Алексей Жуков
лидер продуктовой практики AppSec

Комплексный подход к инструментарию AppSec

От выбора до развертывания в проде

01

Современная разработка

Особенности разработки

- Большие объемы кода
- Разнообразие языков и технологий
- Кадровый дефицит при видимой массовости
- Повсеместное использование сторонних компонентов
- Высочайшие темпы для снижения time to market
- Общая недооценка темы ИБ применительно к R&D

В этой ситуации появление уязвимостей в коде видится неизбежным.
Чтобы вовремя их выявлять и устранять, необходимо проводить анализ кода на уязвимости

Классические пять стадий

1 Отрицание

Какие еще «хакеры», какие «уязвимости»??? Меньше фильмов смотреть надо. Да и не может тут быть никаких уязвимостей...

2 Гнев

Да я в разработке 100500 лет, про какие еще «уязвимости» вы мне тут рассказываете???!!!

3 Торг

Да тут нормально все, никто до вас этого не видел и еще двадцать лет не увидит. И вообще... *(далее список отговорок)*

4 Депрессия

Ух... Это ж сколько теперь переделывать-то... И где же брать ресурсы?

5 Принятие

Да, пожалуй, тут придется что-то срочно исправлять

AppSec —
это, конечно, команда

410 000
разработчиков

3 342
специалиста по ИБ

8 508
security champions

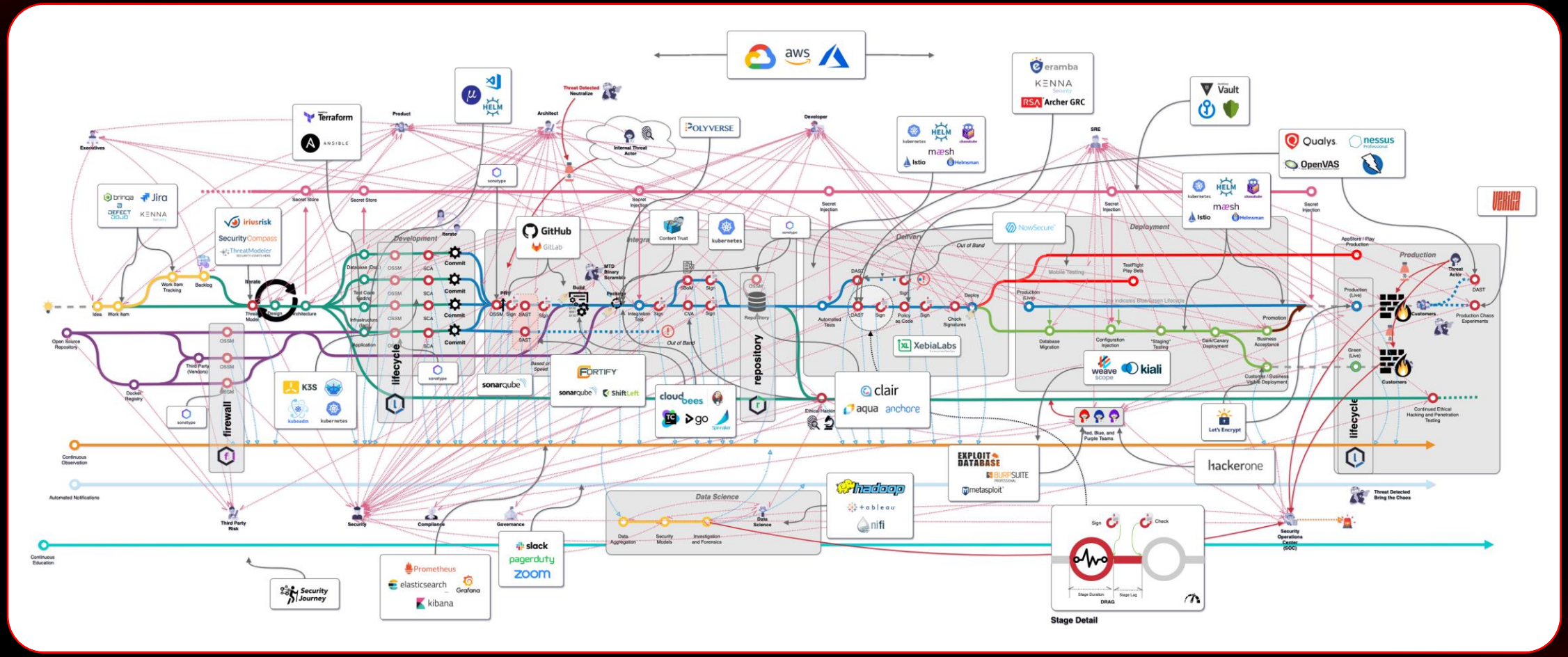
1/122 → 1/35

BSIMM 13

02

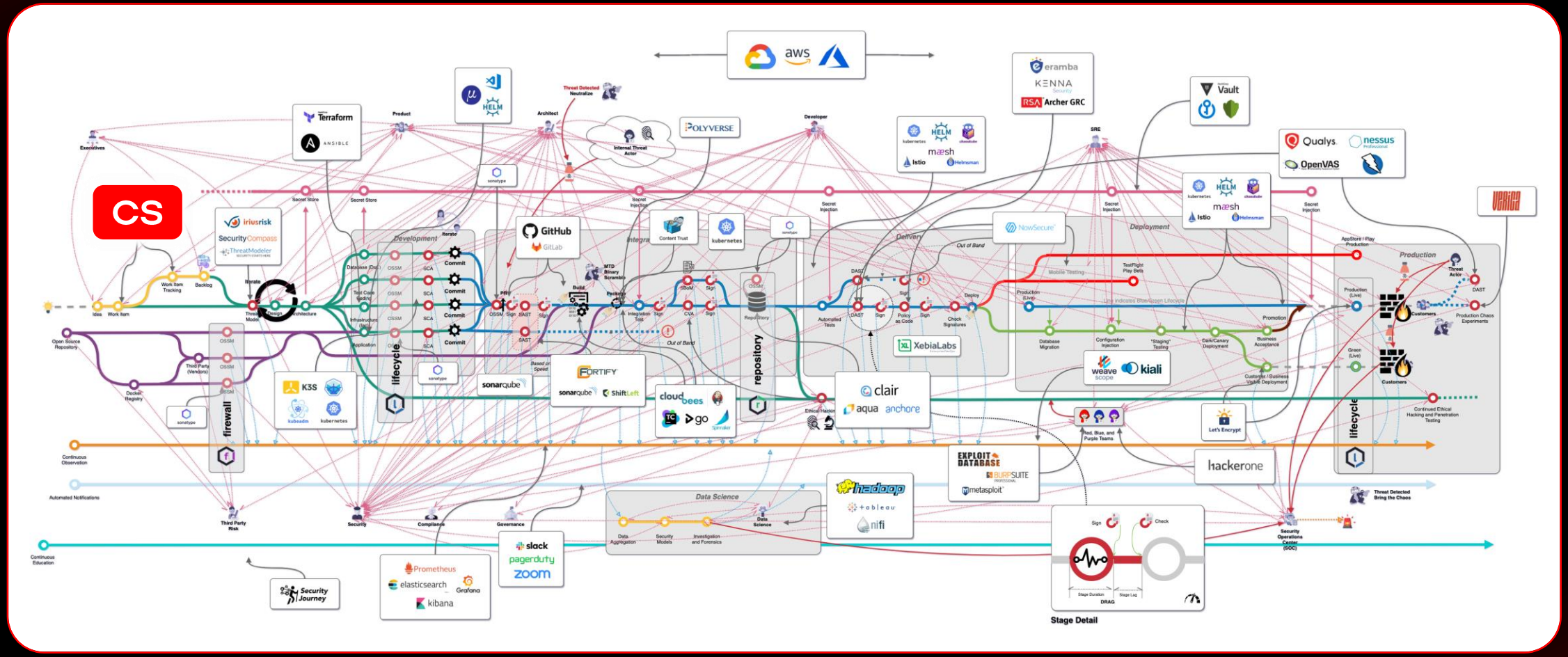
Но AppSec — это еще и инструменты

А точнее, целый набор



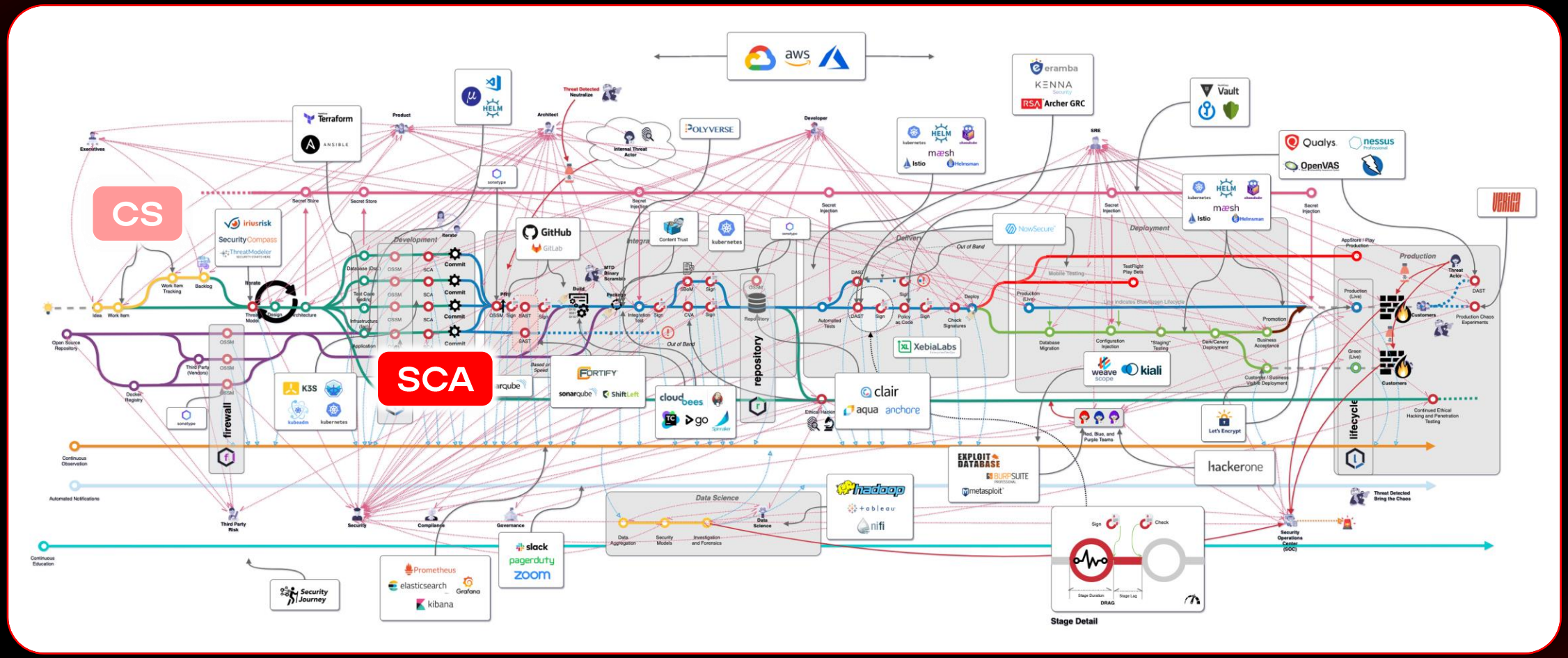
Sonatype DevSecOps Reference Architecture

