ADVISORI

IAM bei Audits im Bereich Softwareengineering in der Cloud

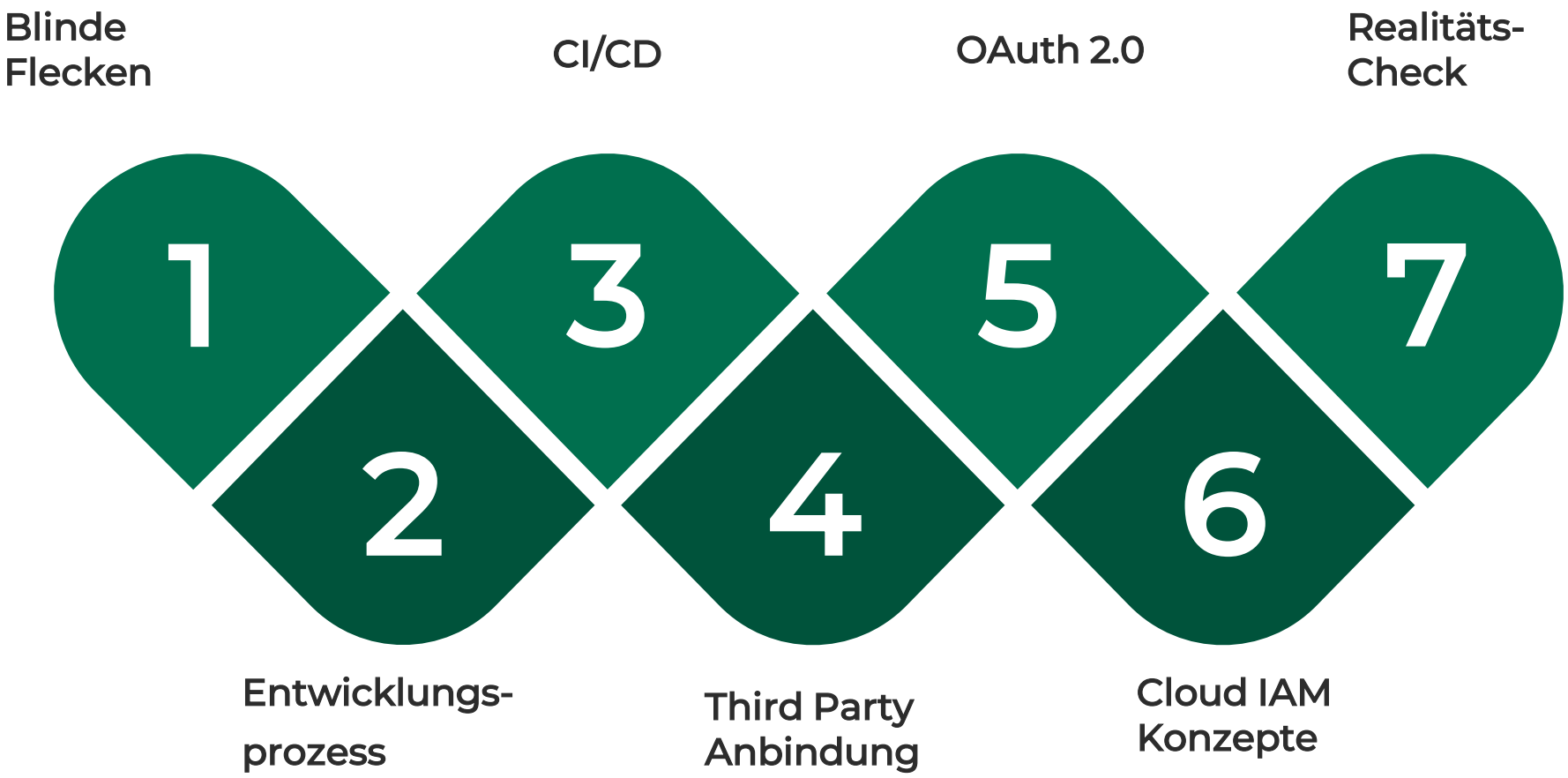
23.11.2023

Wir stellen uns vor

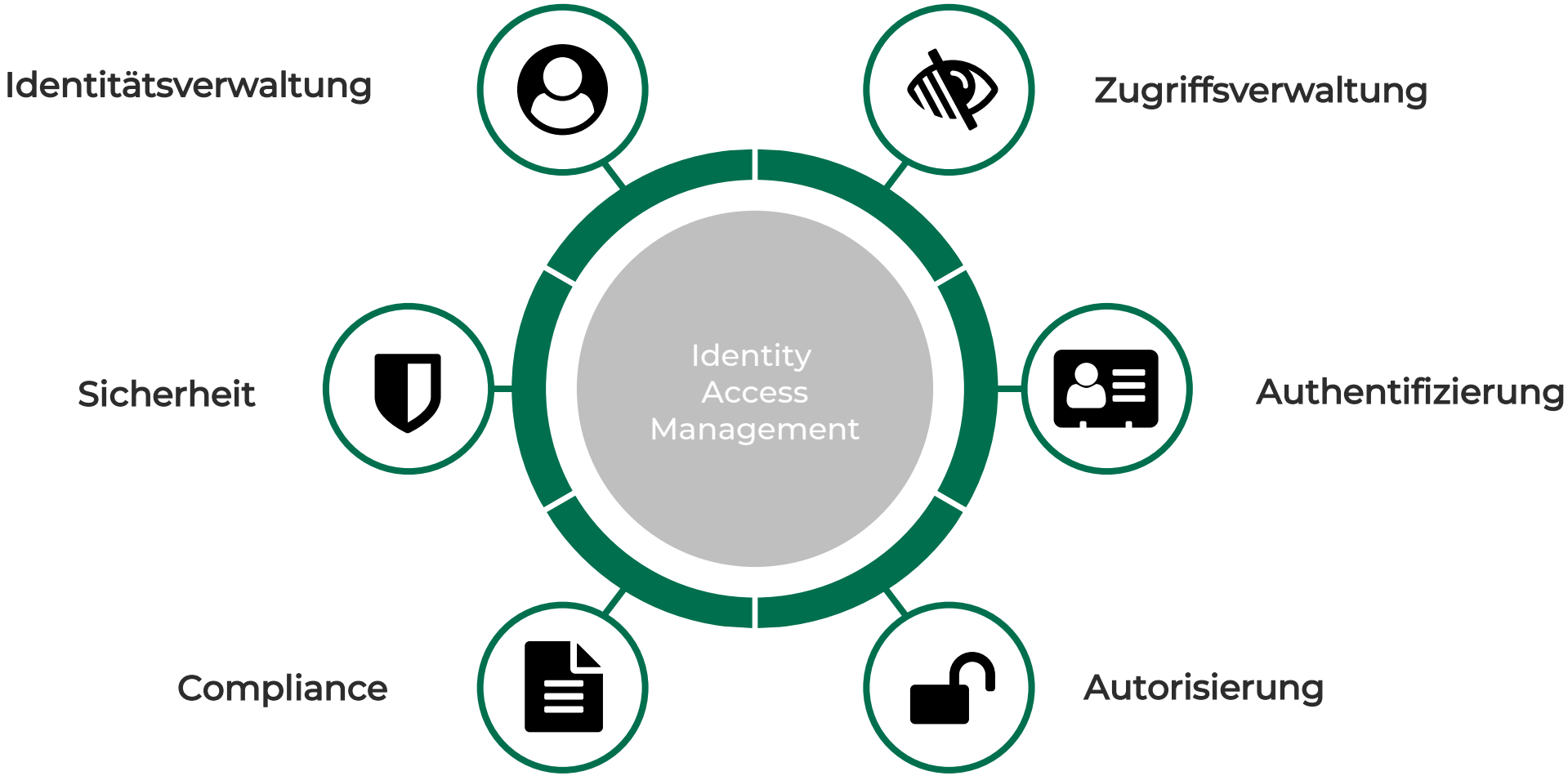
Asan Stefanski
Teamleiter Software Engineering

Felix Eckel
Senior Consultant

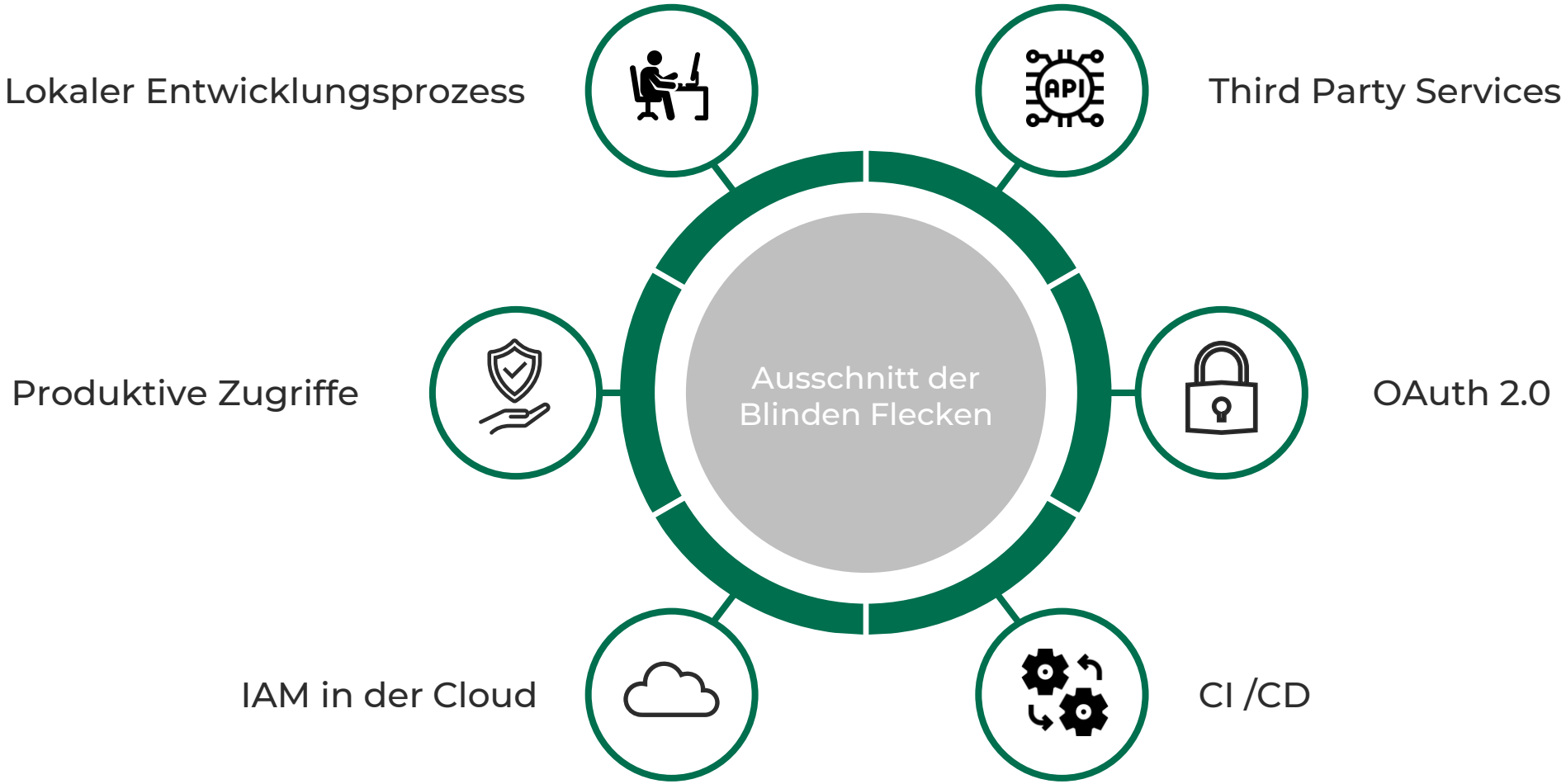
Agenda


Blinde Flecken
1
2
Entwicklungs-prozess
CI/CD
3
4
Third Party Anbindung
OAuth 2.0
5
6
Cloud IAM Konzepte
Realitäts-Check
7

Was ist IAM und warum ist das wichtig?



