Чтобы труба не падала, нужно использовать простые ~~советские~~ OWASP Top 10 CI/CD Security Risks

Артем Пузанков
DevSecOps Cluster Lead

кто я?

DevSecOps Cluster Lead
в MTC Digital
Smarthome & IoT Cluster
внедряю инструменты
выстраиваю процессы
и что-то ещё

Содержание

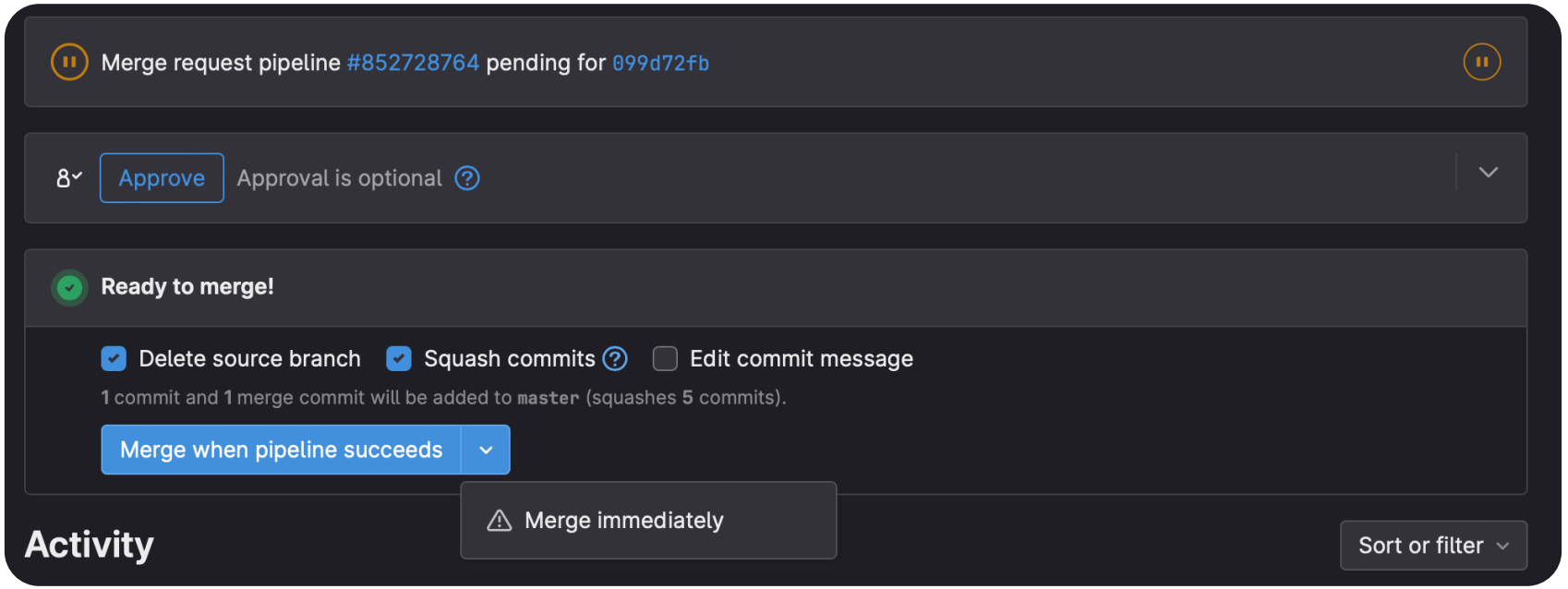
CICD-SEC-1: Insufficient Flow Control Mechanism

Недостаточные механизмы управления потоком

01

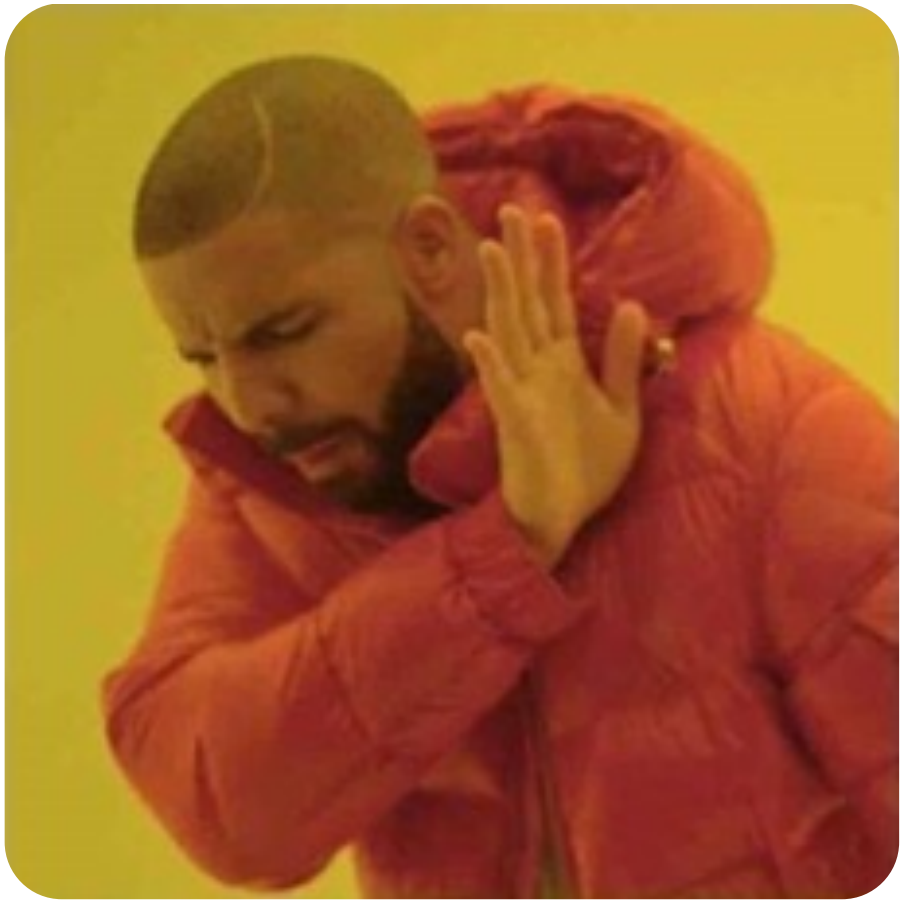
CICD-SEC-1 // Недостаточные механизмы управления потоком

Недостаточные механизмы управления потоком ведут к доступу злоумышленника к SCM и возможности самостоятельно «пушить» вредоносный код по конвейеру, ввиду отсутствия механизмов, обеспечивающих дополнительное одобрение или проверку.



