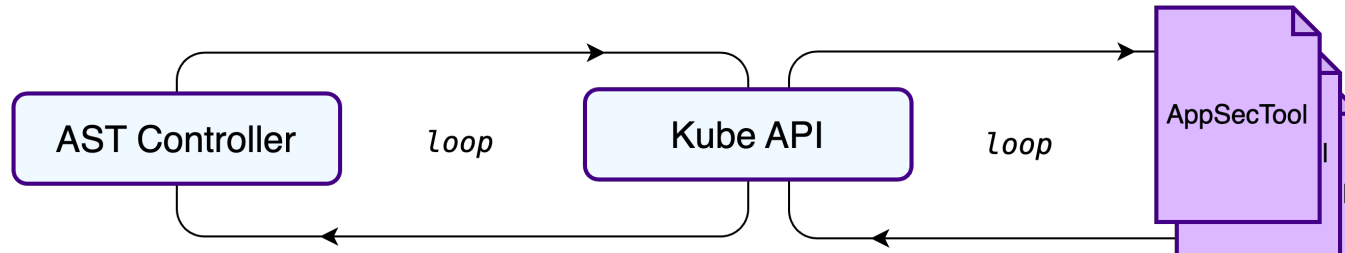
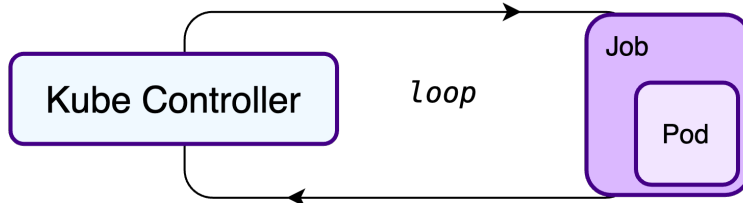
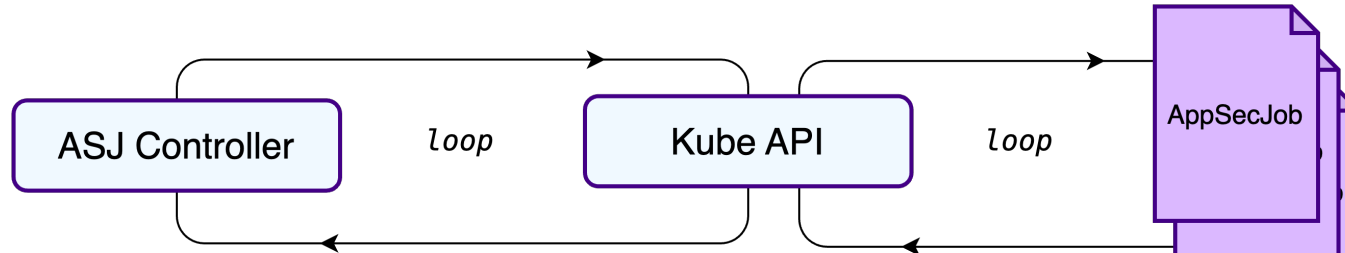
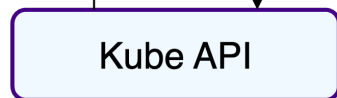
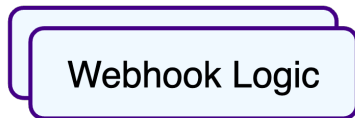
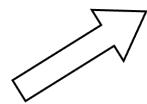
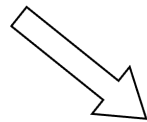
Запуск



