1. Dit document ingevuld indienen via canvascursus Bachelorproef YP0828 ten laatste op 25/02/2022 (17u00), met als filenaam: NAAM\_voornaam\_bachelorproefPitch1 .
2. Kom dit voorstel online toelichten (MS Teams) met je stagedocent en de IMS stagecoördinator (Frank Vandromme. Een individueel tijdslot volgt na tijdige ontvangst van dit ingevulde document via canvas.

**Naam student: Diego Borghgraef**

**Naam stagedocent: Peter Berghmans**

**Naam bedrijfsstagementor of begeleider bachelorproef binnen stagebedrijf:**

*Naam contactpersoon: Julien Piter*

*Bedrijf: EY*

*Adres: De Kleetlaan 2, 1831, Diegem*

*Tel./gsm: +32 (0)470 76 57 91*

*E-mail:* julien.piter@be.ey.com

**Onderwerp of project aangereikt door je stagebedrijf:**

*Omschrijf wat je stagebedrijf heeft voorgesteld om uit te werken als bachelorproef:*

*In eerste instantie ga ik voor EY een Awareness Campagne opstellen waarbij alle verschillende authenticatie methodologieën worden besproken. Dit zal gebeuren aan de hand van interactieve spellen, waarbij ze actief met de authenticatie methodologie zullen bezig zijn. Vervolgens zal een eerste enquête genomen worden met algemene vragen over de besproken authenticatie middelen.*

*Een goede onderzoeksvraag in verband met het besproken onderwerp van authenticatie binnen EY, is een analyse doen naar Multifactor Authenticatie methodologieën voor System domain administrators. Bepalen of MFA methodologieën bestaan en welke? Welke technologieën hiervoor bestaan en hoe ze in elkaar zitten. Vervolgens met de verfaarde informatie een awaraness campagne voeren naar interesse voor implementatie.*

**Een korte omschrijving van de probleemstelling:**

*Wat is het probleem? Wie heeft een probleem? Waardoor is het probleem of vraagstuk ontstaan?*

*In de laatste jaren zien we een sterke stijging in de aantal cyberaanvallen, meer bepaald de “****Privilege Escalation Attacks”.*** *Dit is een techniek waarbij een threat actor ongeoorloofd toegang verkrijgt via gevoelige punten om dan vervolgens met verhoogde toegangsmachtigingen een volledige aanval uit te voeren op systeem domeinen. Indien een threat actor aan de “Domain Controller” toegang vergaard heeft hij toegang over heel het systeem. Vergrendeling van deze systeem accounts is dus van uiterst belang. Een goede implementatie is om Multifactor Authenticatie te verplichten voor het gebruik/wijzigingen van systeem veranderingen voor gebruikers met de hoogste privileges (Domain Administrators).*

**Doelstelling van je bachelorproef:**

*Wat ga je exact oplossen? En wat niet? (afbakening)*

1. *Een analyse voeren voor Multifactor authenticatie methodologieën voor Domain administrators.*
2. *Bepalen welke technologieën haalbaar zijn en hoe ze geïmplementeerd kunnen worden.*
3. *Awareness campagne voeren over interesse van implementatie.*

**Hoofdonderzoeksvraag:**

***“ MFA implementatie voor Systeem Administrators.”***

**Welke bronnen heb je al gevonden?**

*Wat is er bekend over het vraagstuk of je onderwerp? Welke informatie bestaat er binnen het bedrijf over het onderwerp? Wat vind je in de literatuur (vakliteratuur, deskresearch, experten,…)?*

* *Informatie over MFA van System administrators binnen EY werd nog niet verkregen, maar zal de komende weken bekeken worden.*
* *Vakliteratuur over het onderwerp bestaat al:*
  + [*https://techcommunity.microsoft.com/t5/security-compliance-and-identity/how-to-enabling-mfa-for-active-directory-domain-admins-with/m-p/2803878*](https://techcommunity.microsoft.com/t5/security-compliance-and-identity/how-to-enabling-mfa-for-active-directory-domain-admins-with/m-p/2803878)