DevOops 2023

Security для бедных

без ущерба для DevEx

Игорь Кудрин, CIO

mindbox

Кто такие mindbox

200 млн
профилей клиентов

40
кластеров kubernetes

260 ТБ
данных в реляционных хранилищах

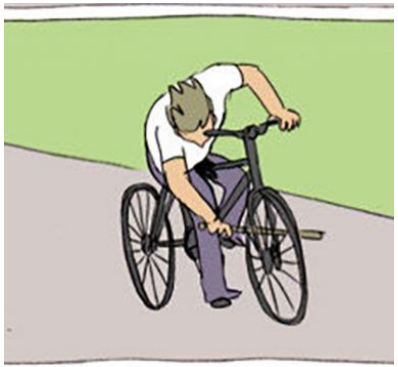
160
разработчиков

16
SRE/DevOps

0
безопасников в пиджаках

Чтобы что?

Выполняем требования сертификаций.
Не геймим.



Не мешаем людям работать.

https://mindbox.ru/security/

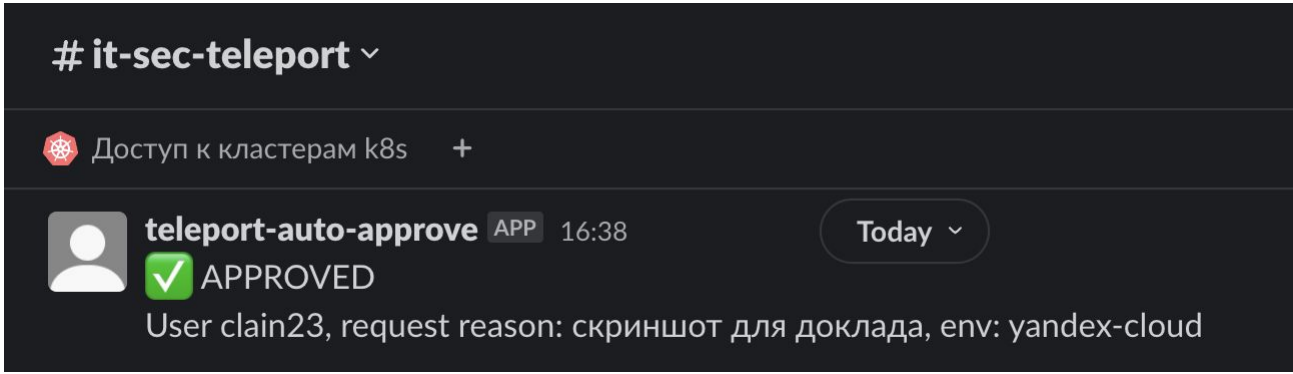
Вижен

Доступы по запросу.
Автоматически.

Доступ временный

```
tsh request create --roles=k8s-admin --reason="скриншот для доклада"

Creating request...
Request ID:     2762f757-2b8e-4d57-94b0-3212a2abfc97
Username:       clain23
Roles:          k8s-admin
Reason:         "скриншот для доклада"
Reviewers:      [none] (suggested)
Access Expires: 2023-08-16 04:37:26
Status:         APPROVED

hint: use 'tsh login --request-id=<request-id>' to login with an approved request

Waiting for request approval...

Approval received, reason="Approve for any reason"
Getting updated certificates...
```

Все аудируется



Сегодня в программе

- SaaS
- VPN
- SSH и RDP
- Kubernetes
- Privileged access management (PAM)
- Databases
- Pipelines

SAML – это дорого

SCIM еще дороже 😢

Plus

A place for small groups to plan & get organized.

$8

per user / month
billed annually
$10 billed monthly

Get started

Everything in Free, and

- ✓ Unlimited blocks for teams
- ✓ Unlimited file uploads
- ✓ 30 day page history
- ✓ Invite 100 guests

Business

For companies using Notion to connect several teams & tools.

$15

per user / month
billed annually
$18 billed monthly

Get started

or Request a Trial

Everything in Plus, and

- ✓ SAML SSO
- ✓ Private teamspaces
- ✓ Bulk PDF export
- ✓ Advanced page analytics
- ✓ 90 day page history
- ✓ Invite 250 guests

Enterprise

Advanced controls & support to run your entire organization.