developer



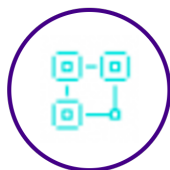
appsec



Клиент



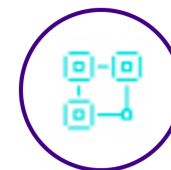
Control Plane



Namespace AppSec

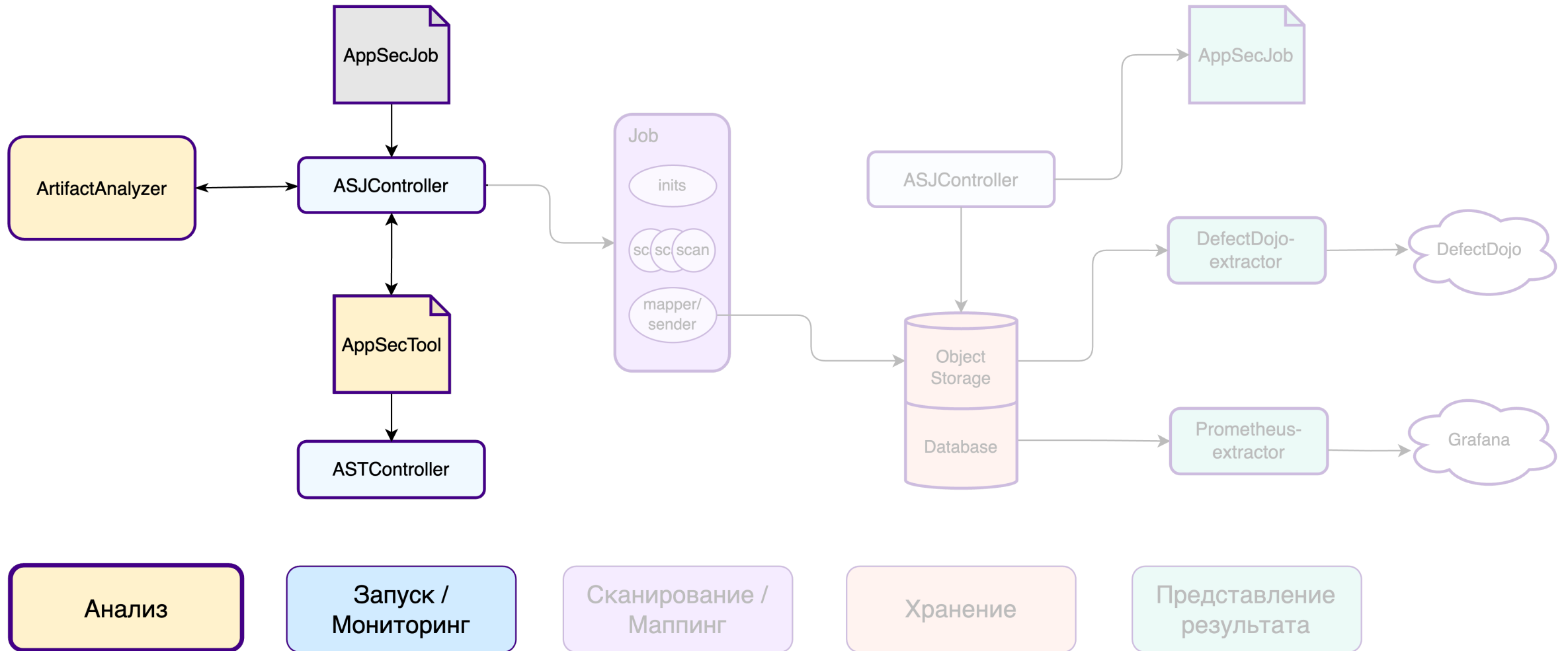


Control Plane



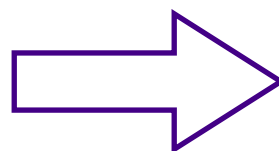
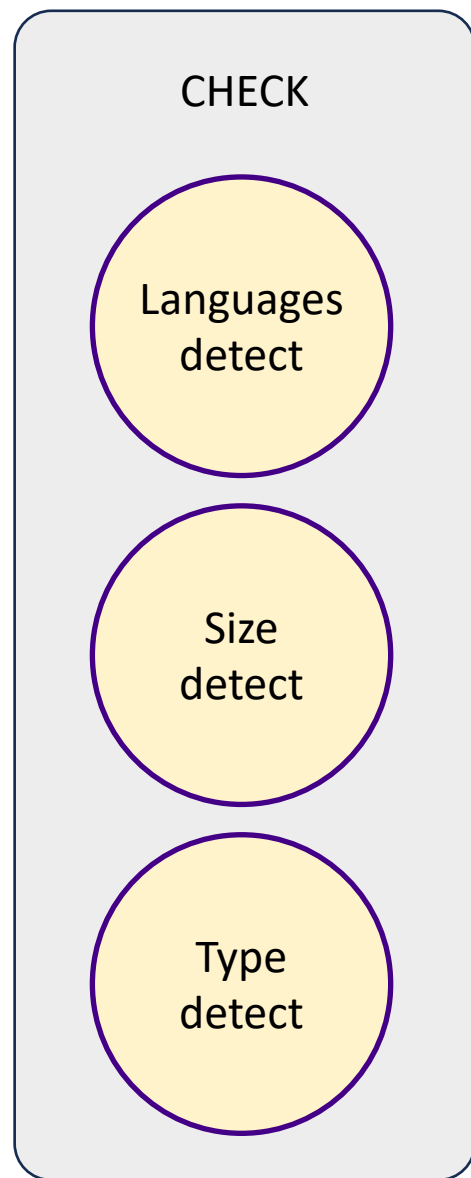
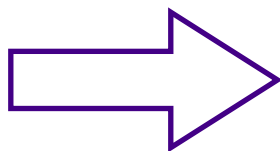
Namespace Клиента