Начнем с инструментов



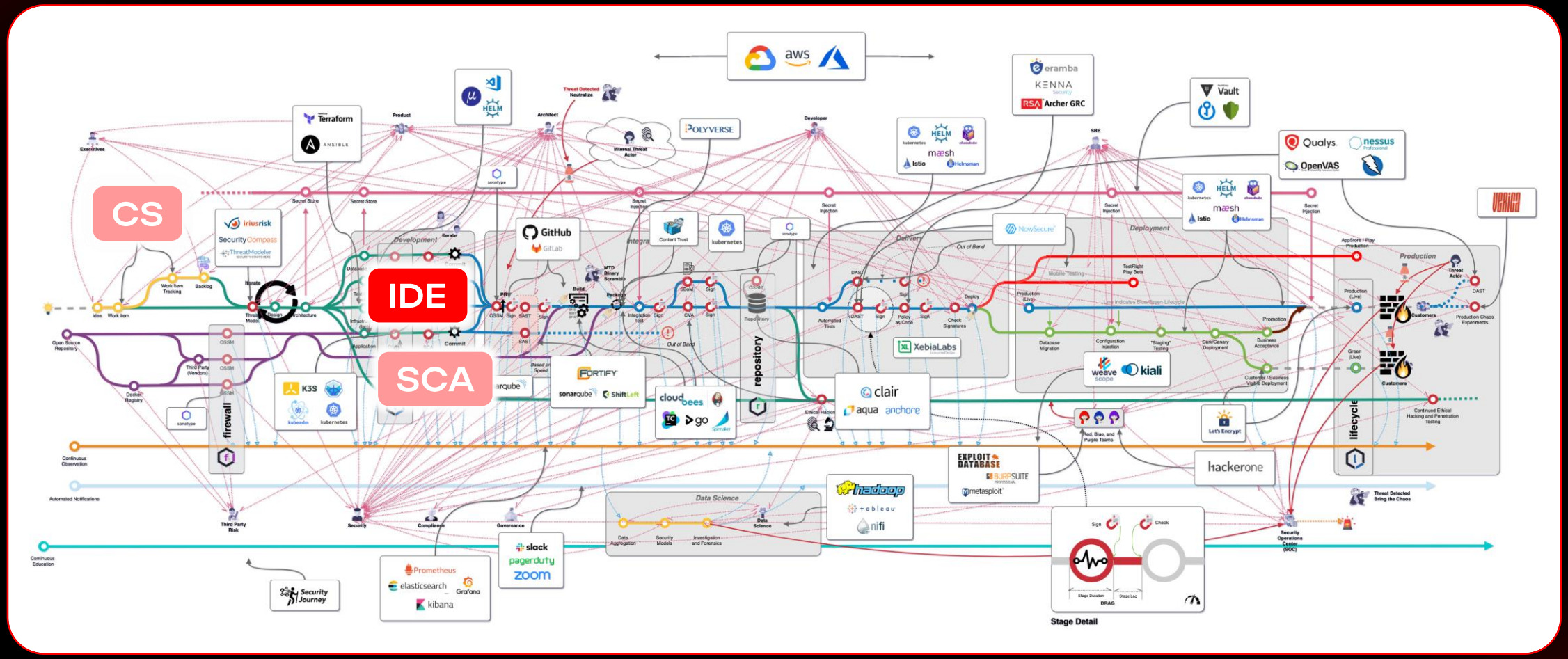
Кода еще нет, а безопасный инструментарий сборки уже нужен

