



**Internship assignment**

# **Automating Security with a Chat Interface**

Contact

Cindy Van den Hoecke  
careers@is4u.be

ActWise NV

Veldkant 33A  
2550 Kontich  
België



## Omschrijving

Met de opkomst van thuiswerken als gevolg van de Covid-19-pandemie, is het gebruik van samenwerkingstools zoals Microsoft Teams en Slack aanzienlijk toegenomen. Deze verandering in de werkomgeving heeft geleid tot verbeterde communicatie tussen teamleden. Tegelijkertijd heeft deze verschuiving ook geleid tot een groter besef van de noodzaak van cyberbeveiliging, aangezien het werken op afstand nieuwe risico's met zich meebrengt.

In deze stageopdracht willen we deze twee trends samenvoegen. Ons doel is om te onderzoeken hoe een beveiligingsoplossing effectiever kan werken door integratie met een samenwerkingstool.

Een sleutelspeler in de wereld van cyberbeveiliging is CyberArk. Dit bedrijf staat bekend als marktleider op het gebied van PAM Security. PAM, oftewel Privileged Account Management, vormt een essentieel onderdeel van de beveiliging voor ieder bedrijf. Het draait om het beheren en beveiligen van toegang tot kritieke systemen en gegevens.

### Magic Quadrant

Figure 1: Magic Quadrant for Privileged Access Management



Onze opdracht richt zich op het samenvoegen van deze PAM-beveiliging met de mogelijkheden van moderne samenwerkingstools. We willen onderzoeken hoe beveiligingstaken efficiënter kunnen worden uitgevoerd via een chatinterface.

Onze beoogde resultaten omvatten de ontwikkeling van specifieke scenario's, zowel vooraf bepaalde als door jou zelf geïdentificeerde scenario's. De vooraf bepaalde scenario's zijn als volgt:

- Noodknop voor Cyberaanvallen:
  - In het geval van een cyberaanval wil je mogelijk specifieke delen van het systeem extra beveiligen, zoals de toegang van een bepaalde gebruiker blokkeren en de wachtwoorden van de aangetaste accounts wijzigen.
- Goedkeuringsproces voor Accounts met Veel Rechten:
  - Accounts met hoge bevoegdheden moeten vaak door een goedkeuringsproces voordat ze worden gebruikt. Dit kan echter omslachtig zijn. Door gebruik te maken van een chatinterface kunnen goedkeuringsprocessen sneller verlopen.
- Wachtwoordherstel:
  - Wachtwoordherstel is een veelvoorkomende handeling. Als deze handeling geautomatiseerd kan worden via een chatinterface, kan dit aanzienlijk tijd besparen.
- Tijdelijke toegang:
  - Soms is tijdelijke toegang tot een bevoorrechte account vereist. Dit proces kan vaak complex zijn. Via een chatinterface kan dit aanzienlijk worden versneld.
- Verdachte Activiteit Detectie:
  - Een geautomatiseerde chatinterface kan worden ingezet om verdachte activiteiten te detecteren. Bijvoorbeeld, als een account meerdere malen probeert in te loggen vanaf verschillende locaties binnen korte tijd, kan dit leiden tot een automatische waarschuwing en verdere beveiligingsmaatregelen.

Om deze gebruiksscenario's te ontwikkelen, maken we gebruik van een tool die CyberArk aanbiedt: Identity Flows. Deze tool integreert met moderne samenwerkingstools en biedt de mogelijkheid om de genoemde scenario's te implementeren.

### Oplevering:

Er zal gevraagd worden om volgende deliverables op te leveren:

1. Opzetten van de PAM omgeving.
2. Uitkiezen welke samenwerkingstool je wilt gebruiken.
3. Het uitvoeren van de verschillende scenario's:
  - a. Noodknop voor Cyberaanvallen
  - b. Goedkeuringsproces voor Accounts met veel rechten
  - c. Wachtwoord herstel
  - d. Tijdelijke toegang
  - e. Verdachte activiteit detectie
  - f. Een vrij te kiezen scenario

### Mogelijke uitbreidingen:

1. Bestudeerd hoeveel werk het kost om de scenario's over te zetten naar een andere samenwerkingstool.

### Projectmethodologie

ActWise hanteert voor haar projecten agile projectmethodologieën, zoals XP en SCRUM. Het project dat hierboven is beschreven, volgt dezelfde aanpak. Deze methodologieën richten zich op het waarborgen van de kwaliteit van softwareoplossingen. Dit wordt bereikt door het project op te splitsen in kortere iteraties en door middel van intensieve communicatie binnen en buiten het projectteam. De nadruk op intensieve communicatie is een intrinsiek kenmerk van agile, wat resulteert in een diepgaande begeleiding tijdens de stageperiode.