Анализ



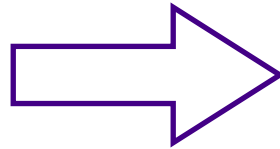
Анализ

Artifact



Анализ

yaml
kind: AppSecTool

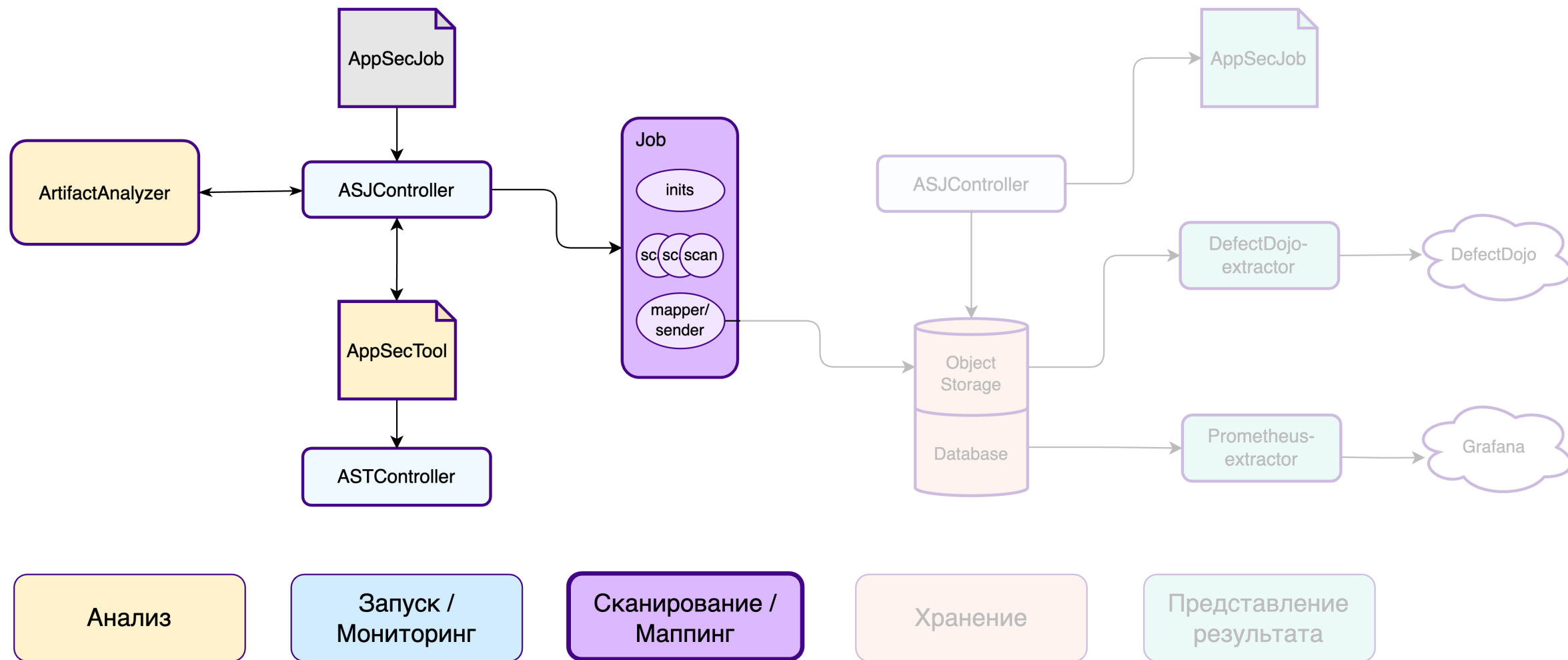


Artifact Info

- Языки
- Размер
- Тип

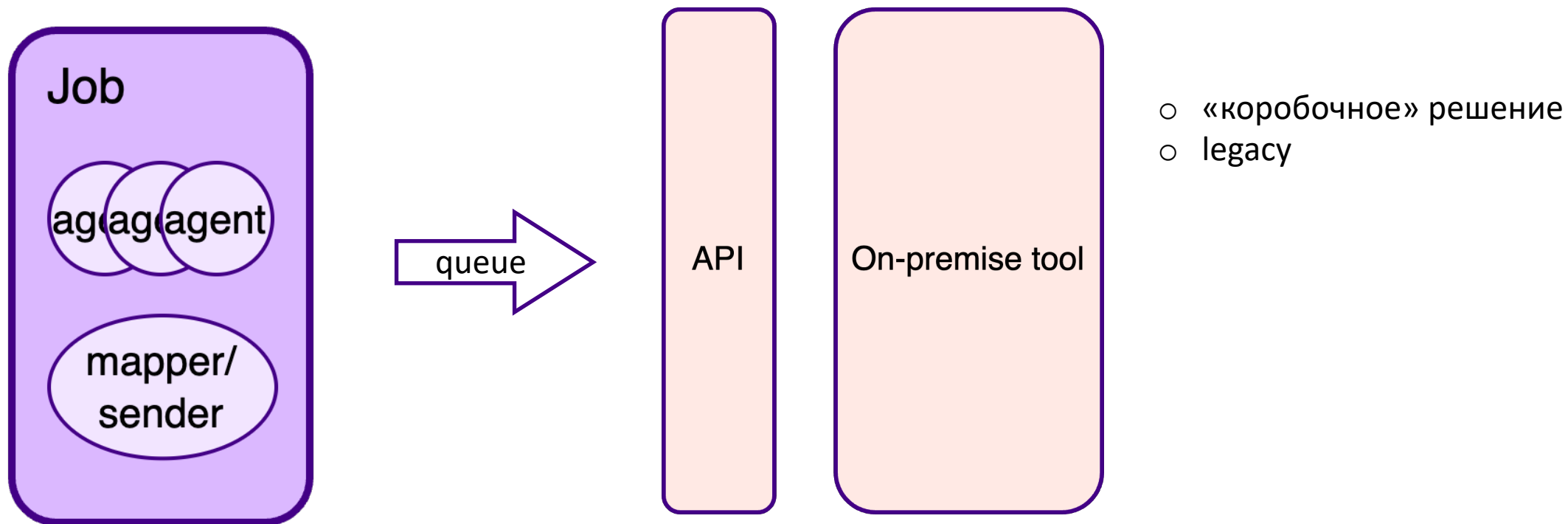
Перечень релевантных инструментов и конфигураций