CICD-SEC-1 // Недостаточные механизмы управления потоком

- Auto-deploy to prod
- Debugging on prod
- Ручной триггер для deploy on prod
- Бесконтрольный push кода в библиотеки on prod
- Бесконтрольный MR branches
- Загрузка артефактов в хранилище без проверок
- Наличие доступа к prod у разработчиков



CICD-SEC-1 // Недостаточные механизмы управления потоком

- Git submodules
- Codeowners
- Исключение push main
- Исключение self-approve MR
- Approve несколькими лицами/ревью кода
- Сборка и развертывание только из main-/release-веток
- CI/CD as Code и его контроль
- Автоматизация всего и вся

CICD-SEC-2: Inadequate Identity and Access Management

Привилегии

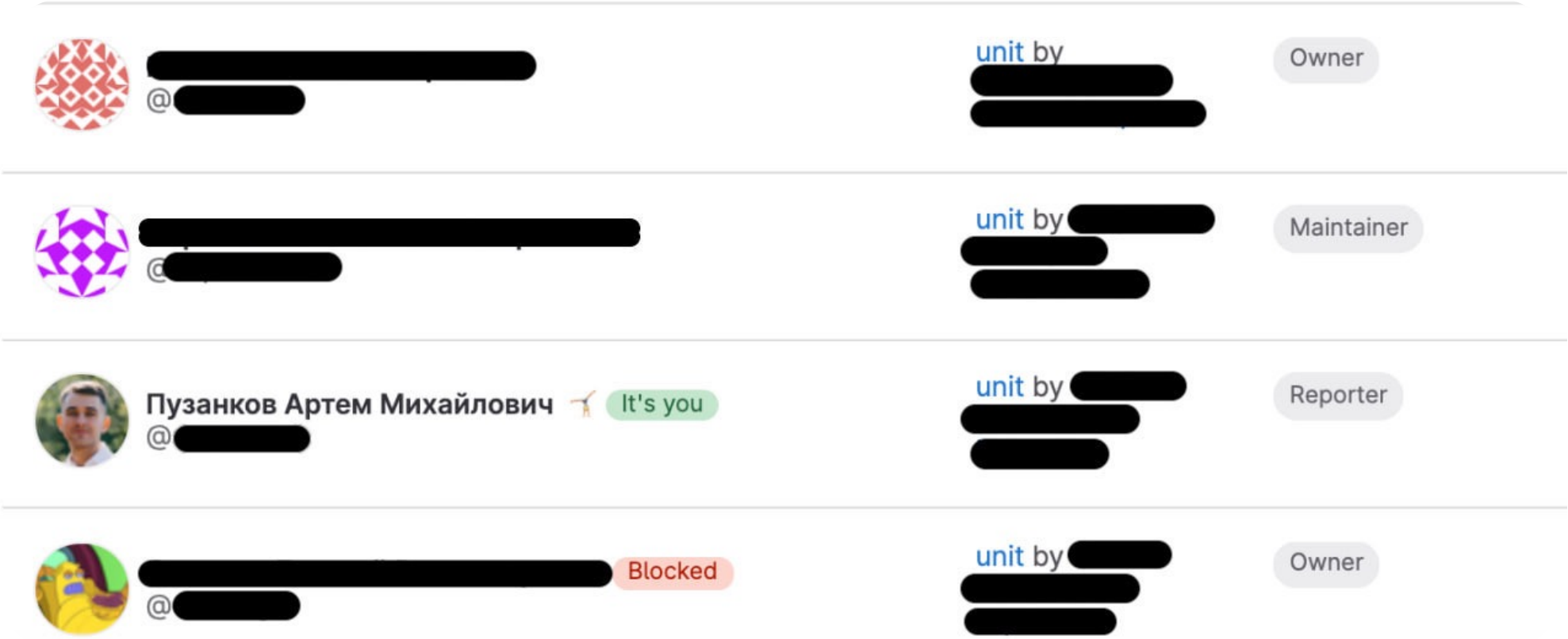
02

CICD-SEC-2 // Привилегии

Риск возникает из-за наличия различных идентификаторов, обилия методов, а также сложности управления и аудита предоставления доступа к SCM. Также не забываем про технические учётные записи.

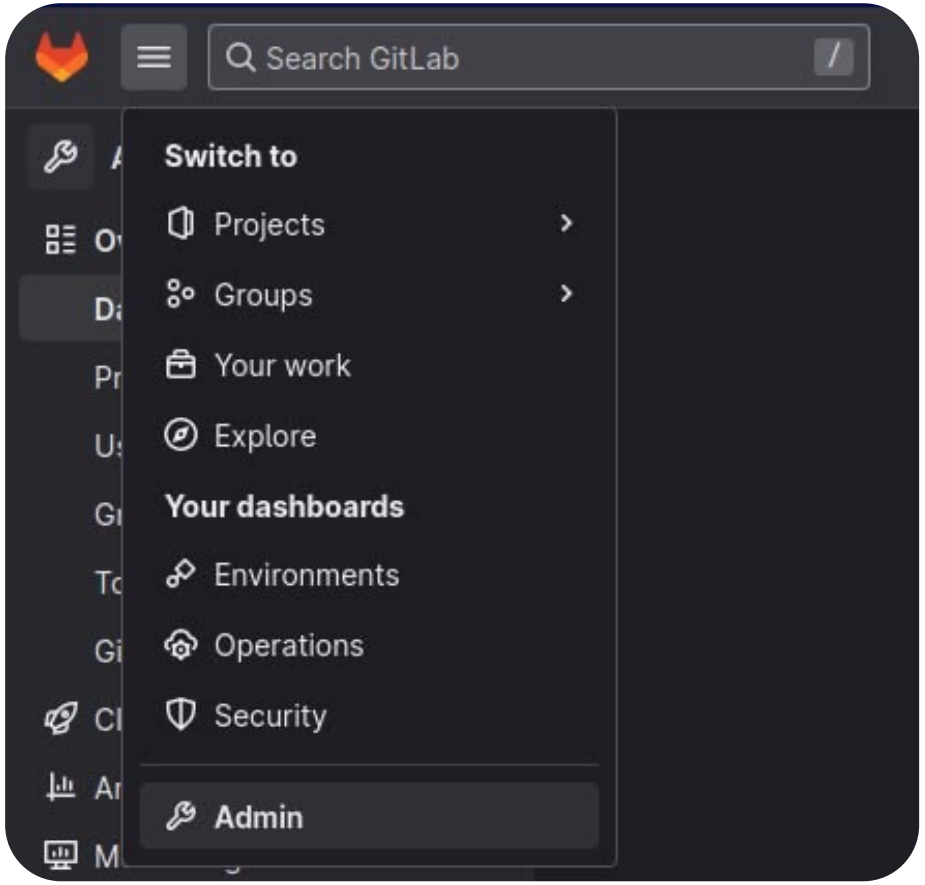
- Shared аккаунты
- Outsourcing
- Выдача избыточных привилегий
- «Забытые» доступы