Was sind die blinden Flecken?



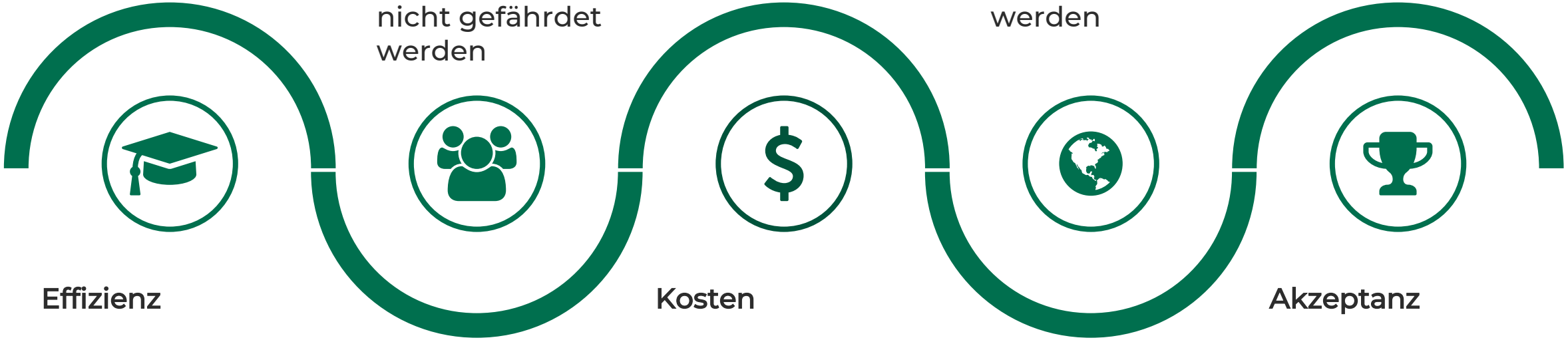
Was sind Anforderungen und Herausforderungen?

Delivery Prozess

- Delivery Prozess darf nicht gefährdet werden

Richtlinien

- Richtlinien wie ISO 27001 müssen eingehalten werden



Effizienz

- Mitarbeiter müssen effizient, arbeits-fähig bleiben

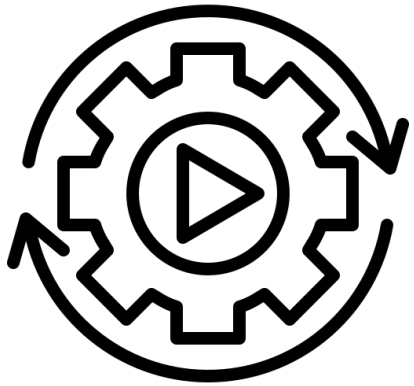
Kosten

- Gesamtkosten dürfen nicht massiv ansteigen

Akzeptanz

- Richtlinien müssen akzeptiert und gelebt werden

Übersicht Lokaler Entwicklungsprozess



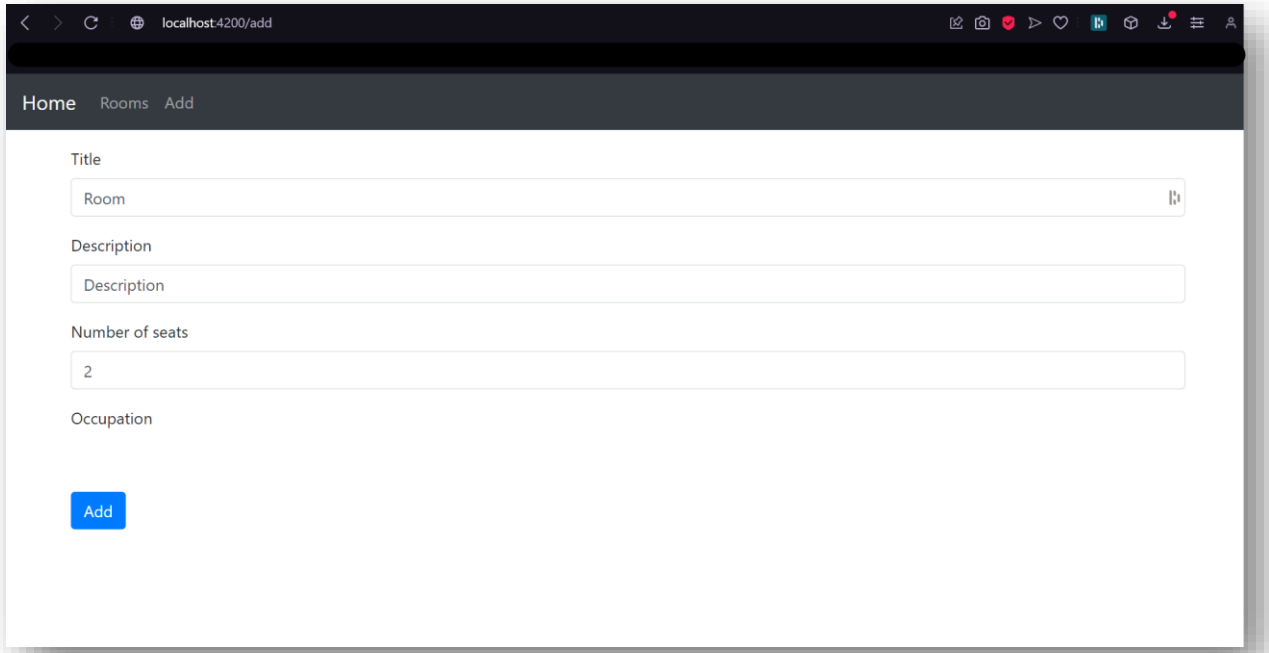
Übersicht Lokaler Entwicklungsprozess

room-add.component.ts

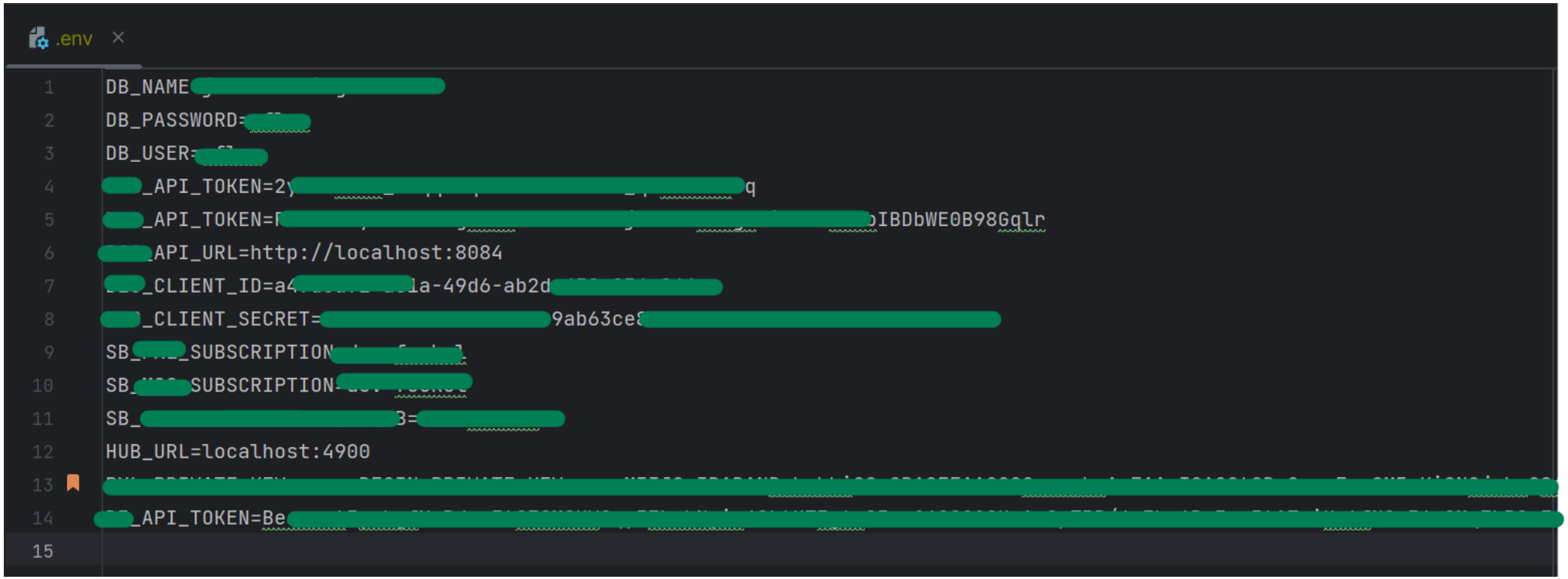
```ts
import {Component, OnDestroy, OnInit} from '@angular/core';
import {FormBuilder, FormGroup, Validators} from "@angular/forms";
import {Room} from "../../models/room.model";
import {RoomService} from "../../services/room.service";
import {Subscription} from "rxjs";

@Component({
  selector: 'app-room-add',
  templateUrl: './room-add.component.html',
  styleUrls: ['./room-add.component.css']
})
export class RoomAddComponent implements OnInit, OnDestroy {
  roomForm!: FormGroup;
  subscriptions: Subscription[] = [];
  submitted: boolean = false;

  constructor(private fb: FormBuilder, private roomService: RoomService) {

  }

  ngOnInit(): void {
    this.roomForm = this.fb.group( controls: {
      title: ['', [Validators.required, Validators.maxLength( maxLength: 50)]],
      description: ['', [Validators.required, Validators.maxLength( maxLength: 200)]],
      numberOfSeats: [null, [Validators.required, Validators.min( min: 1)]],
      occupation: [false]
    });
  }

  get currentRoomForm() {
    return this.roomForm.value;
  }

  onSubmit(): void {
    if (this.roomForm.valid) {
      this.subscriptions.push(
        this.roomService.create(this.currentRoomForm as Room)
          .subscribe( observer: {
            next: (res :Room ) :void  => {
              this.submitted = true;
            },
            error: (e) => console.error(e)
          })
      );
    }
  }

  newRoom(): void {
    this.submitted = false;
    this.roomForm.reset();
  }

  ngOnDestroy(): void {
    this.subscriptions.forEach((e :Subscription ) :void =>{
      e.unsubscribe();
```

ng serve

```
PS C:\Workspace\homework\angular-15-client> npx ng serve
√ Browser application bundle generation complete.

Initial Chunk Files   | Names         |  Raw Size
vendor.js             | vendor        |   2.47 MB |
styles.css, styles.js | styles        | 388.00 kB |
polyfills.js          | polyfills     | 314.28 kB |
main.js               | main          |  47.42 kB |
runtime.js            | runtime       |   6.53 kB |

                      | Initial Total |   3.21 MB

Build at: 2023-11-20T12:47:04.933Z - Hash: a6f852d248611143 - Time: 13597ms

** Angular Live Development Server is listening on localhost:4200, open your browser on http://localhost:4200/ **


√ Compiled successfully.
```

