Supply chain security. Позитивный опыт

Максим Залысин | Positive Technologies

DevOps Conf 2023

О спикере

Максим Залысин

- Больше 15 лет в IT
  - Эксплуатация
  - Разработка
  - Информационная безопасность
- Последние 5 лет руководство командами
- Head of DevOps в Positive Technologies
- Евангелист DevOps-практик

О Positive Technologies

- Больше 20 коробочных и WEB-приложений
- Больше 6000 репозиториев исходного кода
- Почти 800 человек в направлениях разработки
- 25 инженеров в команде DevOps

О докладе

- Результат работы команды DevOps
- 3 части
  - Цепочка поставок приложений
  - Угрозы в цепочке поставок
  - Безопасность цепочки поставок
- Речь без пафоса, слайды без усложнений

Цепочка поставок приложений

У лукоморья дуб зелёный;

Златая цепь на дубе том:

И днём и ночью кот учёный

Всё ходит по цепи кругом.

Александр Сергеевич Пушкин,
«Руслан и Людмила»

Цепочка поставок приложений

Цепочка поставок приложений

Цепочка поставок приложений

Цепочка поставок приложений

Цепочка поставок приложений

Угрозы в цепочке поставок

В ожидании грозного события
все другие события и
нежданные перемены — ничто.

Чарльз Диккенс,
«Дэвид Копперфильд»

Угрозы в цепочке поставок

Угрозы в цепочке поставок

DEV

- Ошибки в исходном коде
- Подмена зависимостей
- Утечка секретов
- Компрометация конвейера

Угрозы в цепочке поставок

BUILD

- ➡ Подмена зависимостей
- ➡ Утечка секретов
- ➡ Компрометация конвейера

Угрозы в цепочке поставок

TEST

- ➡ Утечка секретов
- ➡ Компрометация конвейера

Угрозы в цепочке поставок

DELIVERY

➡ Подмена пакета приложения

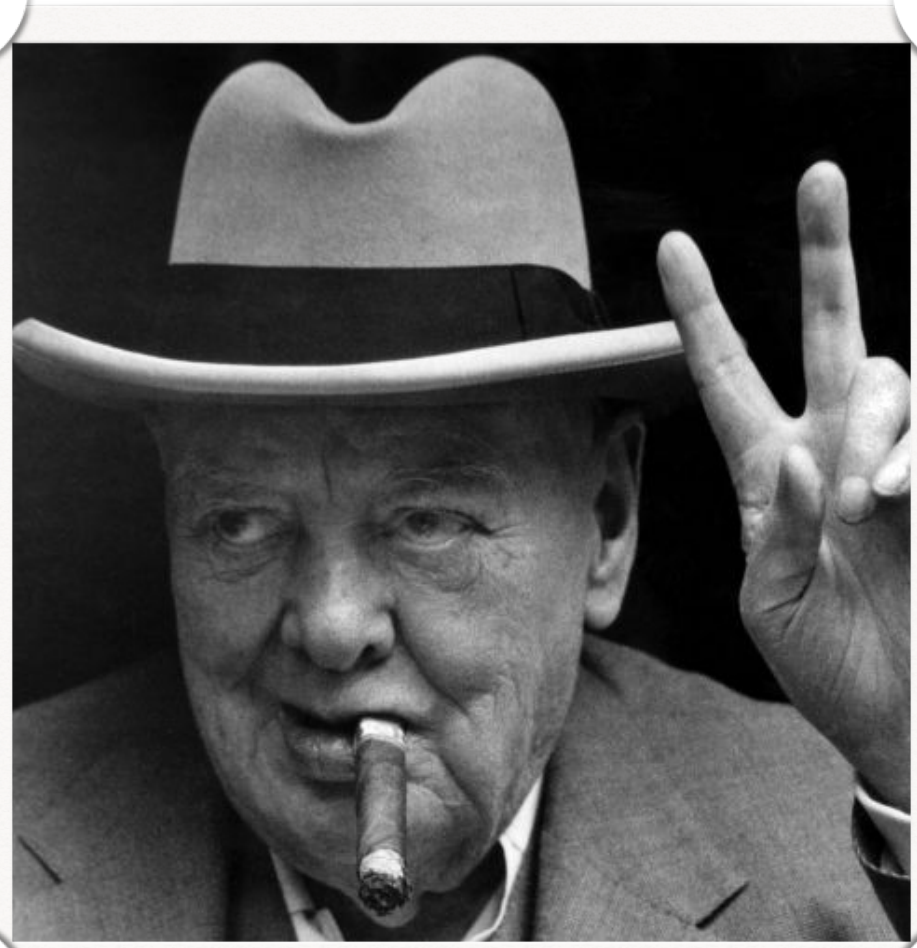
Угрозы в цепочке поставок

- ➡ Ошибки в исходном коде
- ➡ Подмена зависимостей
- ➡ Утечка секретов
- ➡ Компрометация конвейера
- ➡ Подмена пакета приложения

Безопасность цепочки поставок

За безопасность необходимо платить, а за ее отсутствие расплачиваться.

