# Censornet Security Awareness Training

## Handleiding

(Versie 6-11-2024)

# Inhoudsopgave

## Inleiding

Welkom bij de handleiding van de Security Awareness Training (SAT). Dit is een dienst aangeboden in samenwerking met onze business partner Censornet. De training bestaat uit twee componenten: korte online trainingen en oefeningen in de vorm van phishingsimulatie.

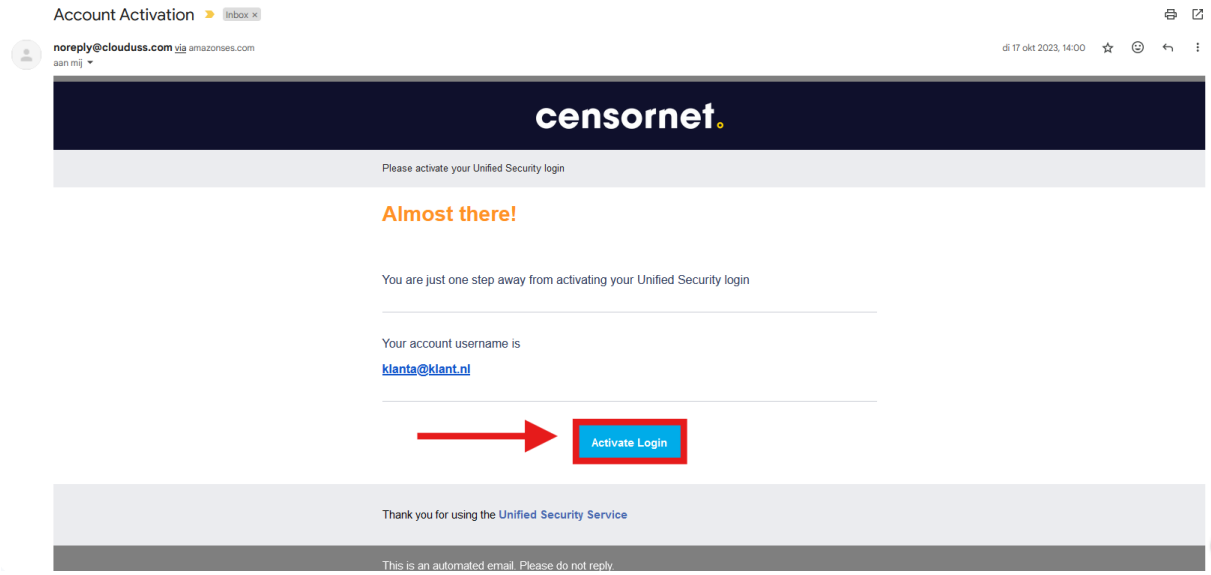
In principe werkt de dienst automatisch. Als je het pakket besteld hebt, krijgt elke medewerker waar een pakket voor is afgesloten automatisch via e-mail de uitnodiging voor de te volgen trainingen. Daarnaast ontvangen deze werknemers op willekeurige momenten nagebootste phishingmails als onderdeel van de phishingsimulatie.

Hoofstuk 1 bevat informatie over het eerste moment van inloggen binnen het portaal en geeft uitleg over de inhoud van de training.
Hoofstuk 2 bevat informatie over het gebruik en de mogelijkheden van het online portaal.

