

**PORTFOLIO I-Talent**

Ruben Vanderheyden

Inhoudsopgave

[Inhoudsopgave iii](#_Toc102070555)

[1 Voorstelling 1](#_Toc102070556)

[2 Overzicht activiteiten 2](#_Toc102070557)

[2.1 Verplichte activiteiten 2](#_Toc102070558)

[2.1.1 Seminaries 2](#_Toc102070559)

[ IT@Breakfast: Droneport 2](#_Toc102070560)

[ AI Deep Dive door Brainjar 2](#_Toc102070561)

[ Infrastructure 2.0 door Gluo 2](#_Toc102070562)

[ Applied AI in the fields of homeland security and financial markets door Belfius 2](#_Toc102070563)

[ Cybersecurity workshop door Eurofins 2](#_Toc102070564)

[ Information security awareness & GDPR door Ordina 2](#_Toc102070565)

[ Digital@Breakfast: Facebook en ik door Tim Verheyden 3](#_Toc102070566)

[ Multi vendor workflow automation door Routz 3](#_Toc102070567)

[ Workshop Kubernetes door Devoteam 3](#_Toc102070568)

[ Chaos Engineering door Inetum-Realdolmen 3](#_Toc102070569)

[ Security en data management binnen de publieke cloud (AWS, Azure, GCP) en impact en risico’s ervan door Veeam 3](#_Toc102070570)

[ Intro to digital forensics door de Federale politie - RCCU 3](#_Toc102070571)

[2.1.2 Innovatie 3](#_Toc102070572)

[ Innovatieroute Security & Cloud 3](#_Toc102070573)

[ Cyber Security Challenge Belgium 4](#_Toc102070574)

[2.1.3 Persoonlijke Ontwikkeling 4](#_Toc102070575)

[ Projectweek 2018-2019 4](#_Toc102070576)

[ POP-sessie 4](#_Toc102070577)

[ POP-sessie 4](#_Toc102070578)

[3 Selectie van activiteiten 5](#_Toc102070579)

[3.1 Cybersecurity workshop door Eurofins 5](#_Toc102070580)

[3.2 Workshop Kubernetes door Devoteam 7](#_Toc102070581)

[3.3 Cyber Security Challenge Belgium 9](#_Toc102070582)

[4 Eindreflectie 12](#_Toc102070583)

# Voorstelling

Ik ben Ruben Vanderheyden. Ik ben een derdejaars student toegepaste informatica. Ik heb voor de afstudeerrichting Systeem en Netwerkbeheer gekozen. Op informatica vlak liggen mijn interesses momenteel bij netwerkbeheer en een beginnende passie voor cybersecurity, voornamelijk het onderzoeken van netwerkverkeer. In mijn vrije tijd doe ik graag aan bouldering.

Het Talento-rapport beschrijft mij als passief, uitvoerend, introvert en meewerkend. Ik kan mij hier redelijk goed in vinden.  
Ik ben een passief denker. Dit betekend dat ik eerder gefocust ben op het uitvoeren van de activiteiten dan het beslissen. Persoonlijk herken ik mij hierin, omdat ik moeilijk beslissingen neem en liever mijn tijd neem om deze zorgvuldig te onderzoeken.

Als uitvoerend persoon, kan ik taken nauwgezet uitvoeren, indien mijn omgeving me hiervoor de nodige methodes en systemen voor voorziet. Ook heb ik spontaan niet de behoefte om een strak werktempo aan te houden, maar kan ik dit wel, als dit van mijn omgeving verwacht wordt. Op het vlak van het werktempo, herken ik mij hier zeker in. Ik heb moeite met een planning of schema aan te houden, tenzij dat ik regelmatige deadlines heb.

Op communicatief vlak ben ik een introvert persoon. Dit is zeker waar. Ik ben een persoon dat tijd nodig heeft om mensen te leren kennen, voordat ik mij vertrouwd voel en open kan communiceren.

Op het gebied van samenwerken, ben ik meewerkend. Ik sta niet graag op de voorgrond in een groep, maar werk graag actief mee tot het bereiken van de doelen van de groep. Ik heb er geen problemen mee om te luisteren en taken uit te voeren, zolang ik niet de leiding moet nemen over de groep. Ik presteer het beste als er een goede sfeer is tussen de groep en duidelijk afgestemde taken.