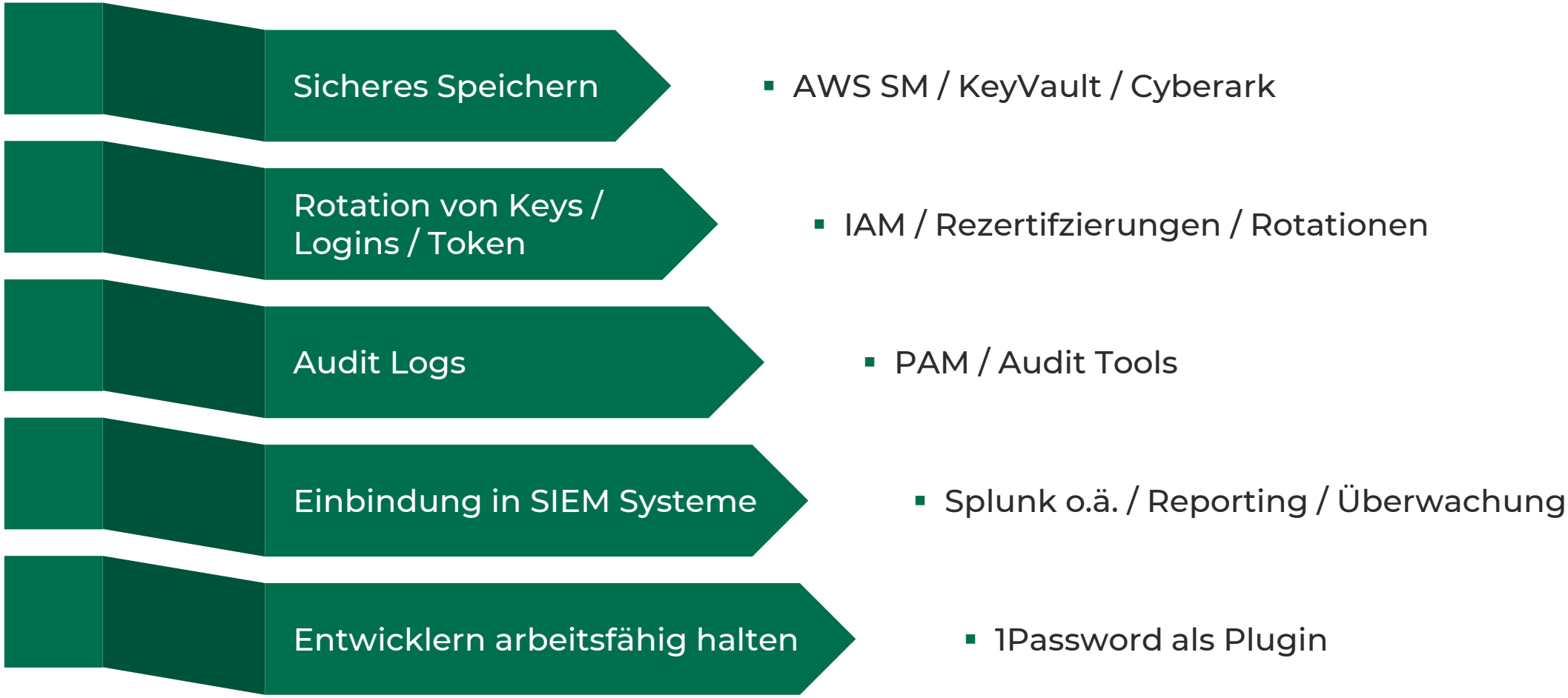


Lokale Keys and Secret



Was ist die Lösung?

Was ist die Lösung?



Häufige Fehler im Umgang mit Key und Secrets

1. Speichern von Passwörtern und im GIT-Repository
2. Quellcode
3. Festplatte
4. Austausch von Keys über Chats, Emails
5. Passwörter werden NICHT rotiert oder deaktiviert und sind zusätzlich personalisiert
6. Keinerlei Überwachung der Accounts durch SIEM / Audit Logs

Was steckt hinter CI/CD?

Alte Arbeitsweise

Lokaler Code

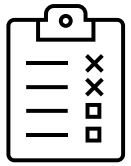
Lokaler Build

Lokaler Test

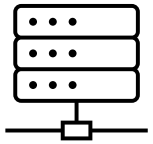
Lokale Bereitstellung

Dev

Manuelle Installation



Manuelle Tests



Betrieb

Monitoring

OPS

Moderne Arbeitsweise

Lokaler Code

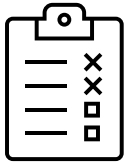
Cloud Code

Cloud Pipeline

Cloud Test

Docker Registry

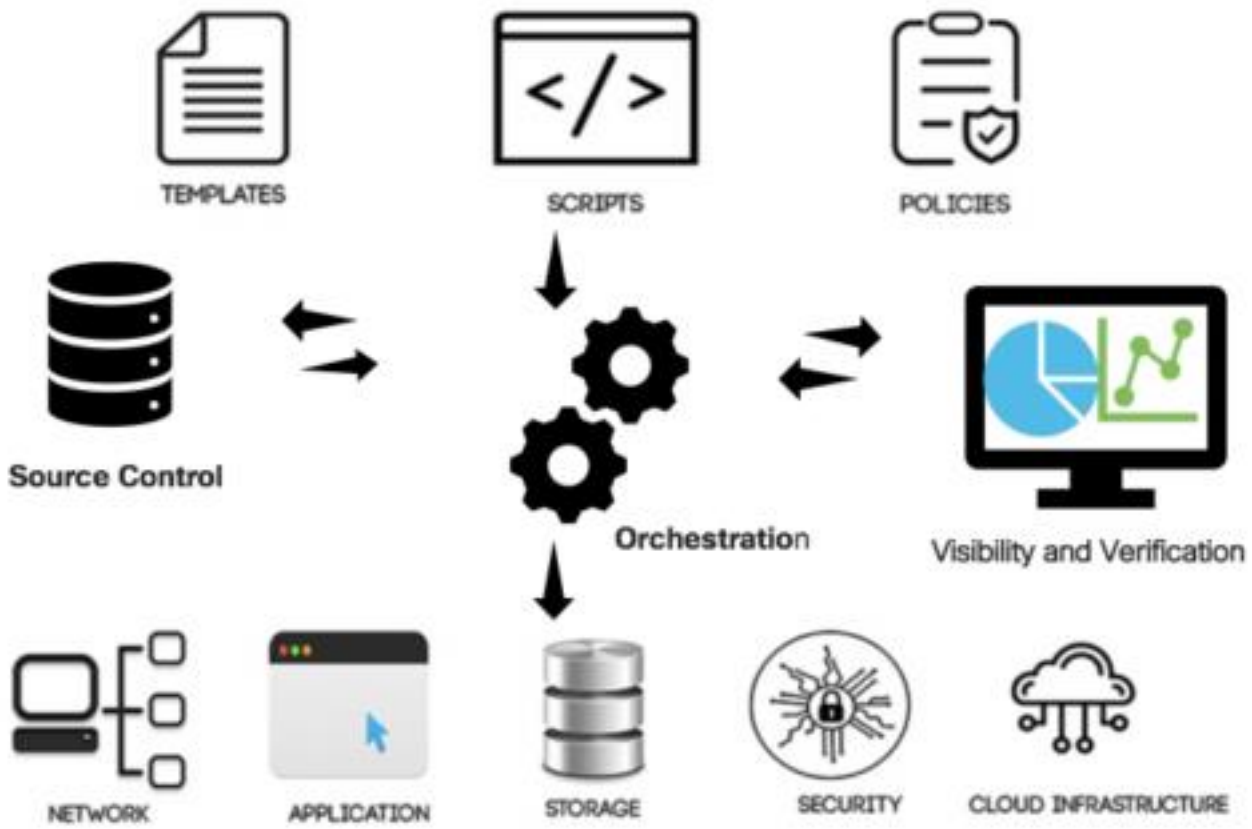
Execute as Container



Integrations Tests

Monitoring

Was ist Infrastructure as Code?




```
0 references
resource "aws_cloudformation_stack" "my-terraform-outputs" {
  name = "my-terraform-outputs"
  template_body = <<STACK
{
  "Resources": {
    "MyQueueArn": {
      "Type": "AWS::SSM::Parameter",
      "Properties": {
        "Name": "my-queue-arn",
        "Type": "String",
        "Value": "${data.aws_sqs_queue.my-queue.arn}"
      }
    },
    "MyQueueUrl": {
      "Type": "AWS::SSM::Parameter",
      "Properties": {
        "Name": "my-queue-url",
        "Type": "String",
        "Value": "${data.aws_sqs_queue.my-queue.url}"
      }
    }
  },
  "Outputs" : {
    "MyQueueArn": {
      "Value": "${data.aws_sqs_queue.my-queue.arn}"
    },
    "MyQueueUrl": {
      "Value": "${data.aws_sqs_queue.my-queue.url}"
    }
  }
}
STACK
}
```