Безопасность стороннего ПО



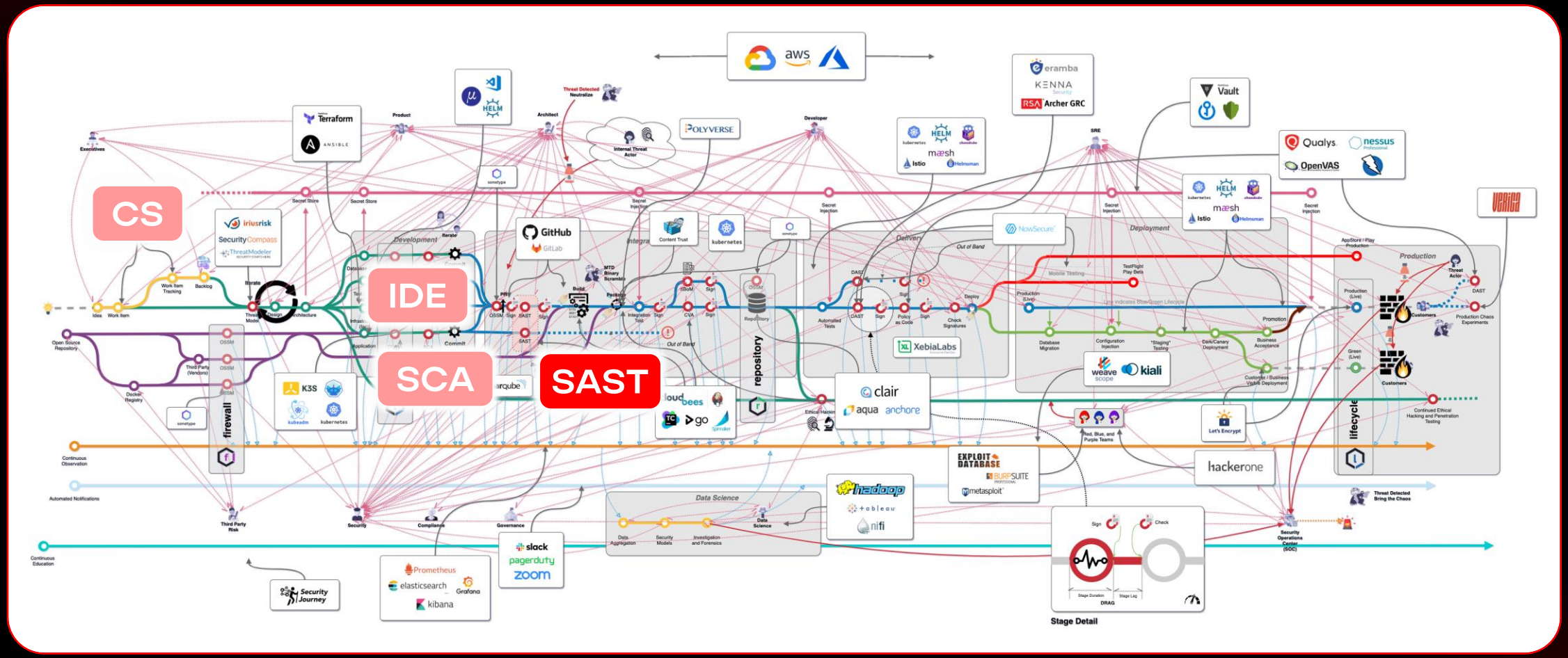
Сторонние библиотеки и фреймворки используют почти все. Нужен анализ на уязвимости

Плагины для IDE



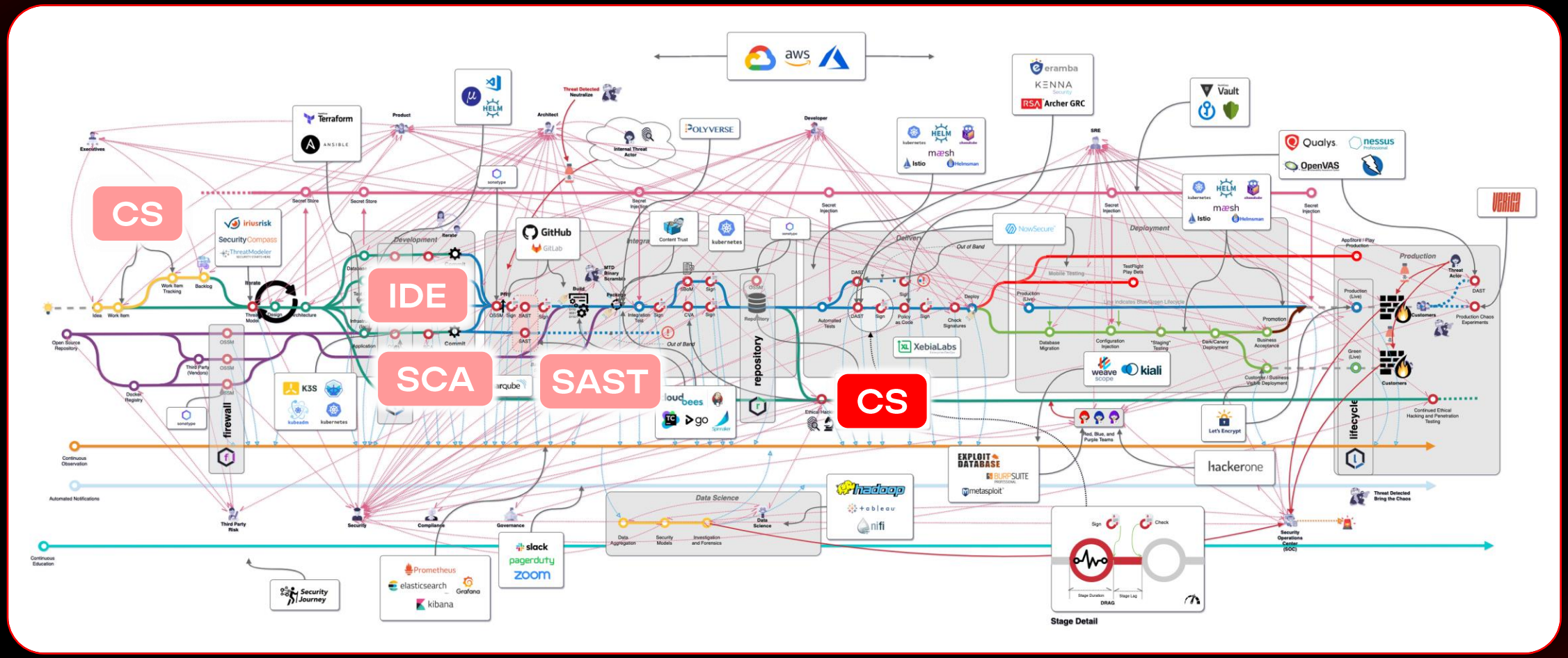
Устраняем уязвимости, не доводя их до коммита