Na mijn studie zou ik graag een job als netwerkbeheerder of in de cybersecuritysector vinden, waarbij ik de mogelijkheid krijg om mijn kennis up-to-date te houden en verschillende nuttige certificaten te behalen, zoals bijvoorbeeld NSE, CCNP of CCIE.

# Overzicht activiteiten

## Verplichte activiteiten

### Seminaries

* **IT@Breakfast: Droneport**

20/02/2019 | 2 uur  
PXL CONGRESS

Een seminarie met ontbijt van het bedrijf Droneport. Het seminarie ging over de ontwikkeling van drones en hoe het bedrijf met drones werkt.

* **AI Deep Dive door Brainjar**

06/03/2019 | 2 uur

PXL

Een seminarie over AI: de basis, de evolutie en de gevaren.

* **Infrastructure 2.0 door Gluo**

13/03/2019 | 3 uur  
PXL  
Een workshop waarbij we hands-on geleerd hebben over AWS en automatisatie.

* **Applied AI in the fields of homeland security and financial markets door Belfius**

27/03/2019 | 3 uur  
Een seminarie over AI, waarbij er voornamelijk werd uitleg werd gegeven over ai, chatbots en web crawlers.

* **Cybersecurity workshop door Eurofins**

08/05/2019 | 2 uur  
PXL  
Een workshop over cybersecurity. We hebben eerst uitleg gekregen over ethische hackers en verschillende manieren van pentesting, gevolgd door capture-the-flag opdrachten.

* **Information security awareness & GDPR door Ordina**

15/05/2019 | 2 uur  
PXL  
Een seminarie waar er aandacht werd gericht op de veiligheid van informatie op het internet.

* **Digital@Breakfast: Facebook en ik door Tim Verheyden**

22/05/2019 | 2 uur  
Een seminarie met ontbijt over de invloed van sociale media.

* **Multi vendor workflow automation door Routz**

27/10/2021 | 3 uur  
PXL  
Seminarie over de werking van Routz en enkele gebruikte systemen.

* **Workshop Kubernetes door Devoteam**

10/11/2021 | 3 uur  
PXL  
Een workshop waarbij we uitleg over de werking van Kubernetes hebben gekregen. Dit werd gevolgd door de workshop, waarbij er verschillende opdrachten waren rond het deployen van pods in Kubernetes.

* **Chaos Engineering door Inetum-Realdolmen**

24/11/2021 | 3 uur  
PXL  
Een seminarie over het concept en de toepassing van chaos engineering.

* **Security en datamanagement binnen de publieke cloud (AWS, Azure, GCP) en impact en risico’s ervan door Veeam**

01/12/2021 | 3 uur  
PXL  
Een seminarie over data binnen een cloud infrastructuur. Er werd uitleg gegeven over de veiligheid van data op een cloud infrastructuur.

* **Intro to digital forensics door de Federale politie - RCCU**

12/01/2022 | 3 uur  
PXL  
Een workshop waarin we verschillende digitale forensische technieken hebben geleerd, zoals data recovery of forensische kopieën.

### Innovatie

* **Innovatieroute Security & Cloud**

30/09/2021 – 21/10/2021 | 25 uur  
PXL  
Een innovatieroute over Security en cloud. Tijdens deze innovatieroute waren er presentaties over VMWare Tanzu, CI/CD door Inuits en Web application penetration testing door The Security Factory.

* **Cyber Security Challenge Belgium**

10/03/2022 – 11/03/2022 | 25 uur  
AI-HUB op de Corda campus  
Een hackathon, waar we als groep gingen zoeken naar vlaggen door gebruik te maken van security technieken.

### Persoonlijke Ontwikkeling

* **Projectweek 2018-2019**

11/02/2019 – 15/02/2019 | 26 uur  
PXL  
De startweek van het researchproject. In deze week hebben we verschillende activiteiten gevolgd over persoonlijke ontwikkeling.

* **POP-sessie**

04/10/2019 | 10 uur  
PXL  
Verschillende workshops over persoonlijke ontwikkeling op de werkvloer.