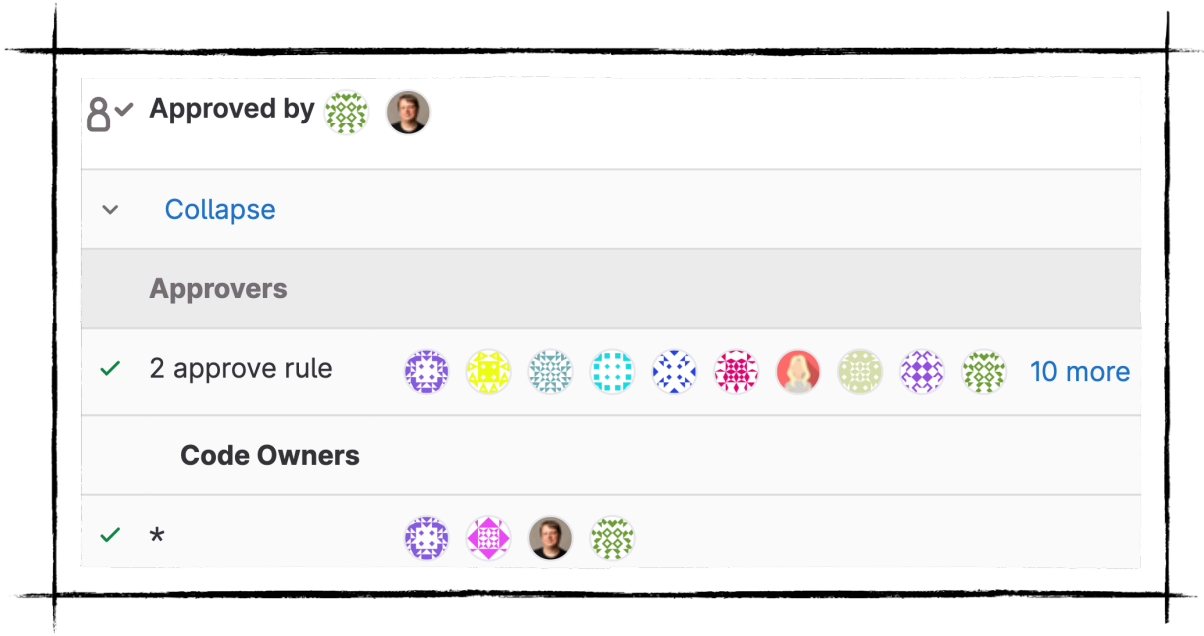
Уинстон Черчилль



Безопасность цепочки поставок

Угроза: Ошибки в исходном коде

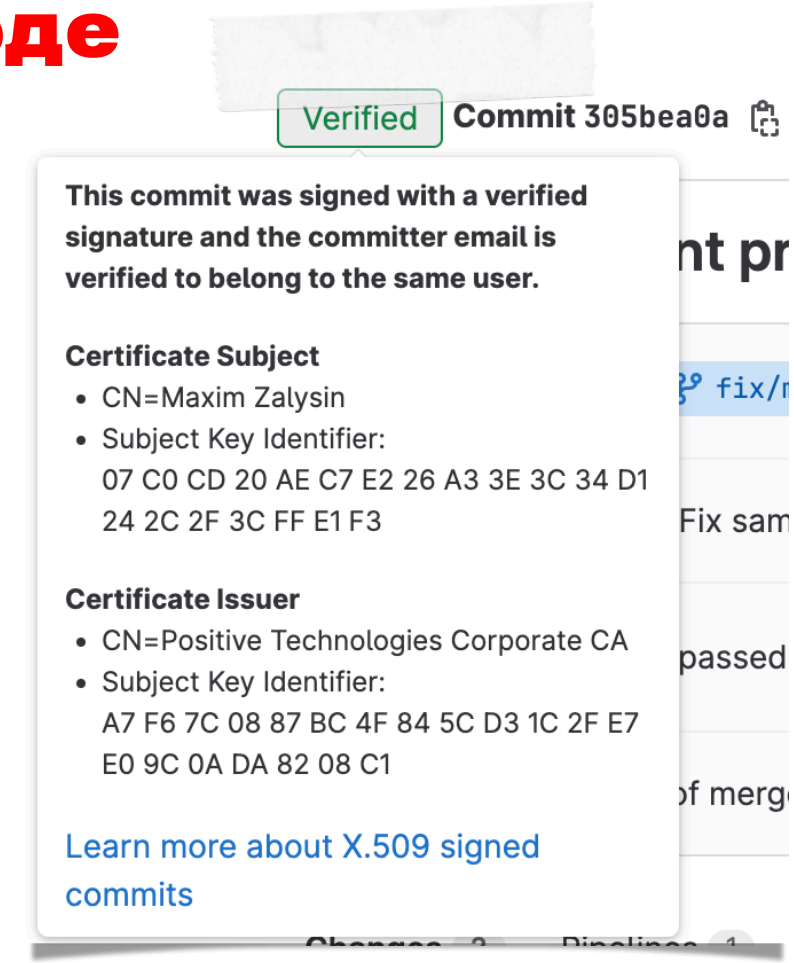
➡ Минимум 2 ревьювера в репозитории



Безопасность цепочки поставок

Угроза: Ошибки в исходном коде

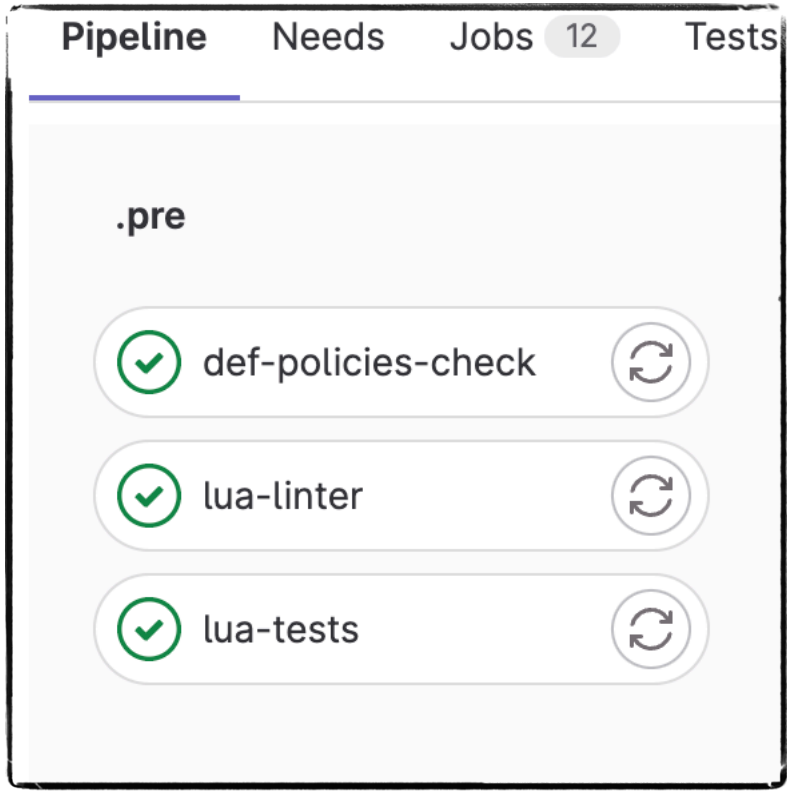
- Минимум 2 ревьювера в репозитории
- **Подписание коммитов персональным сертификатом X.509 и верификация внутренним CA**



Безопасность цепочки поставок

Угроза: Ошибки в исходном коде

- Минимум 2 ревьювера в репозитории
- Подписание коммитов персональным сертификатом X.509 и верификация внутренним CA
- **Проверка кода: линтеры, SAST и тестирование**