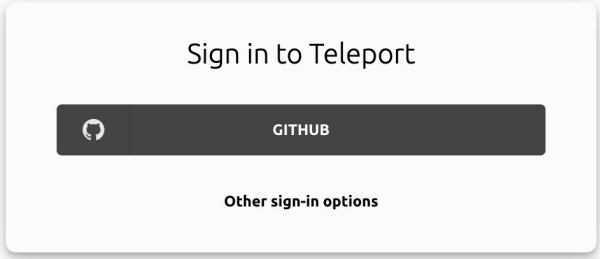
Request a demo

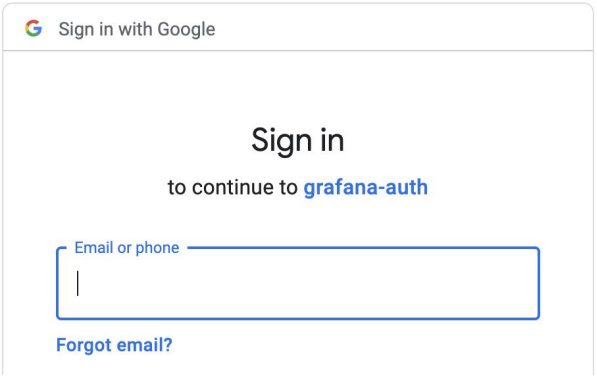
or Request a Trial

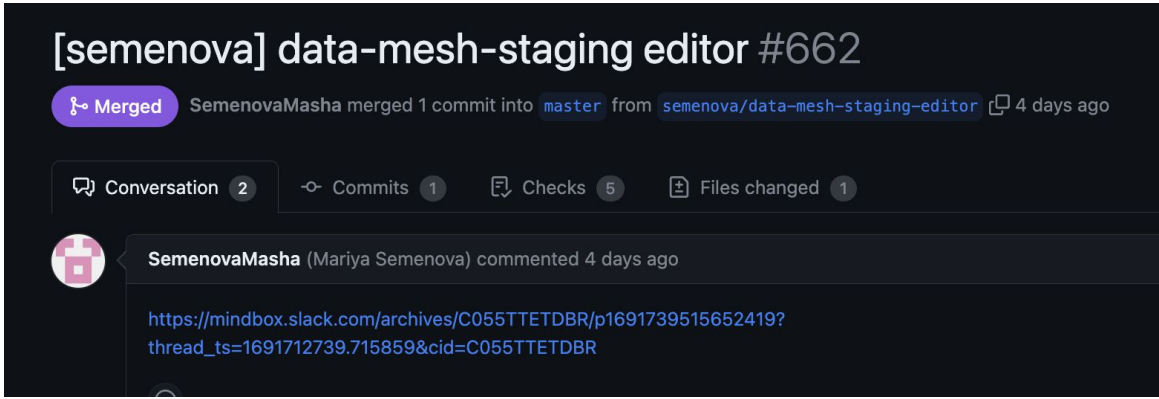
Everything in Business, and

- ✓ User provisioning (SCIM)
- ✓ Advanced security & controls
- ✓ Audit log
- ✓ Customer success manager
- ✓ Workspace analytics
- ✓ Unlimited page history
- ✓ Invite 250 guests

OAuth + Terraform








```
4867          }
4868          "yc" : {
4869            "cloud": []
4870  +         "data-mesh-staging": ["k8s.viewer", "storage.viewer", "storage.editor", "mdb.viewer"]
4871          "data-mesh-production": ["k8s.viewer", "storage.viewer", "mdb.viewer"]
4872          "personalization-production": ["compute.operator"]
4873          "cdp-production": ["storage.viewer"]
```

