SECURITY ACCENT

Reshaping
The Lock

PFE BOOK 2025-2026

Security | IGA | IAM | API | Identity | PAM | Access | Angular

AI | OAuth | CI/CD | IoT | Authorization | Authentication | DevSecOps

Python | GitOps | PBAC | SQL | Grafana | Zero Trust | Java script

01 COMPANY

02 OUR VALUES

03 OFFICE CULTURE

04 INTERNSHIPS

05 APPLICATION PROCESS

01 COMPANY

Company

Established and headquartered in Eschborn, Germany, Security Accent GmbH is a cutting-edge consultancy firm specialized in Identity and Access Management (IAM).

Our company was founded with a vision to offer guidance and unwavering support to clients, aiding them in meeting their information security and compliance requirements.

We provide consultancy in Identity Governance & Administration, Access management, and Privileged IAM as our core services.

02 OUR VALUES

Our Values

Continuous Emerging

Innovation never stops, we do our best to keep ourselves updated with each emerging technology, to keep learning and to keep gathering new experiences.

Straight Talking

With us, you will know what to expect and when. If there is a simpler solution, we will tell you. If we can't do something, we will tell you. We steer clear of small print, and we deliver what we promise.

Focused

We love what we do, and this is what we've chosen to do with most of our waking hours. We work hard, but over everything, we work smart. We feel proud, but we stay humble

Different Accents

Not only in terms of diversity and people's accent, but also in terms of different projects and IT accents. Each project has its own accent, and we make sure to accentuate its success.

03 OFFICE CULTURE

Office Culture

At Security Accent GmbH, we believe in creating a positive company culture that values and engages our employees. We strive to maintain a work environment that is collaborative, inclusive, and supportive of each employee's personal and professional growth.

By fostering a positive and engaging work environment, we believe that we can attract and retain the best talent, ensure that our company remains a great place to work, and achieve our mission of delivering high-quality services to our clients.

Office Culture

JOIN US AND BECOME A SEACER!

Expert Mentorship

Competitive Compensation

Dynamic Work Environment

Future-Ready Learning

Collaborative Culture

Cutting-Edge Technology

04 INTERNSHIPS

Project 1

Building an Enterprise-Grade Online Banking Platform: Identity & API Security

Description:

This project aims to design and implement a secure, enterprise-grade online banking platform. It integrates identity and access management (IAM) using OAuth2, OpenID Connect, and UMA for delegated access.
The backend simulates real banking services using the Open Bank Project, while APIs are exposed and secured via an API Gateway.
A prototype mobile app will be developed to allow secure transaction approvals by managers. The solution will follow best practices from open banking and FAPI standards, demonstrating authentication, authorization, consent handling, and API protection in a realistic banking context.2

Duration
6
months

Open Positions:
2
available

Technologies
- K8s/OpenShift
- OAuth2
- IAM
- APIs
- JS/TS
- Mobile Dev

Requirements:
- Good programming skills
- Familiarity with CI/CD tools
- Familiarity with K8 or OpenShift
- Study: Cybersecurity, Software Engineering

Click to Apply

Project 2

Context-Aware Policy Enforcement for IoT / Edge Systems

Description:

This project focuses on developing a lightweight policy-based access control (PBAC) framework for IoT and edge environments.
The solution dynamically enforces security decisions using contextual factors such as device location, time, and battery level.
It includes implementing a compact on-device policy engine capable of offline operation, a central policy management interface for authoring and distribution, and evaluation through real-world scenarios to measure latency, scalability, and reliability in constrained environments.

Duration
6
months

Open Positions:
2
available

Technologies
- K8s/OpenShift
- Python
- Node.js
- OPA/Rego
- IoT

Requirements:
- Knowledge in Python or Node.js
- Basic understanding IAM
- IoT knowledge is a plus
- Study: Computer Science, Cybersecurity, Software Engineering

Click to Apply

Project 3

Zero Trust Privileged Access Fabric for Hybrid IT/OT Infrastructure

Description:

Industrial environments like SCADA, PLC, and HMI systems are increasingly connected to corporate IT networks, creating new identity and access challenges.
This project aims to design and implement a Zero Trust Identity and Privileged Access Management architecture for hybrid IT/OT infrastructures. It will integrate Access Management, PAM, and fine-grained authorization to secure human and non-human identities (NHI) across industrial assets.
The student will build a functional lab prototype demonstrating centralized authentication, least privilege enforcement, session recording, and continuous verification for both operators and devices.

Duration
6
months

Open Positions:
2
available

Technologies
- WSO2 IS,
- Keycloak
- OpenPLC
- ScadaBR
- K8s
- CI/CD
- Python

Requirements:
- IAM & PAM Knowledge
- OT Security Basics
- Zero Trust Concepts
- Study: Cybersecurity or Automation Engineering

Click to Apply

Project 4

Identity Fabric for Autonomous AI Agents With Real-Time Policy Enforcement

Description:

Autonomous AI agents operate across multiple systems at machine speed, making traditional IAM models obsolete. Existing methods rely on static API keys, broad service accounts, and user tokens that lack delegation, context, or control.
This project develops an identity fabric that gives AI agents verifiable identities, purpose-bound access tokens, and real-time policy enforcement at the data layer.
It integrates WSO2 IS, SPIFFE/SPIRE, and OPA/Rego to ensure every agent action is attributable to a responsible human and aligned with defined purposes.
The solution enables secure, accountable, and context-aware access for autonomous agents across complex digital ecosystems.