# 1 Activatie en inhoud van de training

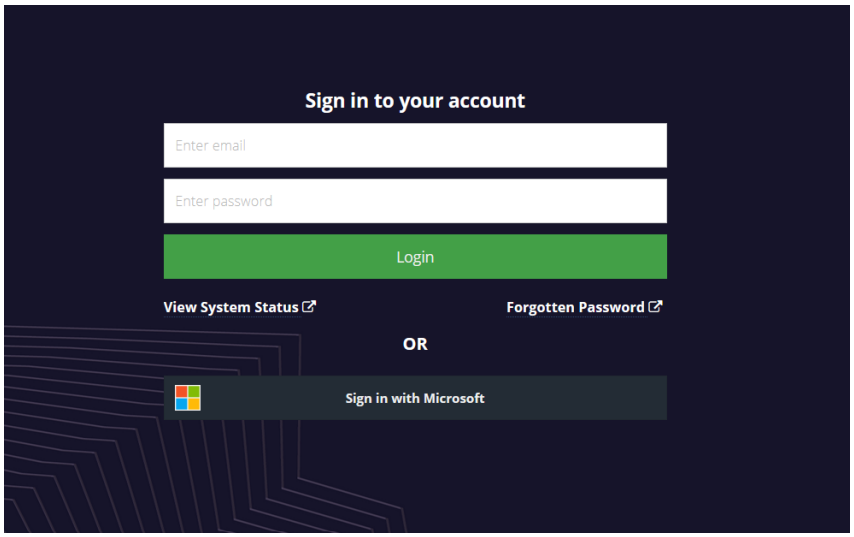
Na het bestellen van KPN Cybersecurity voor MKB ontvang je een activatie e-mail van onze partner Censornet. Deze zie je terug in paragraaf 1.1.

## 1.1 Inloggen online portaal Censornet

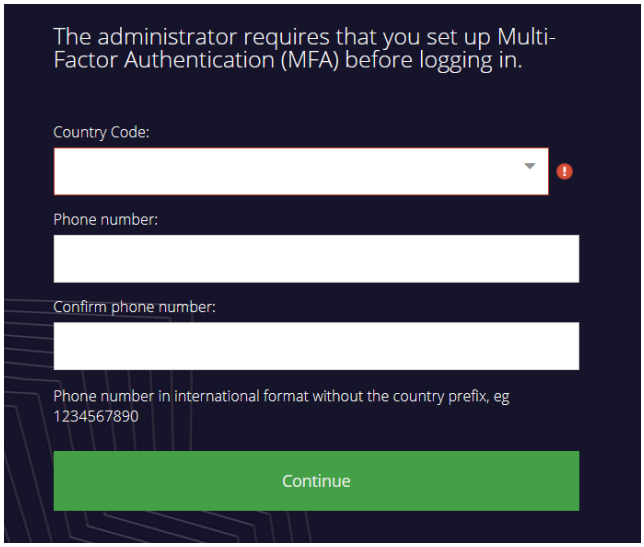



Je kan inloggen via https://dashboard.clouduss.com/#dashboard

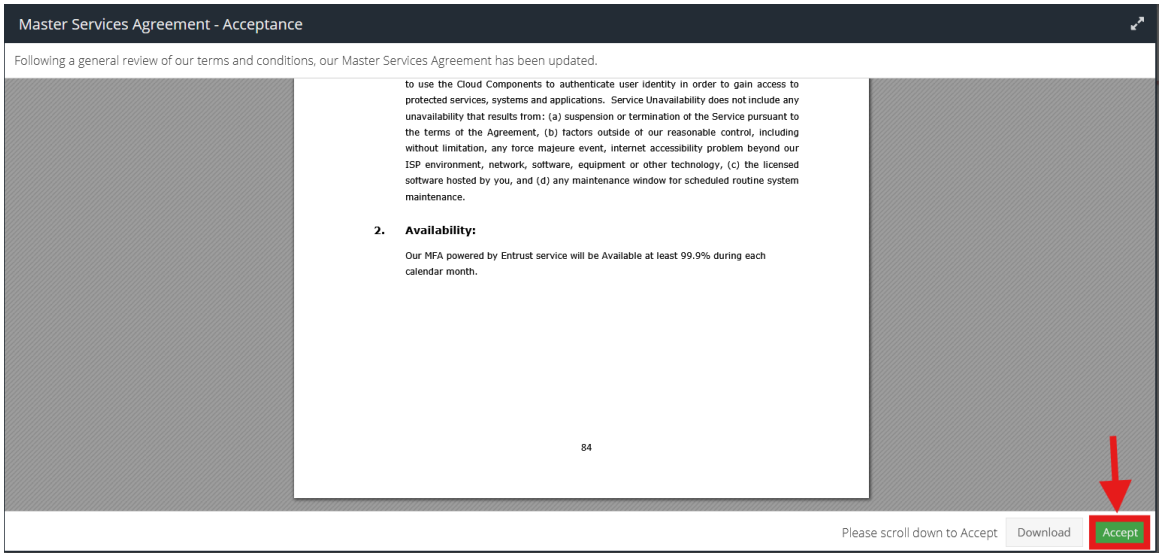
Je krijgt dan onderstaand scherm te zien.