VPN дает доступ в периметр

… и ненадежно

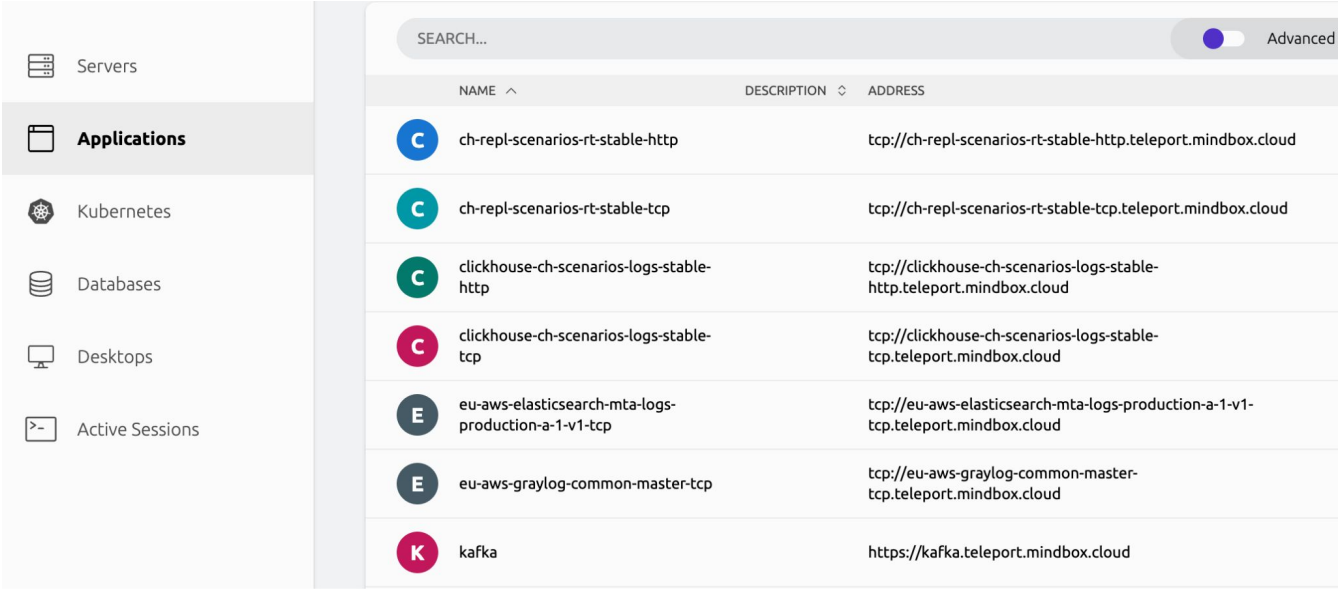
Zero Trust

2FA

RBAC

Audit

Short-lived



SSH и RDP

Revoke при увольнении

Passwordless

Session recording

2FA

Mass SSH

PAM

RBAC

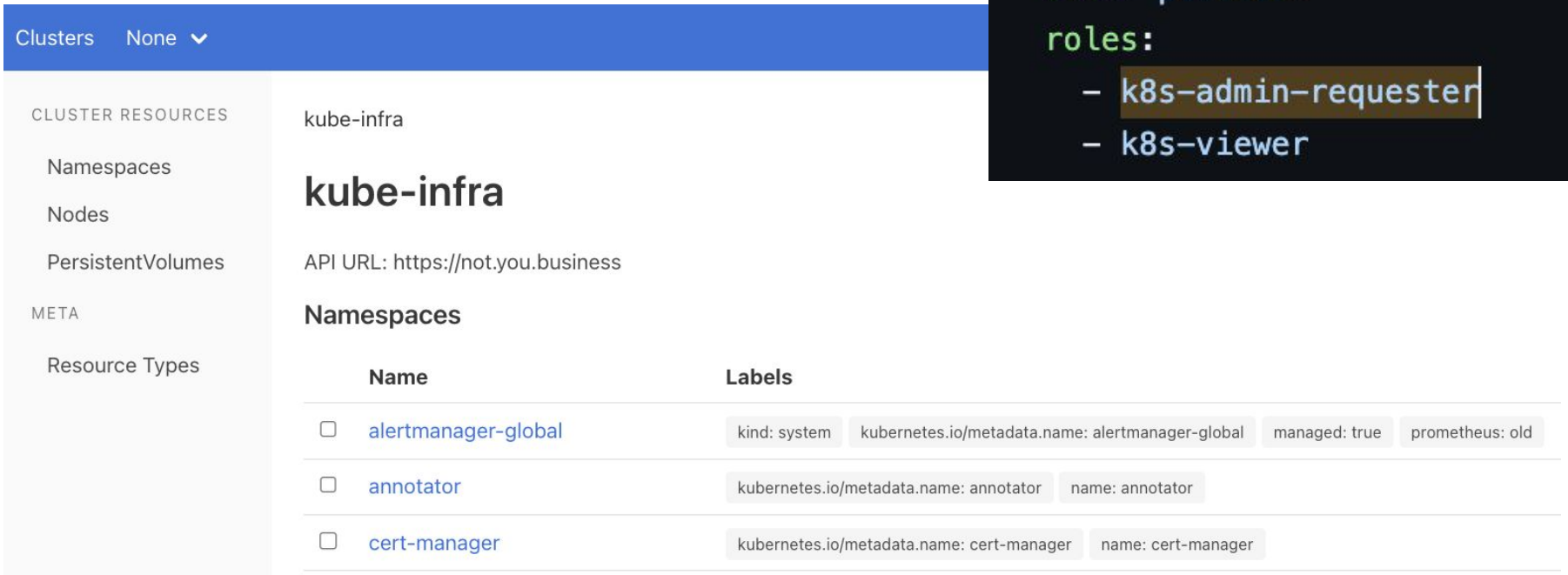
Членство в группе as code
опционально CODEOWNERS