CICD-SEC-2 // Привилегии



CICD-SEC-2 // Привилегии

- Контроль и аудит привилегий
- Исключение shared аккаунтов
- Несколько админов или approver
- Пользователи не могут выдавать права
- Всегда должен применяться принцип наименьших привилегий



https://github.com/gittuf/gittuf

CICD-SEC-3: Dependency Chain Abuse

Злоупотребление цепочкой зависимостей

03

CICD-SEC-3 // Злоупотребление цепочкой зависимостей

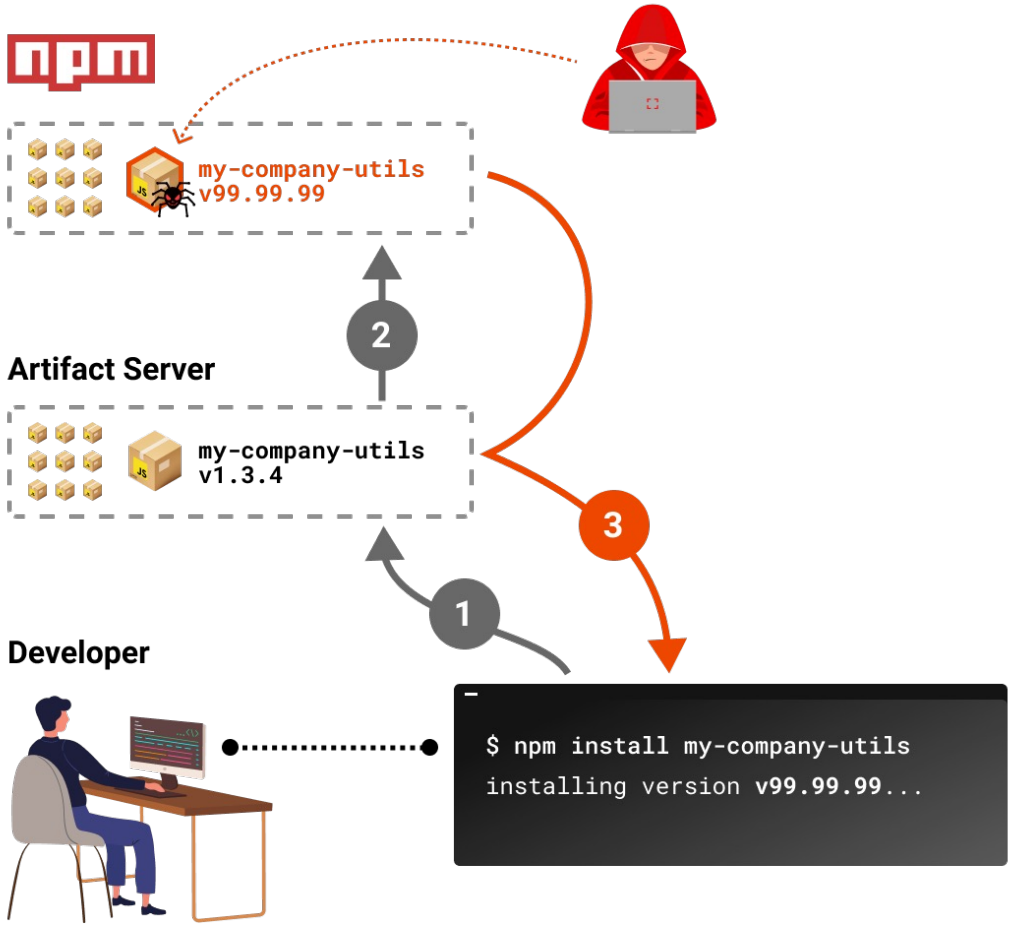
Риски злоупотребления цепочкой зависимостей нацелены на использование вредоносных зависимостей.

Основные векторы:

- Dependency confusion – публикация вредоносных пакетов в общедоступных репозиториях с тем же именем, что и внутренние имена пакетов.
- Перехват зависимостей – получение контроля над учетной записью owner'а.
- Typosquatting – публикация вредоносных пакетов с именами, похожими на имена популярных пакетов, в надежде на опечатку.
- Brandjacking – публикация вредоносных пакетов под видом «брендированного», ложная ассоциации с знакомым брендом.

CICD-SEC-3 // Злоупотребление цепочкой зависимостей

- Проверка всех источников
- Контроль и сканирование зависимостей (OSA, SCA)
- Подпись артефактов и ее проверка
- Минимизирована возможность отдельной сборки влиять на соседние



CICD-SEC-4: Poisoned Pipeline Execution (PPE)

Выполнение «отравленного» pipeline

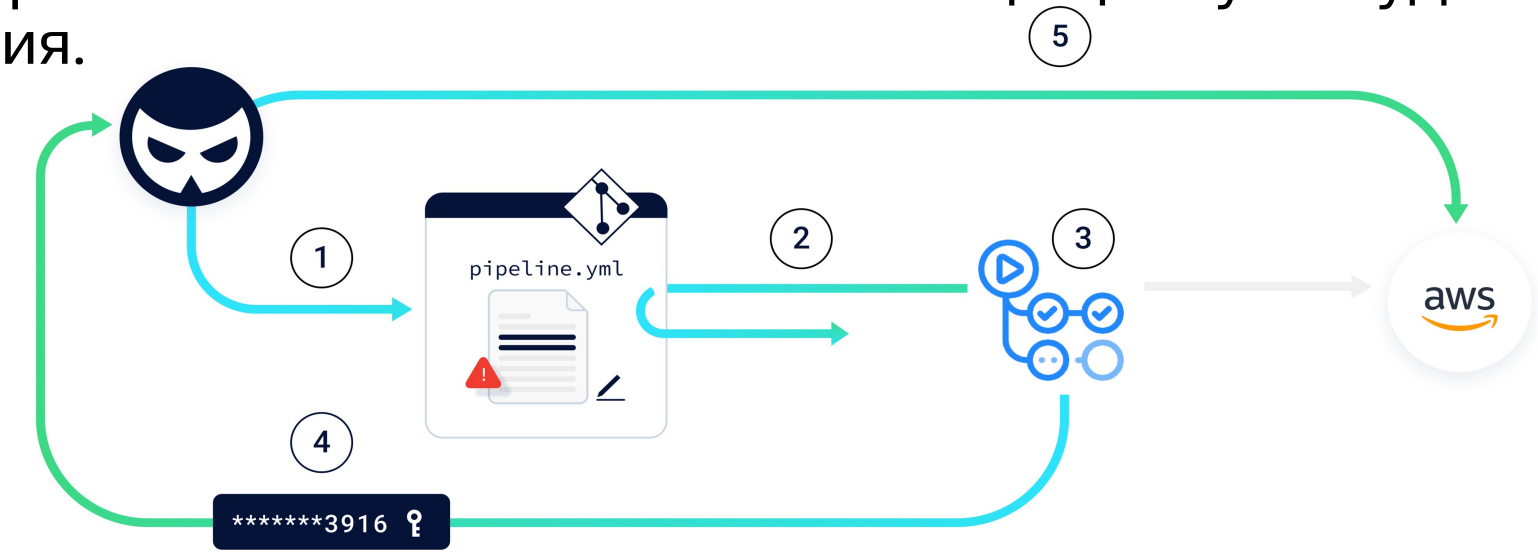
04

CICD-SEC-4 // Выполнение «отравленного» pipeline

Риски выполнения «отравленного» pipeline (PPE) – доступ злоумышленника к системам контроля версий и без доступа к среде сборки. Позволяет манипулировать процессом сборки путем внедрения вредоносного кода в конфигурацию конвейера сборки, тем самым «отравляя».