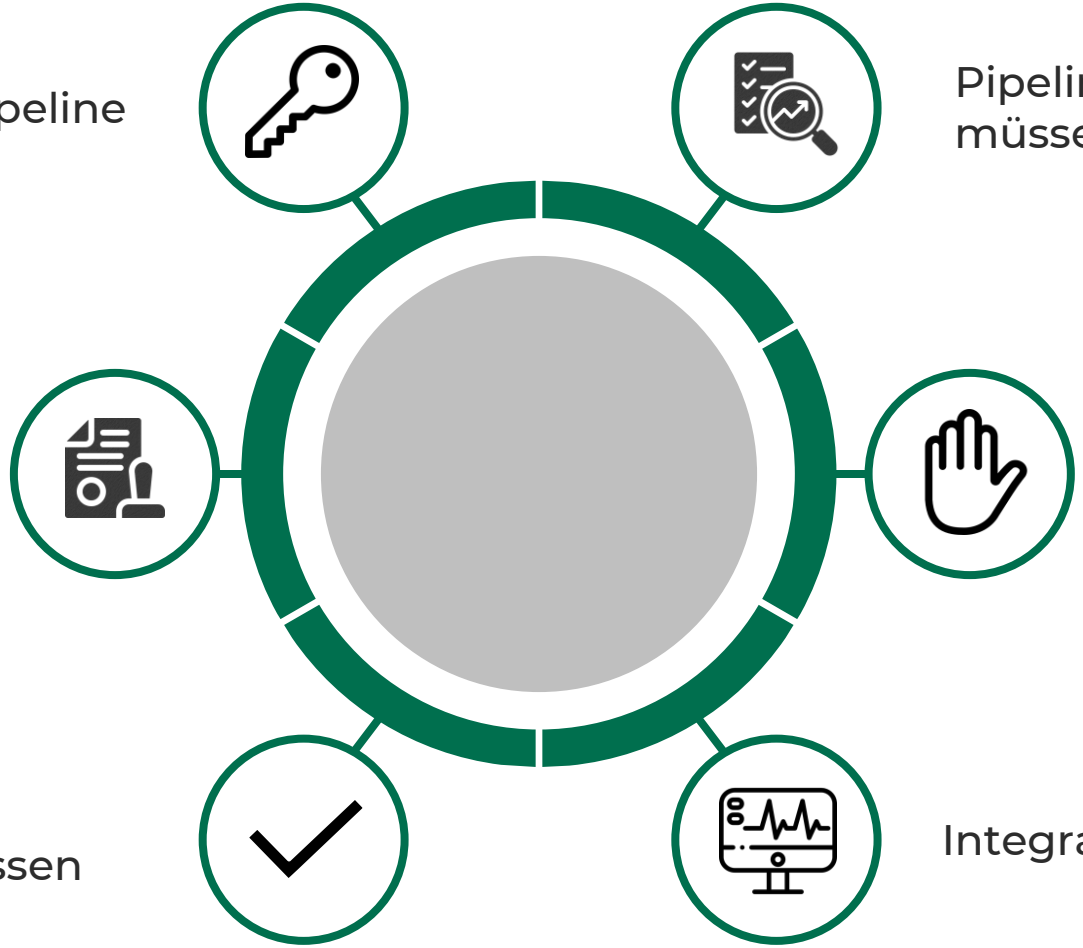
Was sind Herausforderungen und Probleme?

Was sind die Lösungsansätze?

Integration von IAM in der Pipeline

Pipelines und Terraform Skripte müssen auditiert werden

Approval Verfahren in die Pipeline Integrieren



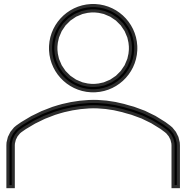
Manuelle Zugriffe über PAM

Einführung von Rezertifizierungsprozessen

Integration von SIEM / SOAR

Integration von Thirdparty Services in eigener Applikation

Praxis Beispiel:



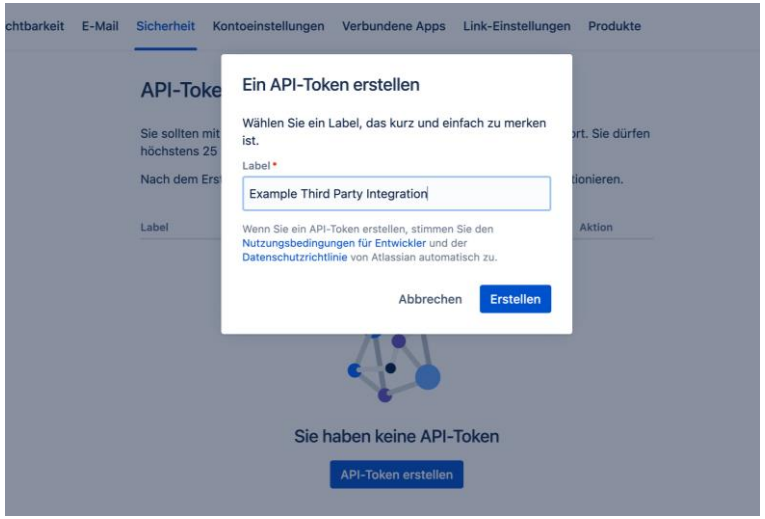
Kunde

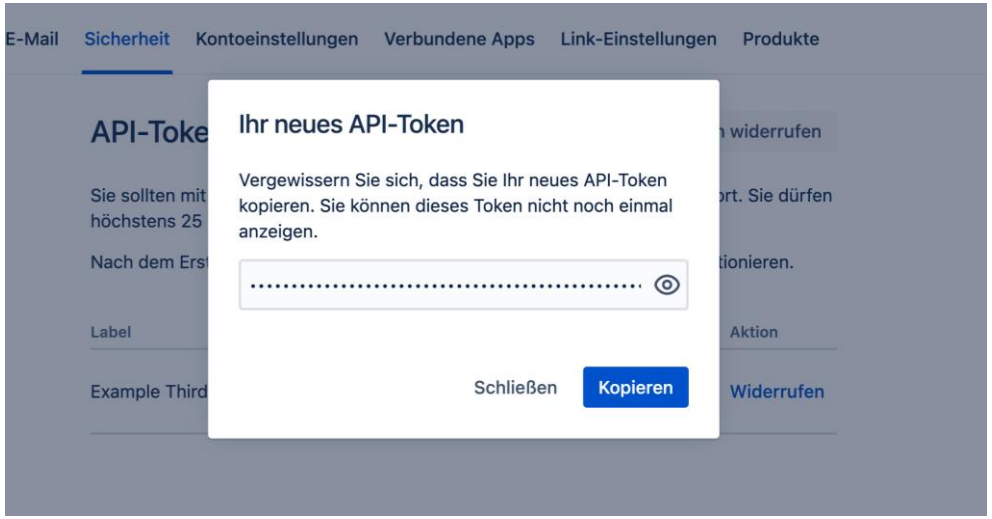
Self-Service-Plattform

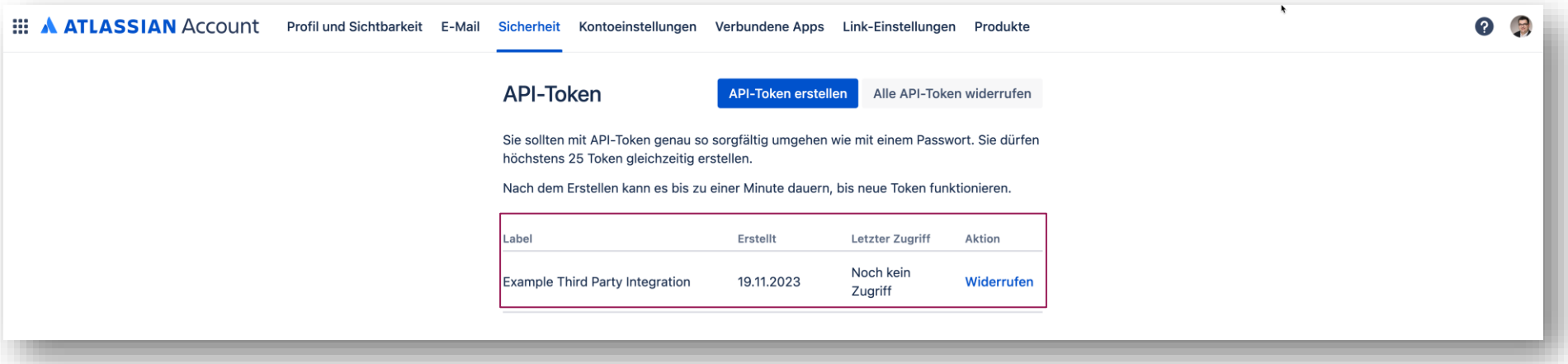
Backend Server

Third Party: Jira

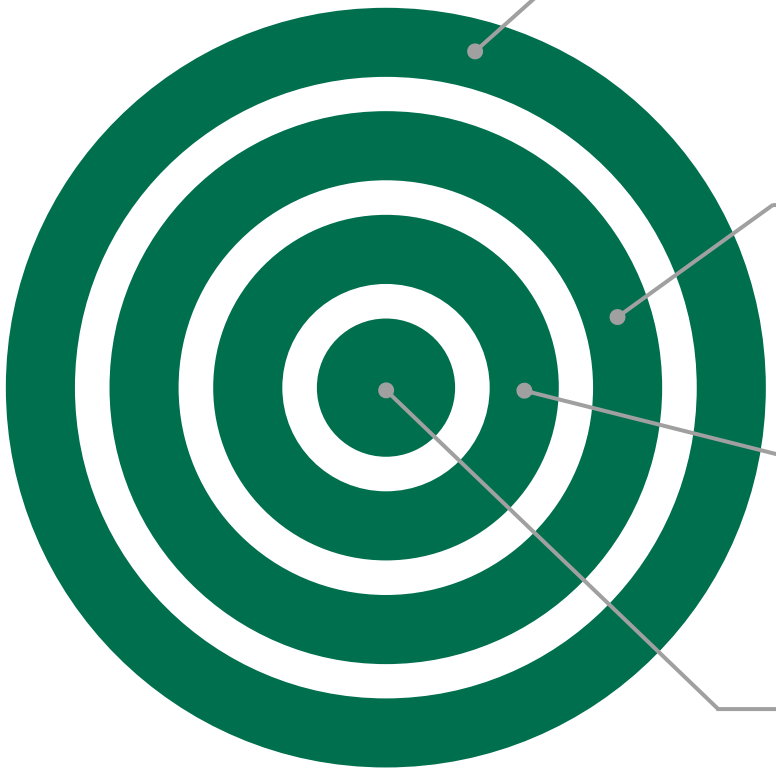
Integration von Thirdparty Services







Wo und wie werden die Keys gespeichert?