Сканирование



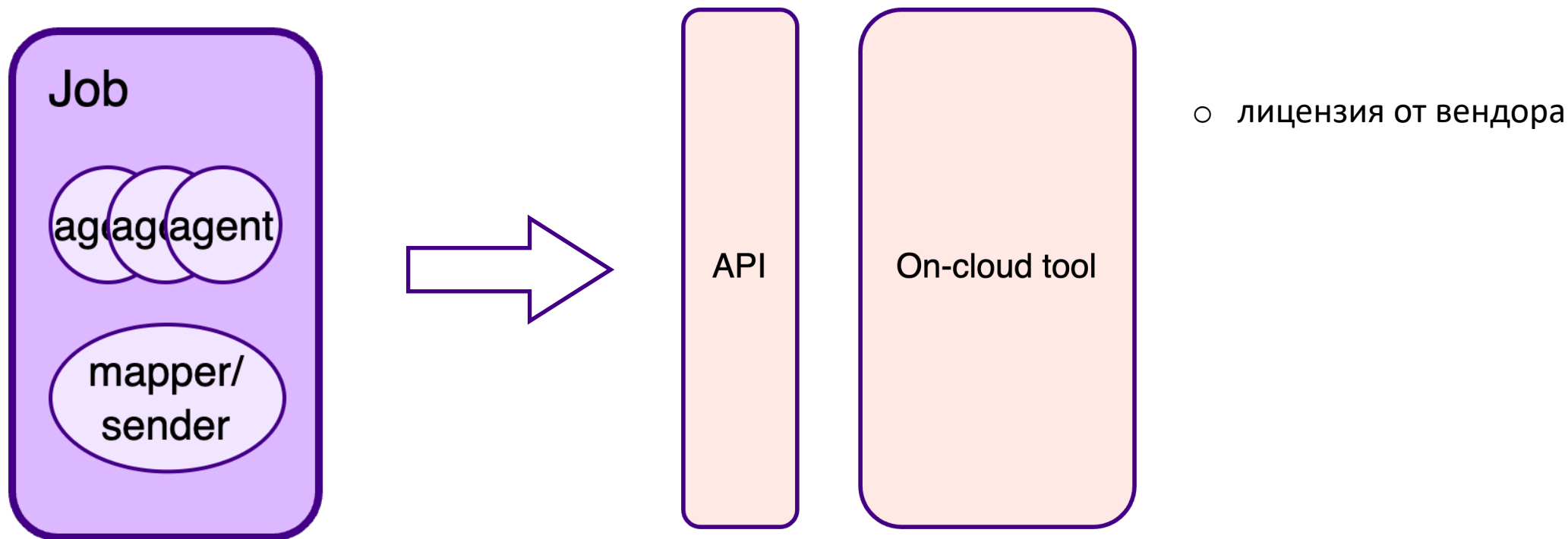
Сканирование

агент к инструменту



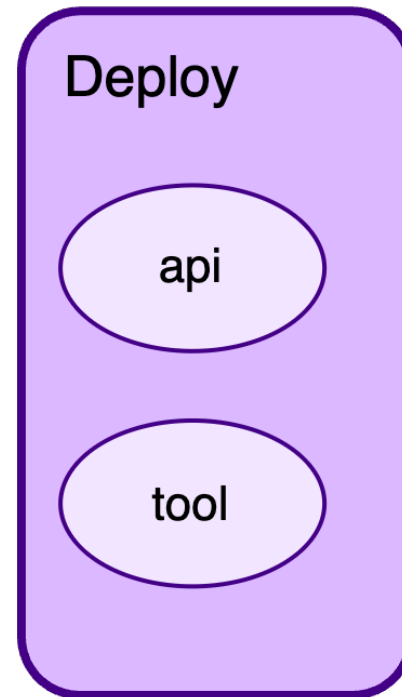
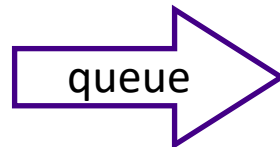
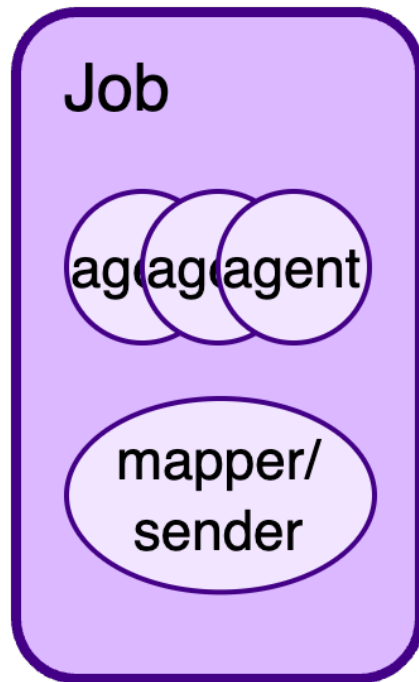
Сканирование