Безопасность цепочки поставок

Угроза: Подмена зависимостей

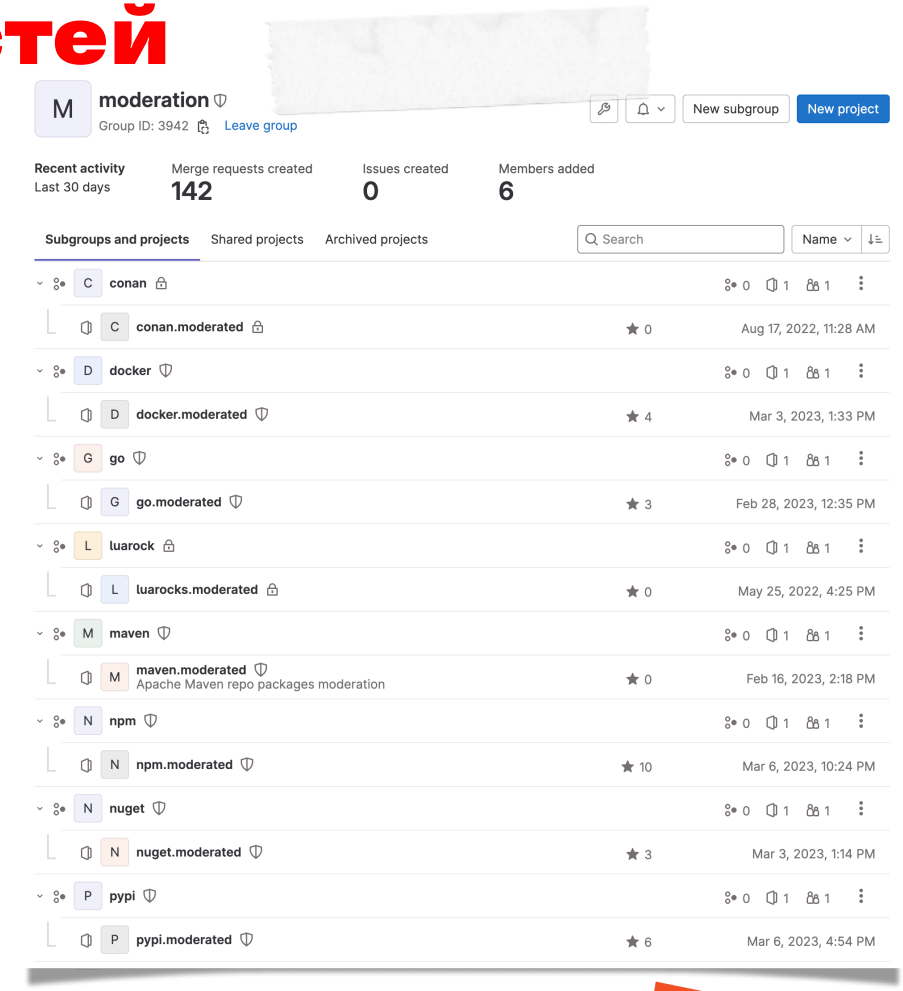
- Фиксация зависимостей в lock-файле, включая версии

```
github.com/jpillora/backoff v1.0.0/go.mod h1:J/6gKK9jxlEcS3zixgDgUAsiuZ7yrSoa/FX5e0EB2j4=
github.com/json-iterator/go v1.1.6/go.mod h1:+SdeFBvtyEkXs7REEP0seUULqWtbJapLOCVDaaPEHmU=
github.com/json-iterator/go v1.1.10/go.mod h1:KdQUCv79m/52Kvf8AW2vK1V8akMuk1QjK/uOdHXbAo4=
github.com/json-iterator/go v1.1.11/go.mod h1:KdQUCv79m/52Kvf8AW2vK1V8akMuk1QjK/uOdHXbAo4=
github.com/julienschmidt/httprouter v1.2.0/go.mod h1:SYymIcj16QtmaHHD7aYtjjsJG7VTCxuUUipMqKk8s4w=
github.com/julienschmidt/httprouter v1.3.0/go.mod h1:JR6WtHb+2LUe8TCKY3cZOxFyyO8IZAc4RVcycCCAKdM=
github.com/konsorten/go-windows-terminal-sequences v1.0.1/go.mod h1:T0+1ngSBFLxvqU3pZ+m/2kptfBszLMUkC4
github.com/konsorten/go-windows-terminal-sequences v1.0.3 h1:CE8S1cTafDpPvMhIxNJKvHsGVBgn1xWYf1NbHQhyw
github.com/konsorten/go-windows-terminal-sequences v1.0.3/go.mod h1:T0+1ngSBFLxvqU3pZ+m/2kptfBszLMUkC4
github.com/kr/logfmt v0.0.0-20140226030751-b84e30acd515/go.mod h1:+0opPa2QZZtGFBFZlji/RkVcI2GknAs/DXo4
github.com/kr/pretty v0.1.0/go.mod h1:dAy3ld7l9f0ibDNOQOHHMYYIIbhfbHSm3C4ZsoJORNo=
github.com/kr/pty v1.1.1/go.mod h1:pFQYn66WHrOpPYNljwOMqo10TkYh1fy3cYio2l3bCsQ=
github.com/kr/text v0.1.0/go.mod h1:4Jbv+DJW3UT/LiOwJeYQe1efqtUx/iVham/4vfdArNI=
github.com/matttproud/golang_protobuf_extensions v1.0.1 h1:4hp9jkHxhMHkqkrB3Ix0jegS5sx/RkqARlsWZ6pIwiU
github.com/matttproud/golang_protobuf_extensions v1.0.1/go.mod h1:D8He9yQNgCq6Z5Ld7szi9bcBfOoFv/3dc6xS
github.com/modern-go/concurrent v0.0.0-20180228061459-e0a39a4cb421/go.mod h1:6dJC0mAP4ikYIbvyc7fijjWJd
github.com/modern-go/concurrent v0.0.0-20180306012644-bacd9c7ef1dd/go.mod h1:6dJC0mAP4ikYIbvyc7fijjWJd
github.com/modern-go/reflect2 v0.0.0-20180701023420-4b7aa43c6742/go.mod h1:bx2lNnkwVCuqBIxFjflWJWanXIb
github.com/modern-go/reflect2 v1.0.1/go.mod h1:bx2lNnkwVCuqBIxFjflWJWanXIb3RllmbCylyMrvgv0=