Статический анализ кода



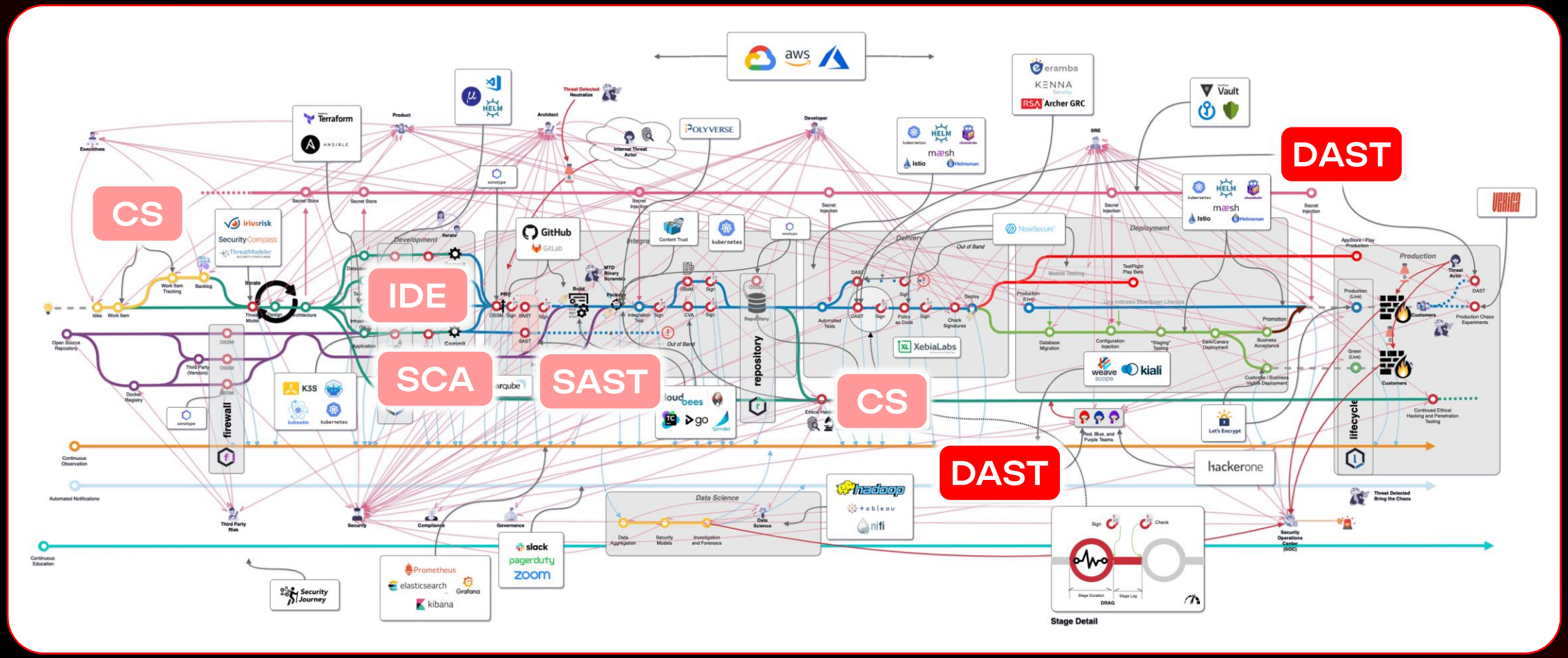
Первое правило статического анализа: никаких правил