агент к инструменту



Сканирование

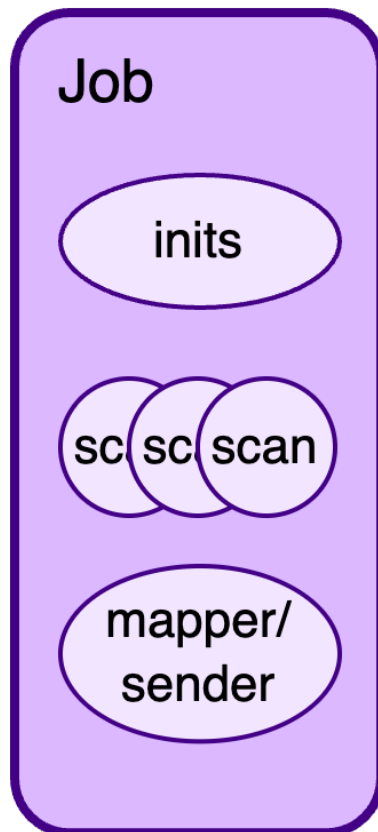
агент к инструменту



- инструмент поддерживает отдельная команда
- реплики по количеству ресурсов

Сканирование

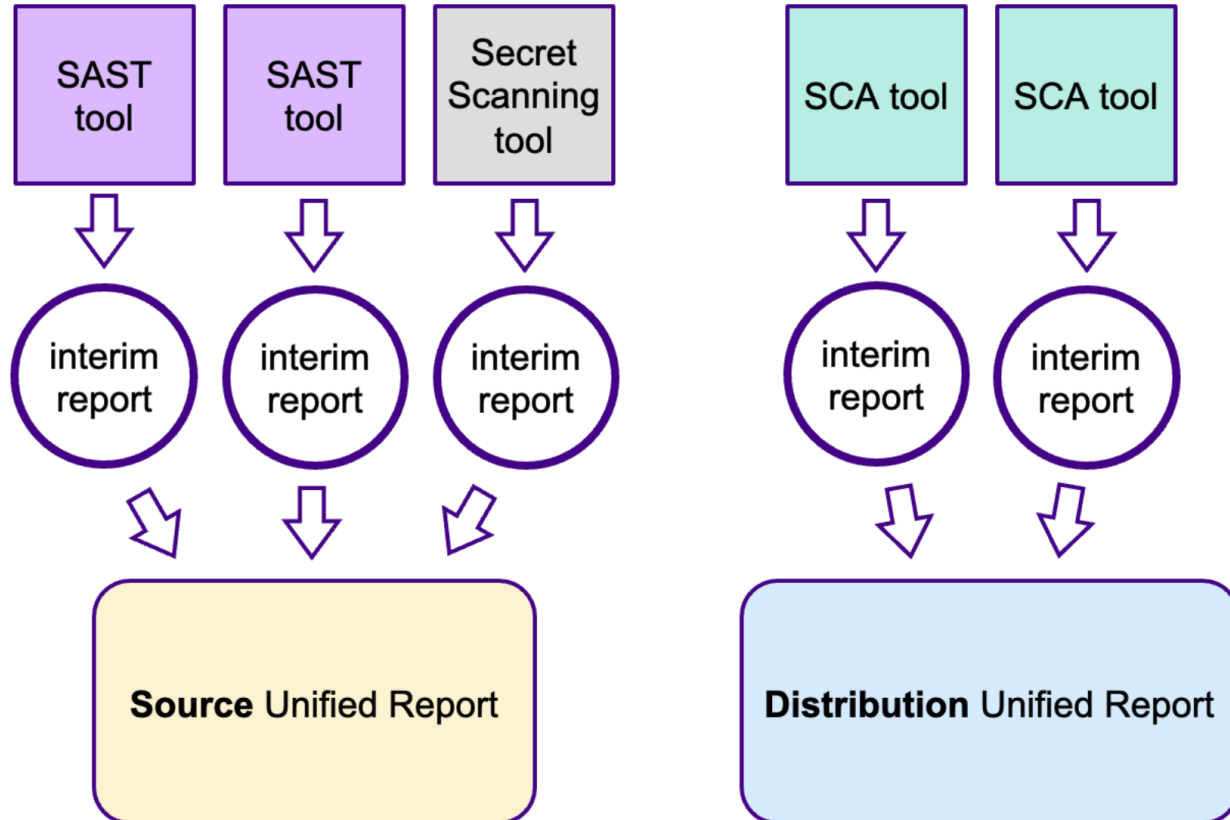
инструмент



- инструмент в контейнере
- получение артефакта в init-контейнере
- выделение необходимого количества ресурсов под конкретный запуск
- нет очередей
- все артефакты сканирования в области работы джобы

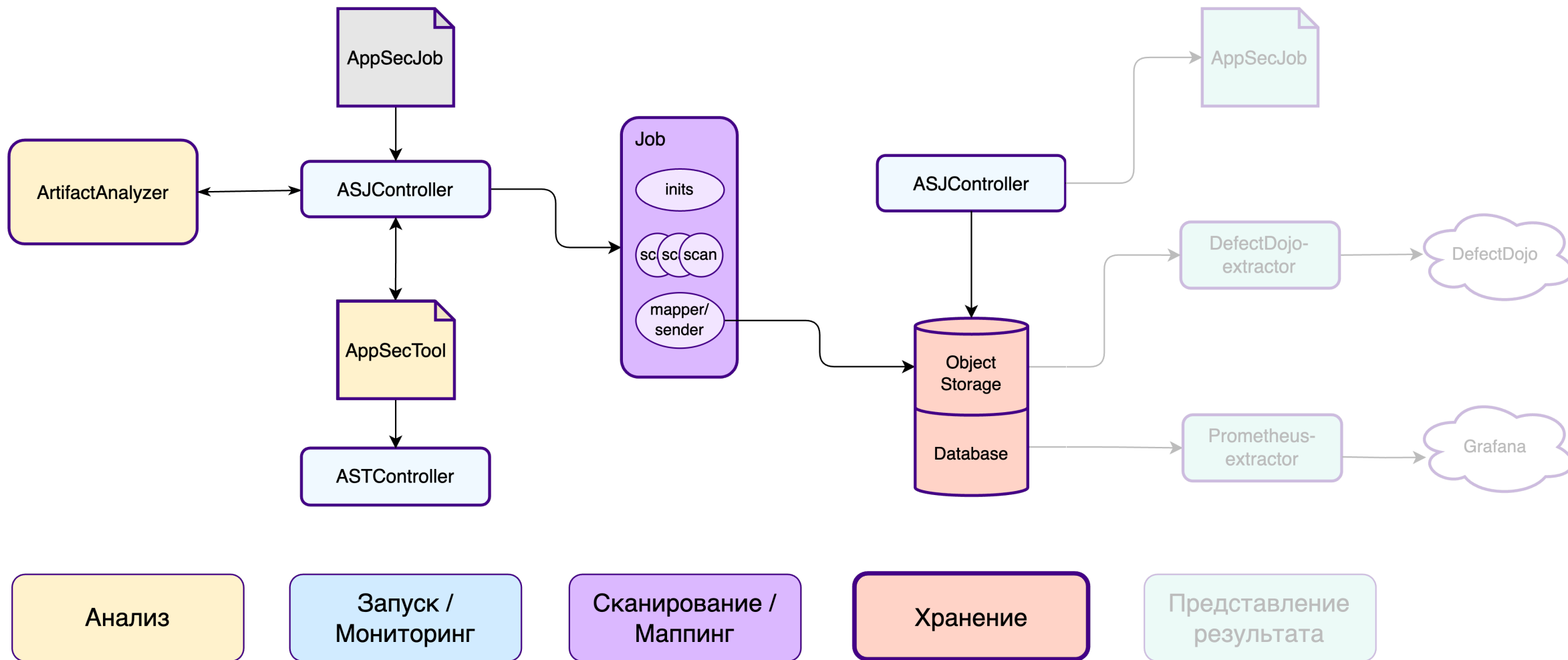
- ? медленнее старт
- ? обновление правил