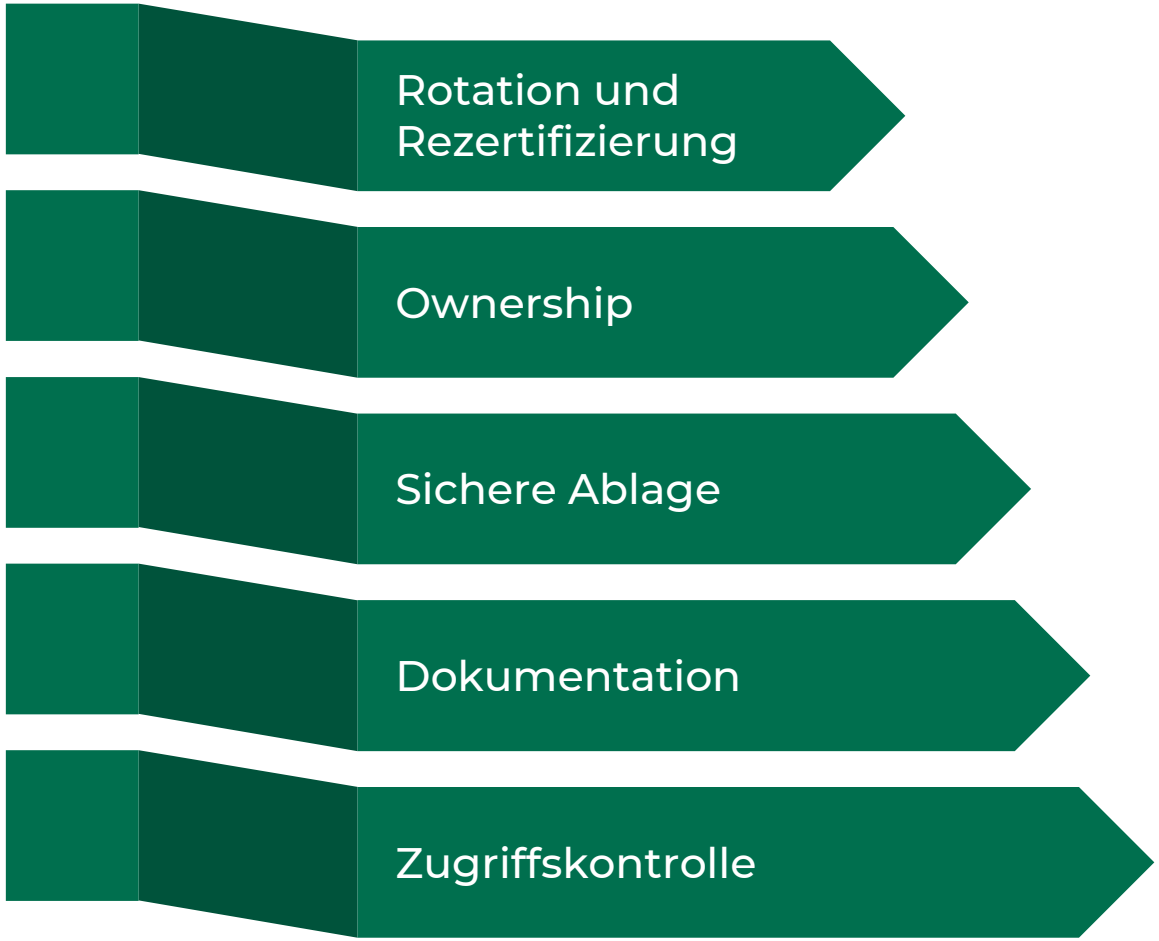
Lokal z. B. in .env File

Im statischen Code

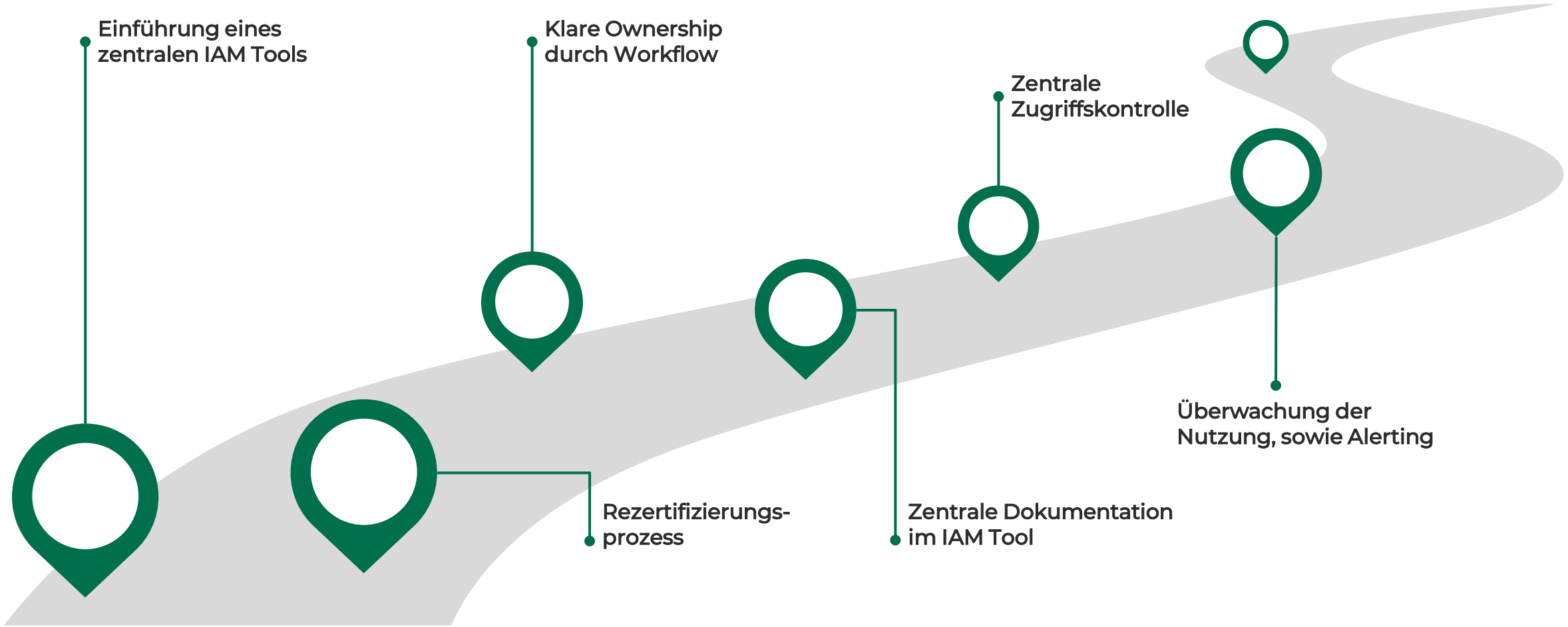
Als Klartext in den Cloud Settings

Secret Manager / Key Cloak / Passwort Manager

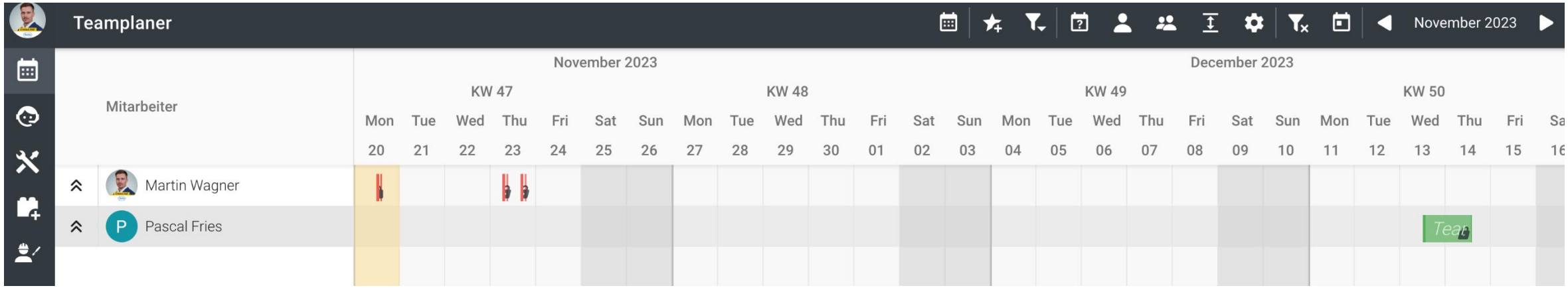
Welche Probleme ergeben sich daraus?

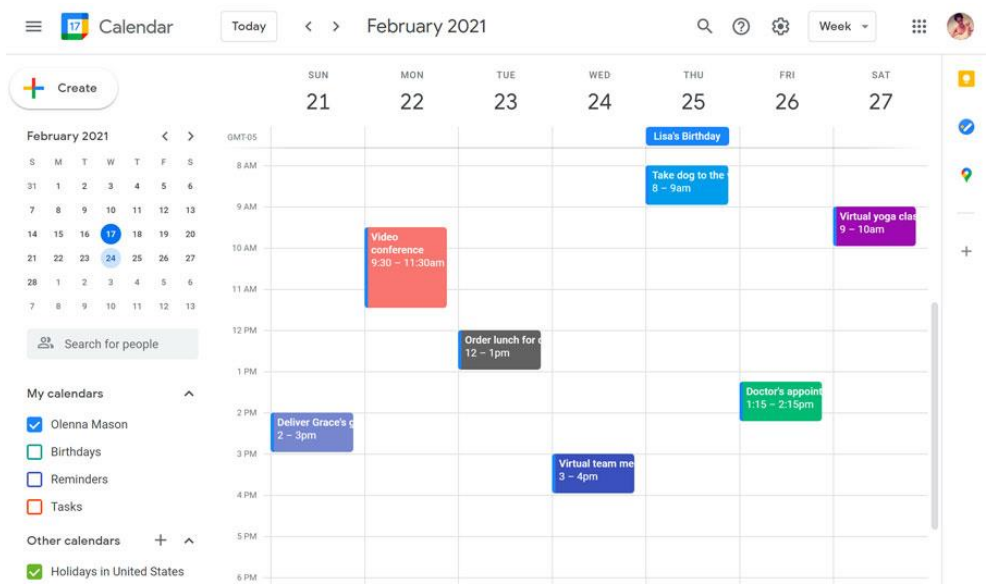


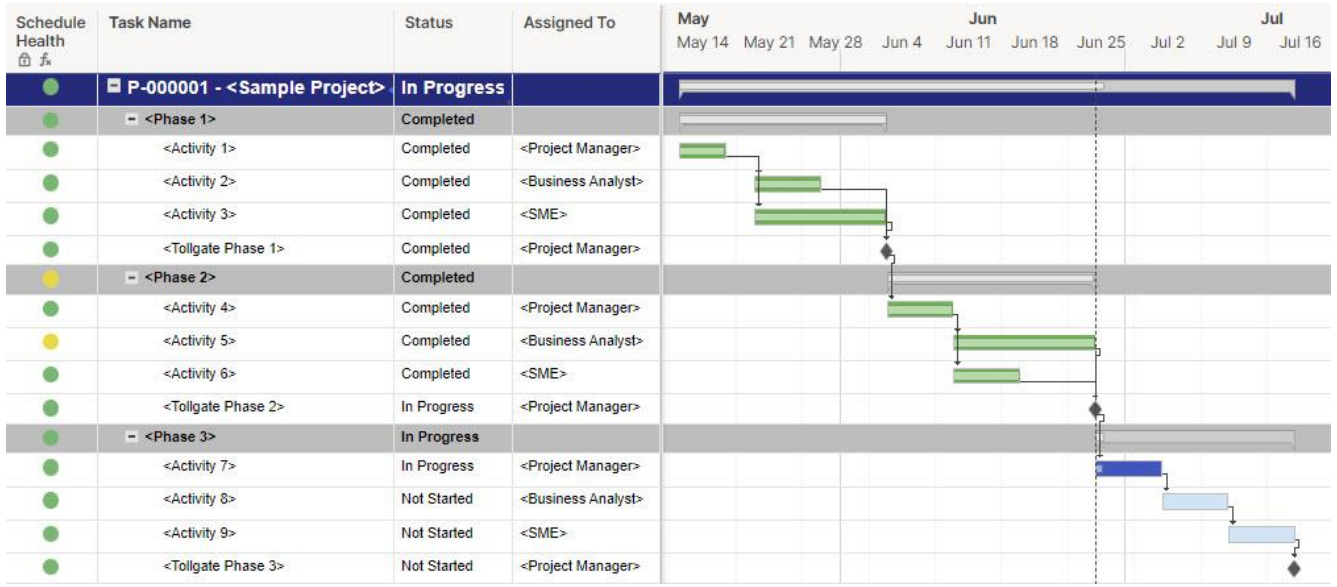
Wie lösen wir das nun?



