



Wekelijks Verslag Stage ACA IT-Solutions

IT Factory

Academiejaar 2022-2023

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

Wim Hembrechts

Inhoud

1 Week 1 (27/2 – 3/3)	5
1.1 Maandag 27/2	5
1.2 Dinsdag 28/2	5
1.3 Woensdag 1/3	5
1.4 Donderdag 2/3	5
1.5 Vrijdag 3/3	6
2 Week 2 (6/3 – 10/3)	7
2.1 Maandag 6/3	7
2.2 Dinsdag 7/3	7
2.3 Woensdag 8/3	7
2.4 Donderdag 9/3	7
2.5 Vrijdag 10/3	7
3 Week 3 (13/3 – 17/3)	8
3.1 Maandag 13/3	8
3.2 Dinsdag 14/3	8
3.3 Woensdag 15/3	8
3.4 Donderdag 16/3	8
3.5 Vrijdag 17/3	8
4 Week 4 (20/3 – 24/3)	9
4.1 Maandag 20/3	9
4.2 Dinsdag 21/3	9
4.3 Woensdag 22/3	9
4.4 Donderdag 23/3	9
4.5 Vrijdag 24/3	9
5 Week 5 (27/3 – 31/3)	10
5.1 Maandag 27/3	10
5.2 Dinsdag 28/3	10
5.3 Woensdag 29/3	10
5.4 Donderdag 30/3	10
5.5 Vrijdag 31/3	10
6 Week 6 (3/4 – 7/4)	11
6.1 Maandag 3/4	11
6.2 Dinsdag 4/4	11
6.3 Woensdag 5/4	11
6.4 Donderdag 6/4	11
6.5 Vrijdag 7/4	11
7 Week 7 (10/4 – 14/4)	12
7.1 Maandag 10/4	12
7.2 Dinsdag 11/4	12
7.3 Woensdag 12/4	12
7.4 Donderdag 13/4	12
7.5 Vrijdag 14/4	12
8 Week 8 (17/4 – 21/4)	13
8.1 Maandag 17/4	13

8.2 Dinsdag 18/4.....	13
8.3 Woensdag 19/4.....	13
8.4 Donderdag 20/4.....	13
8.5 Vrijdag 21/4.....	13
9 Week 9 (24/4 - 28/4).....	14
9.1 Maandag 24/4.....	14
9.2 Dinsdag 25/4.....	14
9.3 Woensdag 26/4.....	14
9.4 Donderdag 27/4.....	14
9.5 Vrijdag 28/4.....	14
10 Week 10 (1/5 - 5/5).....	15
10.1 Maandag 1/5.....	15
10.2 Dinsdag 2/5.....	15
10.3 Woensdag 3/5.....	15
10.4 Donderdag 4/5.....	15
10.5 Vrijdag 5/5.....	15
11 Week 11 (8/5 - 12/5).....	16
11.1 Maandag 8/5.....	16
11.2 Dinsdag 9/5.....	16
11.3 Woensdag 10/5.....	16
11.4 Donderdag 11/5.....	16
11.5 Vrijdag 12/5.....	16
12 Week 12 (15/5 - 19/5).....	17
12.1 Maandag 15/5.....	17
12.2 Dinsdag 16/5.....	17
12.3 Woensdag 17/5.....	17
12.4 Donderdag 18/5.....	17
12.5 Vrijdag 19/5.....	17
13 Week 13 (22/5 - 26/5).....	18
13.1 Maandag 22/5.....	18
13.2 Dinsdag 23/5.....	18
13.3 Woensdag 24/5.....	18
13.4 Donderdag 25/5.....	18
13.5 Vrijdag 26/5.....	18

1 WEEK 1 (27/2 – 3/3)

1.1 Maandag 27/2

Bij het toekomen heb ik eerst de andere stagiairs en mijn stagementor ontmoet. Vervolgens kregen we een korte rondleiding door het bedrijf. Hierna kregen we onze laptop. Op deze laptop hebben we dan de initiële configuratie gedaan zodat we aan de slag konden. Ook hebben we toen de nodige accountgegevens gekregen van de standaard gebruikte tools. Hierna werd ik bij mijn stagebegeleider gezet om zo de details van mijn stage te overlopen. Na de middag kreeg ik de opdracht om mij verder in te lezen in de opdracht en kon ik terecht met al mijn vragen.