Мэппинг



- Объединяем сработки из нескольких отчетов
- Ищем пересечение
- Повышаем уверенность в их релевантности
- Все сработки приводим в унифицированный формат

Хранение

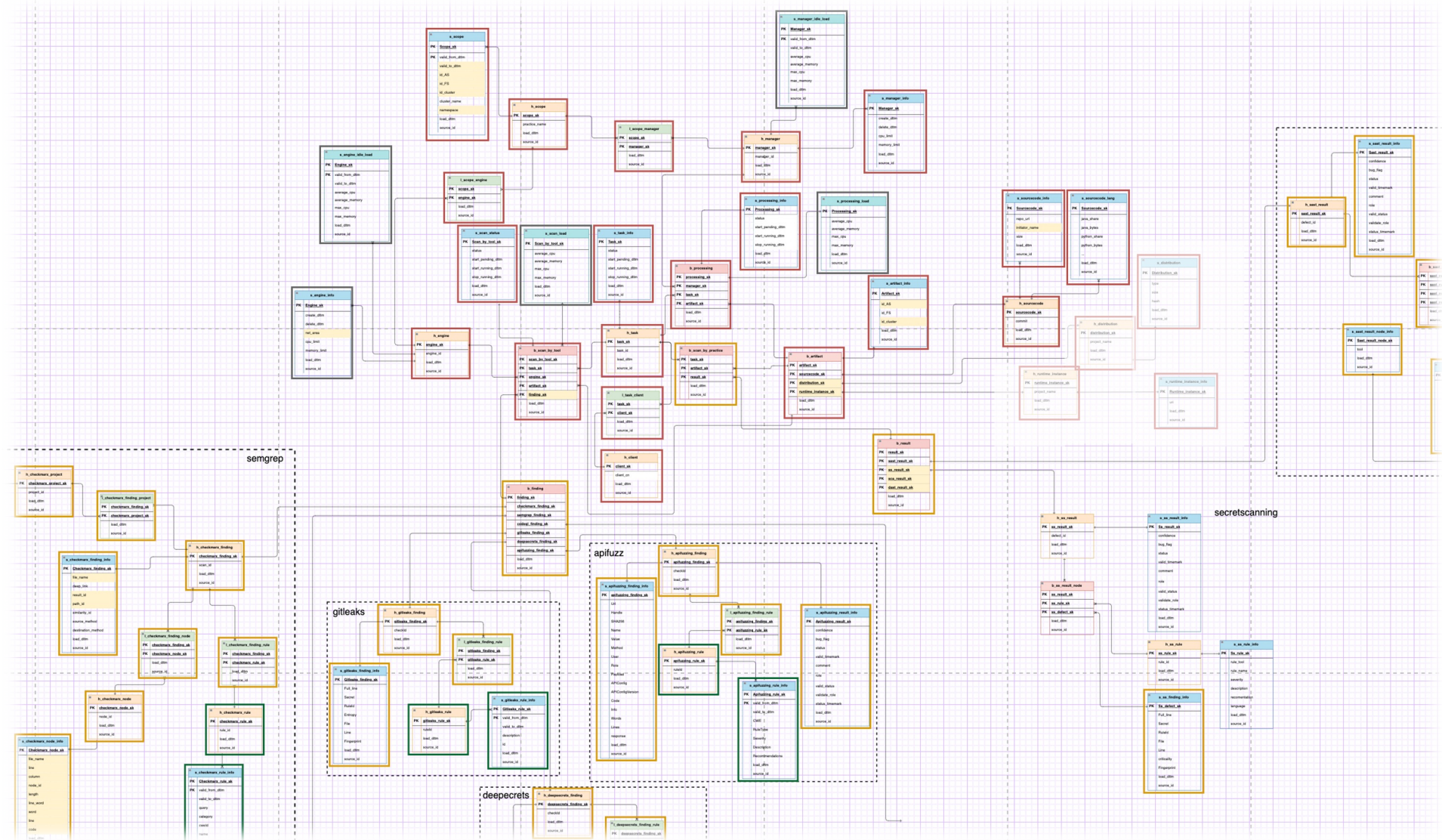


Хранение

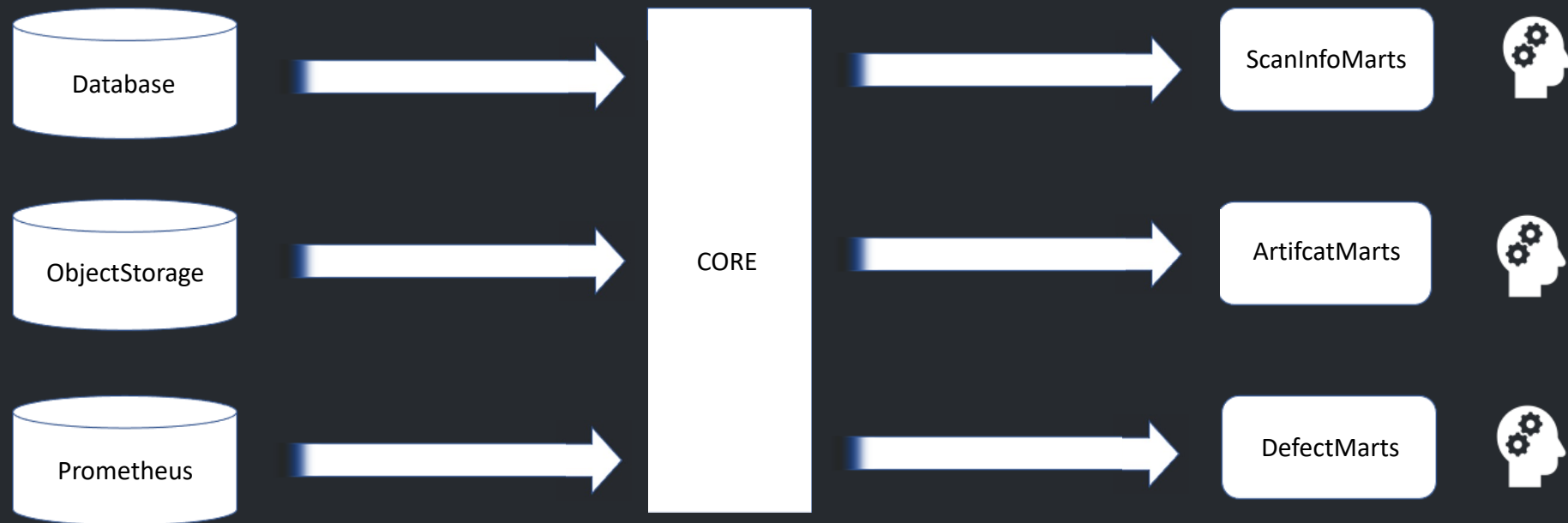
- отражение ключевых бизнес-сущностей
- управление дефектами
- интеграция с системой триажа