* **POP-sessie**

13/10/2021 | 3 uur  
Een workshop over teamwork en werken in een groep.

Graphical user interface, text

Description automatically generated  
Figuur 1: Overzicht totaal aantal uren

# Selectie van activiteiten

## Cybersecurity workshop door Eurofins

Omschrijving

Dit seminarie was een workshop waarbij we eerst uitleg kregen over cybersecurity en verschillende vormen van penetration testing. Dit werd gevolgd door een workshop, waarbij we de technieken gingen toepassen aan de hand van capture-the-flag challlenges.

Kern

Het seminarie begon met een uitleg over Eurofins en de types van testen dat Eurofins toepast. Hierna kregen we een uitleg over hacken en verschillende technieken van cybercriminaliteit. Hier werdt een voorbeeld aangehaald van hoe hackers stroomomvormers kunnen hacken en zo zorgen voor grootschalige stroomuitval. Er werd een basisuitleg gegeven over cybercriminaliteit vandaag, zoals phishing, ransomware, etc.. Vervolgens volgde een uitleg over ethisch hacken en verschillende basis penetration testing technieken. Er werd uitgelegd hoe een ethisch hacker te werk gaat om een website te testen. De verschillende fases, die een ethische hacker volgt, zijn recon, scannen van de website, toegang verkrijgen, toegang behouden en de sporen van het hacken wissen.

Na de uitleg volgde een workshop, waarbij we in groepjes de verschillende technieken gingen toepassen met behulp van verschillende programma’s in een Kali Linux virtuele machine. Dit is een besturingssysteem, waarin verschillende hacker tools zitten. Er werd een kwetsbare machine ter beschikking gesteld, waarop we de opdrachten konden uitvoeren. Het doel van de opdracht was om de verschillende vlaggen te vinden en om administrator van het systeem te worden. Ik had bij het begin van de workshop zo goed als geen kennis over cybersecurity en de technieken, die gebruikt werden. Met de hulp van mijn groep hebben we de workshop toch tot een goed einde gebracht.

De workshop bestond uit verschillende fases. De recon stap werd bij deze workshop overgeslagen, dus zijn we meteen met de scan stap begonnen. We gingen we aan scannen doen met behulp van nmap, voor netwerken te scannen en dirb, een tool om website content te scannen. We zagen hier dat er een paar poorten openstonden, zoals poort 22 voor ssh en poort 60 voor http, waarop een Apache webserver draaide. Dirb liet zien dat er een secret directory was, waarop we met een wachtwoord konden inloggen.

Text

Description automatically generated  
Figuur 2: Terminal met het dirb commando

Graphical user interface, application

Description automatically generated  
Figuur 3: website met de geheime directory

In de source code stond een gecodeerde sleutel. Deze hebben we gedecodeerd met base64. Hierop hebben we een hash identifier gebruikt om te kijken welke hash dit kon zijn. De meeste voor de hand liggende optie was SHA-256. Vervolgens gebruikte we een wachtwoord brute-force programma om dit wachtwoord te cracken.  
Toen we ingelogd waren, was de volgende opdracht een steganografie opdracht. Dit was een afbeelding, waarin een zip-bestand met verschillende bestand zat, waaronder een tekstbestand met een ssh key. We maakten gebruik van steghide om deze informatie te vinden. We hadden niet de juiste rechten om de connectie te verkrijgen, maar met behulp van het crowbar programma geraakten we binnen.

Hier vonden we een bestand flag/user.txt waarin we de eerste vlag vinden: Eurofind{try\_harder}.  
Vervolgens moesten we aan privilige escalation doen, waarbij we als root moesten inloggen.

Dit deel van de opdracht hebben we niet succesvol kunnen oplossen, wegens ons gebrek aan ervaring en kennis. Met wat hulp konden we het find commando gebruiken om te zoeken naar bestanden van root. Hier vonden we dat er een script eurofins\_listener, waarmee we op poort 4444 een secret konden vinden. Door gebruikt te maken van het nc commando konden we de volgende flag vinden.