Не sudo а specific rights
например kafka-maintenance

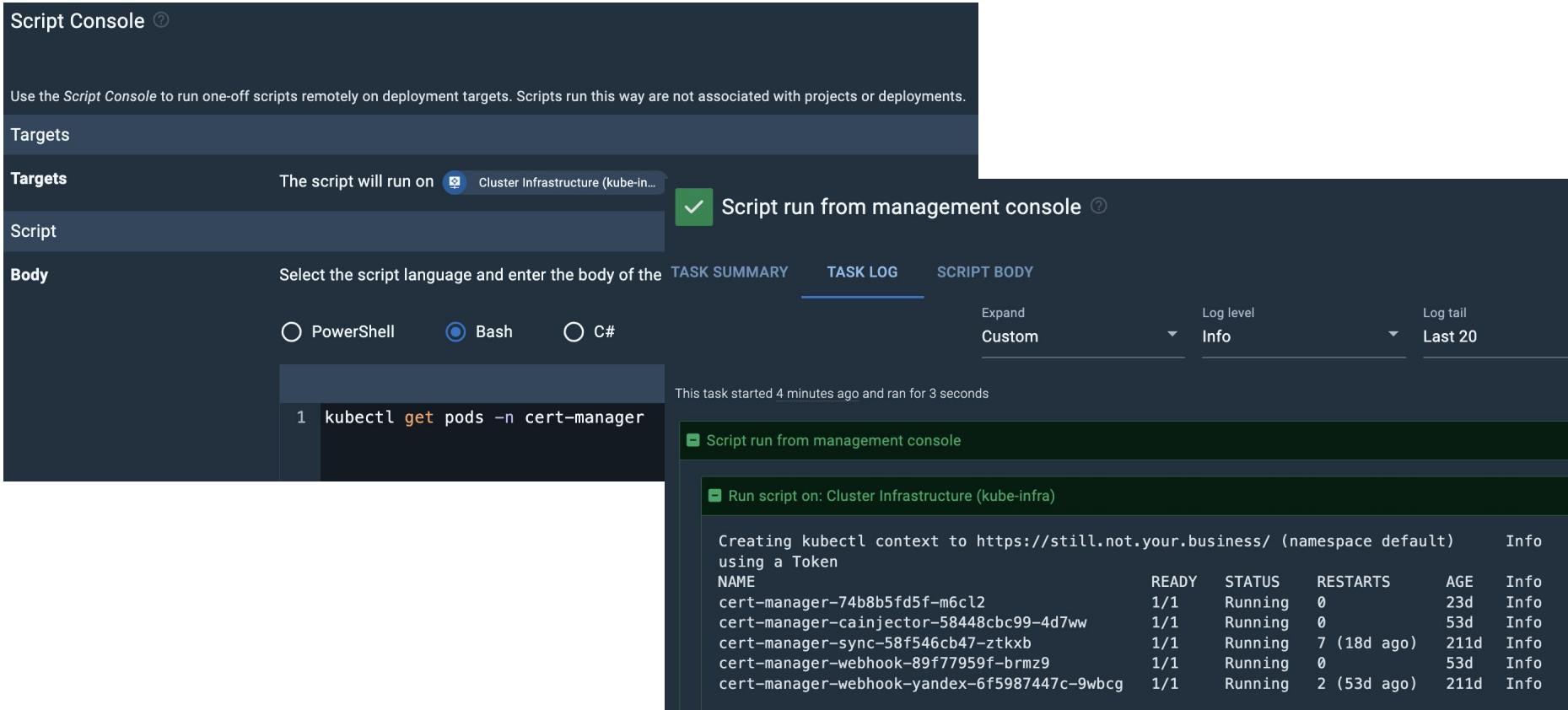
```
- organization: mindbox-cloud
  team: flant
  roles:
    - flant
- organization: mindbox-cloud
  team: product-cdp-admin
  roles:
    - product-cdp-admin
    - apps-all
- organization: mindbox-cloud
  team: it
  roles:
    - k8s-dev
- organization: mindbox-cloud
  team: devwip
  roles:
    - k8s-viewer
```