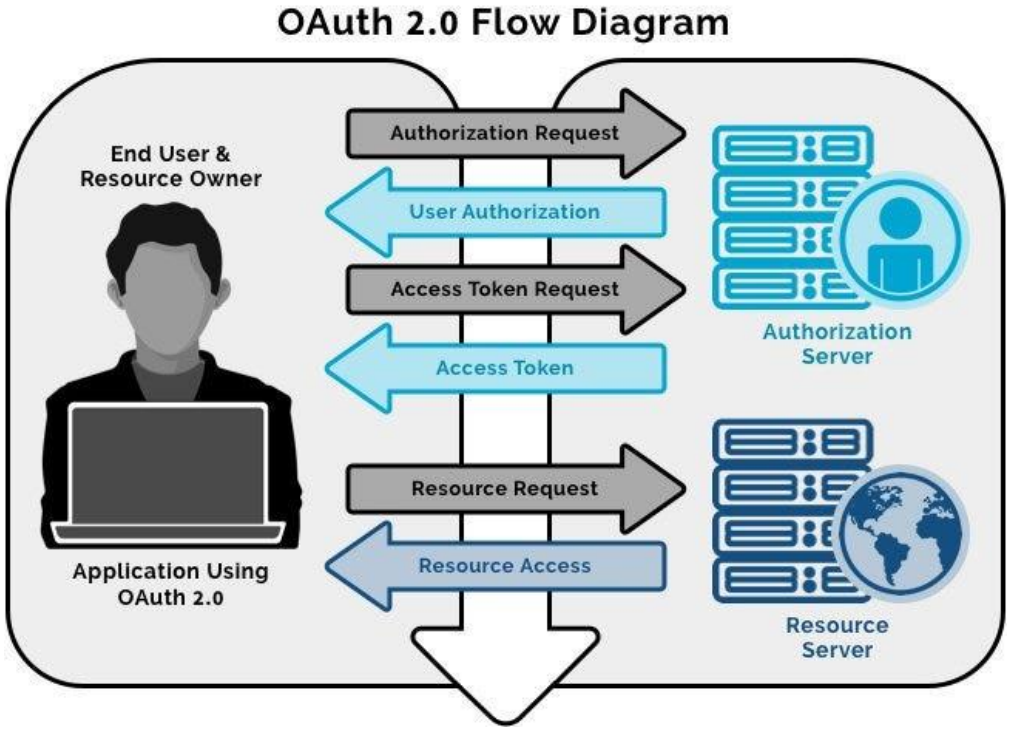
Use Case SAAS Ressourcenmanager

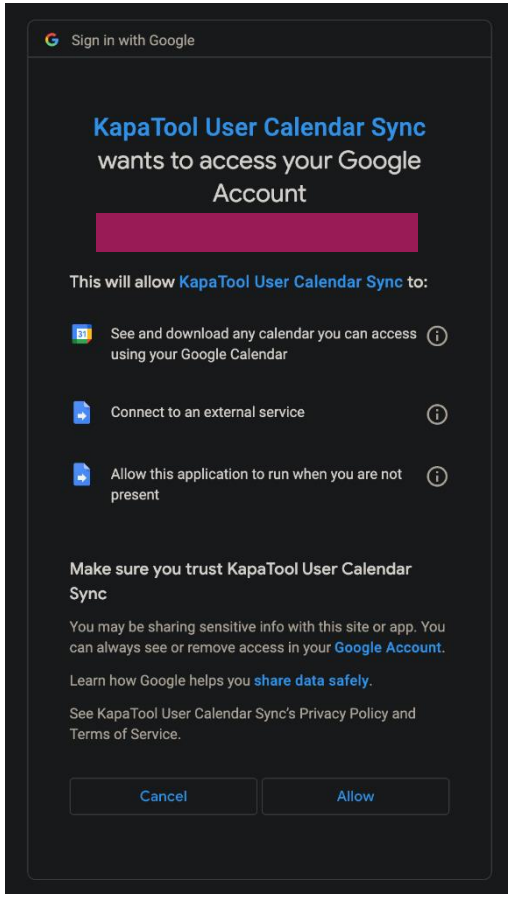


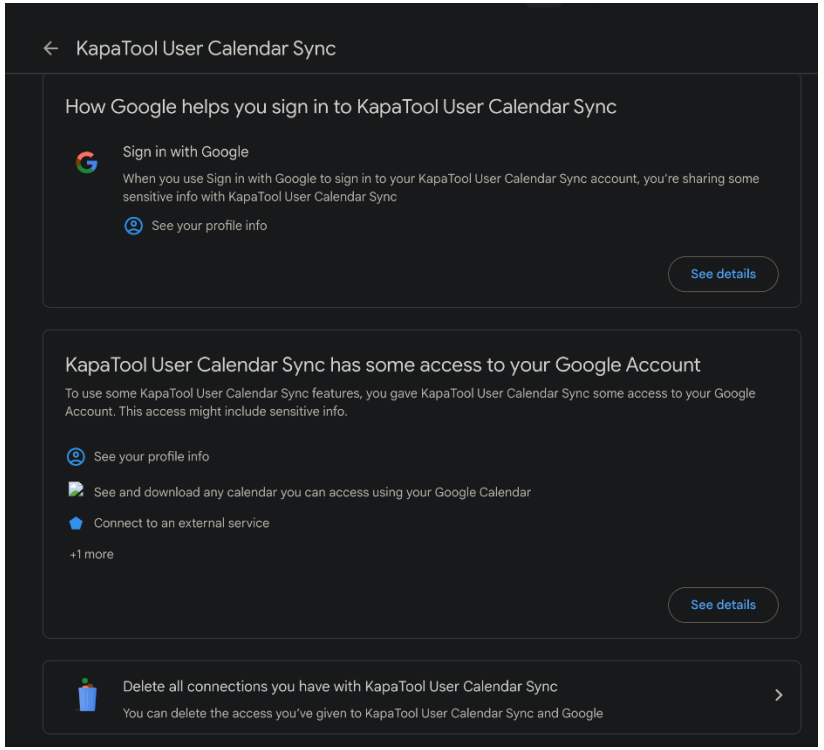




Was steckt hinter dem OAuth 2.0 Protokoll?



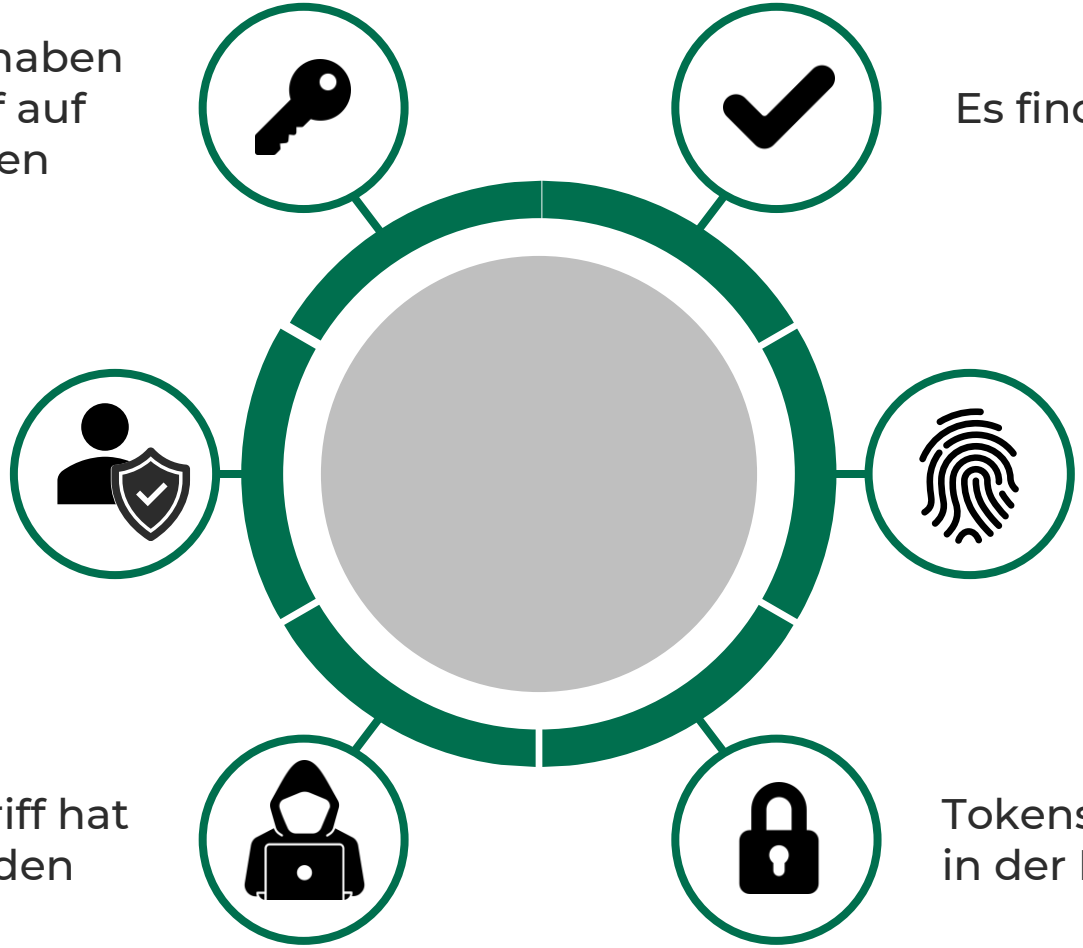




Was bedeutet das für ein Unternehmen?

Third Party Provider haben dauerhaften Zugriff auf Service - Ressourcen

Es findet keine Rezertifizierung statt



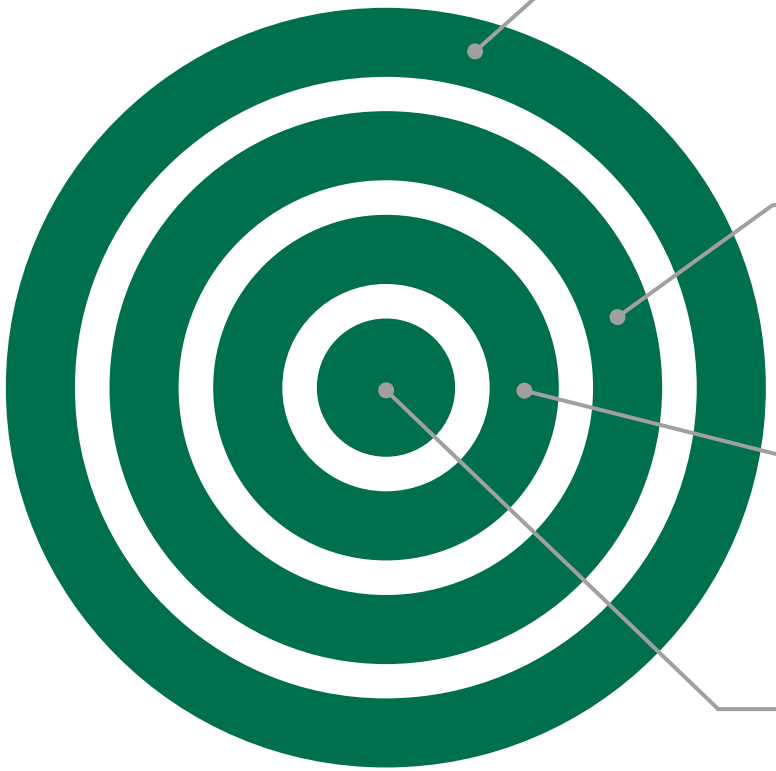
Kunden erkennen den Unterschied nicht zwischen Third Party und Original

potentieller Datenschutzverstoss

Jeder Developer mit DB Zugriff hat Zugriff auf Daten der Kunden

Tokens werden unverschlüsselt in der Datenbank gespeichert

Wie gehen wir damit um?



