THOMAS MORE

Geautomatiseerde Microsoft 365 Beveiligingsanalyse

Realisatiedocument – Stage RESILIX

Renzo Lemmens
Student Bachelor in de Elektronica-ICT – Cloud & Cyber Security

2024 - 2025

Inhoudsopgave

1. Inleiding

Dit realisatiedocument beschrijft de uitvoering van mijn stageopdracht bij RESILIX, waarbij ik me richtte op het automatiseren van hun Microsoft 365 Security Assessments, ook wel aangeduid als de “Geautomatiseerde M365 Beveiligingsanalyse”.

De inhoud van dit document is gebaseerd op het eerder opgestelde projectplan, waarin de onderzoeksaanpak en de te realiseren oplossing gedetailleerd werden beschreven. De centrale vraagstelling en doelstellingen van het onderzoek vormden daarbij het uitgangspunt voor een grondige analyse van het probleemgebied. Op basis van de verkregen inzichten heb ik vervolgens een concrete en praktische oplossing ontwikkeld.

De structuur van dit document is als volgt opgebouwd:
1. **Onderzoek** – Ik bespreek de toegepaste onderzoeksmethode, de verzamelde gegevens en de conclusies die hieruit voortkwamen.
2. **Realisatie** – Ik licht toe hoe de oplossing tot stand kwam, welke keuzes ik maakte tijdens het ontwikkelproces, en met welke uitdagingen ik te maken kreeg.
3. **Besluit** – Ik reflecteer op het volledige proces, evalueer de behaalde resultaten en formuleer aanbevelingen voor eventuele vervolgstappen.

Om de meerwaarde van de gerealiseerde oplossing objectief aan te tonen, zal er op het einde van de stageperiode een benchmark uitgevoerd worden. Deze vergelijking meet hoeveel tijd wordt uitgespaard bij het uitvoeren van een M365 Security Assessment met behulp van de geautomatiseerde aanpak in vergelijking met de traditionele werkwijze. De resultaten van deze meting worden meegenomen in het besluit en vormen een belangrijk element in de evaluatie van het succes van de opdracht.

Met dit document wil ik aantonen hoe ik theoretische inzichten heb vertaald naar een toepasbare en waardevolle oplossing die effectief bijdraagt aan de werking van RESILIX.

2. Analyse

Aan het begin van mijn stage werd ik ondergedompeld in de huidige werkwijze van RESILIX met betrekking tot Microsoft 365 Security Assessments. Deze verkenningsfase had als doel om inzicht te krijgen in het bestaande proces, de waaier aan diensten die RESILIX aanbiedt, de gebruikte tools voor het uitvoeren van assessments, en de manier waarop resultaten nadien worden verwerkt en gerapporteerd aan de klant.

Deze initiële analyse hielp om niet alleen de technische omgeving te begrijpen, maar ook om de probleemstelling en de verwachtingen omtrent de te realiseren oplossing scherp te stellen. De nood aan automatisering kwam duidelijk naar voren: ondanks de bestaande tooling was er sprake van overlappingen tussen de tools, manuele stappen in het rapportageproces en een gebrek aan centralisatie en efficiëntie.

2.1. Doel van het onderzoek

Het concrete doel van het onderzoek was het analyseren van de bestaande tools die binnen RESILIX gebruikt worden voor Microsoft 365 Security Assessments. Meer specifiek ging het om:

- Het berekenen van de mate van overlap tussen de verschillende tools;
- Het identificeren van unieke en ontbrekende controles (‘gaten’) in het huidige proces;
- Het bepalen van welke functionaliteit in de uiteindelijke oplossing moet worden opgenomen op basis van de bevindingen uit het vergelijkend onderzoek.

Deze analyse zou niet alleen helpen om de juiste technische keuzes te maken in het realisatietraject, maar ook om een oplossing te ontwikkelen die écht meerwaarde biedt en geen redundantie introduceert.

2.2. Methode van vergelijking

Voor het uitvoeren van deze vergelijking werd een technisch vergelijkingsdocument opgesteld in de vorm van een Excel-sheet (***zie bijlage 1***). Hierin werden alle “checks” (controlepunten of analyses) opgelijst die ik kon identificeren binnen elk van de onderzochte tools. Vervolgens werd voor elke check aangeduid of deze ook aanwezig was in de andere tools. Concreet vergeleek ik de volgende tools:

- **Semperis Purple Knight**: een bekende assessmenttool gericht op Active Directory & Entra ID;
- **ORCA**: een cloudbeveiligingsplatform dat ook Microsoft 365-configuraties en -risico’s in kaart brengt (voornamelijk gericht op Microsoft Defender for Office 365 - andere tools gaan veel breder);
- **CISA ScubaGear**: een open source tool van de Amerikaanse overheid voor het uitvoeren van security baselines;
- **Maester**: hoewel deze tool momenteel niet actief gebruikt wordt binnen RESILIX, werd ze opgenomen in de vergelijking als potentiële aanvulling binnen de toekomstige toolingstack.