Als je voor de eerste keer inlogt, dien je ter bescherming Multi Factor Authenticatie (MFA) te activeren. Daarvoor voer je je mobiele nummer in, waarna je een SMS ontvangt. Deze gebruik je om MFA te activeren.




Ook word je gevraagd om de algemene voorwaarden te accepteren. Lees deze door, scroll helemaal naar beneden en klik op het groene vlakje **ACCEPT**. Als het vakje **ACCEPT** grijs blijft, ververs de pagina dan door op je toetsenbord op **F5** te drukken of door bovenin je browser de link aan te klikken en nogmaals op enter te drukken.




## 1.2 Uitleg van de Security Awareness Training (SAT)

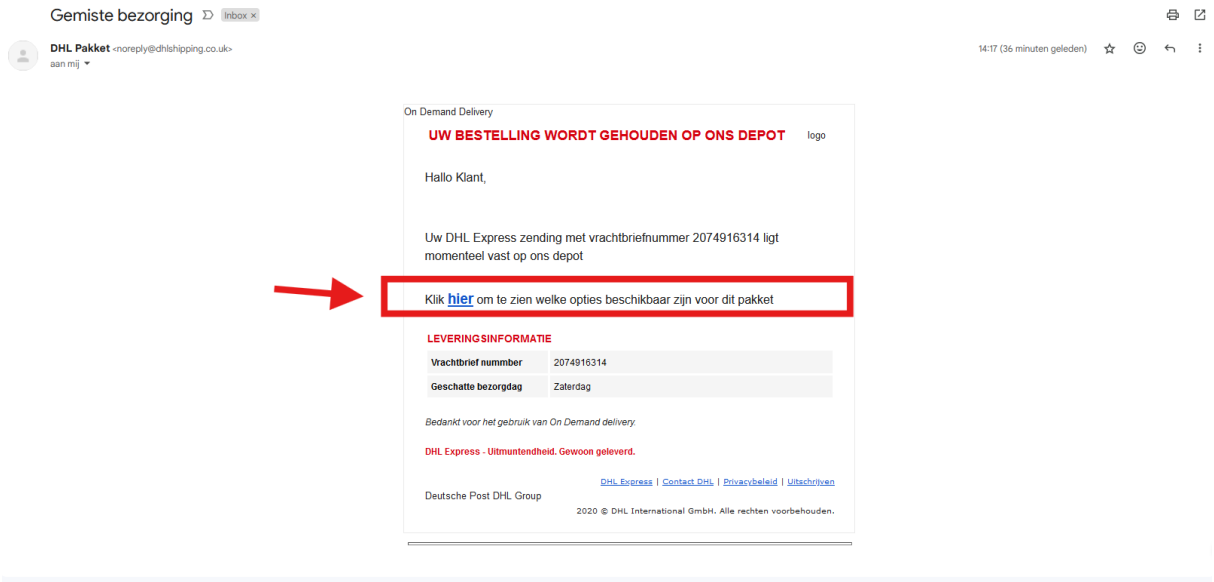
De training bestaat uit twee componenten: korte online trainingen en oefeningen in de vorm van phishingsimulatie. Hieronder leggen we de werking uit.

## 1.3 Hoe werkt de phishingsimulatie?

Vanuit het Censornet platform worden automatisch nagebootste phishingmails en uitnodigingen voor de online trainingen naar je werknemers gestuurd. De nagebootste phishingmails worden op onregelmatige tijden en verschillende datums verzonden om zo de voorspelbaarheid te verkleinen. Dit gaat vanzelf; jij en je werknemers hoeven hiervoor niets te doen.

## 1.4 Een voorbeeld phishingmail

Een voorbeeld van een nagebootste phishingmail is te zien in onderstaande afbeelding.