1.2 Dinsdag 28/2

Op dag 2 kreeg ik de opdracht om een work breakdown structuur op te stellen zodat er een concrete planning was van de komende weken. Om deze planning op te stellen heb ik enkele links doorgenomen die ik ga moeten gebruiken tijdens mijn onderzoeksfase om zo de tijd die ik bij elke opdracht ga nodig hebben beter in te schatten. Verder heb ik ook een meeting gehad met mijn stagebegeleider om de EKS cluster setup op AWS te doorlopen waarom ik mijn stage opdracht ga moeten uitvoeren. Deze setup ga ik dan later nog verder doorgronden zodat ik deze volledig snap.

1.3 Woensdag 1/3

In het begin van dag 3 zijn ik en mijn stagebegeleider door mijn WBS gegaan om te kijken of deze goed en haalbaar is. Hierna heb ik deze aangepast met de feedback die ik gekregen had. Hierna ben ik aan de slag gegaan om de EKS cluster setup op AWS te doorgronden. Na de middag heb ik nog een korte meeting gehad om te overlopen hoe Kubernetes op de EKS clusters wordt gebruikt en hoe applicaties worden opgezet op deze clusters. Verder zijn we ook nog over de monitoring software gegaan. Hierna ben ik verder bezig geweest met het doorgronden van de clusters setup.

1.4 Donderdag 2/3

Verder doorgronden van de cluster setup op AWS om te kijken wat er juist wordt opgezet en hoe dit alles juist wordt opgezet. Hierbij heb ik heel wat documentatie van AWS moeten bekijken om al deze verschillende resources goed te kunnen snappen. Ook heb ik hier heel wat Terraform documentatie moeten doornemen omdat dit een van de tools is waarmee de infrastructuur wordt opgezet.

1.5 Vrijdag 3/3

Deze dag was ik iets later op kantoor aangezien ik onderweg naar stage een ongeluk heb gehad met de wagen. Hiervoor heb ik dan ook de nodige stappen ondernomen om al dit op te lossen. Nadat dit gebeurd was ben ik wederom verder aan de slag gegaan met het doorgronden van de EKS cluster setup en heb ik verder onderzocht hoe Kubernetes op deze clusters werkt en hoe dit gebruikt wordt om de applicaties te draaien.

2 WEEK 2 (6/3 - 10/3)

2.1 Maandag 6/3

Maandag heb ik het laatste stukje van de EKS cluster setup op AWS bekeken. Hierna had ik wel het gevoel het grootste deel te snappen zodat ik hier later op kan verder werken. Daarna ben ik aan de slag gegaan met ervaring opdoen van de gebruikte tools en plug-ins binnen het bedrijf. Ik heb de dag afgerond samen met Leonardo, wij hebben samen de toegang tot mijn eigen AWS-account en omgeving in orde gemaakt.

2.2 Dinsdag 7/3

Deze dag ben ik volledig bezig geweest met ervaring op te doen met de nodige tools die ik tijdens mijn opdracht voortdurend ga nodig hebben. Dit zijn er wel een aantal.

2.3 Woensdag 8/3

In de voormiddag heb ik de laatste nodige ervaring opgedaan met de gebruikte tools. Voornamelijk plug-ins die het werk tijdens mijn stage kunnen versnellen en vergemakkelijken. In de namiddag ben ik aan de slag gegaan met het opzetten van een lokale cluster op mijn laptop waarop ik alle zaken eerst ga uittesten alvorens deze op de effectieve AWS-omgeving uit te voeren.

2.4 Donderdag 9/3

Verder opzetten van de lokale test cluster op eigen laptop. In de namiddag beginnen doornemen van de EKS best practices en extra mogelijke componenten die AWS aanbiedt. In eerste instantie ben ik hier diagonaal aan het doorgaan om een ruw overzicht te krijgen wat er allemaal instaat zodat ik mij later in de belangrijke zaken kan verdiepen.