De Excel-sheet zelf is opgebouwd met als doel de technische vergelijking overzichtelijk en systematisch te kunnen uitvoeren. Elke rij vertegenwoordigt één specifieke security check, terwijl de kolommen de relevante informatie hiërarchisch structureren. De kolomopbouw is als volgt:

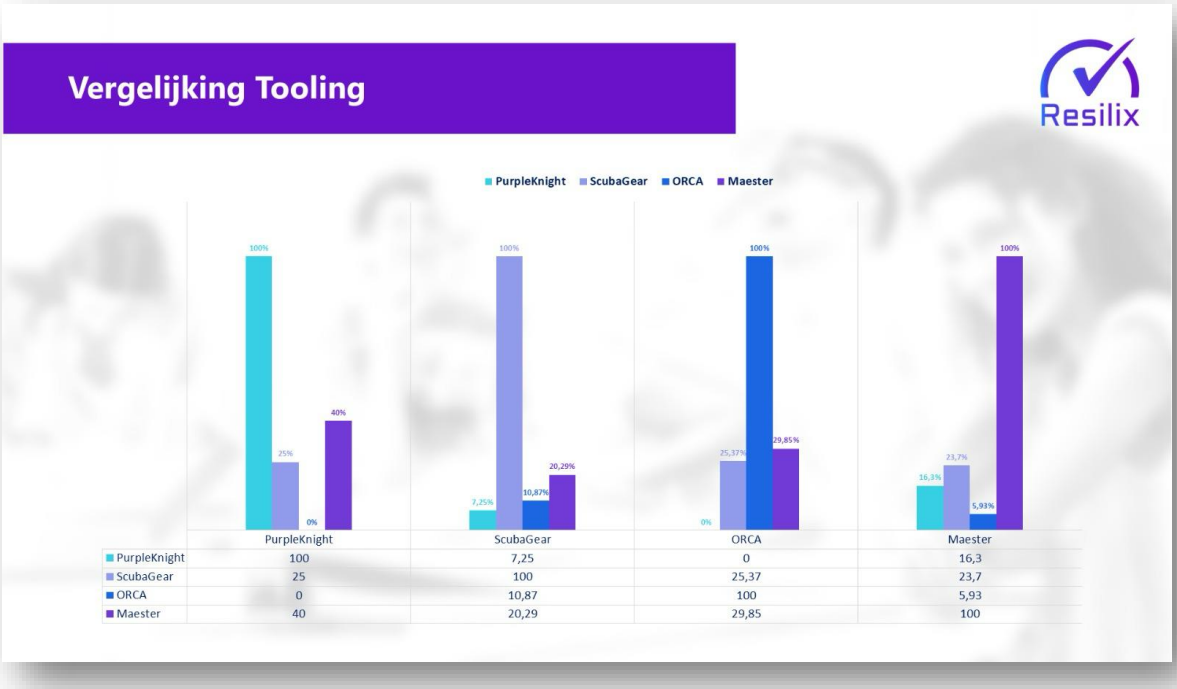
- **Category**: het overkoepelende beveiligingsdomein (bijvoorbeeld “Identity Management”)
- **Subcategory**: een verfijning binnen de categorie, om checks logisch te groeperen;
- **Rule Name**: de naam van de specifieke controle of regel;
- **Description**: een korte uitleg van wat de check precies nagaat;
- **Also in ... ?:** per tool wordt in deze kolommen aangeduid of de check daar eveneens beschikbaar is, met behulp van de binaire waarden true (aanwezig) of false (niet aanwezig);
- **Remarks**: optionele toelichting, bijvoorbeeld over context, beperkingen of interpretatie van de check.

De resultaten van deze vergelijking vormen het logische vertrekpunt voor de verdere ontwikkeling van de oplossing. De inzichten uit de Excel-analyse maken het mogelijk om gericht keuzes te maken over welke

functionaliteit essentieel is, welke overlap vermeden kan worden, en waar automatisering de grootste meerwaarde biedt. Zo dient de vergelijking niet alleen als analyse-instrument, maar ook als gefundeerde basis voor de afbakening en realisatie van de uiteindelijke oplossing.