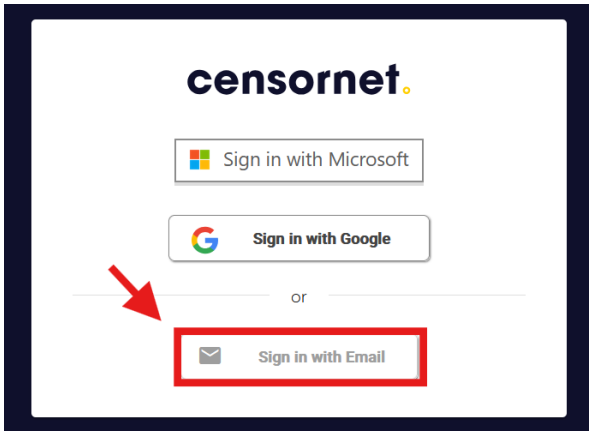

Wanneer je medewerkers per ongeluk op de link klikken, zien ze het volgende:


## 1.5 Hoe maak je gebruik van de online trainingen?

De uitnodigingen voor de online trainingen worden automatisch per e-mail aan je medewerkers verzonden. Wanneer je in de e-mail op **Take course** klikt, wordt je doorgestuurd naar de inlogpagina van **Censornet**.

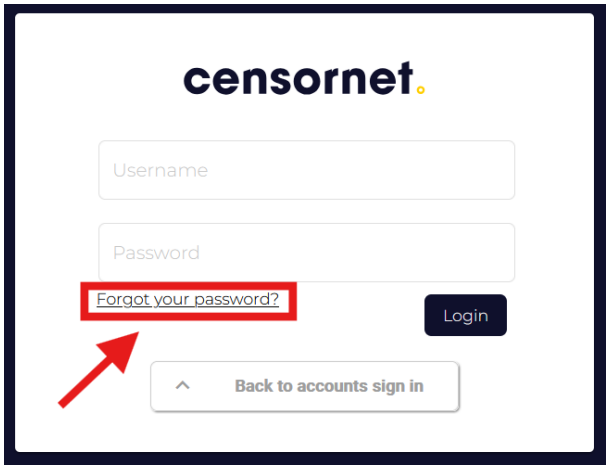

Klik op **Sign in with e-mail**.

Vul vervolgens je gegevens in en klik op **Login**.

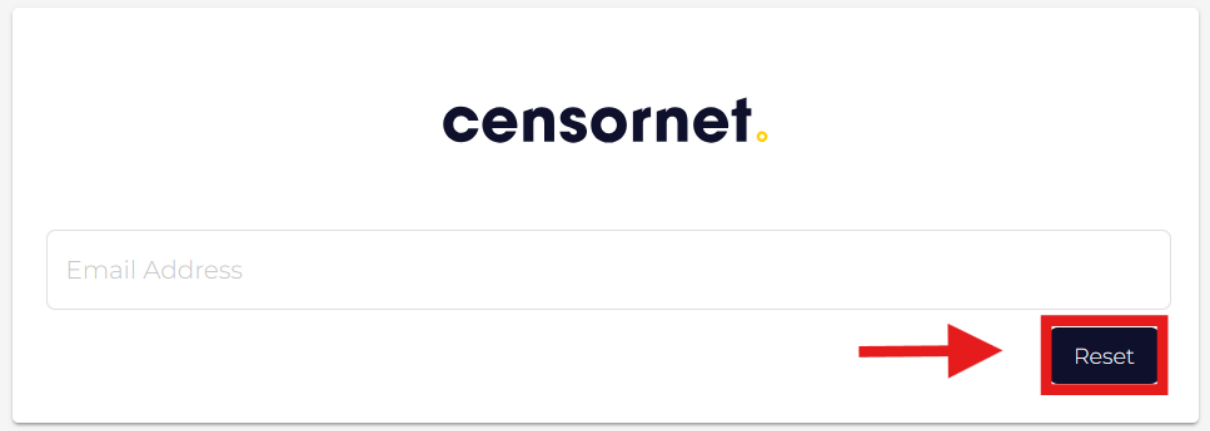



Als je voor de eerste keer inlogt, moet je je wachtwoord instellen.

Om je wachtwoord in te stellen klik je op **Forgot your password**.