2.5 Vrijdag 10/3

Laatste stukje van de lokale testcluster in orde brengen met behulp van Leonardo. Hierna alles van Kubernetes opfrissen omdat het toch al even geleden was dat ik hiermee in aanraking ben gekomen. In de namiddag ben ik verder bezig geweest met de EKS best practices vluchtig door te lezen.

3 WEEK 3 (13/3 - 17/3)

3.1 Maandag 13/3

Maandag ben ik verder doorgegaan met het vluchtig doorlezen van de EKS best practices die AWS zelf aanbiedt. Deze dag heb ik zoals vorige maandag een korte sync gehad met Jan om te kijken hoe alles verloopt en of ik met eventuele vragen zit. Ook heb ik samengezeten met Jana om te kijken hoe de stage verloopt en of ik goed opgevangen ben in het team.

3.2 Dinsdag 14/3

Dinsdag ben ik zo goed als heel de dag bezig geweest met het doornemen van de EKS best practices. Verder heb ik ook nog wat extra zaken bekeken die eventueel mogelijk zijn om toe te passen op de testomgeving in AWS

3.3 Woensdag 15/3

Deze dag ben ik aan de slag gegaan met mij te verdiepen in het pod security gedeelte van de best practices, om te kijken wat hierin allemaal mogelijk is en wat de voor en nadelen zijn van de bepaalde oplossingen of tools. Dit kan ik dan later afstemmen met het team om te kijken wat haalbaar en nuttig is om te implementeren

3.4 Donderdag 16/3

Donderdag verliep hetzelfde als de dag voordien en heb mij verder verdiept in de pod security voor EKS. Na de werkuren zijn wij dan met het team een leuke teambuilding activiteit gaan doen.

3.5 Vrijdag 17/3

De laatste dag van week 3 ben ik begonnen met mij verder te verdiepen in de encryptie van de secrets die in Kubernetes worden opgeslagen en de AWS-service die hiervoor gebruikt wordt. In de namiddag heb ik dan de presentatie deels voorbereid voor het bezoek van mijn stagebegeleider aan het bedrijf van volgende maandag.

4 WEEK 4 (20/3 - 24/3)

4.1 Maandag 20/3

Maandag ben ik verder bezig geweest met mijn presentatie voor te bereiden. De tekst die erin stond was vorige vrijdag al afgerond, enkel de layout moest nog wat aangepast worden in thema van ACA. Op de middag is mijn stagebegeleider van Thomas More op bezoek geweest bij het stagebedrijf. Na dit bezoek ben ik verder aan de slag gegaan met de encryptie van secrets in etcd m.b.v AWS KMS.

4.2 Dinsdag 21/3

Deze dag heb ik helemaal gespendeerd met onderzoeken van de mogelijkheden binnen AWS KMS om de encryptie van secrets te implementeren. Eveneens heb ik onderzocht of dit wel effectief nodig is en wat de voor- en nadelen hiervan zijn.

4.3 Woensdag 22/3

Om even een pauze te nemen van de encryptie heb ben ik woensdag aan de slag gegaan met het scannen van CVE's in containers alvorens die gestart worden alsook welke tools hiervoor kunnen gebruikt worden en wat de eventuele voor- en nadelen zijn van deze tools.

4.4 Donderdag 23/3

Donderdag zag het er hetzelfde uit als de dag voordien. Onderzoek voor het scannen van CVE's in containers.

4.5 Vrijdag 24/3

Verder heb ik het deeltje rond encryptie terug vastgenomen om dit volledig af te ronden. Daarna heb ik in de namiddag samen met het volledige team een 2-wekelijkse sync gehad. Hierna terug bezig geweest met scannen naar CVE's in containers.

5 WEEK 5 (27/3 - 31/3)

5.1 Maandag 27/3

Maandag begon met het verder onderzoeken van tool Trivy om CVE's te scannen in containers. Ook had ik een korte sync met mijn stagementor. Hierdoor kwam ik te weten dat ik nog 2 zaken vergeten wat i.v.m. het encrypteren van secrets in etcd, namelijk of dit mogelijk is op een al bestaande cluster en een kosten voorspelling.