Контейнеры: развертывание



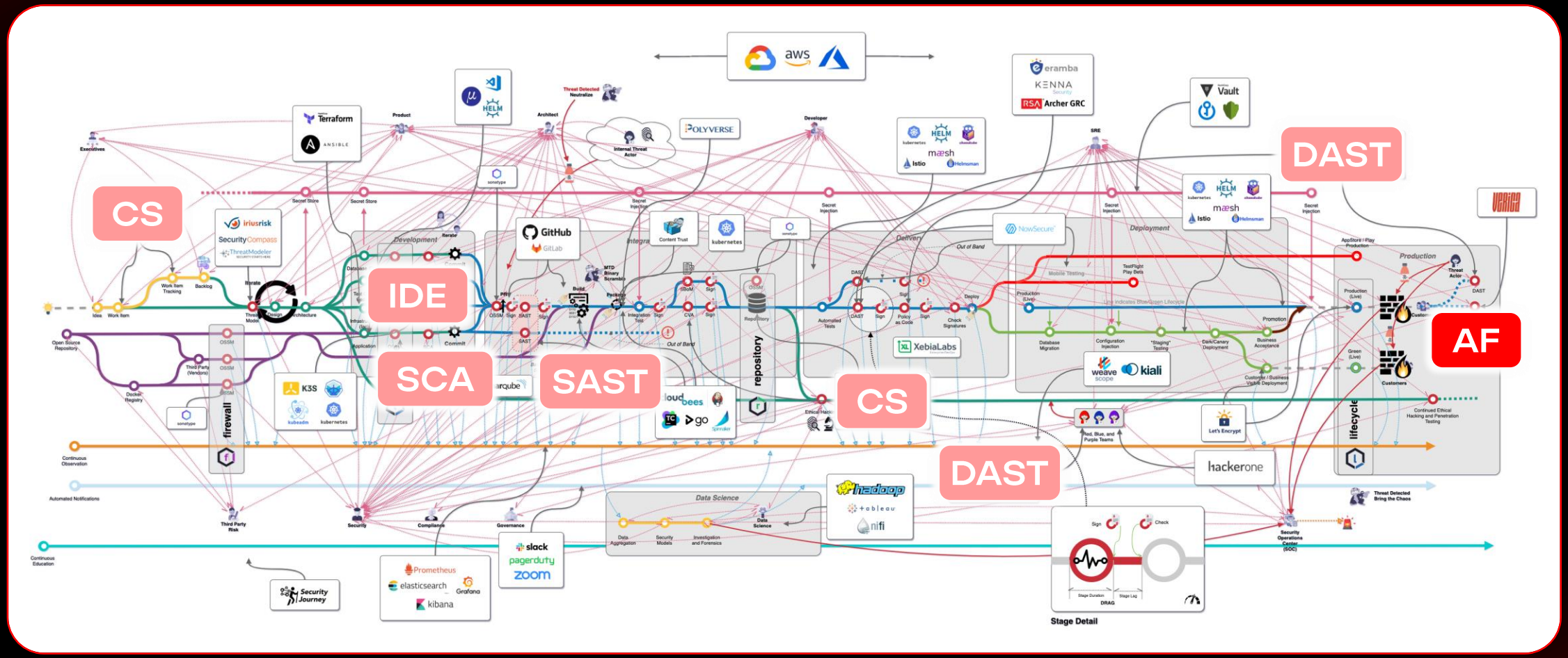
Интеграция с API оркестратора позволяет контролировать действия, выполняемые в кластере

Динамический анализ



Анализ запущенного приложения глазами хакера

Защита приложения в «проде»



Решения класса web application firewall позволяют защитить приложение в проде

Кстати, еще кое-что о «проде»

69%

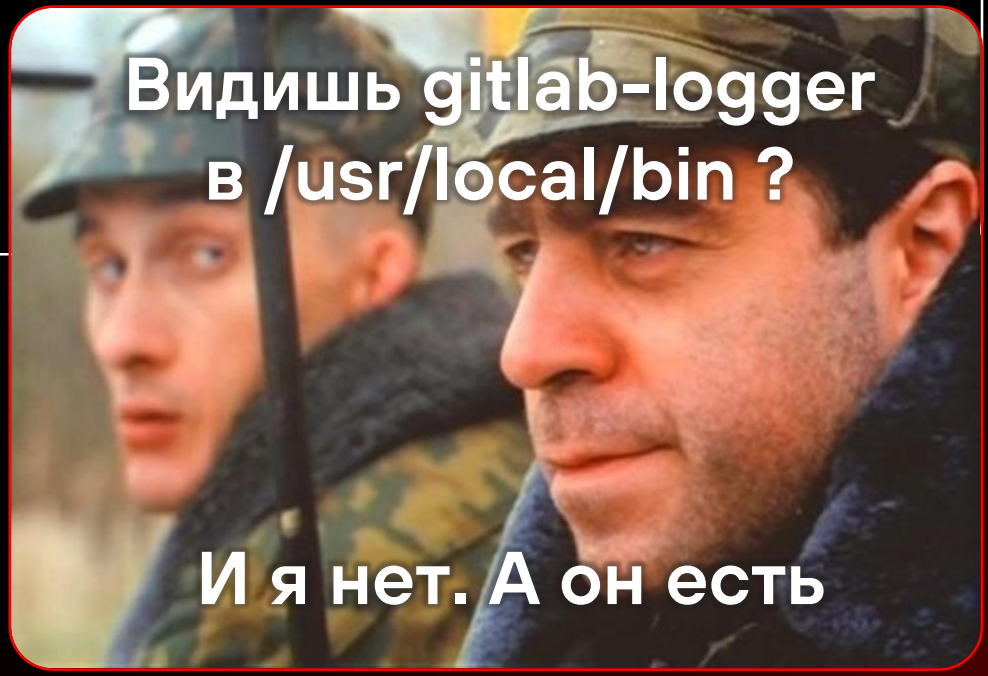
Уровень внедрения Kubernetes среди организаций во всем мире