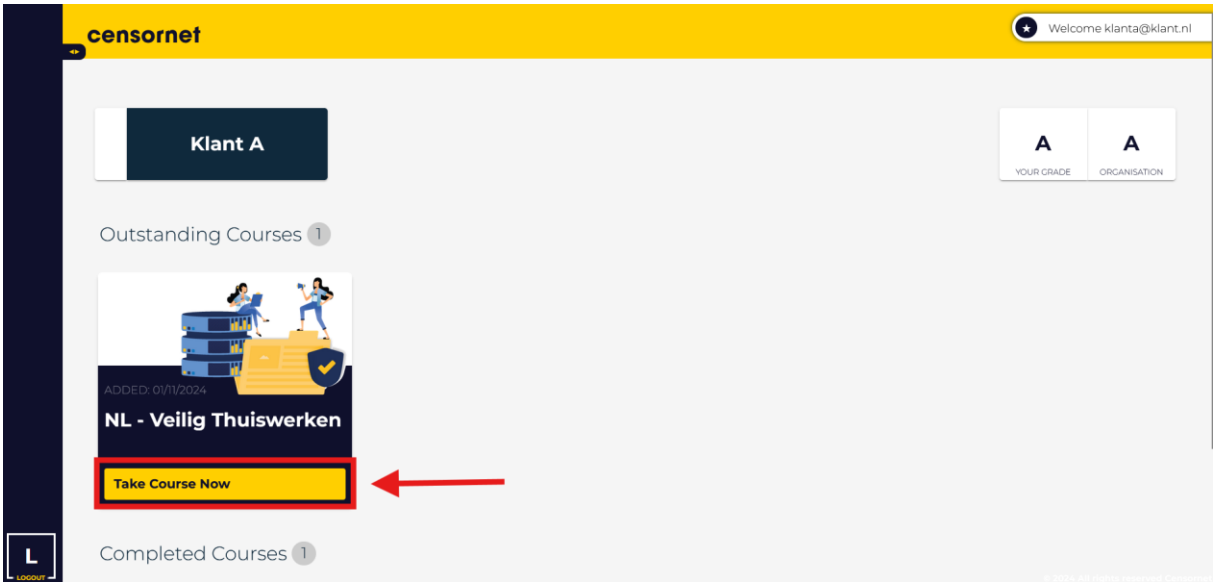

Vul je e-mailadres in en klik op **Reset**.




Je ontvangt een e-mail van Censornet om je nieuwe wachtwoord in te stellen.

Als je je wachtwoord ingesteld hebt, kun je echt inloggen.

Na inloggen zie je een overzicht van de openstaande training(en). Om de training te starten klik op **Take Course Now**.



# 2 Gebruik van het online portaal

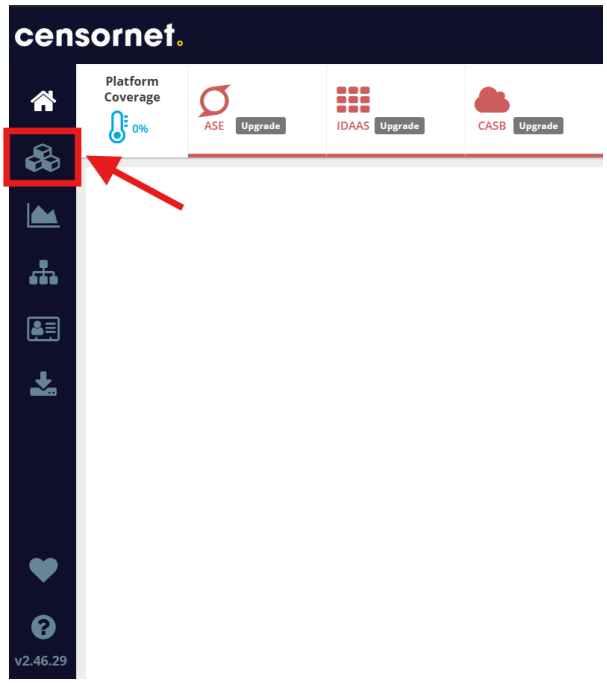
Dit hoofdstuk bevat meer informatie over de mogelijkheden en het gebruik van het online portaal van Censornet, waarmee je als werkgever een overzicht kan zien van de voortgang van de trainingen en waar je zelf phishingmails kan verzenden.