5.2 Dinsdag 28/3

Dinsdag ben ik begonnen met het onderzoeken van Open Policy Agent Gatekeeper die als vervanging gaat dienen van Pod Security Policies die uitgefaseerd worden bij Kubernetes v1.25.

5.3 Woensdag 29/3

Deze dag heb ik bekeken wat ik nodig heb om de kosten voorspelling te maken om AWS KMS te implementeren. Hiervoor heb ik eerst een query voor moeten zoeken. Hierna ben ik verder aan de slag gegaan met OPA Gatekeeper.

5.4 Donderdag 30/3

Het deel van OPA Gatekeeper afgerond en begonnen met kijken wat kube-bench en Kubescape kunnen betekenen in het huidige setup. Deze tools doen ongeveer hetzelfde (compliance testing & configuratie controle) maar doen dit op verschillende manieren.

5.5 Vrijdag 31/3

Verder onderzoeken wat kube-bench en Kubescape kunnen doen en wanneer welke het beste van pas komt.

6 WEEK 6 (3/4 - 7/4)

6.1 Maandag 3/4

Week zeven ben ik begonnen met het onderzoeken van tools die ongewenste of gevaarlijke processen kunnen opsporen in Kubernetes. Verder heb ik ook nog een sync gehad met mijn stagementor. Ook heb ik gekeken naar tools die voor RBAC hardening policies kunnen afdwingen.

6.2 Dinsdag 4/4

Dinsdag ben ik met beide topics van de dag voordien bezig geweest en heb ik mijn onderzoek hierin verder gezet.

6.3 Woensdag 5/4

Deze dag ben ik voornamelijk bezig geweest met onderzoek naar tools voor RBAC hardening. Maar in aanloop naar mijn presentatie van komende dinsdag (11/4) heb ik mijn documentatie van mijn onderzoek opgeschoond en verder aangevuld.

6.4 Donderdag 6/4

Documentatie verder opschonen en verder aanvullen met zaken die nog ontbraken. Documentatie doorgestuurd naar mijn stagementor voor feedback. En deze feedback dan ook onderzocht en beantwoord.

6.5 Vrijdag 7/4

Documentatie aanvullen en in aanloop van mijn presentatie en mijn effectieve presentatie in elkaar steken.

7 WEEK 7 (10/4 - 14/4)

7.1 Maandag 10/4

Geen werkdag vanwege de wettelijke feestdag.

7.2 Dinsdag 11/4

Laatste zaken voor mijn presentatie voorbereid en deze dan ook effectief gebracht. Feedback van na de presentatie opgenomen en hiermee aan de slag gegaan alsook de volgende stappen besproken met mijn stagementor. Een van die volgende stappen was de waarde en volgorde van elk onderzocht deel te bepalen en ook mijn keuze tussen 2 tools (OPA/Gatekeeper en Kyverno) beargumenteren.

7.3 Woensdag 12/4

De implementatie volgorde bepalen en achteraf ook bespreken samen met mijn stagementor aan de hand van een kosten/baten tabel. De verschillen tussen OPA/Gatekeeper en Kyverno verder bekijken om een uiteindelijke keuze te maken.

7.4 Donderdag 13/4

De Kyverno Helm charts doorgronden en een basis setup implementeren om mijn lokale testomgeving via Helm templating. Een deploy script schrijven voor Kyverno later op EKS te implementeren. Kyverno policies analyseren en kijken welke van toepassing kunnen zijn.

7.5 Vrijdag 14/4

Kyverno deploy uitvoeren op EKS cluster met vooraf geschreven deploy script. Uiteraard ook de nodige testen uitvoeren om te kijken of alles werkt naar behoren. Heel wat policies toevoegen en testen of deze werken zoals het hoort. In de namiddag ook een korte sync met mijn stagementor om te kijken hoe de implementatie lukt en of er ergens problemen zijn.

8 WEEK 8 (17/4 - 21/4)

8.1 Maandag 17/4

In de voormiddag heb ik het laatste stukje van Kyverno getest door nog enkele policies te implementeren. Verder heb ik ook nog een sync gehad met mijn stagementor. Ook ben ik aan de slag gegaan met het opzetten van een ingress controller en een sealed-secrets controller om zo achteraf de secret encryptie op te zetten op de testomgeving.