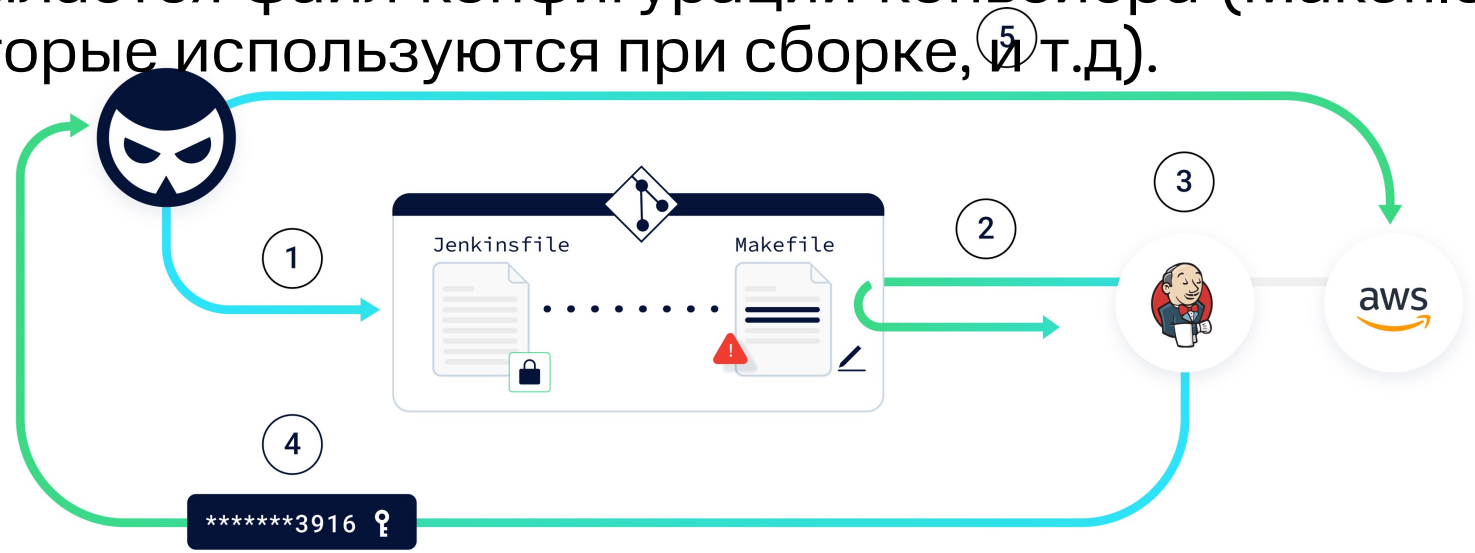
PPE бывают:

- Direct/прямой PPE – изменение файла конфигурации CI в репозитории, либо отправляя изменения в незащищенную удаленную ветку репозитория.



CICD-SEC-4 // Выполнение «отравленного» pipeline

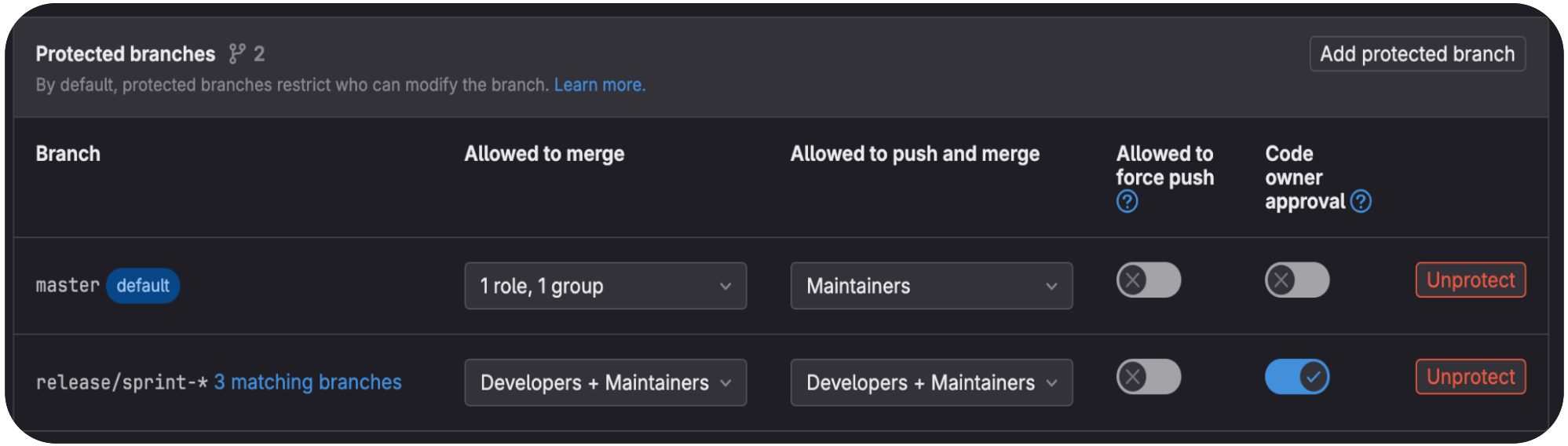
- Indirect/косвенный PPE – когда D-PPE нереализуемо, злоумышленник все равно может «отравить» конвейер, внедрив вредоносный код в файлы, на которые ссылается файл конфигурации конвейера (Makefile, файлы в том же репо, которые используются при сборке, и т.д).



- Public PPE – злоумышленнику требуется доступ к репо, в котором находится файл конфигурации конвейера, или к файлам, на которые он ссылается, но в общедоступные проектах/репо.