Reflectie

Ik had aan het begin van dit seminarie zo goed als geen kennis over cybersecurity of hacken in het algemeen. Ik was wel zeer gemotiveerd om hier meer over te leren, omdat ik dit een interessant onderwerp vond. Het gebrek aan kennis was zeker op te merken nadat we de eerste vlag hadden. We zaten vast en hadden niet echt een idee hoe dat we verder moesten gaan, tot dat we een hint kregen.

Het was een zeer interessant seminarie, wat mij wel interesse in penetration testing heeft gegeven. Hoewel ik niet van plan ben om verder te gaan als penetration tester, gaat deze informatie zeker nuttig zijn als ik een carrière in de cybersecurity wil gaan volgen. Ik heb door dit seminarie af en toe eens een opdracht op Hack the box of try hack me gedaan, maar niet regelmatig en meestal ook geen opdrachten die moeilijk genoeg waren om mij uit te dagen. Dit wil ik in de toekomst zeker veranderen, zodat ik mijn kennis op het gebied van cybersecurity kan uitbreiden. Ik heb de kennis wel in het achterhoofd gehouden, wanneer ik als jobstudent webservers moest opzetten voor klanten. Het heeft mij geholpen om bepaalde security zwakheden uit deze servers te halen.

Ik heb deze opdracht geselecteerd omdat hier mijn interesse in cybersecurity is gestart. Op het moment van dit seminarie lag mijn interesse meer in netwerken, maar dit heeft zeker een interesse in cybersecurity aangewakkerd. Hoewel ik verder niet echt iets met deze interesse heb gedaan op dit moment tot de Cyber Security Challenge, is dit toch wel waar het begonnen is.

## Workshop Kubernetes door Devoteam

Omschrijving

Dit was een workshop waarbij we uitleg over de werking van Kubernetes hebben gekregen. Dit werd gevolgd door de workshop, waarbij er verschillende opdrachten waren rond het deployen van pods in Kubernetes.

Kern

De workshop begon met een uitleg over containers in Kubernetes. Er is een mogelijkheid om containers te isoleren door gebruik te maken van namespaces en cgroups. Cgroups kunnen gebruikt worden om resources te isoleren. Verder werd er uitleg gegeven over pods en hoe containers en volumes als onderdeel van een pod werken. Een pod bevat 1 of meerdere containers met gedeelde opslag en netwerk resources. Er werd ook uitleg gegeven over de mogelijk om applicaties te scalen in Kubernetes. We maakten voor deze workshop gebruik van Minikube. Dit is een programma dat een lokale Kubernetes cluster opzet.

In het workshop gedeelte gingen we toepassen wat we geleerd hadden over pods in Kubernetes. We begonnen met het deployen van een container. Hier moesten we verschillende vragen over oplossen, zoals waarom eerst de package bestanden gekopieerd worden, gevolgd door npm install en dan een kopie van alle bestanden, in plaats van eerst een kopie van alles te doen. Je maakt eerst een kopie van de package bestanden, zodat dit een aparte stap is en de volgende keren overgeslagen kan worden. Als we alles eerst koppieren, moeten we elke keer dat er iets veranderd een npm install uitvoeren.

Vervolgens hebben we een pod gedeployed, waarin 1 container zit met de applicatie. Ook hier moesten we verschillende vragen over beantwoorden. We zijn hierna verder gegaan met het toepassen van replica sets. Een replica set is een controller, die de pod specificatie gaat gebruiken als template en ervoor gaat zorgen dat er altijd een bepaald aantal pods werkend zijn. Door gebruik te maken van replica sets, kunnen we makkelijk de hoeveelheid pods gaan aanpassen.

Om het systeem automatisch de hoeveelheid pods aan te passen, maken we gebruik van een HPA (Horizontale pod autoscaler). We kunnen de HPA instellen dat deze de hoeveelheid pods gaat aanpassen afhankelijk van de hoeveelheid gebruikte resources.

Hierna hebben we gebruik gemaakt van services, zoals ClusterIP en NodePort. ClusterIP is de default service en zorgt voor een enkel intern logische punt voor toegang. Dit is enkel voor intern cluster verkeer.  
De NodePort service opent een statische poort voor een groep van pods op alle nodes in de cluster. Deze poorten kunnen door verkeer van buiten de cluster bereikt worden. Al het verkeer dat naar deze poorten gaat wordt via een loadbalancer gestuurd en verdeelt over de verschillende geselecteerde pods.  
We hebben eerst een ClusterIP service toegepast en daarna een NodeIP service.