31%

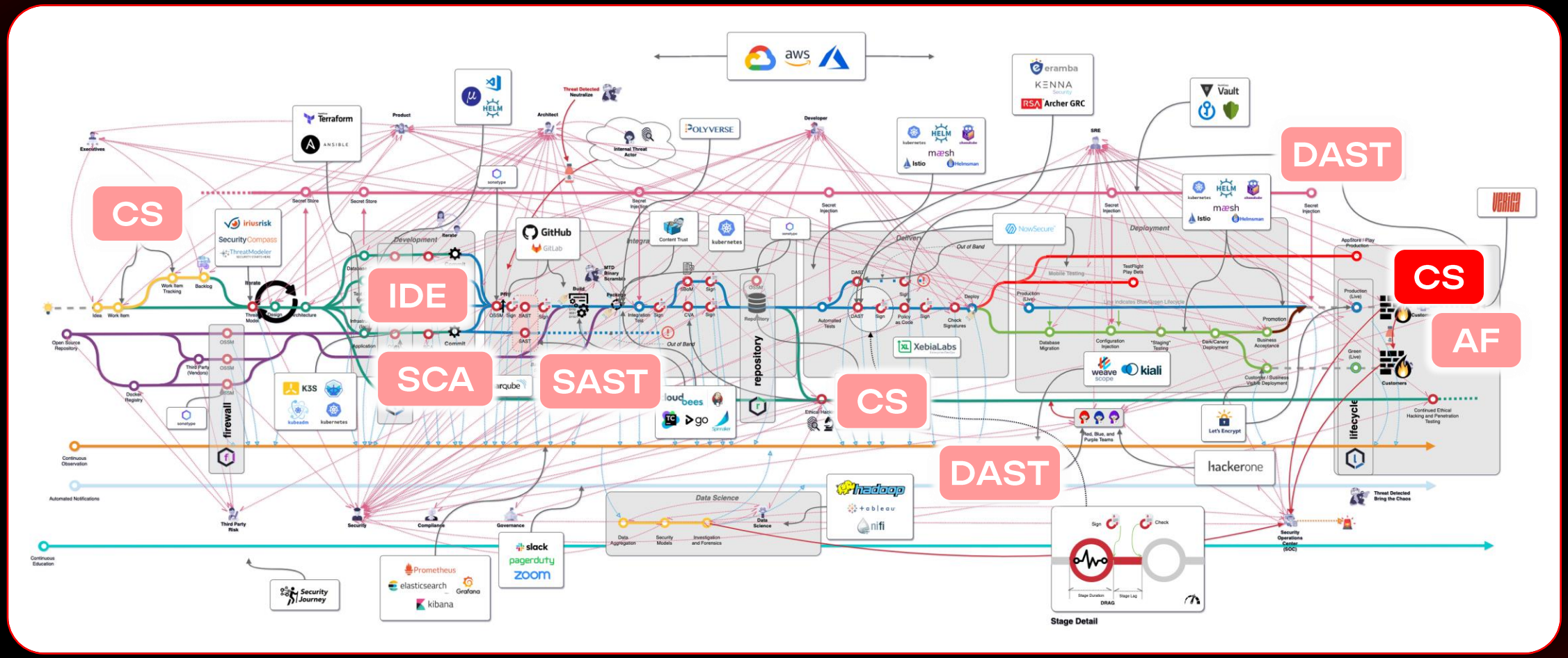
Доля разработчиков в мире, использующих Kubernetes

Контейнеры — это отдельный мир

```
root@k8s-04:~# ps -ax | grep gitlab-logger
  12719 ?        Sl   229:51 /usr/local/bin/gitlab-logger /var/log/gitlab-shell
  18229 ?        Sl   414:34 /usr/local/bin/gitlab-logger /var/log/gitlab
2788169 pts/1    S+     0:00 grep gitlab-logger
root@k8s-04:~# ls -la /usr/local/bin
total 8
drwxr-xr-x  2 root root 4096 Jan 12  2023 .
drwxr-xr-x 10 root root 4096 Jan 12  2023 ..
root@k8s-04:~#
```