Kubernetes

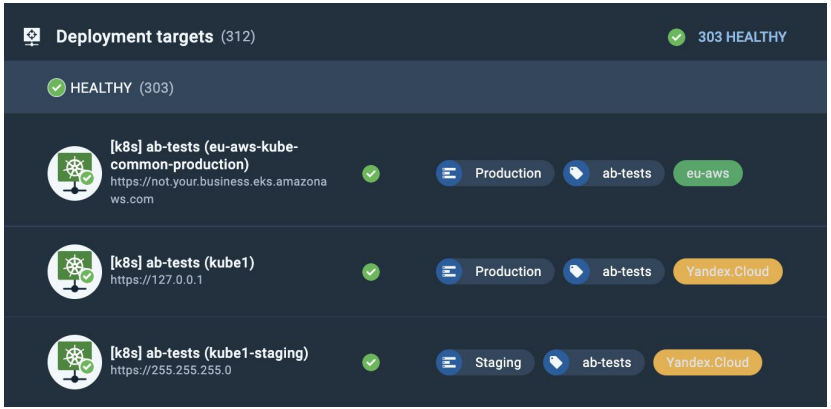
```
- organization: mindbox-cloud
  team: platform
  roles:
    - k8s-admin-requester
    - k8s-viewer
```



Kubernetes + Octopus Deploy



Kubernetes + Octopus Deploy




```
8   resource "octopusdeploy_token_account" "main" {
9     name  = "[k8s] ${var.name} (${var.cluster_name})"
10    token = data.kubernetes_secret.deploy_service_account_token.data.token
11
12    tenanted_deployment_participation = "Tenanted"
13    tenant_tags                       = var.octopus_tenant_tags
14
15    environments = var.octopus_environments
16    lifecycle {
17      ignore_changes = all
18    }
19  }
```

```
"ab-tests" = {
  quotas = {
    limits = {
      cpu    = "2"
      memory = "8Gi"
    }
  }

  deploy_circuits = {
    production = [
      "legacy_stable",
      "legacy_eu",
    ]
    staging = [
      "staging",
    ]
  }

  labels = {
    product = "caprica"
  }

  github = "https://github.com/mindbox-cloud/ab-tests"
}
```