We hebben geen loadbalancer toegepast, maar hier werd een demo van getoont op het Google Cloud platform van Devoteam.

Om makkelijker nieuwe versies van de applicatie te deployen, maken we gebruik van Deployments. Deployments zijn een controller, die replica sets gaan beheren. We kunnen hier door gebruik maken van rolling updates om de nieuwe versie te deployen, zonder downtime. Er word een nieuwe replica set gemaakt voor de nieuwe versie van de applicatie en 1 per 1 gaan de oude pods vervangen worden. Dit kan er wel voor zorgen dat verschillende gebruikers op hetzelfde moment op verschillende versies van de applicatie zitten.

Reflectie

Dit was een zeer nuttig en leerrijk seminarie. Ik had nooit les gehad over Kubernetes en het semester dat dit seminarie plaats vond, hadden we ook het IT-project. In dit project moesten we een applicatie ontwikkelen en deployen op een Kubernetes cluster. Als systeem- en netwerkbeheerder moesten we deze Kubernetes cluster opzetten op de gegeven infrastructuur. Dit was de eerste keer dat ik in aanraking kwam met een Kubernetes cluster en hierdoor had ik er dus weinig kennis over. Dankzij dit seminarie, had ik meer kennis over hoe pods in Kubernetes werken. Deze kennis kon ik direct gebruiken voor het IT-project. Deze kennis heeft geholpen om mijn IT-Project tot een succesvol einde te brengen.

De workshop was een goede manier om kennis en ervaring op te doen over Kubernetes pods. De opdrachten waren goed en uitgebreid uitgelegd. De vragen over de opdrachten verplichten mij om na te denken over de commando’s die ik aan het uitvoeren was. Hierdoor begreep ik de workshop beter en heb ik meer kennis kunnen opdoen.

Hoewel mijn interesse meer in netwerken en cybersecurity ligt, zal deze kennis ook zeker nuttig zijn in de toekomst, omdat clusters meer en meer gebruikt gaan worden. De kennis van Kubernetes kan mij helpen om cluster beter te beveiligen.

Ik heb voor deze opdracht gekozen, omdat dit een workshop was die meteen relevant was voor het IT-project dat ik afgelopen semester heb uitgevoerd. Dit was het seminarie dat mij het meeste aansprak, terwijl het niet direct in mijn gebied van interesse lag.

## Cyber Security Challenge Belgium

Omschrijving

De Cyber Security Challenge is een wedstrijd, waarbij het de bedoeling is om verborgen vlaggen te vinden. Alle opdrachten zijn security gerelateerd. Er doen verschillende universiteiten en hogescholen aan mee. De top 40 teams mocht door naar de finale. Ik deed samen met 3 andere studenten mee. We hadden als doel om in de top 100 teams te geraken.

Kern

De Cyber Security challenge begon voor ons op 10 maart om 10 uur. We hadden als team besloten om samen 2 dagen op de AI-hub op de Corda campus samen te komen, zodat we beter als groep konden werken. Niemand van ons had echt ervaring met Cyber security en het oplossen van challenges. Hierom hebben we ervoor gekozen dat iedereen aan challenges kon werken, die hun interessant leken. Om mij voor te bereiden heb ik naar de write-ups van de vorige jaren gekeken en zelf een paar challenges proberen op te lossen op de website van de Cyber Security Challenge.  
Afbeelding met tekst, plafond, binnen, computer

Automatisch gegenereerde beschrijving  
Figuur 4: team foto

Dag 1 begon goed. We waren allemaal gemotiveerd en benieuwd naar wat de inhoud van de opdrachten ging zijn. We hebben vooral individueel gewerkt, waarbij iedereen aan een zelfgekozen opdracht werkte, maar wel alles samen besproken om te kijken of er iemand een idee had over de opdracht. We zijn zeer vlot gestart en al snel vonden we de oplossingen voor de eerste opdrachten. We hielden continue het scorebord in de gaten, omdat we benieuwd ware hoe we ten opzichte van de andere teams deden. Dit gaf ons er zicht op hoe ons tempo was in vergelijking met de andere teams.