8.2 Dinsdag 18/4

Dinsdag heb ik toch nog een stukje voor Kyverno gedaan omdat ik merkte dat ik enkele zaken vergeten was toe te testen. Ook heb ik een document gemaakt met alle informatie over de Kyverno configuratie en de procedure om policies te implementeren. Daarna ben ik ook al een beetje aan de slag gegaan om alles klaar te zetten voor de secret encryptie.

8.3 Woensdag 19/4

Document over Kyverno en Kyverno policies procedure aanvullen en afmaken en alles definitief klaarzetten voor de secret encryptie.

8.4 Donderdag 20/4

Beginnen met het implementeren van de secret encryptie door de nodige code aan te passen en te laten evalueren door mijn stagementor. Tijdens het wachten ben ik ook al aan de slag gegaan met de volgende tool te implementeren. De Trivy Operator heb ik lokaal op mijn testcluster gezet en al wat uitgetest.

8.5 Vrijdag 21/4

Secret encryptie effectief opzetten en testen of alles werkt zoals verwacht. Aangezien niet alles werkte zoals verwacht, heb ik nog wat extra moeten onderzoeken. Ook ben ik verder bezig geweest met het testen van de Trivy Operator. In de namiddag heb ik samen met het team ook nog een 2 wekelijkse sync gehad en vermeld hoe de implementatie van de onderzochte tools verloopt.

9 WEEK 9 (24/4 - 28/4)

9.1 Maandag 24/4

Maandag ben ik begonnen met het deployen van de Trivy Operator op de EKS testomgeving nadat ik alles had uitgetest op mijn lokale testcluster. Verder heb ik getest of alles van de Trivy Operator goed werkte op de EKS omgeving. Daarnaast ben ik ook nog bezig geweest met het onderzoeken waarom de secret encryptie niet volledig werkte zoals verwacht. Hier heb ik nog geen oplossing voor gevonden. Net zoals elke maandag heb ik ook een korte sync gehad met mijn stagementor.

9.2 Dinsdag 25/4

Verder onderzoeken waarom de secret encryptie in EKS niet werkt zoals verwacht. Daarnaast ook al aan de slag gegaan met Falco als runtime threat detection tool om gevaarlijke of ongewenste processen te kunnen detecteren.

9.3 Woensdag 26/4

Woensdag begon de dag iets minder aangezien we op kantoor te maken hadden met een stroompanne. Hierdoor heb ik 1,5u niet kunnen werken. Nadat de stroompanne opgelost was ben ik bezig geweest met het deployen van Falco op mijn lokale testcluster. Dit lukte niet volledig aangezien er compatibiliteitsprobleem was met mijn lokale testcluster. Vandaar dat ik meteen begonnen ben met het deployen op de EKS testomgeving.

9.4 Donderdag 27/4

Heel de dag bezig geweest met het implementeren en testen van Falco rules om ongewenste of gevaarlijke processen te kunnen detecteren in de containers die draaien op de EKS testomgeving.

9.5 Vrijdag 28/4

Hetzelfde als de dag voordien, heel de dag Falco rules testen en proberen om te kijken of er meldingen tevoorschijn komen op het Falcosidekick dashboard.

10 WEEK 10 (1/5 - 5/5)

10.1 Maandag 1/5

Geen werkdag vanwege de wettelijke feestdag.

10.2 Dinsdag 2/5

Met de volgende tool in het rijtje aan de slag gaan, Kubescape. Deze tool gaat kijken of de cluster op de juiste manier opgezet is en of er configuratiefouten aanwezig zijn in de cluster. Daarnaast ook bezig geweest met het voorbereiden van een technische demo voor de dag nadien.

10.3 Woensdag 3/5

Nog wat extra voorbereiden voor de technische demo en deze dag ook effectief geven voor sommige in het team. Hierbij hoorde natuurlijk ook het verzamelen van feedback. Hierna heb ik gekeken welke zaken ik nog effectief moet doen of verwezenlijken tijdens mijn stage. Een van deze zaken is het oplijsten van welke Kyverno policies de moeite waard zijn.