Einbindung IAM Tool inkl. Rezertifizierung

- Zugriff auf DB nur noch per PAM sogar für Test

Zugriff auf Schnittstellen mit Audit Logs

- Verschlüsseln der Keys wie Refreshtoken etc.

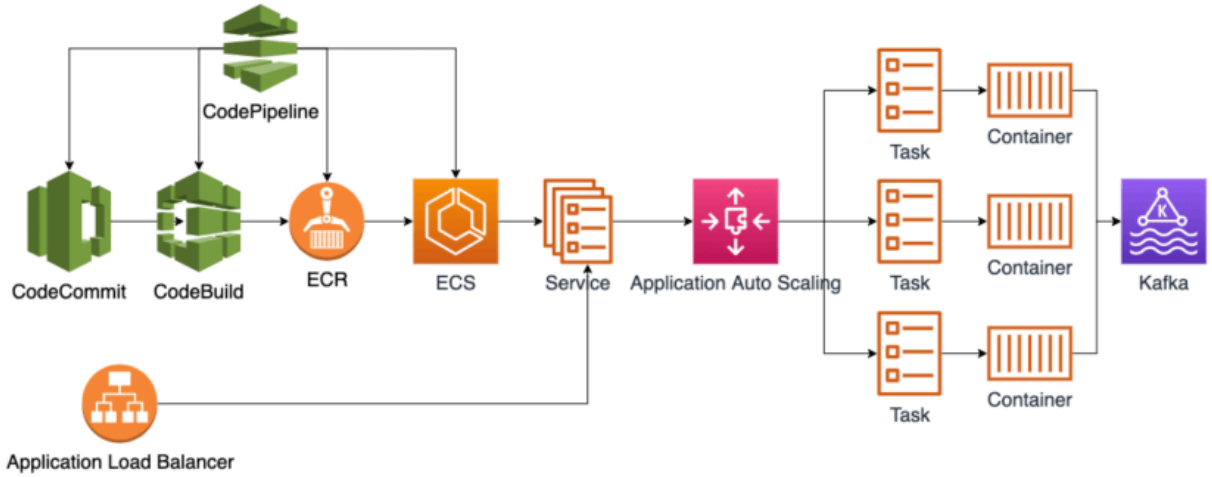
Trennung der Services Requests

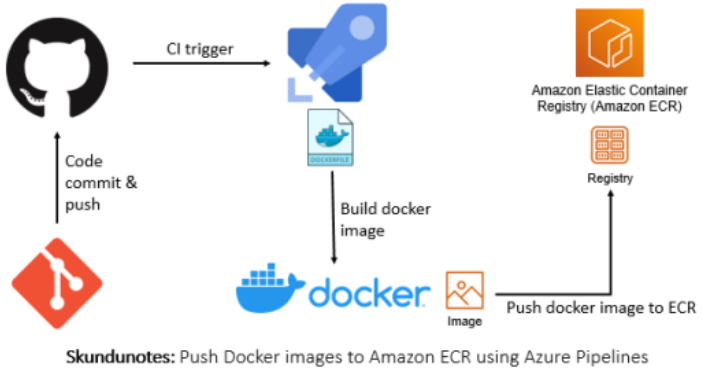
- Wenn möglich System User verwenden mit Audit Logs

Schulung der Mitarbeiter über Technologie

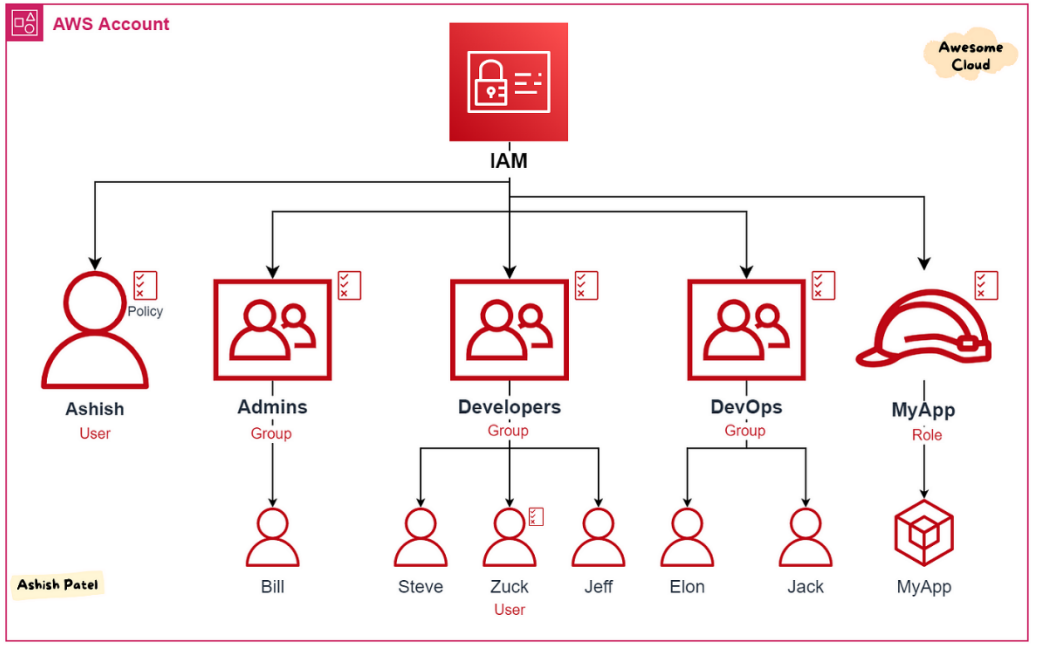
- Überwachung der Freigaben durch SIEM und SOAR

Welche Komplexität steckt hinter IAM in der Cloud?





Skundunotes: Push Docker images to Amazon ECR using Azure Pipelines



Herausforderungen

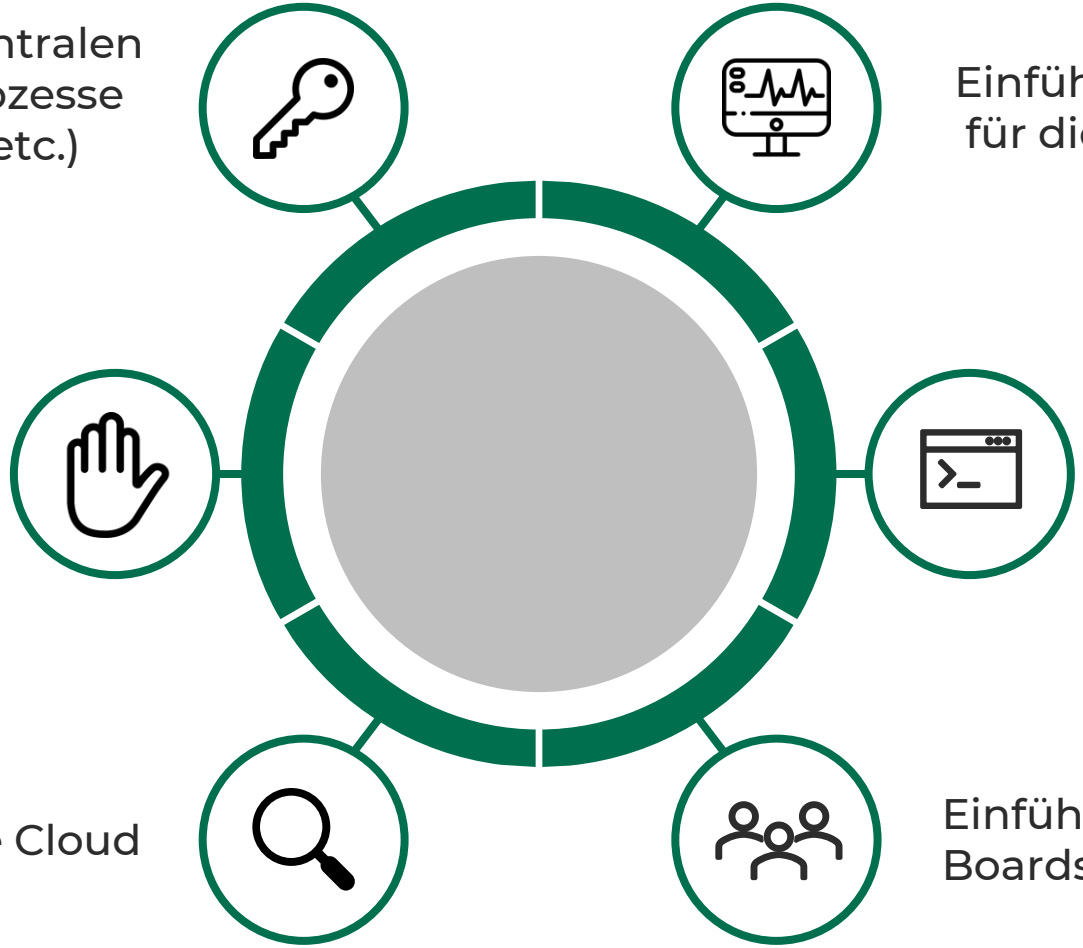
- Wie wird die Konfiguration auditiert?
- Es findet kein Rezertifizierung für IAM statt
- Keine Integration in IAM Prozesse
- Keine Überwachung durch SIEM / SOAR für SOC
- Zentrales und sauberes Audit Log
- Developer haben Administratorzugriff
- SDK Keys sind nicht teil des IAM Prozesses

Lösungen

Einführung eines zentralen IAM Tools sowie Prozesse (Rezertifizierung etc.)