2.3. Bespreking van de resultaten

Uit de vergelijking blijkt dat er aanzienlijke verschillen zijn in de mate van overlap tussen de onderzochte tools. Hieronder geef ik enkele kernbevindingen weer



Figuur 1 - Visuele representatie analyseresultaten.

- **Purple Knight**: vertoont **25%** overlap **met ScubaGear** en **40% met Maester**, maar heeft **geen enkele overlap met ORCA**. Dit suggereert dat Purple Knight voornamelijk unieke controles bevat die niet in ORCA terug te vinden zijn.
- **ScubaGear:** toont beperkte overlap met **Purple Knight (7,25%)** en **ORCA (10,87%)**, maar een relatief hogere **overlap met Maester (20,29%)**, wat wijst op enkele gedeelde principes of aanpakken.
- **ORCA**: heeft zelf een **overlap van 25,37% met ScubaGear** en **29,85% met Maester**, maar bevestigt via de vergelijking vanuit Purple Knight dat ORCA nauwelijks gemeenschappelijke checks bevat met de overige tools. Merk op dat ORCA enkel gericht is op Microsoft Defender for Office 365.
- **Maester:** opgenomen als suggestieve aanvulling, vertoont een gematigde overlap met **Purple Knight (16,3%)** en **ScubaGear (23,7%)**, maar **slechts 5,93% met ORCA**.

Deze resultaten maken duidelijk dat **geen enkele tool een volledige dekking biedt** en dat er zowel aanzienlijke overlap als hiaten bestaan.

Een opvallend inzicht uit de analyse is dat Maester zich ontpopt als het meest geschikte vertrekpunt voor het **ontwikkelen van een eigen oplossing** binnen RESILIX. De tool toont niet alleen de hoogste mate van overlap met de andere tools, maar blijkt ook inhoudelijk breed inzetbaar en uitbreidbaar.
Door Maester als fundering te gebruiken, kan een aanzienlijk deel van de benodigde functionaliteit hergebruikt of versterkt worden, wat het ontwikkeltraject efficiënter maakt en tegelijk toelaat om gericht in te spelen op de specifieke noden van RESILIX.

Om de potentie van de eigen tool extra te toetsen, ontwikkelde ik een Proof of Concept. Gebaseerd op de broncode van Maester, integreerde ik de RESILIX-huisstijl en schreef ik eigen testen. De succesvolle uitvoering hiervan bevestigde de technische haalbaarheid en versterkte het vertrouwen om verder op deze tool te bouwen en te ontwikkelen

Tijdens het onderzoek kwam ook naar voren dat de meeste tools in grote mate gebaseerd zijn op PowerShell-scripts. Deze ontdekking was voor mij bijzonder waardevol, aangezien ik tijdens mijn opleiding reeds vertrouwd raakte met PowerShell binnen de lessen Windows Server. In het bijzonder heb ik tijdens een Case Study gewerkt met Pester Tests – een testframework voor PowerShell – wat me toeliet om de werking van de tools sneller te doorgronden, de bestaande checks te analyseren en eigen controlesystemen op te zetten. Deze voorkennis speelde een cruciale rol in het beoordelen van de kwaliteit van de bestaande scripts en het opstellen van een solide basis voor de eigen automatiseringsoplossing binnen RESILIX.

2.4. Abstract

Er werd onderzoek gedaan naar de werking van de tools die momenteel door RESILIX gebruikt worden voor het uitvoeren van Microsoft 365 Security Assessments, met als doel overlap en hiaten in kaart te brengen.

Aan de hand van een gestructureerde vergelijking, opgebouwd in een Excel-sheet met binaire classificatie (true/false), werd een technische analyse uitgevoerd van vier tools:

- Semperis Purple Knight;
- Cammuray ORCA;
- CISA ScubaGear;
- Maester

De tools bleken grotendeels te bestaan uit PowerShell-scripts, wat me toeliet om dankzij mijn voorkennis uit de lessen Windows Server snel inzicht te krijgen in hun werking en opbouw.

De resultaten tonen aan dat geen enkele tool een volledige dekking biedt, maar dat er onderling wel significante overlappingen en leemtes bestaan. Vooral Maester kwam uit de vergelijking naar voren als een breed inzetbare en uitbreidbare oplossing met de hoogste mate van overlap met andere tools.

Op basis van deze inzichten werd beslist om deze tool als technische fundering te gebruiken voor het ontwikkelen van een eigen geautomatiseerde oplossing die optimaal aansluit bij de noden van RESILIX.