10.4 Donderdag 4/5

Verder bezig geweest met het kijken welke Kyverno policies de moeite zijn en welke eventuele extra policies ook kunnen worden geïmplementeerd in de toekomst. Om wat afwisseling te hebben ben ik ook bezig geweest met het kijken hoe we onze eigen Falco rules kunnen toevoegen.

10.5 Vrijdag 5/5

Verder kijken welke Kyverno policies de moeite waard zijn en hoe we onze eigen Falco rules kunnen toevoegen. Daarnaast ook een stage opvolging gehad met Jana om te kijken hoe de stage verloopt. Verder heb ik ook de maandelijkse team retro en 2 wekelijkse sync bijgewoond.

11 WEEK 11 (8/5 - 12/5)

11.1 Maandag 8/5

Deze dag ben ik heel de dag bezig geweest met het voorbereiden van de oefen presentatie op school die later die dag plaatsvond.

11.2 Dinsdag 9/5

Verder aan de slag gaan met de feedback van de demo presentatie van de voorbije week. Bekijken hoe we custom rules kunnen toevoegen aan Falco en of het mogelijk is om de default rules die standaard bij Falco geleverd worden eventueel uitgezet kunnen worden.

11.3 Woensdag 10/5

Na een oplossing voor het probleem van de dag voordien gevonden te hebben, dit alles nog even uittesten en zorgen dat de oplossing zeker werkt en geen andere problemen met zich mee brengt. Bekijken welke scanners we bij de Trivy Operator allemaal gaan opzetten en welke er niet echt nuttig zijn en beter af staan.

11.4 Donderdag 11/5

Daarna verder gaan met het laatste puntje van de dag voordien en om wat afwisseling te hebben ook werken aan de uiteindelijke documentatie die opgeleverd moet worden voor zowel school als het stagebedrijf.

11.5 Vrijdag 12/5

De laatste dag van de week zag er hetzelfde uit als de dag voordien. Maar deze dag werd er iets meer gewerkt aan de documentatie aangezien het stukje van de Trivy Operator afgehandeld was.

12 WEEK 12 (15/5 - 19/5)

12.1 Maandag 15/5

Heel de dag bezig geweest met mijn documentatie in orde te maken zowel voor het stagebedrijf als de documenten voor de hogeschool.

12.2 Dinsdag 16/5

Net zoals de dag voordien heel de dag bezig geweest met mijn documentatie in orde te maken zowel voor het stagebedrijf als de documenten voor de hogeschool.

12.3 Woensdag 17/5

Net zoals de dagen voordien heel de dag bezig geweest met mijn documentatie in orde te maken zowel voor het stagebedrijf als de documenten voor de hogeschool.

12.4 Donderdag 18/5

Geen werkdag vanwege de wettelijke feestdag.

12.5 Vrijdag 19/5

Voornamelijk verder werken aan de documentatie. Maar daarnaast ook de eindpresentatie voor de maandag daarop voorbereiden.

13 WEEK 13 (22/5 - 26/5)

13.1 Maandag 22/5

Eindpresentatie voorbereiden voor stagebedrijf en deze presentatie ook effectief voorbrengen. Hierbij heb ik heel wat feedback gekregen. Ik ben de rest van de dag voornamelijk bezig geweest met het aanpassen van mijn presentatie. Daarnaast ook verder gewerkt aan mijn documenten.

13.2 Dinsdag 23/5

Net zoals de dagen voordien heel de dag bezig geweest met mijn documentatie in orde te maken zowel voor het stagebedrijf als de documenten voor de hogeschool.

13.3 Woensdag 24/5

Net zoals de dagen voordien heel de dag bezig geweest met mijn documentatie in orde te maken zowel voor het stagebedrijf als de documenten voor de hogeschool.

13.4 Donderdag 25/5

Net zoals de dagen voordien heel de dag bezig geweest met mijn documentatie in orde te maken zowel voor het stagebedrijf als de documenten voor de hogeschool.

13.5 Vrijdag 26/5

Voornamelijk mijn documentatie volledig afmaken en zien dat alles van documentatie beschikbaar is voor het stagebedrijf zodat ze hier verder mee aan de slag kunnen gaan.