## 2.1 Dashboard

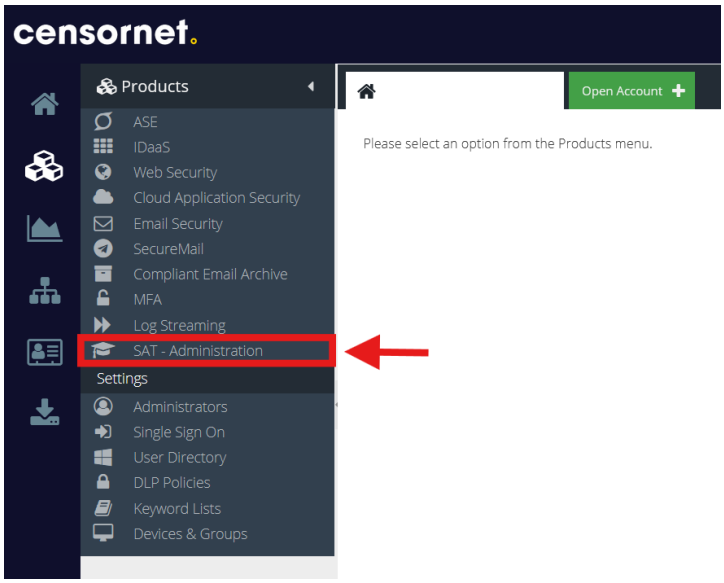
Met behulp van het dashboard binnen het online portaal van SAT kun je de voortgang zien van je medewerkers. Je hebt inzage in hoe vaak en door wie de trainingen zijn gevolgd en afgerond. Ook kun je zien hoe vaak en door wie er op de link in de phishingmails is geklikt.
Hiermee kun je gericht sturen op de kennis en knowhow rondom cybersecurity binnen jouw organisatie.

## 2.2 Het gebruik van het online portaal van Censornet

Om in het online portaal van SAT te komen, log je in via https://dashboard.clouduss.com/#dashboard (zie paragraaf 1.1 voor de instructies).
Wanneer je ingelogd bent, klik je op het icoon met de **drie blokken (Products)** aan de linkerkant van het menu.

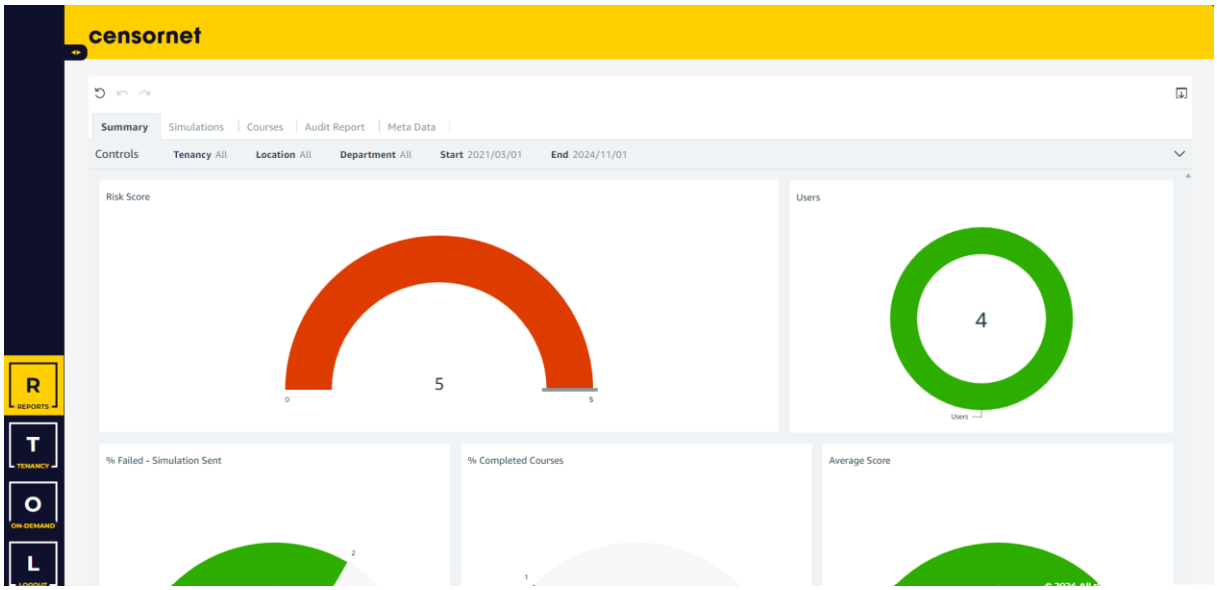



Wanneer het menu onder **Products** is uitgeklapt, klik je op **SAT Administration** in het onderliggende menu.