3. Realisatie - RESILIX 365 SECURITY

RESILIX 365 SECURITY is ontworpen met als doel het uitvoeren van Microsoft 365 Security Assessments op een efficiënte, gestandaardiseerde en reproduceerbare manier.

De broncode zelf kan niet gedeeld worden, aangezien die eigendom is van het stagebedrijf. Om die reden wordt de realisatie op een bondige manier beschreven, met focus op de functionele opbouw en de onderliggende logica, zonder vertrouwelijke of bedrijfsspecifieke details vrij te geven**. Waar mogelijk wordt de werking verduidelijkt aan de hand van screenshots of code snippets**, zodat de gebruikte aanpak en structuur toch concreet geïllustreerd kunnen worden zonder inbreuk te maken op de vertrouwelijkheid van de code.

3.1. Van Maester naar RESILIX 365 SECURITY

De initiële realisatie startte met het opzetten van een Proof of Concept (PoC). Hiervoor werd de GitHub-broncode van Maester gekloond en lokaal aangepast. De focus lag op drie centrale aanpassingen:

- **Integratie van de RESILIX-huisstijl** in output (rapporten en logging), zodat de tool visueel aansluit bij de bedrijfsidentiteit.
- **Aanpassing en uitbreiding** van **bestaande checks**: waar nodig werden bestaande regels geherformuleerd of uitgebreid om meer context te bieden binnen de RESILIX-omgeving.
- **Ontwikkeling van eigen checks**, gebaseerd op noden die tijdens de analyse naar voren kwamen maar niet door bestaande tools werden afgedekt.

3.2. Powershell en Pester Framework

RESILIX 365 SECURITY is compatibel met **PowerShell 7.0**. Deze versie ondersteunt **cross-platform compatibiliteit**, wat betekent dat de tool probleemloos werkt op **Windows, MacOS en Linux**. Dit vergroot de inzetbaarheid van de oplossing aanzienlijk en maakt het voor zowel medewerkers als klanten met uiteenlopende IT-omgevingen mogelijk om de tool op een flexibele manier te gebruiken.

De testen in RESILIX 365 SECURITY zijn gebaseerd op de logica van het **Pester Framework**, een testframework voor PowerShell. Dankzij deze structuur konden eigen geschreven checks eenvoudig gevalideerd worden. Dit maakte iteratief ontwikkelen en debuggen een stuk efficiënter en verhoogde de betrouwbaarheid en onderhoudbaarheid van de tool.

3.3. Functionele componenten

De gerealiseerde tool bevat momenteel de volgende kernfunctionaliteiten:

- **Automatische inventarisatie van M365-configuraties** (zoals conditional access policies, MFA-instellingen, rollen en permissies);
- **Scoringmodel** gebaseerd op het **Resilix Pragmatic Scoring System** (**RPSS**), waarmee risico's per check systematisch worden gewogen en beoordeeld.
- **Rapportgeneratie** in zowel **Markdown** als **HTML**, opgemaakt in de **huisstijl van RESILIX**, met per check een samenvatting, bijhorende RPSS-score, aanbevelingen, relevante documentatie en directe links naar het betrokken object binnen de M365-omgeving.
- **Modulair scriptontwerp**, waardoor het eenvoudig is om toekomstige checks toe te voegen zonder de bestaande logica te breken.
- **Interactieve authenticatie,** om vlot connectie te maken met de M365-omgeving van de klant.

3.4. Pester-testlogica

Binnen het project RESILIX 365 SECURITY werd het Pester-framework gebruikt om geautomatiseerde controles uit te voeren op Microsoft 365-configuraties. Elke test toetst een specifieke beveiligingsinstelling en rapporteert of deze voldoet aan de gewenste standaard. Deze aanpak zorgt voor reproduceerbare, gestructureerde en betrouwbare risicoanalyses.

STRUCTUUR

Elke test volgt een vaste opbouw in Pester:

```
Describe "<ORG>" {
    It "<TAG>:<DESCRIPTION>" {
        $result = Test-<NAME>
        $result | Should -Be $<true/false> -Because "<REASON>"
    }
}
```

Figuur 2 – Sjabloon voor Pesterlogica.

- **<ORG>**: Naam of onderwerp van de testgroep, vaak de bron (bv. RESILIX of Microsoft).
- **<TAG>**: Unieke code van de test, bv. R365-001.
- **<DESCRIPTION>**: Korte omschrijving van wat getest wordt.
- **Test-<NAME>**: De functie die de check uitvoert.
- **<true/false>**: Verwachte uitkomst (bijvoorbeeld $true als MFA verplicht moet zijn).
- **<REASON>**: Uitleg waarom deze instelling belangrijk is.