github.com/mwitkow/go-conntrack v0.0.0-20161129095857-cc309e4a2223/go.mod h1:qRWi+5nqEBWmkhHvq77mSJWrC
github.com/mwitkow/go-conntrack v0.0.0-20190716064945-2f068394615f/go.mod h1:qRWi+5nqEBWmkhHvq77mSJWrC
github.com/opsgenie/opsgenie-go-sdk-v2 v1.2.8 h1:qF/rRi8GSU2mjBXfJIyMj9GGmjedsV3Gm1uYbiGlCRk=
github.com/opsgenie/opsgenie-go-sdk-v2 v1.2.8/go.mod h1:4OjcxgwdXzezqytxN534MooNmrxRD50geWZxTD7845s=
github.com/pkg/errors v0.8.0/go.mod h1:bwawxfHBFNV+L2hUp1rHADufV3IMtnDRdf1r5NINEl0=
github.com/pkg/errors v0.8.1/go.mod h1:bwawxfHBFNV+L2hUp1rHADufV3IMtnDRdf1r5NINEl0=
github.com/pkg/errors v0.9.1 h1:FEBLx1zS214owpjy7qsBeixbURkuhQAwrK5UwLGTwt4=
github.com/pkg/errors v0.9.1/go.mod h1:bwawxfHBFNV+L2hUp1rHADufV3IMtnDRdf1r5NINEl0=
github.com/pmezard/go-difflib v1.0.0 h1:4DBwDE0NGyQoBHbLQYPwSUPoCMWR5BEzIk/f1lZbAQM=
github.com/pmezard/go-difflib v1.0.0/go.mod h1:iKH77koFhYxTK1pcRnkKkqfTogsbg7gZNVY4sRDYZ/4=
github.com/prometheus/client_golang v0.9.1/go.mod h1:7SWBe2y4D6OKWSNQJUaRYU/AaXPKyh/dDVn+NZz0KFw=
github.com/prometheus/client_golang v1.0.0/go.mod h1:db9x61etRT2tGnBNRi70OPL5FsnadC4Ky3P0J6CfImo=
github.com/prometheus/client_golang v1.7.1/go.mod h1:PY5Wy2awLA44sXw4AOSfFBetzPP4j5+D6mVACh+pe2M=
github.com/prometheus/client_golang v1.11.0 h1:HNkLOAEQMIDv/K+04rukrLx6ch7msSRwf3/SASFAGtQ=
github.com/prometheus/client_golang v1.11.0/go.mod h1:Z6t4BnS23TR94PD6BsDNk8yVqroYurpAkEiz0P2BEV0=
github.com/prometheus/client_model v0.0.0-20180712105110-5c3871d89910/go.mod h1:MbSGuTsp3dbXC40dX6PRTW
github.com/prometheus/client_model v0.0.0-20190129233127-fd36f4220a90/go.mod h1:xMI15A0UPsDsEKsMN9yxem
github.com/prometheus/client_model v0.2.0 h1:uq5h0d+GuxiXLJLNABMgp2qUWDPiLvgCzz2dUR+/W/M=
github.com/prometheus/client_model v0.2.0/go.mod h1:xMI15A0UPsDsEKsMN9yxemIoYk6Tm2C1GtYGdfGttqA=
github.com/prometheus/common v0.4.1/go.mod h1:TNfzLD0ON7rHzMJeJkieUDPYmFC7Snx/y86RQel1bk4=
github.com/prometheus/common v0.10.0/go.mod h1:Tlit/dnDKsSWFlCLTWaA1cyBgKHSMdTB80sz/V91rCo=
github.com/prometheus/common v0.26.0 h1:iMAkS2TDoNWnKM+Kopnx/8tnEStIfpYA0ur0xQzzhMQ=
```