CICD-SEC-4 // Выполнение «отравленного» pipeline

- Protected branches, codeowners, git submodules/include, раздельные репозитории
- Сегментированная инфраструктура dev/prod
- Для файлов назначены ответственные
- Нет влияния на соседние сборки



CICD-SEC-5: Insufficient PBAC (Pipeline-Based Access Controls)

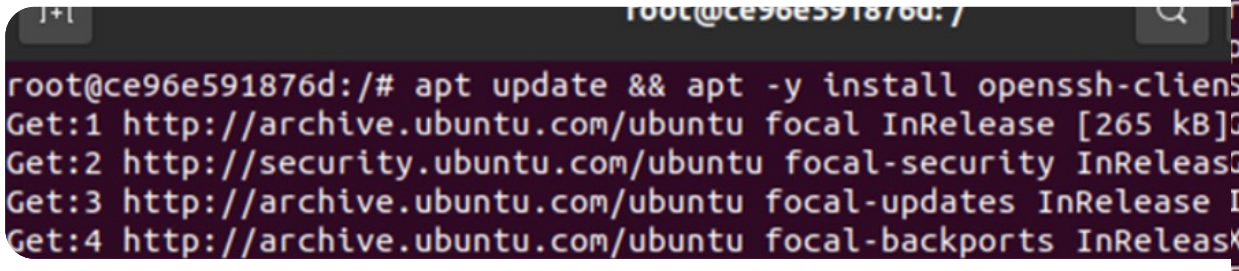
Ошибки доступа

05

CICD-SEC-5 // Ошибки доступа

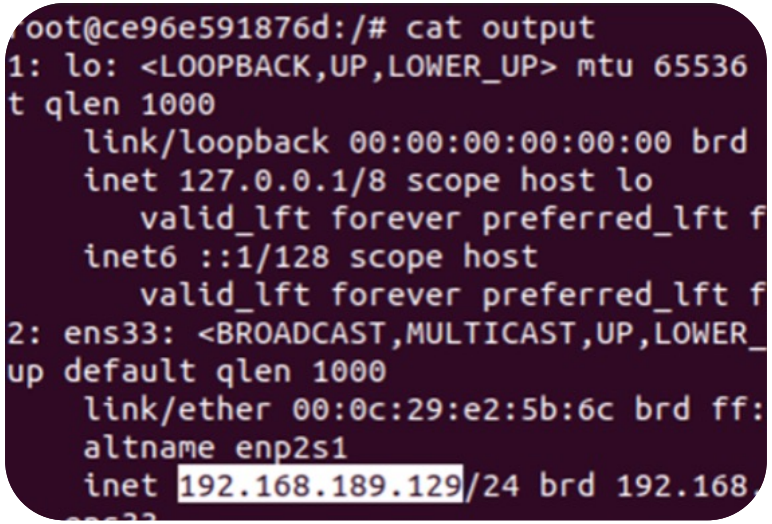
Системы CI/CD, которые выполняют конвейеры, имеют доступ:

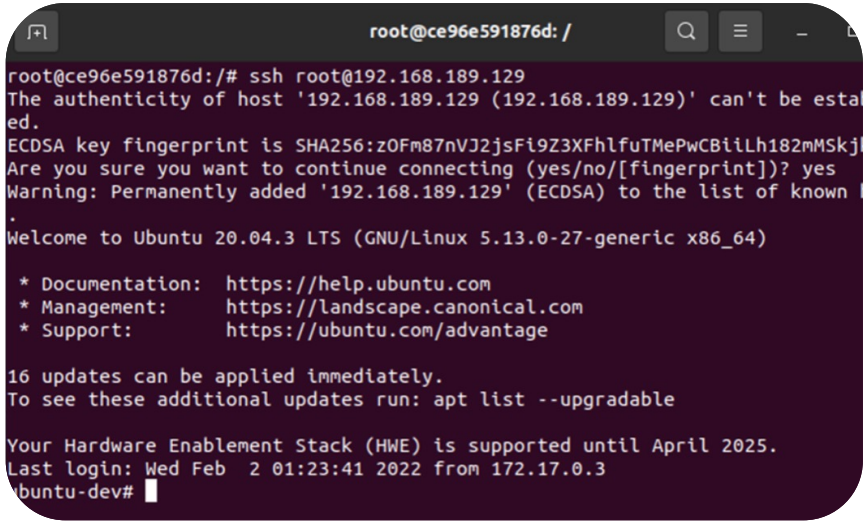
- к сторонней информации, секретам, сервисам;
- к прошлым, соседним, следующими сборкам или репозиториям;
- к хостовой ОС;
- в интернет.



CICD-SEC-5 // Ошибки доступа

Например, злоумышленник может «поднять» контейнер с более высокими привилегиями (--privileged/--cap-add=SYS_ADMIN), чем требуется, «сбежать», и выполнять printenv, для записи вашего SSH-ключа в файл authorized_keys root-пользователя, да и всё что почудится.





CICD-SEC-5 // Ошибки доступа

- Различные секреты для dev/prod
- Разделение инфраструктуры dev/prod
- Сброс в «чистое» состояние после сборки
- Данные сборки не сохраняются и не влияют на другие сборки
- Доступ только к необходимым ресурсам
- Разработчик – только в dev

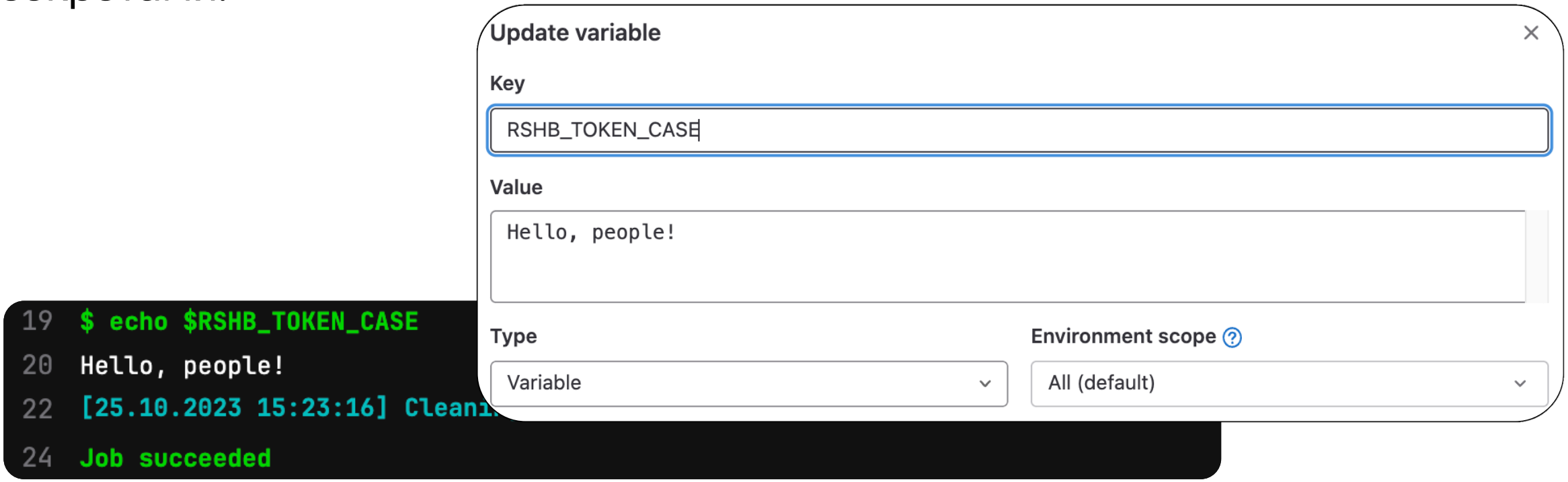
CICD-SEC-6: Insufficient Credential Hygiene