De functie **Test-<NAME>** is gedefinieerd in een aparte PowerShell-file, bijvoorbeeld **Test-MfaGlobalAdmins.ps1**. Hierin zit de logica om data op te halen uit de Microsoft 365-omgeving, meestal via de Microsoft Graph API of andere relevante cmdlets.

```
function Test-XXX {
    $result = $true

    try {
        # Gegevens ophalen, vergelijken met verwacht resultaat
        # Indien niet in orde:
        # $result = $false
    }
    catch {
        $result = $false
        Write-Error $_.Exception.Message
    }

    return $result
}
```

Figuur 3 - Sjabloon voor testfunctie

De testfunctie verwerkt deze gegevens, vergelijkt ze met het verwachte beveiligingsbeleid (zoals vastgelegd in de Pester-logica), en geeft een Boolean-waarde $result terug. Deze waarde is $true als de configuratie voldoet aan het beleid, en $false indien niet.

3.5. Gebruik van RESILIX 365 SECURITY

Vooraleer de tool gebruikt kan worden, moet de gebruiker de Resilix-module importeren die ervoor zorgt dat alle commandlets van RESILIX 365 SECURITY beschikbaar zijn.

```
PS /Users/renzo/Downloads/Resilix-365-Security> Import-Module ./powershell/Resilix.psm1
```

Figuur 4 – Importeren van de vereiste modules in Powershell.

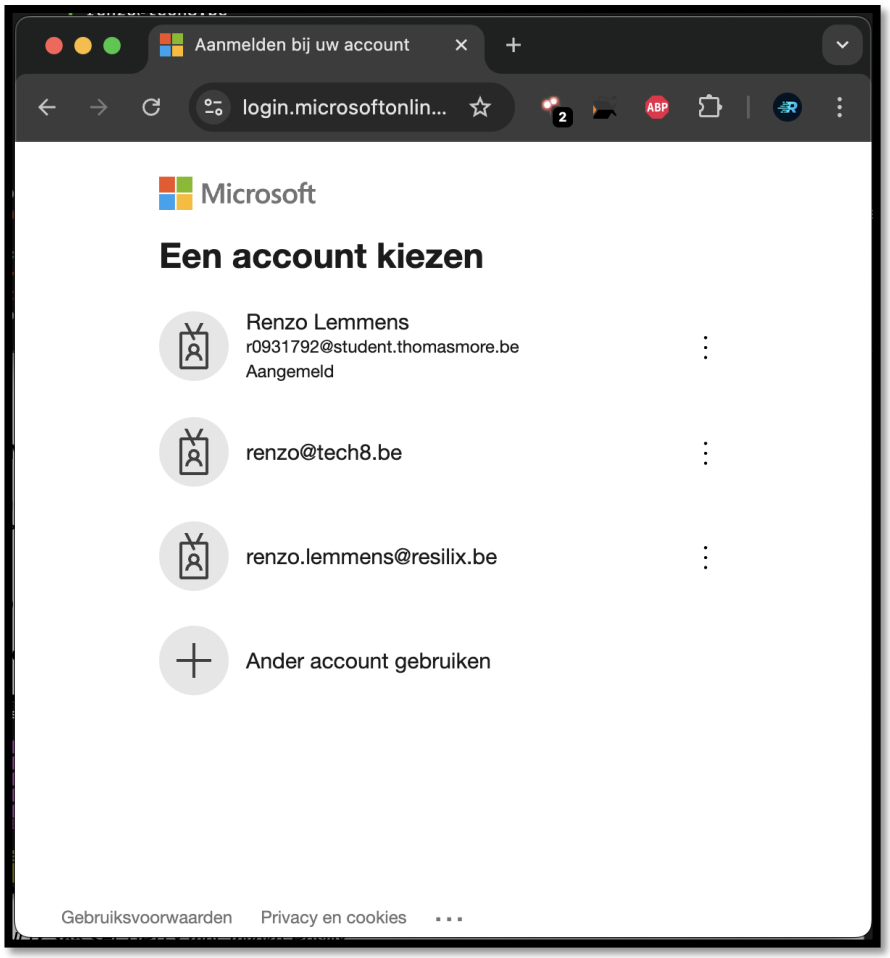
Zodra alle modules beschikbaar zijn, kunnen we commandlets van RESILIX 365 SECURITY gebruiken.