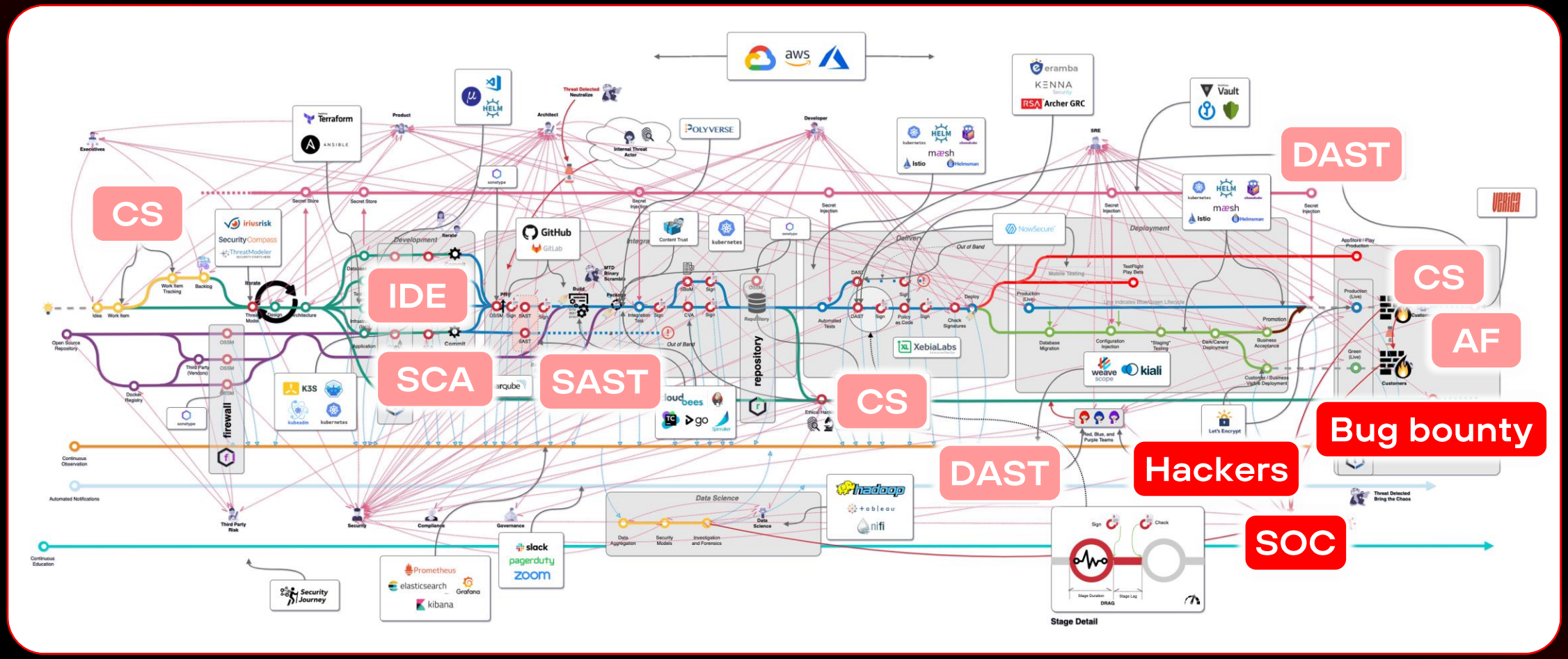


Контейнеры: рантайм

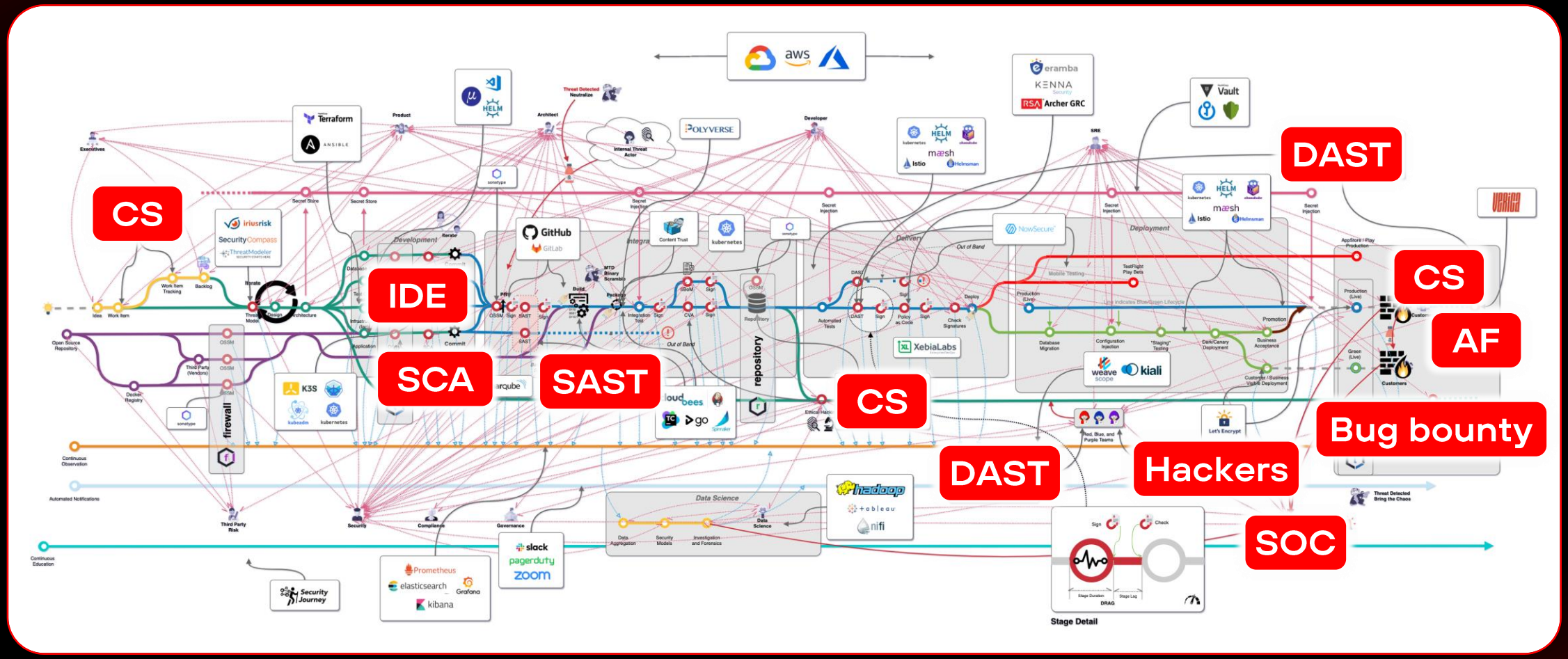


«Классические» инструменты кибербезопасности слабо заточены на работу с контейнерами

Но не только инструменты



Все достаточно позитивно



Обеспечивается комплексный подход к разработке с помощью инструментов безопасности

t.me/positive_technologies

habrahabr.ru/company/pt

t.me/POSIdev

Спасибо!