Databases

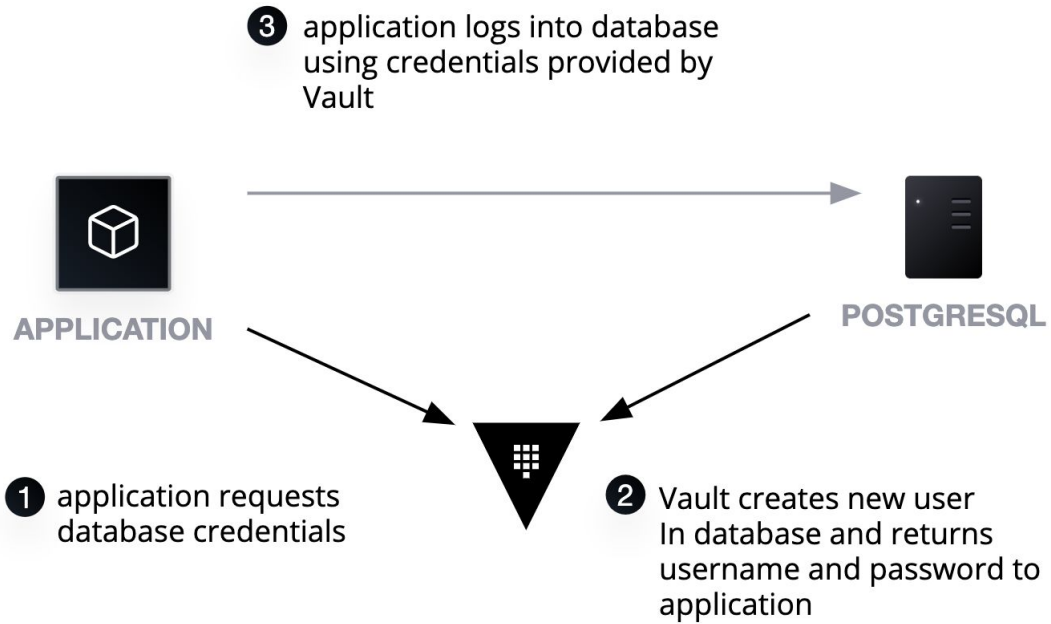
✅ Сетевой доступ - VPN / Teleport DB Access / Teleport TCP Application

❓ Где хранить учетки приложений

❓ Как ротировать

❓ Как подключаться разработчикам

Databases



https://developer.hashicorp.com/vault/docs/secrets

- Cassandra
- Couchbase
- Elasticsearch
- HanaDB
- IBM Db2
- InfluxDB
- MongoDB
- MongoDB Atlas
- MSSQL
- MySQL/MariaDB
- Oracle
- PostgreSQL
- Redis
- Redis ElastiCache
- Redshift
- Snowflake

А если Vault не умеет?

```
apiVersion: v1
kind: Secret
metadata:
  name: "jwt-secret"
type: Opaque
data:
  # retrieve the secret data using lookup function and when not exists, return an empty dictionary / map as result
  {{- $secretObj := (lookup "v1" "Secret" .Release.Namespace "jwt-secret") | default dict }}
  {{- $secretData := (get $secretObj "data") | default dict }}
  # set $jwtSecret to existing secret data or generate a random one when not exists
  {{- $jwtSecret := (get $secretData "jwt-secret") | default (randAlphaNum 32 | b64enc) }}
  jwt-secret: {{ $jwtSecret | quote }}
```

CI/CD

```yaml
jobs:
    build:
        # ...
        steps:
            # ...
            - name: Import Secrets
              id: import-secrets
              uses: hashicorp/vault-action@v2
              with:
                url: https://vault.mycompany.com:8200
                token: ${{ secrets.VAULT_TOKEN }}
                caCertificate: ${{ secrets.VAULT_CA_CERT }}
                secrets: |
                    secret/data/ci/aws accessKey | AWS_ACCESS_KEY_ID ;
                    secret/data/ci/aws secretKey | AWS_SECRET_ACCESS_KEY ;
                    secret/data/ci npm_token
            # ...
```

https://docs.github.com/en/actions/security-guides/security-hardening-for-github-actions

Сколько тратить?

– Стоимость сертификации

– ФОТ

– ПО

1%

*23,5 млн.р. в 23 году

Итого

– Идем от бизнеса

– Едим слона по кускам, не обязательно вливать миллионы

– Работает только если не ошиблись при найме
плюс конечно NDA и прочие страшилки для сотрудников

Предпоследний слайд

Вопросы?

Материалы

- Доклад от Wildberries на PHDays про Teleport
- Продолжение на Highload
- Решения
  - https://github.com/gravitational/teleport
  - https://github.com/hashicorp/vault
  - https://github.com/hashicorp/boundary
  - https://github.com/infrahq/infra
  - https://github.com/OctopusDeploy