Секреты

06

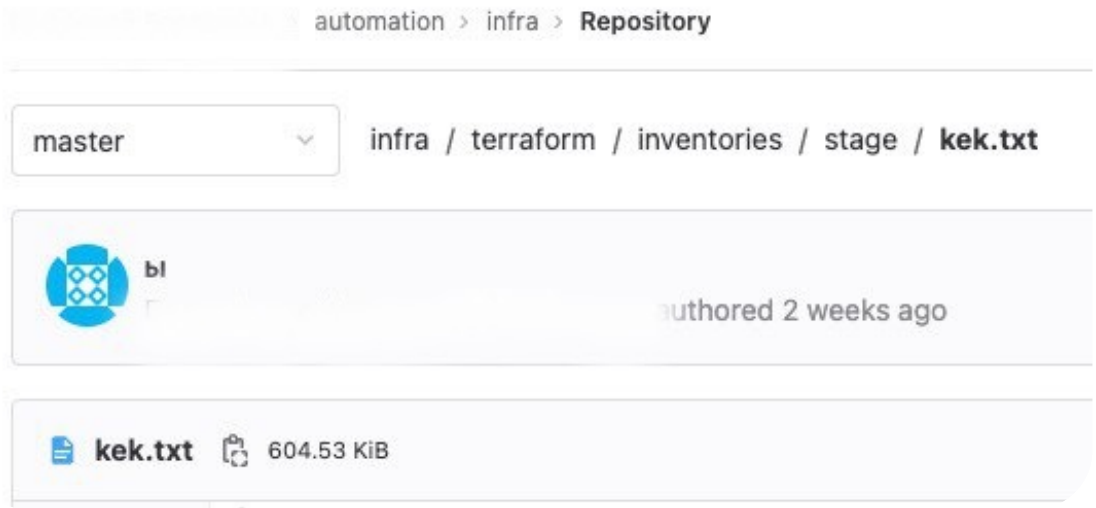
CICD-SEC-6 // Секреты

Риски недостаточной гигиены credentials связаны со способностью злоумышленника получать и использовать различные секреты и токены, распространяющиеся по конвейеру, из-за небезопасного управления секретами.



CICD-SEC-6 // Секреты

- Credentials везде: код, Dockerfile/docker-compose/ манифесты/чарты/слои контейнера/логи
- Ввод учетных данных в консоль в открытом виде
- Небезопасная передача секретов




```
### Kafka
##########################################################################################
kafka.producer.bootstrap-servers=10.7[redacted]
kafka.producer.batch-size=2048
kafka.producer.compression-type=none
kafka.producer.acks=1
kafka.producer.delivery-timeout=300
kafka.producer.request-timeout=100
kafka.producer.retry-backoff=100
kafka.producer.request-per-connection=1
kafka.producer.sasl.mechanism=SCRAM-SHA-512
kafka.producer.sasl.jaas-config=org.apache.kafka.common.security.scram.ScramLoginModule required username="[redacted]" password="[redacted]";
kafka.producer.topic.correction-data=[redacted]
kafka.producer.topic.[redacted]
##########################################################################################
### Logs
##########################################################################################
logging.config=classpath:config/logback-spring-master.xml
logbook.format.style=http
logbook.filter.enabled=true
logbook.exclude[0]=/actuator/**
##########################################################################################
## Monitoring
##########################################################################################
management.prometheus.metrics.export.enabled=true
management.endpoints.web.exposure.include=health,prometheus,refresh
management.endpoint.refresh.enabled=true
management.endpoint.health.show-details=always
##########################################################################################
## RTCM
##########################################################################################
rtcm.message.corrections=10[7-9][0-9]|11[1-2][0-9]
rtcm.message.ephemeris=1019, 1020, 1042, 1044, 1045
##########################################################################################
### Rabbit MQ
##########################################################################################
#spring.rabbitmq.host=[redacted]
#spring.rabbitmq.port=[redacted]
#spring.rabbitmq.username=[redacted]
#spring.rabbitmq.password=[redacted]
#spring.rabbitmq.dynamic=true
```

CICD-SEC-6 // Секреты

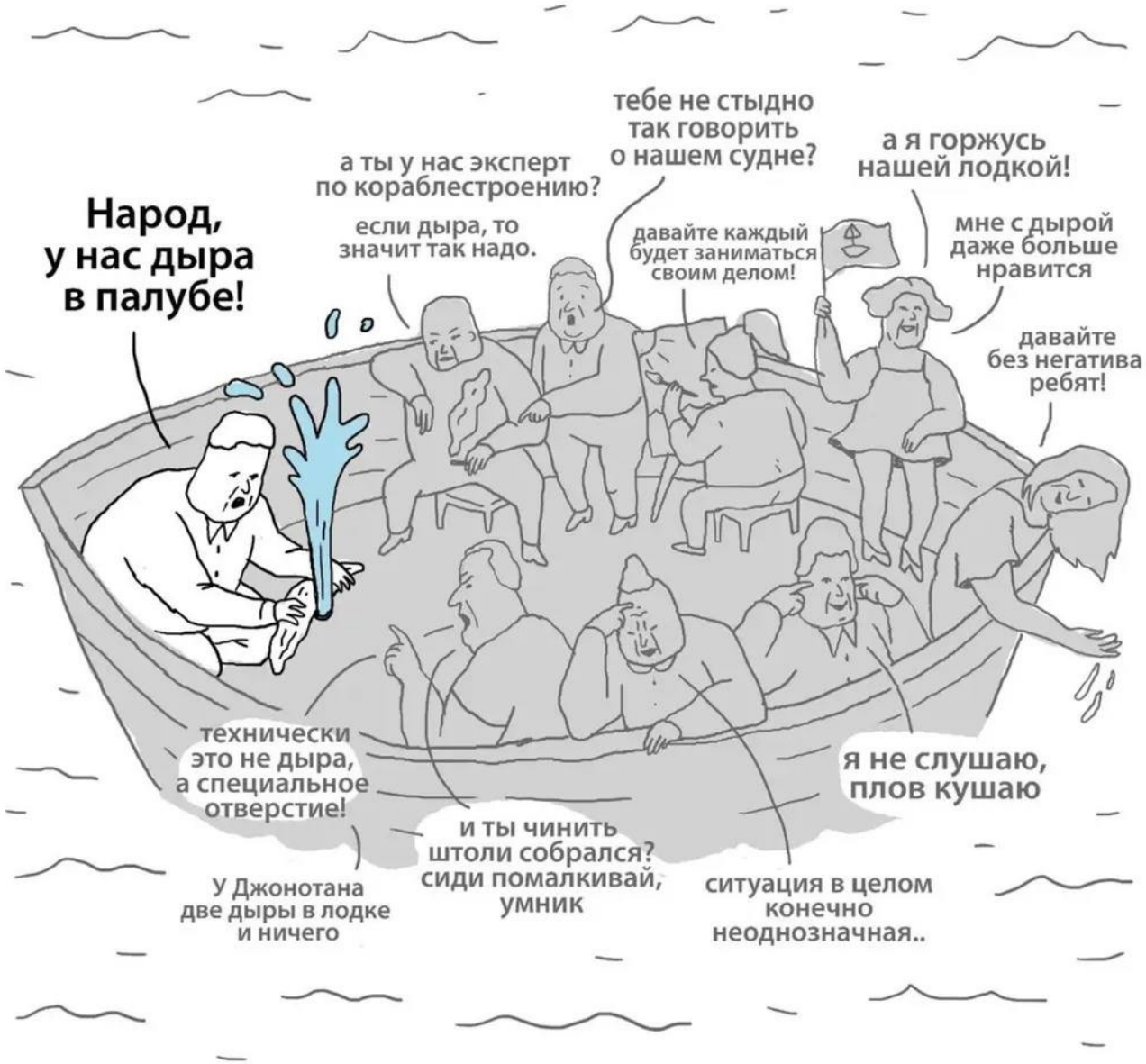
- Поиск секретов в коде (gitleaks, etc.)
- Protected branches (masked/protected variables)
- Хранилище секретов (must have)
- Контроль доступа к секретам
- Ротация секретов

