



**Internship assignment**

# **Accessing the Privileged Access Security as a Service**

Contact

Cindy Van den Hoecke  
careers@is4u.be

ActWise NV

Veldkant 33A  
2550 Kontich  
België



WWW.ACTWISE.EU

CAREERS@ACTWISE.EU

## Internship Assignment

### Integrating Idaptive MFA and lifecycle management with CyberArk Privileged Account Management

#### Description

Securing privileged accounts within an organization is a challenge in today's complex IT environments and has been identified by all independent consulting firms as one of the top priorities within IT security. Staying ahead of internal and external cyber threats requires a deep understanding of how to manage and monitor access to these most sensitive accounts.

As the market leader in Privileged Account Security, CyberArk (<https://www.cyberark.com>) offers its privileged account management (PAM) solution for this purpose which is a digital vault that can run both on-prem and in the cloud. Recently, CyberArk has also purchased Idaptive as its MFA, SSO and lifecycle management solution. This can be used to strongly secure access to the digital vault.

IS4U wants to explore how the setup and configuration of Idaptive together with CyberArk can provide an optimal solution for the customer. Any access to the CyberArk digital vault must follow the 'least privilege' principle. This means that you only get access when needed and only to those accounts that you need. Idaptive can handle the authentication here with its Multi-factor solution and the authorizations on CyberArk with its provisioning solution



### Example use case:

As a customer, I have set up a new Windows or Linux server with an associated privileged root or administrator account. I want to store these accounts securely in the CyberArk environment and make them available to my administrators through this platform when they need admin access to the servers. I want these administrators to be able to access these accounts only after 2-factor authentication.

Also, this customer has an application team that only sporadically needs these accounts for updates and maintenance purposes. They only get access to these accounts periodically and only after strong authentication.

### Mimimum requirements

The students are asked to deliver at least the following functionalities:

- Installation of the CyberArk environment and all of its components (A redundant environment including high availability and disaster recovery)
- Installation of Idaptive
- Integrating Idaptive with CyberArk for MFA and provisioning
- Implementation of use cases for granting least privilege access to CyberArk's digital vault
- Monitoring and recording of privileged sessions

Optional:

- Approval workflow and/or provide mandatory reason before the use of a privileged account becomes available

### Project Methodology.

ActWise uses agile project methodologies such as XP and SCRUM for its projects. The project described above is no exception. These methodologies focus on the quality of software solutions. This is achieved by dividing the project into shorter iterations and very intense communication within and outside the project team. Intense communication is inherent to agile and consequently leads to a thorough internship guidance.