- отражение данных аудита и мониторинга

Хранение

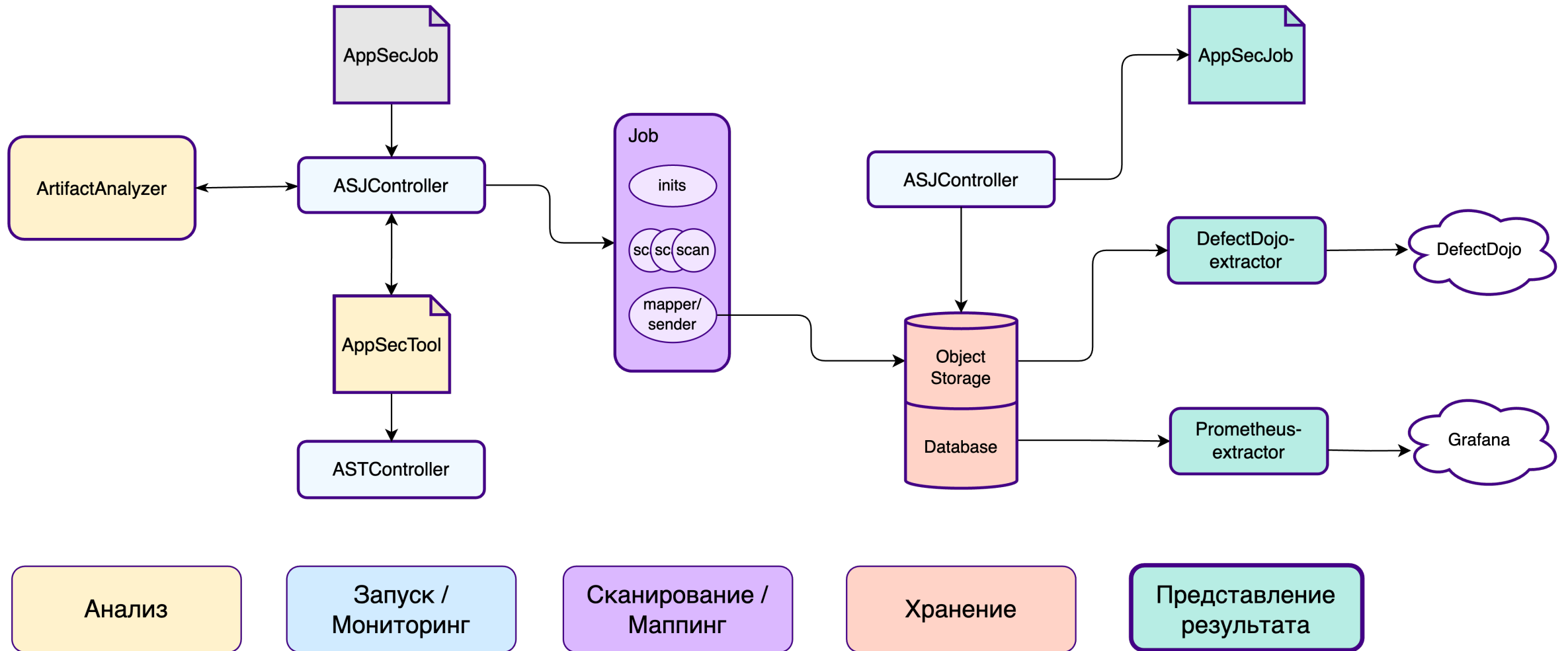
DWH



Хранение



Представление результата



Представление результата

- «мета»-результат в статусе AppSecJob
- дефекты в DefectDojo --> триаж --> интеграция с Jira
- метрики работы инструментов в Prometheus --> построение дашбордов в Grafana