CICD-SEC-7: Insecure System Configuration

Небезопасная конфигурация системы

07

CICD-SEC-7 // Небезопасная конфигурация системы



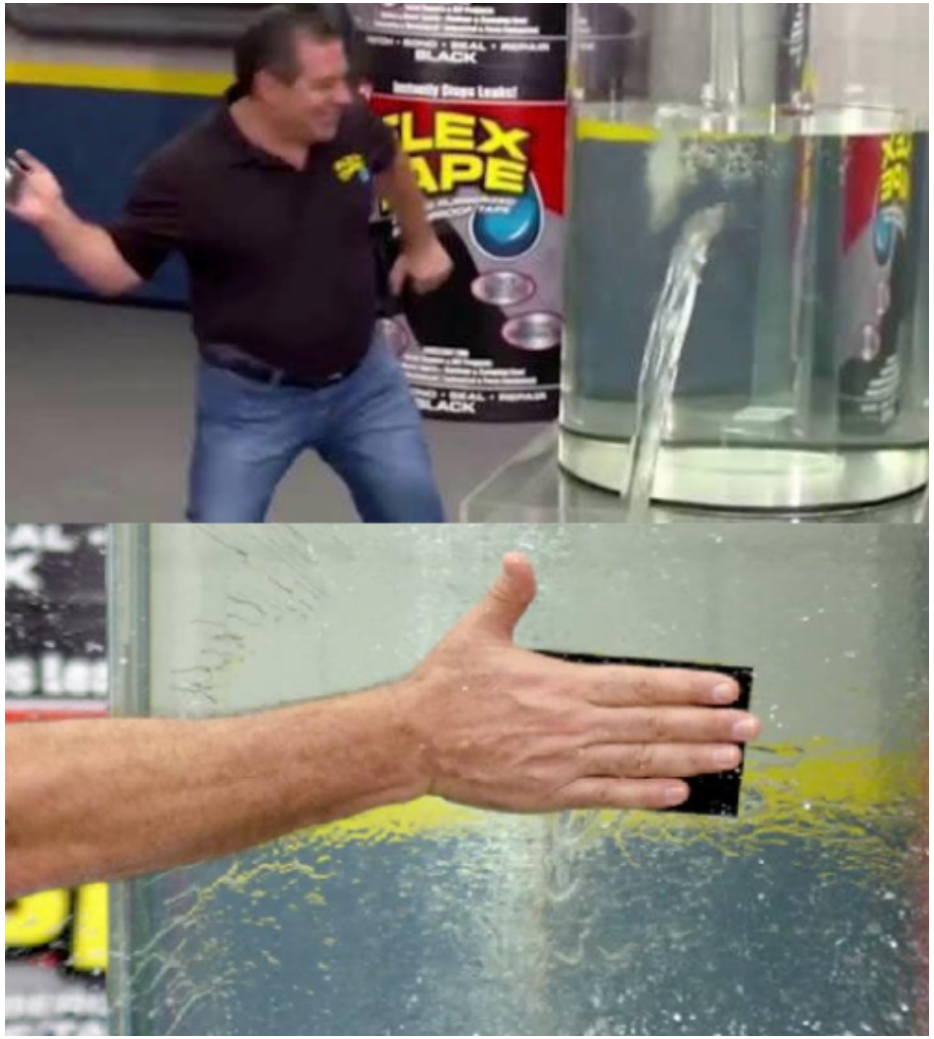
CICD-SEC-7 // Небезопасная конфигурация системы

Риски, связанные с небезопасными конфигурациями системы, могут возникнуть из-за уязвимостей в настройках безопасности, конфигурациях и средствах защиты различных систем в экосистеме конвейера CI/CD.

- Настройки по умолчанию небезопасны
- Dependency confusion
- Отсутствие гигиены секретов
- Отсутствие важных исправлений безопасности
- Возможность доступа к внутренним сервисам компании

CICD-SEC-7 // Небезопасная конфигурация системы

- Аудит настроек безопасности
- Ревью IaC и файлов конфигурации
- Следование security by default
- Минимально необходимый сетевой доступ
- Конфигурация по умолчанию безопасна
- Отслеживание и контроль любых изменения конфигурации
- Своевременные обновление устаревших версий/ патчинг безопасности