Безопасность цепочки поставок

Угроза: Подмена зависимостей

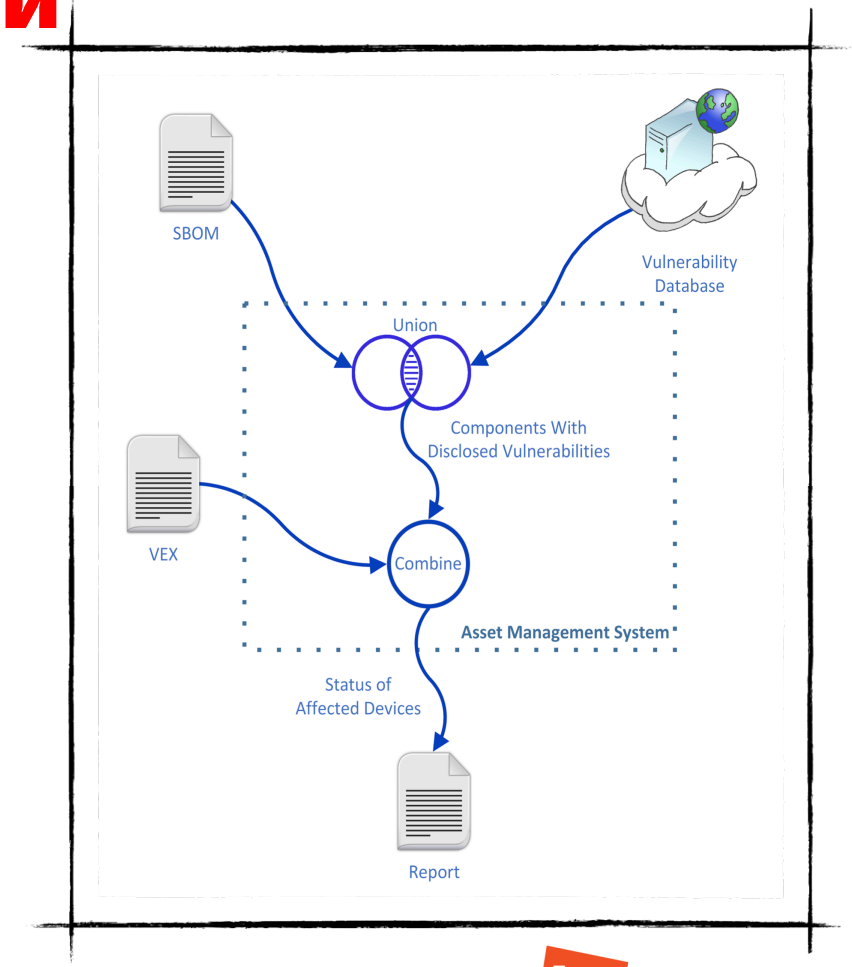
- Фиксация зависимостей в lock-файле, включая версии
- **Локальные репозитории для всех зависимостей с модерацией**



Безопасность цепочки поставок

Угроза: Подмена зависимостей

- Фиксация зависимостей в lock-файле, включая версии
- Локальные репозитории для всех зависимостей с модерацией
- **Формирование и контроль SBOM + VEX**