Einführung von SIEM / SOAR für die Cloud

Einführung von PAM für die manuelle Konfiguration

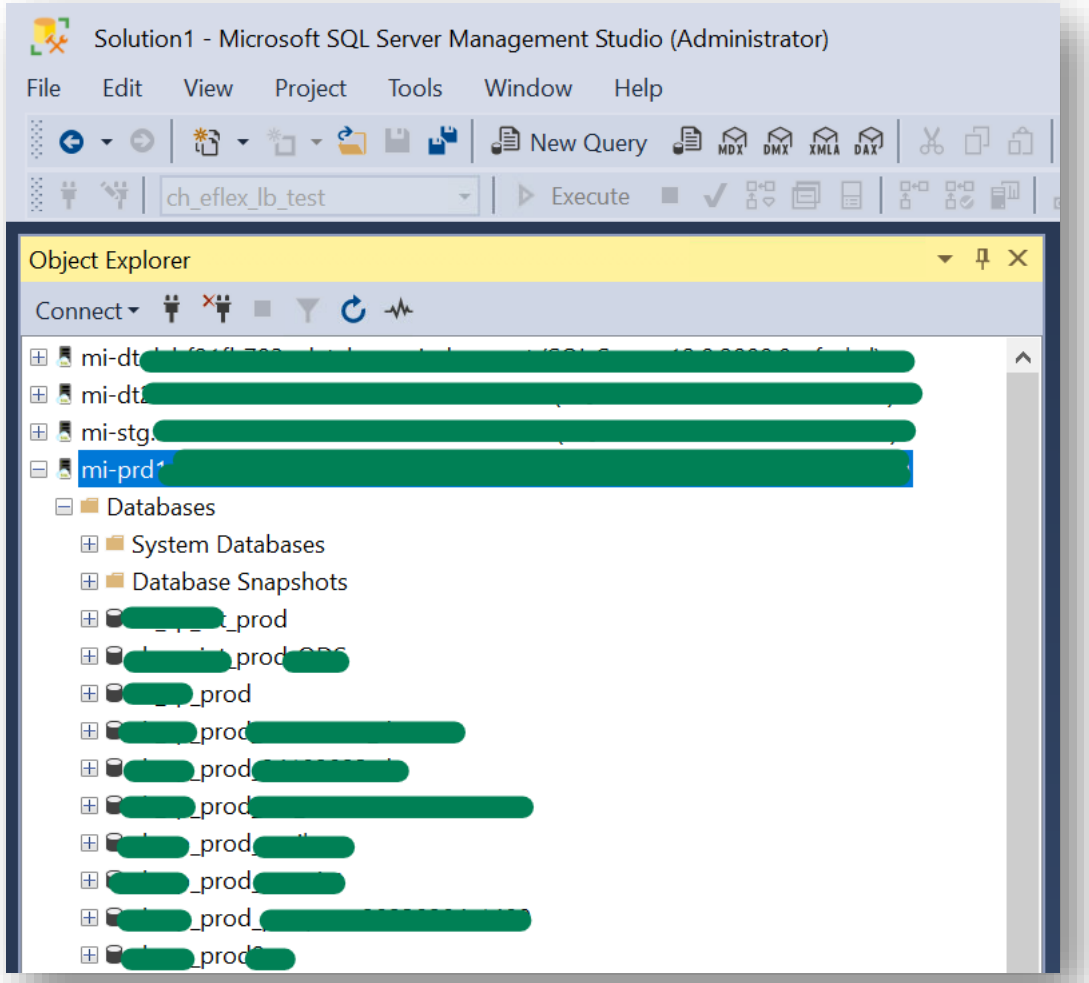


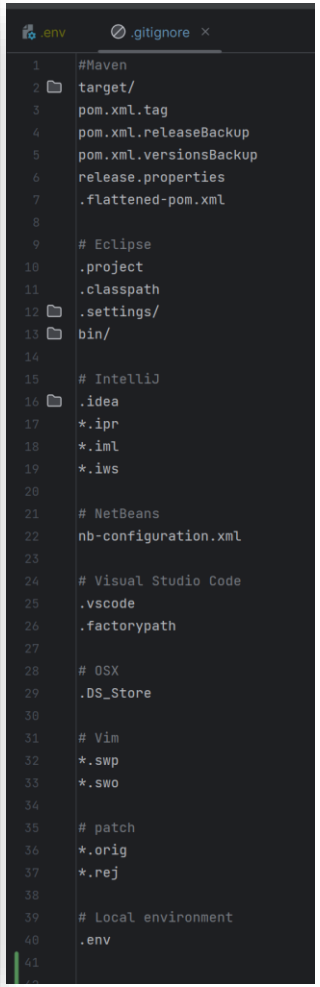
Konfiguration durch Terrafrom

Audit Prozess für die Cloud

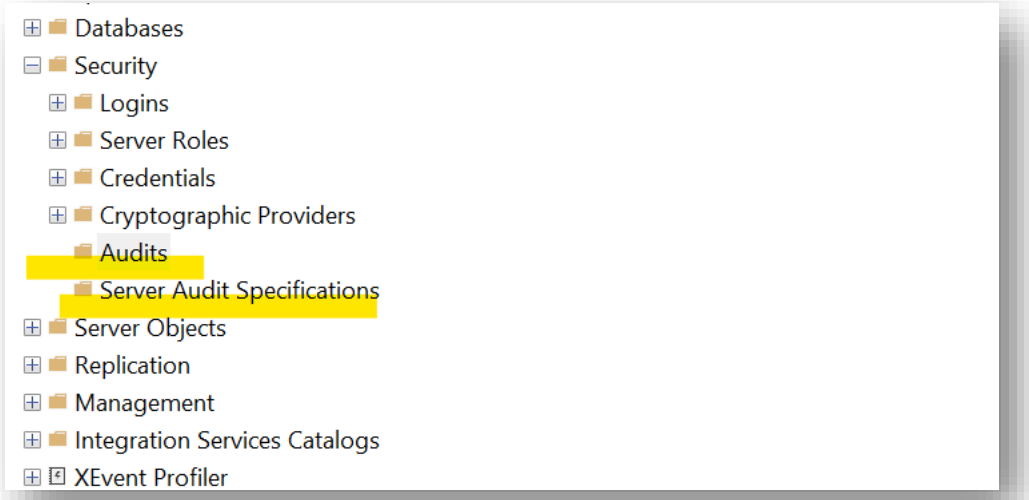
Einführung eines Architektur Boards

Wie wird mit produktiven Umgebungen umgegangen?

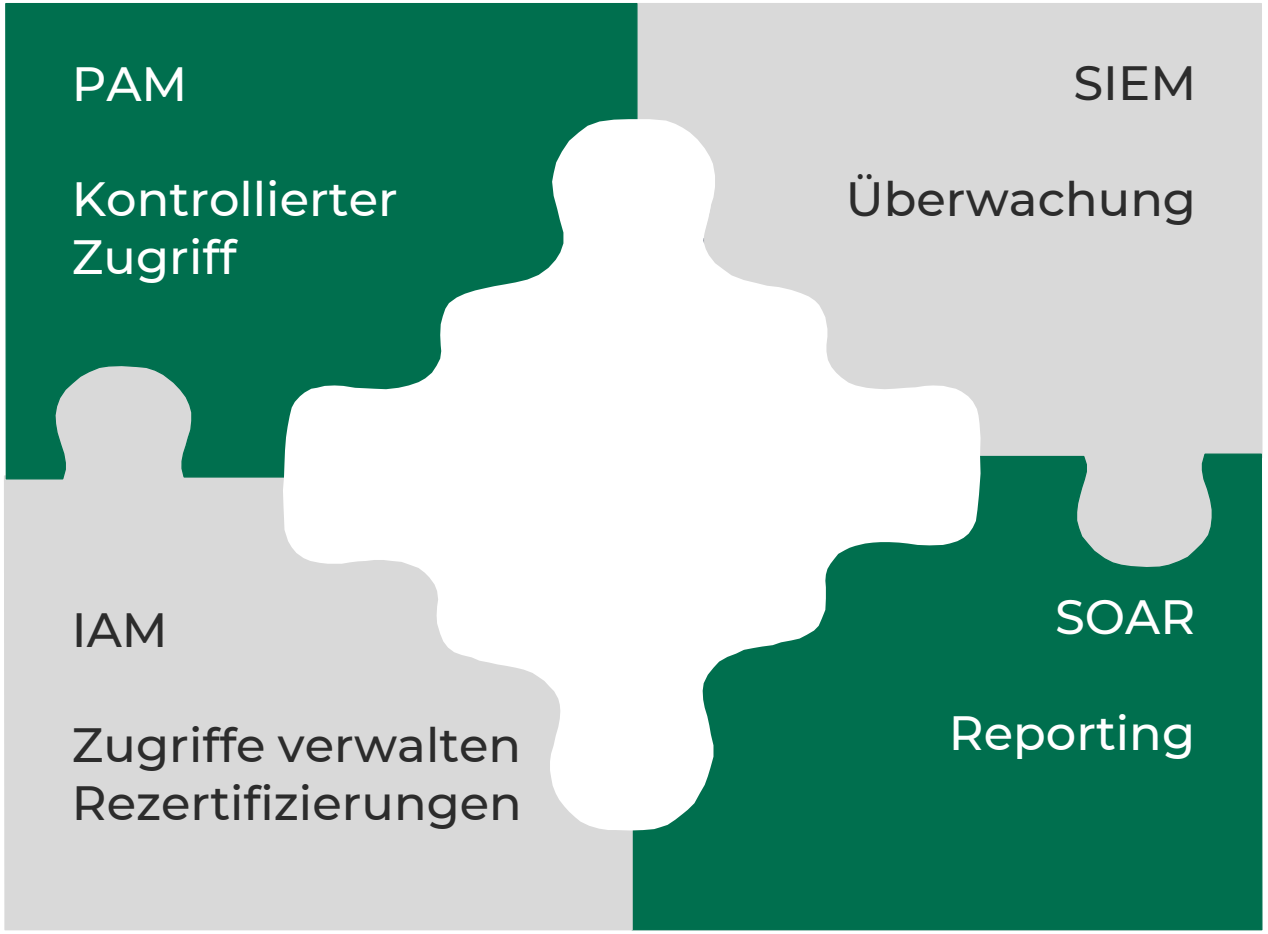




1. Datenbankzugriffe
2. Dateien werden lokal gespeichert
3. Überwachung selten etabliert
4. Rotation selten der Fall
5. Developer Accounts fehlen oft in IAM Tools
6. Cloud ist oft aus IAM/SIEM/ exkludiert



Was ist die Lösung?



Fazit

- ✓ Blinde Flecken sind nur die Spitze des Eisbergs
- ✓ Risiko von Software Entwicklung reduzieren und potentielle Sicherheitslücken schließen
- ✓ Prozesse etablieren, welche Produkte nicht nur sicher machen sondern auch Kosten moderat halten
- ✓ Prozesse, die den Entwicklungsprozess nicht einschränken, verlangsamen oder die Kosten erhöhen
- ✓ Wir müssen den Prozess in die Entwicklung integrieren, Qualität und Vertrauen erhöhen
- ✓ Prozesse müssen gelebt werden
- ✓ Es müssen Wege gefunden werden, um diese Herausforderungen zu meistern
- ✓ ISMS für Software Entwicklung

DANKE FÜR IHRE AUFMERKSAMKEIT

Sprechen Sie uns an

Ihre Kontaktperson

Asan Stefanski

Felix Eckel

E-Mail asan.stefanski@advisori.de
felix.eckel@advisori.de

ADVISORI FTC GmbH
Kaiserstraße 44
60329 Frankfurt am Main

Web www.advisori.de
Xing advisori.de/xing