Het cmdlet '**Connect-Resilix'** kan gebruikt worden om interactief te authenticeren bij Microsoft. De standaardbrowser opent na het uitvoeren van dit commandlet om in te loggen bij Microsoft.

Hiervoor hebben we een account uit de organisatie nodig, met enkel **Global Reader** rechten. In dit geval gebruik ik mijn eigen RESILIX-account.

```
PS /Users/renzo/Downloads/Resilix-365-Security> Connect-Resilix
```

Figuur 5 - Verbinden met de M365-omgeving met het commandlet 'Connect-Resilix'.



Figuur 6 - Interactieve authenticatie bij Microsoft, dat automatisch verzoekt om in te loggen via de standaardbrowser.

Zodra de connectie met de Microsoft 365-omgeving succesvol tot stand is gebracht, start de gebruiker de analyse met Invoke-Resilix. Tijdens de uitvoering wordt er verbose output weergegeven, waarin telkens wordt aangegeven welke check actief is. De gebruiker kan optioneel een specifieke subset van checks opgeven via de -Path <pad>-parameter, bijvoorbeeld om enkel zelfgeschreven of aangepaste tests uit te voeren.

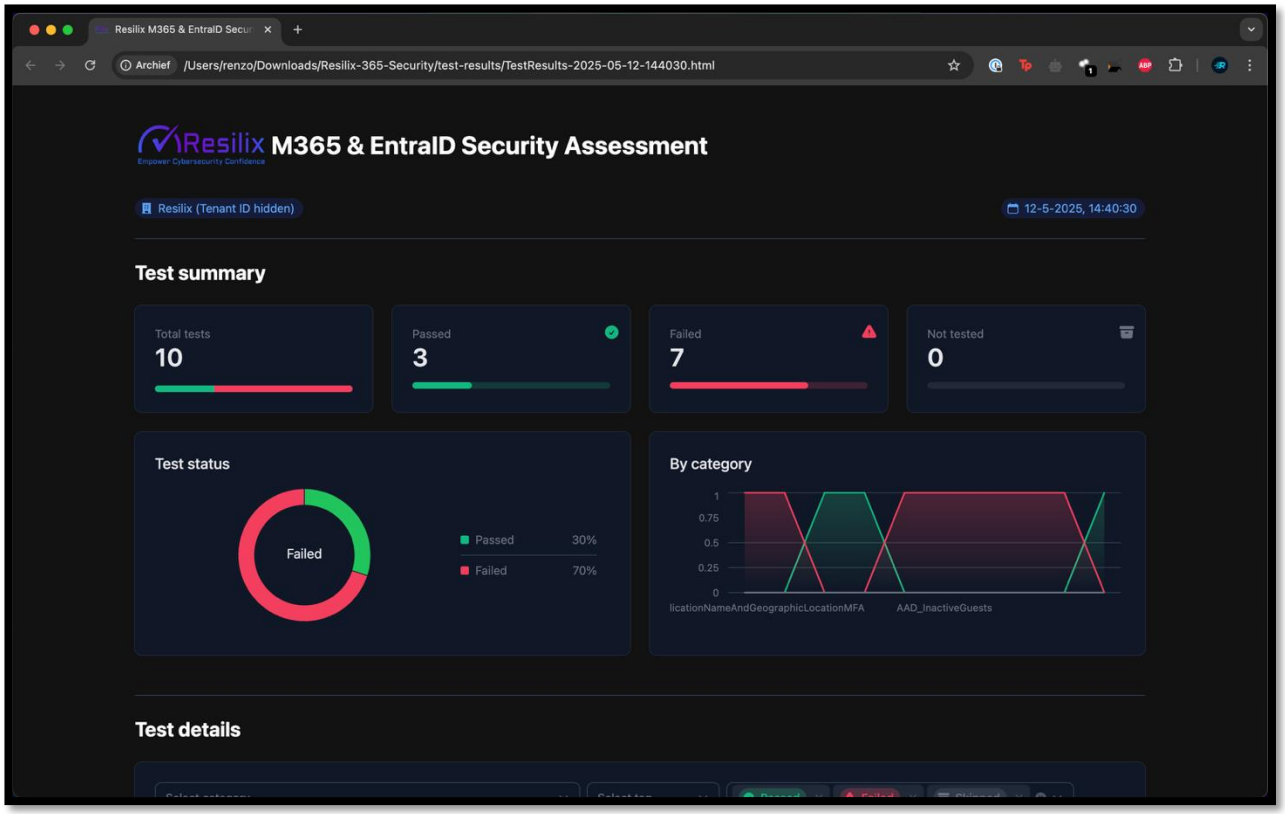
Elke check voert logica uit op basis van opgehaalde gegevens uit de Graph API, en evalueert of de configuratie voldoet aan het verwachte resultaat (true/false). De check wordt vervolgens aangeduid als geslaagd of gefaald, afhankelijk van de uitkomst.