Безопасность цепочки поставок

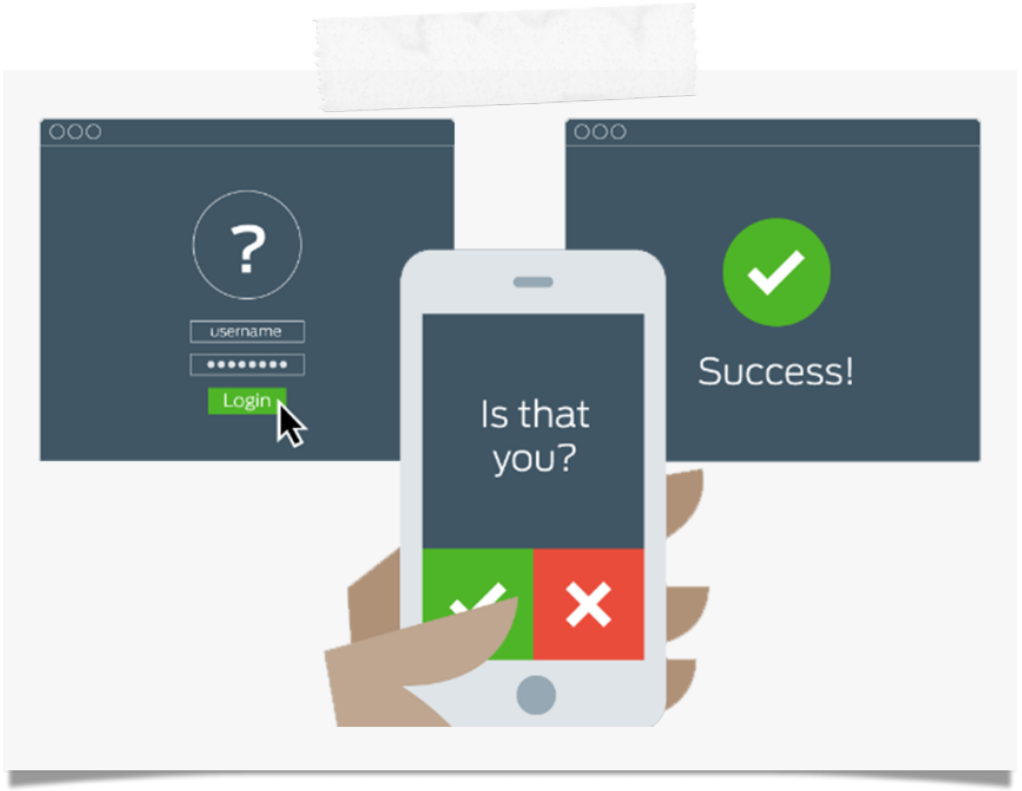
Угроза: Подмена зависимостей

- Фиксация зависимостей в lock-файле, включая версии
- Локальные репозитории для всех зависимостей с модерацией
- Формирование и контроль SBOM + VEX
- **SAST для всех внешних зависимостей**

Безопасность цепочки поставок

Угроза: Утечка секретов

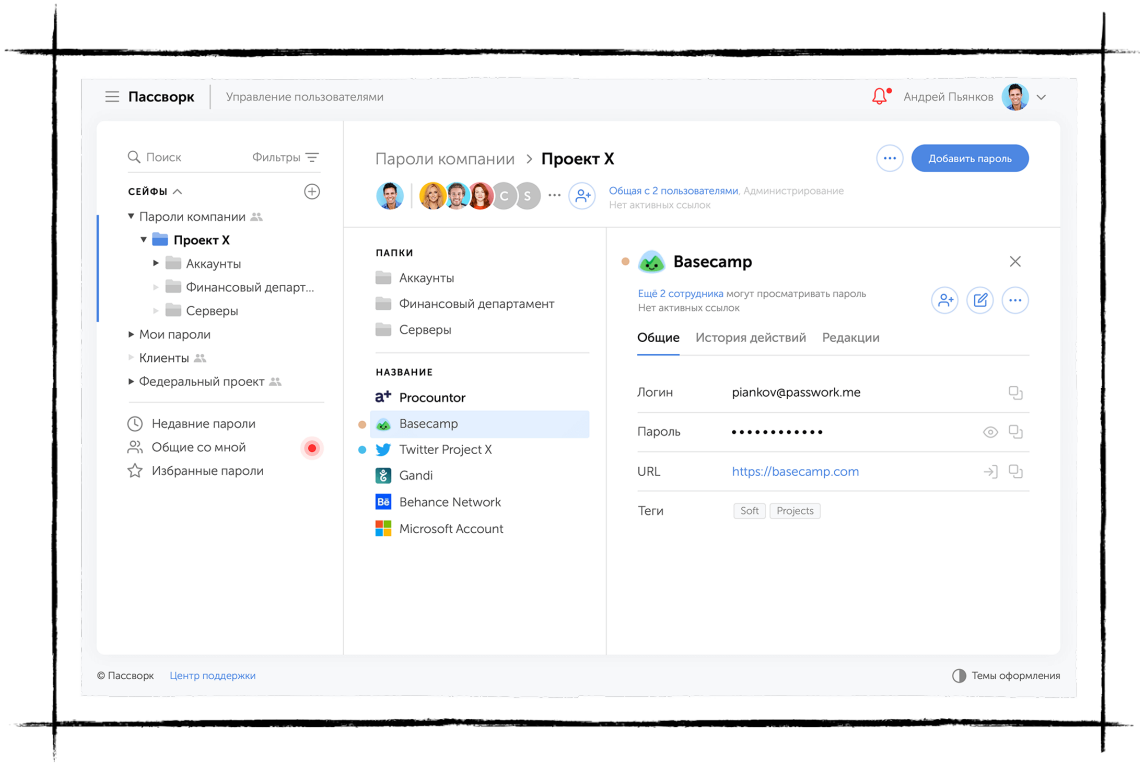
- ➡ 2FA для доступа во внутренние ресурсы