We hadden elk onze eigen interesses, waarbij sommige teamleden meer kennis hadden over reverse engineering of cryptografie. Zelf heb ik voornamelijk gekeken naar de verschillende opdrachten over forensisch onderzoek. Deze opdrachten waren voornamelijk rond het onderzoeken van onderschept netwerkverkeer. Bij deze opdrachten werd er een pcap bestand voorzien. Dit is een bestand met onderschepte netwerkpakketen.   
Bij de Challenge hideout, heb ik met wireshark een filter toegepast op de pakketten, waardoor ik enkel de TCP-pakketten kon zien. In deze TCP-pakketten kon je de verschillende bezochte links zien. Tussen deze links stond een pastebin link, waarop de vlag in de header te vinden was.

De andere forensische opdrachten waren moeilijker. Hoewel ik een paar keer dicht bij was geraakt, heb ik uiteindelijk geen andere forensische opdrachten kunnen oplossen. Ik heb veel geleerd over het onderzoeken van netwerkverkeer.

Graphical user interface

Description automatically generated  
Figuur 5: Screenshot van Wireshark met het pakket dat de vlag bevat

A screenshot of a computer

Description automatically generated with medium confidence  
Figuur 6: Screenshot van de pastebin website, waarin de vlag te vinden was

We zijn de eerste dag geëindigd rond positie 60. Dit gaf ons als team wel vertrouwen en zelfzekerheid dat we ons doel van de top 100 konden behalen. We hadden het gevoel dat er een kans was dat we de finale konden we halen, maar we wisten dat dit een moeilijke opdracht ging worden.

De tweede dag verliep redelijk moeizaam. Het tempo lag lager, omdat we de meeste opdrachten, die we konden oplossen al hadden opgelost. Hierdoor waren we minder gemotiveerd, maar elke keer dat we een opdracht oploste, kregen we meer motivatie. We hebben deze dag ook meer in groep gewerkt, zodat we samen konden brainstormen over de moeilijkere opdrachten. We hebben er hier een aantal kunnen oplossen, maar de punten, die we kregen, waren enkel genoeg om onze positie te behouden.

Als eindresultaat, zijn we uiteindelijk op plaats 67 geëindigd. Dit is veel hoger dan de top 100, die we wouden bereiken. We waren allemaal zeer tevreden met dit resultaat. Het was spijtig dat we de finale niet behaald hadden, maar we wisten dat het moeilijk ging worden om dit te halen.

  
Figuur 7: Eindresultaat

Reflectie

Ik begon met weinig kennis aan de challenge en wist dat het een uitdaging ging worden. Ik heb tijdens de challenge veel kennis opgedaan over het oplossen van de opdrachten. Het was een zeer leerrijke en leuke ervaring om aan deel te nemen. Ik heb hier een interesse voor cybersecurity ontwikkeld, vooral op het gebied van netwerken. De challenge heeft mij laten zien dat

Persoonlijk had ik op dag 2 iets minder motivatie, maar ik had een paar opdrachten, die ik sowieso wou proberen op te lossen. Hoewel de motivatie als groep lager lag, gaf dit mij toch een doel, waaraan ik gefocust kon werken. Als het lang duurde om de oplossing te zoeken, heb ik wel een paar keer van opdracht veranderd, waardoor ik meerdere opdrachten half opgelost had. Dit was zeker geen goede manier om opdrachten op te lossen. Ik ben namelijk een aantal keer dicht bij de oplossing geweest. In de toekomst moet ik zeker ervoor zorgen dat ik mij op 1 opdracht focus tot ik een oplossing vind.

Ik heb deze opdracht gekozen, omdat ik hier een interesse/passie voor cybersecurity heb op gedaan. Voor dat ik aan de opdracht begon, leek het mij wel interessant om mee toe doen, maar had ik er geen idee van dat ik het oplossen van de challenges zo leuk ging vinden. Het is spijtig dat ik sommige challenges, die ik wou oplossen, niet heb kunnen oplossen. Dit geeft me wel de motivatie om in mijn vrije tijd meer met cybersecurity bezig te zijn, zodat ik mijn kennis kan uitbreiden. Het zoeken naar de oplossing wasIk wil mijn kennis uitbreiden en uiteindelijk een baan vinden in de cybersecurity.