Figuur 7– Uitvoeren van RESILIX 365 SECURITY met 'Invoke-Resilix'.

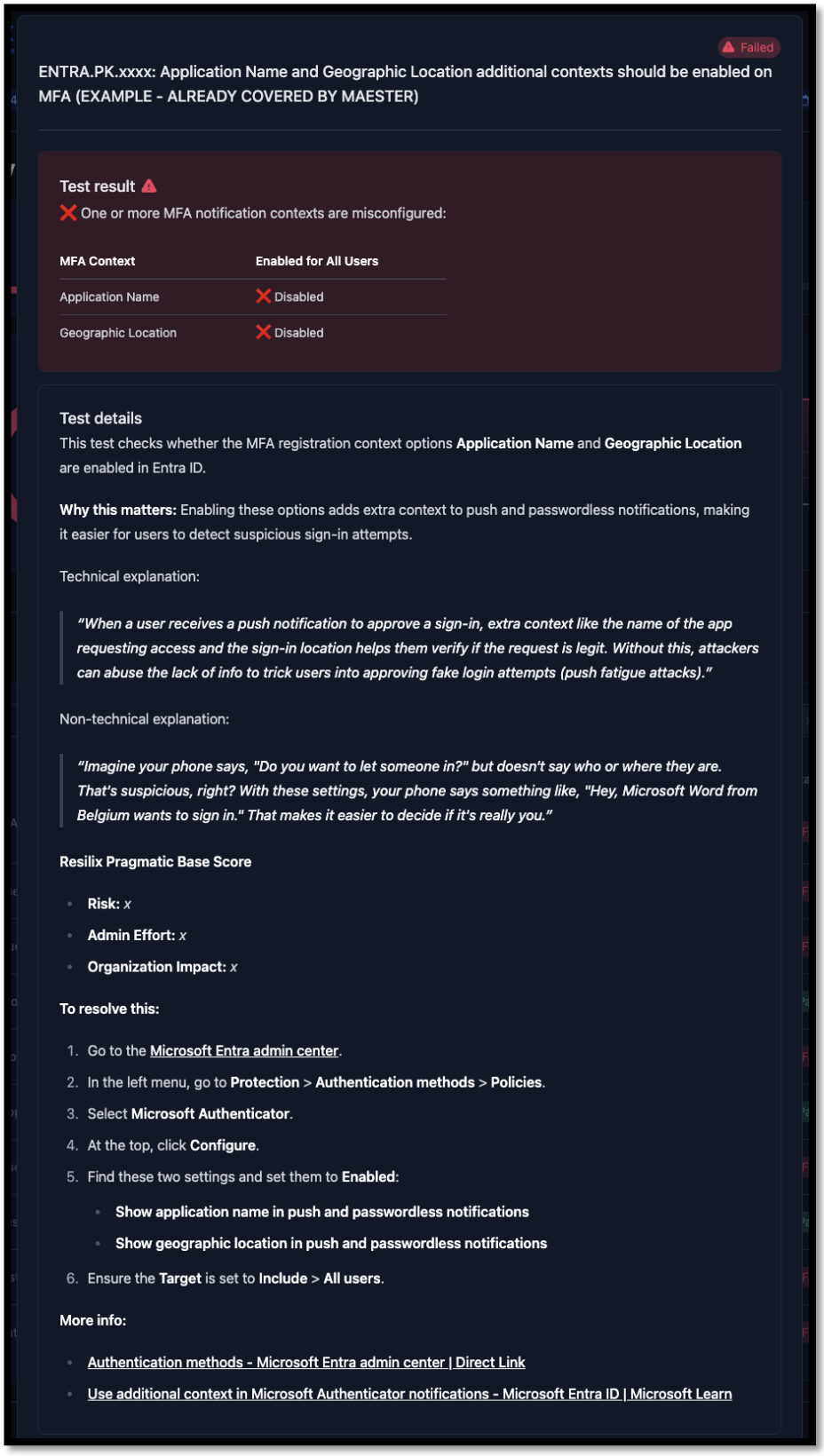
Figuur 8 – Uitvoer van de tool na het voltooien.

Na voltooiing worden de resultaten verwerkt in een rapport in zowel HTML als Markdown. Het HTML-bestand opent automatisch in de standaardbrowser en beide rapporten worden opgeslagen in een submap test-results binnen de map waarin het script werd uitgevoerd.