CICD-SEC-8: Ungoverned Usage of 3rd Party Services

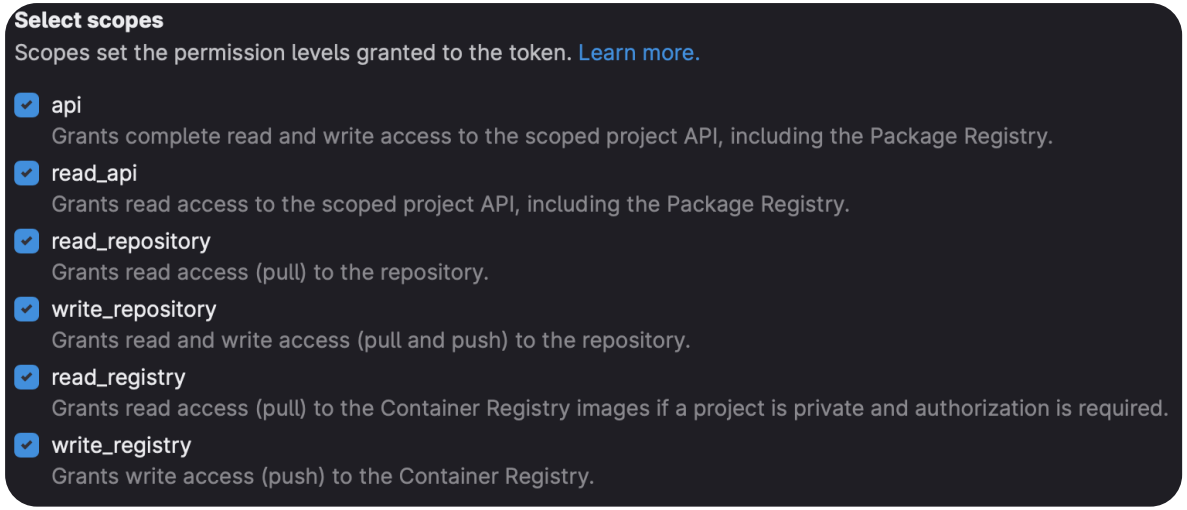
Интеграции

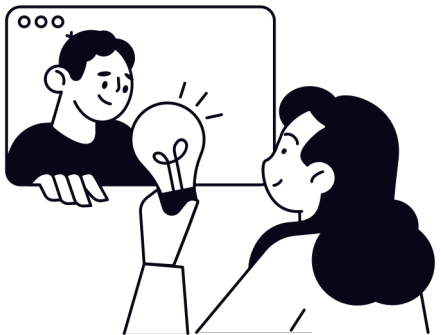
08

CICD-SEC-8 // Интеграции

Неконтролируемые интеграции приводят к тому, что сторонние сервисы могут легко получить доступ к ресурсам в CI/CD конвейере. Сторонние сервисы могут оказывать вредоносное воздействие на систему.

- Потеря контроля над интеграциями
- Нет контроля токенов доступа
- Отзыв прав без отзыва интеграций





CICD-SEC-8 // Интеграции

- Процессы предоставления, удаления и аудита прав для интегрируемых сервисов
- Актуализация интеграций
- Минимально необходимый доступ
- Контроль/отзыв доступов

CICD-SEC-9: Improper Artifact Integrity Validation

Supply Chain

09

CICD-SEC-9 // Supply Chain

Недостаточная проверка целостности артефактов в процессе CI/CD может позволить злоумышленнику подменить артефакт, созданный конвейером, на вредоносный.

- Проверка целостности артефактов
- Подпись кода и артефактов
- Проверка подписи на всех этапах
- Подпись всех сторонних артефактов в local storage
- Push только доверенными лицами
- Контроль артефактов (CICD-SEC-3)

CICD-SEC-10: Insufficient Logging and Visibility

Ошибки логирования

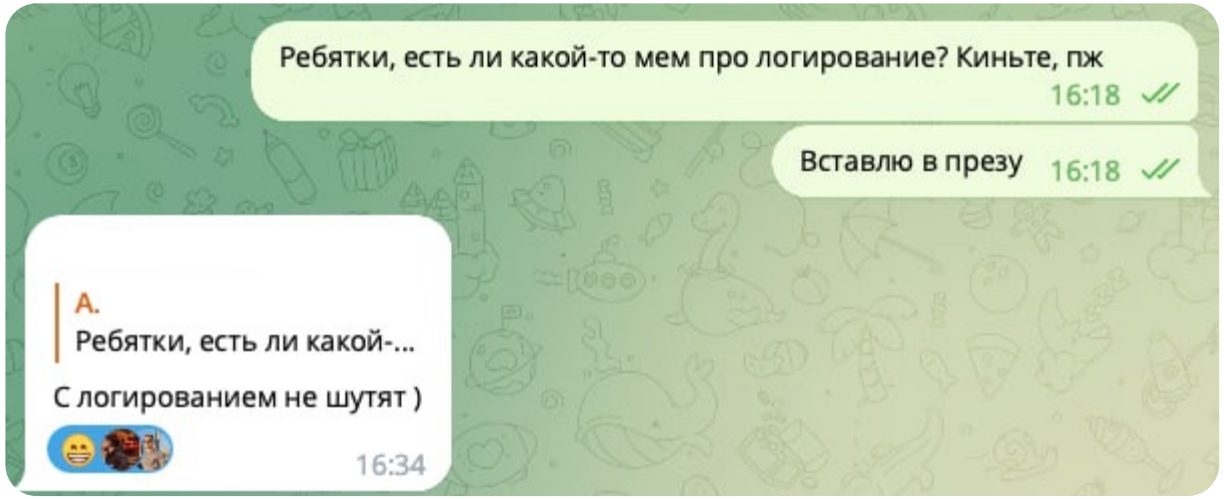
10

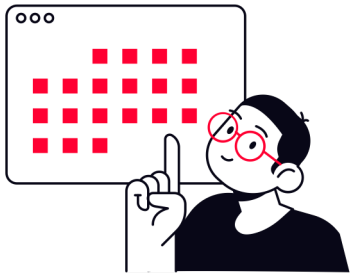
CICD-SEC-10 // Ошибки логирования

Ошибки логирования позволяют злоумышленнику осуществлять вредоносные действия в среде CI/CD, избегая обнаружения любом этапе.

Всё плохо, если отсутствуют:

- регистрация критичных событий
- инвентаризация активов
- карта инструментов
- анализ событий и оповещений





CICD-SEC-10 // Ошибки логирования

Необходимо реализовать возможность сбора и анализа файлов и данных, которые могут использоваться для отслеживания действий пользователей и обнаружения возможных внешних угроз.

- Блокирование систем при обнаружении инцидентов
- Есть данные для разбора инцидентов и совершенствования процесса мониторинга
- Отслеживать состояние систем, действия пользователей
- Логирование событий для всех систем
- SIEM
- События анализируются
- Уведомления об аномалиях

И всё безопасно?

*если в проекте у разработчика full права

Conclusion

Заключение

11

Conclusion // Заключение

- prod – только проверенный код
- Лишить возможности влиять на процесс сборки
- Привилегии и доступы
- Независимая сборка разных сервисов
- Настройки конфигурации безопасны
- Сторонние сервисы изолированы от основного продукта
- Continual improvement безопасности

Теперь не упадёт

Спасибо!

Артем Пузанков