NAME	STATUS	LOW	MEDIUM	HIGH	CRITICAL	TOP 3 VULNERABILITIES
appsecjob-1	So-so	18	5	0	0	1. CWE-79-3 (5.4): Cross-site Scripting (XSS) in User Comments 2. CWE-200 (5.0): Exposure of Sensitive Information in Error Messages 3. CWE-20 (3.1): Improper Input Validation in API Endpoints
appsecjob-2	Feel bad	12	3	1	0	1. CVE-2023-12288 (8.2): Remote Code Execution (RCE) via Unsanitized Input 2. CWE-200 (5.0): Exposure of Sensitive Information to an Unauthorized Actor 3. CWE-26 (4.6): Improper Input Validation in File Uploads
appsecjob-3	Critical	22	2	2	1	1. CVE-2023-67890 (9.1): SQL Injection in User Login Form 2. CVE-2023-54449 (8.6): Remote Code Execution (RCE) via Insecure Deserialization 3. CWE-200 (7.9): Exposure of Sensitive Information to an Unauthorized Actor
appsecjob-4	Great	15	2	0	0	1. CWE-20 (2.8): Improper Input Validation in API Endpoints 2. CWE-200 (3.5): Exposure of Sensitive Information in Error Messages 3. CWE-20 (2.5): Improper Input Validation in File Uploads

Security Quality Gate



JMESPATH

```
attestations:
  - predicateType: "cosign.sigstore.dev/attestation/vuln/v1"
    conditions:
      - all:
          - key: "{{ images[0].attestations[?(@.predicateType ==
'cosign.sigstore.dev/attestation/vuln/v1')].details.vulnerabilities[?(@.severity ==
'Critical')] | length(@) }}"
            operator: GreaterThan
            value: 0
          - all:
          - key: "{{ images[0].attestations[?(@.predicateType ==
'cosign.sigstore.dev/attestation/vuln/v1')].details.vulnerabilities[?(@.severity ==
'High')] | length(@) }}"
            operator: GreaterThan
            value: 2
      - key: "{{ images[0].attestations[?(@.predicateType ==
'cosign.sigstore.dev/attestation/vuln/v1')].predicateType }}"
        operator: Equals
        value: "cosign.sigstore.dev/attestation/vuln/v1"
preconditions:
  all:
    - key: "{{ images[0].attestations[?(@.predicateType ==
'cosign.sigstore.dev/attestation/vuln/v1')].predicateType }}"
      operator: Equals
      value: "cosign.sigstore.dev/attestation/vuln/v1"
```

```
validate:
  message: |
    Образ не прошел проверку из-за следующих уязвимостей:
    - Критические: {{ images[0].attestations[?(@.predicateType == 'cosign.sigstore.dev/attestation/vuln/v1')].details.vulnerabilities[?(@.severity ==
'Critical')] | length(@) }}
    - Высокие: {{ images[0].attestations[?(@.predicateType == 'cosign.sigstore.dev/attestation/vuln/v1')].details.vulnerabilities[?(@.severity == 'High')]
| length(@) }}
    - Средние: {{ images[0].attestations[?(@.predicateType == 'cosign.sigstore.dev/attestation/vuln/v1')].details.vulnerabilities[?(@.severity ==
'Medium')] | length(@) }}
    - Низкие: {{ images[0].attestations[?(@.predicateType == 'cosign.sigstore.dev/attestation/vuln/v1')].details.vulnerabilities[?(@.severity == 'Low')] |
length(@) }}
```

Сегодня рассмотрели

- что есть приложение
- почему devSECops это всё ещё сложно
- CR как интерфейс для пользователя
- как работает k8s-оператор
- что делать с приложением до скана
- что делать с отчётами после скана
- что делать с инструментами во время скана



Overall профит



...> **управление на уровне абстракций k8s**

- разгрузка очередей на сканирование
- выбор инструментов на основе характеристик артефакта
- сканирование на ресурсах разработчика
- унифицированный результат



Overall профит

- управление на уровне абстракций k8s



…→ **разгрузка очередей на сканирование**

- выбор инструментов на основе характеристик артефакта
- сканирование на ресурсах разработчика
- унифицированный результат



Overall профит

- управление на уровне абстракций k8s
- разгрузка очередей на сканирование



…→ **выбор инструментов на основе характеристик артефакта**

- сканирование на ресурсах разработчика
- унифицированный результат



Overall профит

- управление на уровне абстракций k8s
- разгрузка очередей на сканирование
- выбор инструментов на основе характеристик артефакта



…→ **сканирование на ресурсах разработчика**

- унифицированный результат



Overall профит

- управление на уровне абстракций k8s
- разгрузка очередей на сканирование
- выбор инструментов на основе характеристик артефакта
- сканирование на ресурсах разработчика



…→ **унифицированный результат**



Вопросы?

Алена Жилина

DevSecOps-инженер

Вячеслав Давыдов

DevSecOps-инженер