Безопасность цепочки поставок

Угроза: Утечка секретов

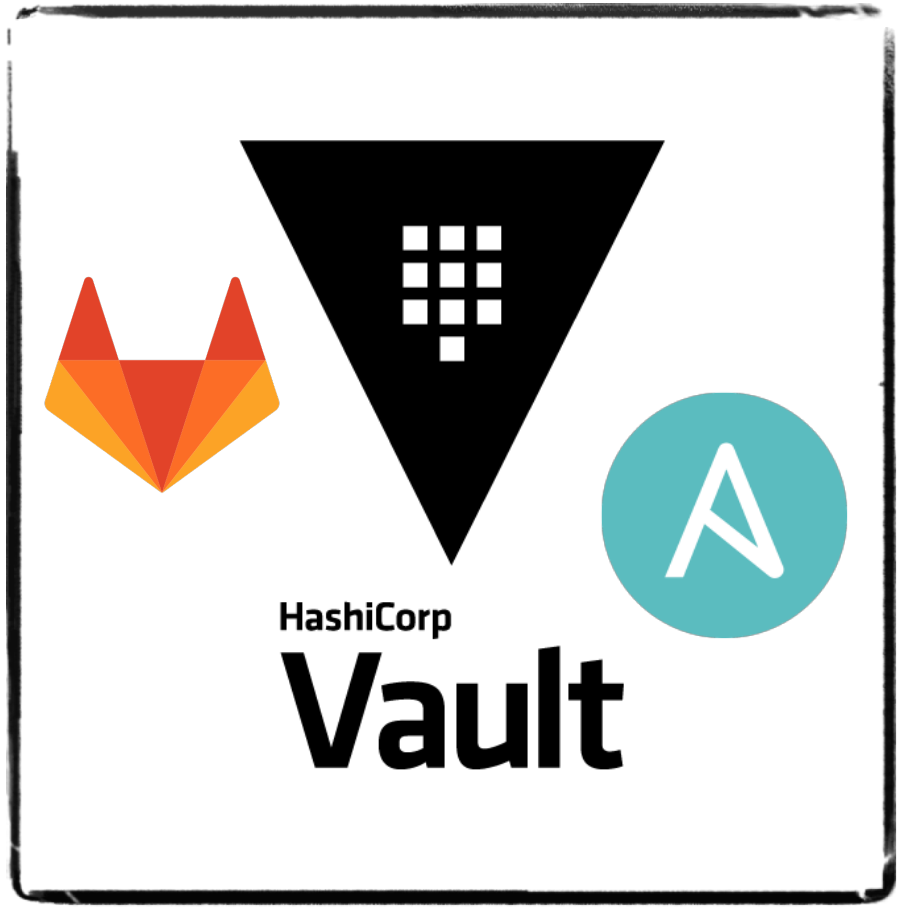
- 2FA для доступа во внутренние ресурсы
- **Секреты команд в «парольнице»**



Безопасность цепочки поставок

Угроза: Утечка секретов

- 2FA для доступа во внутренние ресурсы
- Секреты команд в «парольнице»
- **Секреты в HashiCorp Vault и интеграция с CI и Ansible**



Безопасность цепочки поставок

Угроза: Компрометация конвейера

- Актуализация ОС, hardening и контроль наличия всех security-патчей на серверах конвейера

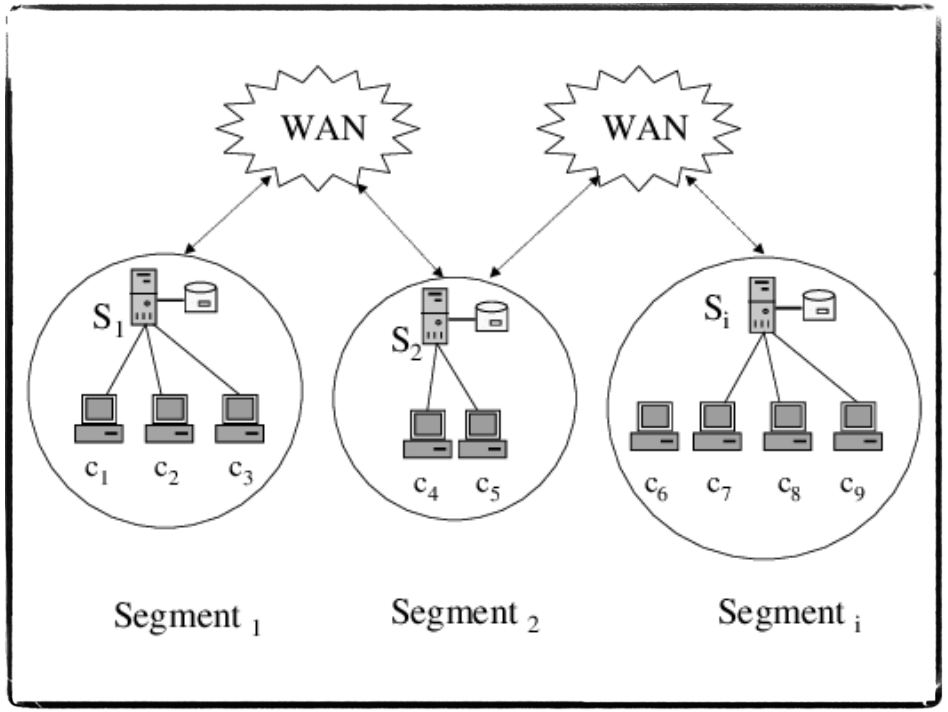
```
aaronk@tecmint:~$ sudo apt-get install unattended-upgrades
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  bsd-mailx default-mta | mail-transport-agent needrestart
The following NEW packages will be installed:
  unattended-upgrades
0 upgraded, 1 newly installed, 0 to remove and 332 not upgraded.
Need to get 41.7 kB of archives.
After this operation, 418 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 unattended-upgrades all
Fetched 41.7 kB in 2s (20.7 kB/s)
Preconfiguring packages ...
Selecting previously unselected package unattended-upgrades.
(Reading database ... 284557 files and directories currently installed.)
Preparing to unpack .../unattended-upgrades_1.1ubuntu1.18.04.14_all.deb ...
Unpacking unattended-upgrades (1.1ubuntu1.18.04.14) ...
Setting up unattended-upgrades (1.1ubuntu1.18.04.14) ...

Creating config file /etc/apt/apt.conf.d/20auto-upgrades with new version
```