# Eindreflectie

Hoewel ik altijd al interesse voor computers had, was de keuze voor deze richting niet voor de hand liggend voor mij. Ik ben mijn carrière hoger onderwijs gestart met een jaar biologie aan de Universiteit Hasselt, omdat mijn interesse eerder hier lag. Deze studie heb ik na een jaar jammer genoeg moeten beëindigen omdat de studie niet was wat ik mij had ingebeeld en het niveau voor mij persoonlijk te hoog lag. Mijn volgende studie was al snel bepaald, de interesse voor informatica was er altijd al. Ik ben geen spijt van de keuzes, die ik heb gemaakt, want zonder deze keuzes zou ik niet zijn wie ik nu ben.

Met 5 jaar studeren aan de PXL, vind ik dat ik een goede basis heb opgebouwd voor mijn toekomstige carrière. De meeste vakken zijn vlot verlopen, maar bij de programeer-vakken bleef ik toch vaak hangen. Dit jaar (Mijn 5de jaar) had ik buiten de projecten, enkel nog .Net Advanced en Java Advanced te doen, twee 2de jaar vakken. Op mijn 3de jaar vakken was ik namelijk al door. De SnB vakken gingen allemaal vlot, maar Java en .Net zijn altijd struikelblokken geweest. Ik heb hier wel uit geleerd dat ik sneller om hulp moet vragen aan mijn omgeving. Ik heb tijdens mijn studie een passie voor netwerken en cybersecurity gekregen en wil hier in de toekomst zeker verder mee gaan en certificaten behalen in deze gebieden om mijn kennis te vergroten.

Tijdens mijn 5 jaar aan de PXL, ben ik 4 jaar jobstudent geweest bij Jerotronics. Dit is een IT-consultancy bedrijf, waar ik als systeem en netwerkbeheerder werkte. Ik heb hier veel ervaring en kennis opgedaan, voornamelijk op het vlak van netwerken. Het werk van zeer gevarieerd, het kon wisselen tussen het opzetten van netwerkinfrastructuur, het opzetten van webservers of de klant helpen met problemen die ze ervaren.

Sterktes

Ik ben een zeer rustige persoon en kan goed met stress omgaan. Dit betekent dat ik in stressvolle situaties meestal het hoofd wel koel kan houden.

Teamwork is een van de sterktes, die ik op de PXL heb geleerd. Door middel van groepswerk en verschillende projecten heb ik geleerd hoe ik persoonlijk het beste in een groep werk. Als ik in een groep werk, ben ik geen leider. Ik doe wat er van mij verwacht wordt en probeer anderen te helpen met hun deel.

Werkpunt

Socialer worden is een punt waarin ik aan het proberen ben te verbeteren. Ik ben redelijk verlegen en vind het moeilijk om nieuwe mensen te leren kennen. Ik ben hier wel mee bezig om dit te verbeteren door tijdens de pauzes tussen de lessen af en toe eens met iemand die ik niet ken te gaan praten.

X-Factor

Bij een traject op de PXL staat de X-factor altijd centraal.

A picture containing icon

Description automatically generated  
Figuur 8: X-factor

Op vlak van (em)passie staat mijn huidige passie voor cybersecurity en netwerken centraal. Ik heb tijdens de opleiding geleerd dat ik het liefst werk met netwerkinfrastructuren of focus op het verbeteren van de beveiliging van mijn systemen.

Ik ben vooral ondernemend en innovatief geweest op mijn werk als jobstudent. Hier heb ik als systeem en netwerkbeheerder kunnen nadenken over de beste optie voor onze klanten en deze daarna toe te passen.

Voor samen(net)werking het IT-project een goed voorbeeld, ik heb hier samengewerkt met een groep, waarin ik op voorhand niemand kende. Door de groep te leren kennen en samen in te spelen op de sterktes van ieder teamlid, hebben we deze opdracht tot een succesvol einde kunnen brengen.

De seminaries die ik heb gevolgd van andere afstudeerrichtingen zijn een voorbeeld van multi- & disciplinariteit. Ik heb meerdere seminaries gevolgd over AI, om meer te leren over deze nieuwe technologie.