Duration
6
months

Open Positions:
2
available

Technologies
- WSO2 IS
- SPIFFE/SPIRE
- OPA/Rego
- OAuth2
- MCP
- Grafana

Requirements:
- Identity security knowledge
- AI systems understanding
- K8s & CI/CD skills
- Study: Computer Science, Cybersecurity, AI, Data Science

Click to Apply

Project 5

Building a Governed Multi-Tenant Environment Management Platform

Description:

This project aims to design and implement a modern, cloud-native platform that manages the entire lifecycle of solution environments from provisioning and configuration to monitoring, optimization, and decommissioning.

Built on Infrastructure-as-Code (IaC), Kubernetes, and GitOps principles, the platform enables secure, reusable, and automated environment creation for complex enterprise solution stacks.

It integrates governance, policy enforcement, and cost-control mechanisms while ensuring compliance, observability, and reliability through standardized workflows and self-service automation.

Duration

6

months

Open Positions:

2

available

Technologies

- K3s
- Argo CD
- Terraform
- Ansible
- Helm
- Longhorn
- Velero
- React

Requirements:

- Cloud automation skills
- DevOps and GitOps
- Infrastructure as Code
- Study: Computer Science, Cybersecurity, Information Technology Engineering

Click to Apply

Project 6

Development of a Custom Marketplace for Open Banking APIs

Description:

The goal of this project is to design and develop a web-based marketplace that allows financial institutions and fintechs to discover, and subscribe to Open Banking APIs. The marketplace will leverage WSO2 API Manager and WSO2 Identity Server to provide secure API exposure, authentication, and access management.

The project involves creating a React-based front-end integrated with WSO2 API Manager as the backend API gateway. WSO2 Identity Server will handle user authentication, single sign-on (SSO), and role-based access control. The system will include API discovery, rating, and subscription workflows with an intuitive developer portal interface. The backend will expose REST APIs for managing API metadata, subscriptions, and analytics dashboards.

Duration

6

months

Open Positions:

1

available

Technologies

- REST APIs
- MySQL
- Docker
- GIT
- React
- WSO2 API Manager
- WSO2 IS

Requirements:

- API Management
- Access Management
- IAM Basics
- Study: Computer Science, Information Technology Engineering

Click to Apply

Project 7

Implementing User Click Recording and Behavioral Profiling

Description:

This project aims to implement a user behavior tracking system that records user interactions (clicks, scrolls, navigation) and builds dynamic behavioral profiles to enhance customer experience insights.

The intern will integrate the OpenReplay session replay platform into a web application to capture user sessions. The collected data will be processed to generate behavior-based profiles . Insights will be visualized through dashboards, providing actionable information for marketing, UX, and product teams. Integration with existing IAM tools (like WSO2 IS) will ensure privacy and consent management compliance.

Duration

6

months

Open Positions:

1

available

Technologies

- OpenReplay
- JavaScript/React
- Python (For Analytics)
- WSO2 IS
- PostgreSQL
- Grafana

Requirements:

- Analytic thinking
- Access Management
- IAM Basics
- Study: Computer Science, Cybersecurity, Information Technology Engineering

Click to Apply

Project 8

DevSecOps automation for continuous API Security Automation

Description:

This project focuses on automating API security validation throughout the CI/CD pipeline. It aims to implement vulnerability scanning, policy enforcement, and compliance checks using open-source tools integrated with WSO2 Identity Server.

The intern will create a CI/CD pipeline that integrates static and dynamic security analysis (SAST/DAST) tools, automates vulnerability reporting, and enforces policies before deployment. Integration with WSO2 Identity Server will enable pre-deployment API validation. The pipeline will include automated compliance validation against security baselines such as OWASP API Top 10 and GDPR-related checks

Duration

6

months

Open Positions:

1

available

Technologies

- WSO2 IS
- OWASP ZAP
- SonarQube
- Bash scripting
- Kubernetes
- Jenkins (or GitHub Actions)
- Docker

Requirements:

- Automation
- Information Security
- IAM Basics
- Study: Computer Science, Cybersecurity, Information Technology Engineering

Click to Apply

05 APPLICATION PROCESS

Application Process

Application

View project details and submit your application

Screening

We assess all submissions to select the best fits

Contact

Shortlisted candidates will be reached for a first HR evaluation

Interview

The selected candidates will be invited for the technical interview

Selection

Successful candidates will be assigned to their preferred project

Onboarding

Let the adventure begin!

SECURITY ACCENT

FOLLOW US ON