Безопасность цепочки поставок

Угроза: Компрометация конвейера

- Актуализация ОС, hardening и контроль наличия всех security-патчей на серверах конвейера
- **Отключение от интернета, сетевая сегментация и повсеместный HTTPS в CI**



Безопасность цепочки поставок

Угроза: Компрометация конвейера

- Актуализация ОС, hardening и контроль наличия всех security-патчей на серверах конвейера
- Отключение от интернета, сетевая сегментация и повсеместный HTTPS в CI
- **Устранение «зоопарка» CI**

Безопасность цепочки поставок

Угроза: Компрометация конвейера

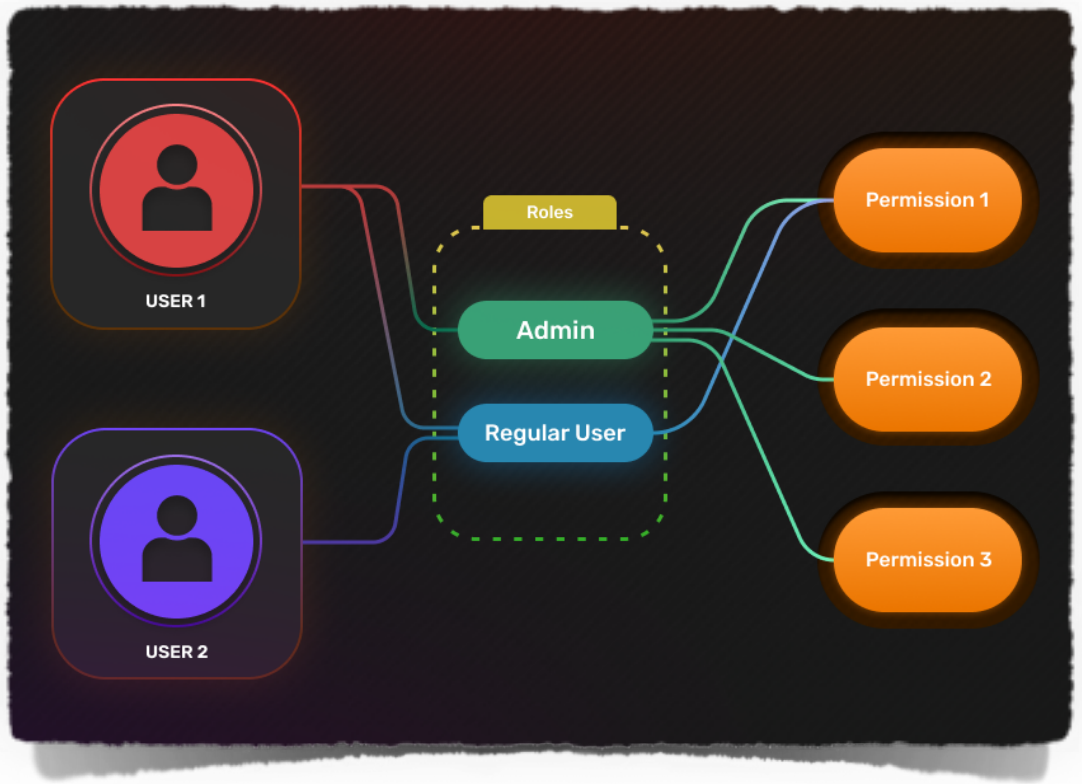
- Актуализация ОС, hardening и контроль наличия всех security-патчей на серверах конвейера
- Отключение от интернета, сетевая сегментация и повсеместный HTTPS в CI
- Устранение «зоопарка» CI
- **Подключение SIEM к серверам конвейера, аудит настроек конвейера и репозиториев**

MaxPatrol SIEM

Безопасность цепочки поставок

Угроза: Подмена пакета приложения

- Ролевая модель доступа к хранилищу артефактов



Безопасность цепочки поставок

Угроза: Подмена пакета приложения

- Ролевая модель доступа к хранилищу артефактов
- **Подписание релизных артефактов**

Послесловие

➡ Оцени угрозы цепочки поставок

Послесловие

- Оцени угрозы цепочки поставок
- **Развивай безопасность непрерывно**

Послесловие

- Оцени угрозы цепочки поставок
- Развивай безопасность непрерывно
- **Присоединяйся к Telegram каналу *Op!DevOps***

Ваши вопросы?

… и QR-код для оценки доклада

DevOps Conf 2023