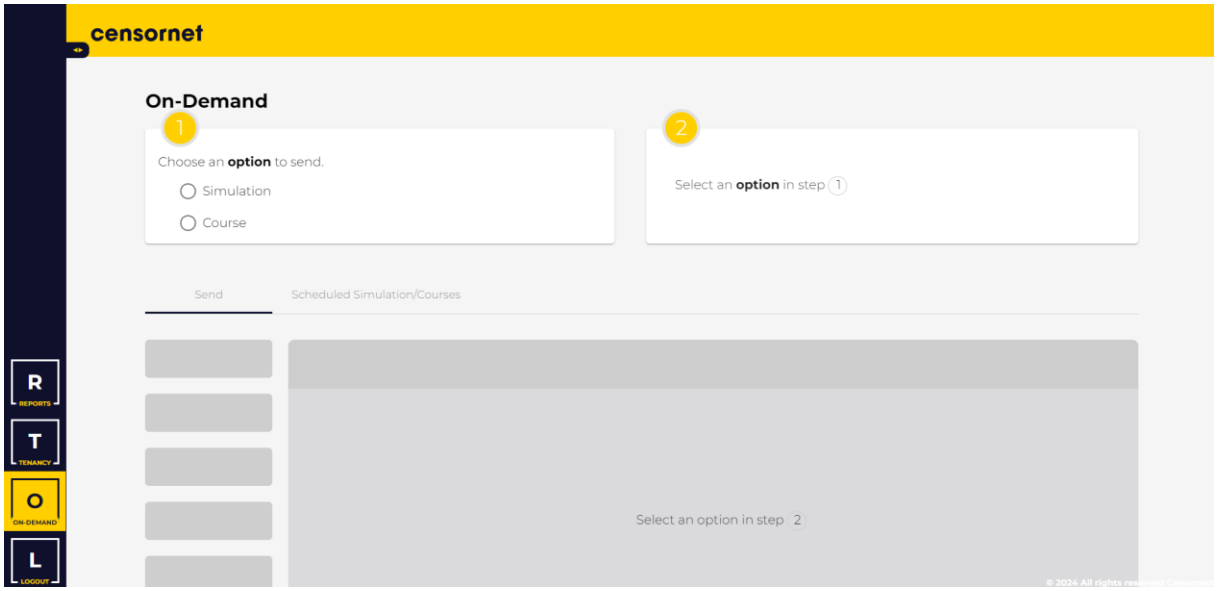

## 2.3 Rapportages

Onder de knop **Reporting** kan je meer inzicht krijgen in de resultaten van de trainingen. Zo zie je bijvoorbeeld hoeveel medewerkers de trainingen hebben gevolgd en afgerond, in hoeveel gevallen dit succesvol was en een overall risicoprofiel op basis van de trainingen. Indien gewenst kan je de tegels in het dashboard volgen om meer gedetailleerde informatie te zien over die specifieke indicator.




## 2.4 Zelf aan de knoppen

In het geval je zelf controle wil wanneer een phishingmail of training wordt verzonden en welke e-mail of trainingsmodule dat moet zijn, kan je dit regelen met behulp van **On-Demand**. Bij stap 1 (onderstaande scherm) kies je tussen **Simulation** (phishing simulatie) of **Course** (online training). Bij stap 2 maak je een keuze welke training of phishingmail je naar je medewerkers stuurt.


censornet
On-Demand
1
Choose an option to send.
Simulation
Course
2
Select an option in step 1
Send
Scheduled Simulation/Courses
R
REPORTS
T
TENANCY
O
ON-DEMAND
L
LOGOUT
Select an option in step 2