Elk rapport bevat per check een score, een korte samenvatting en aanbevelingen, verrijkt met rechtstreekse links naar de betrokken objecten in Microsoft 365.



Figuur 9 – Overzicht van HTML-rapport dat automatisch, na voltooiing, opent in de standaardbrowser.



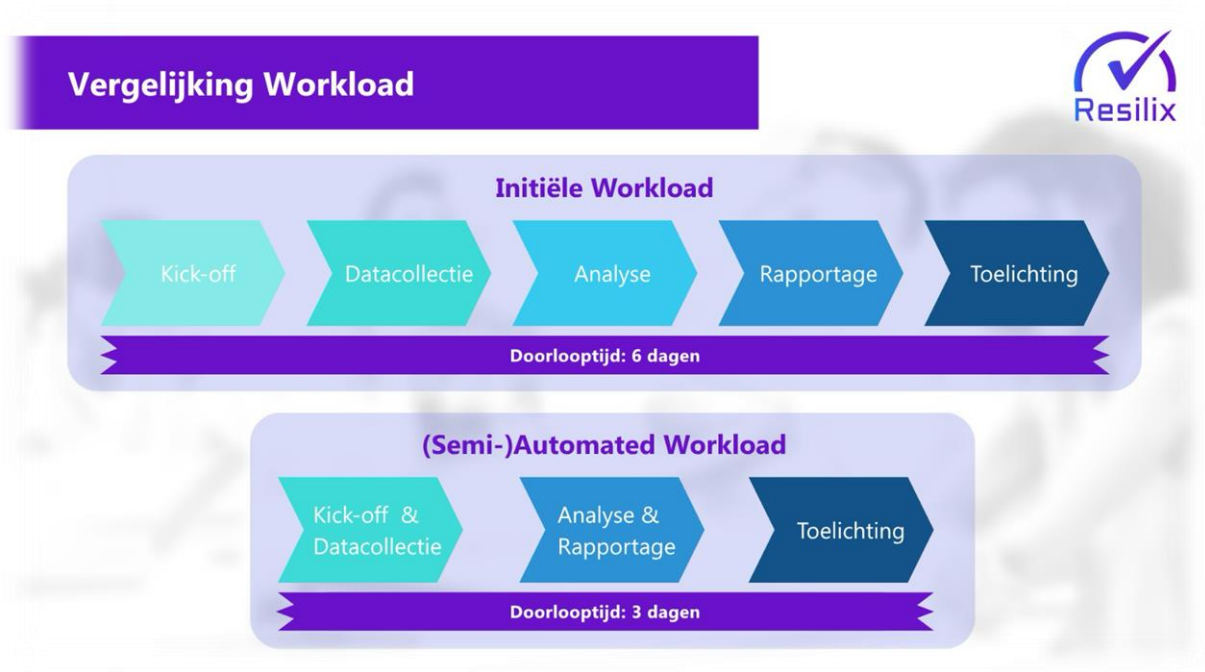
Figuur 10 – Voorbeeld van detailvenster met resultaten en uitleg voor een specifieke controle.

4. Besluit

Deze stageopdracht bij RESILIX bood de kans om theoretische inzichten om te zetten in een tastbare en waardevolle oplossing binnen een realistische bedrijfscontext. Door middel van een grondige analyse van bestaande Microsoft 365 Security Assessment-tools, werd vastgesteld dat geen enkele van de onderzochte tools – *Purple Knight, ORCA, ScubaGear en Maester* – een volledige dekking bood. Deze vaststelling legde de basis voor het ontwikkelen van een eigen oplossing: **RESILIX 365 SECURITY.**

Het ondersteunen van **PowerShell 7.0** maakt de tool platformonafhankelijk en breed inzetbaar. Door het gebruik van het Pester-framework voor het opzetten van tests, kon op een gestructureerde manier worden gewerkt aan betrouwbaarheid en onderhoudbaarheid. De tool is modulair opgebouwd, biedt een pragmatisch scoringsmodel (**RPSS**), en genereert heldere rapporten afgestemd op de huisstijl van RESILIX.

4.1. Bewijs van meerwaarde



Figuur 11 - Visuele representatie benchmark tijdsbesparing met RESILIX 365 SECURITY t.o.v. traditionele aanpak

Om de **meerwaarde** van de tool objectief aan te tonen, werd een **benchmark** uitgevoerd waarbij de traditionele werkwijze werd vergeleken met het gebruik van **RESILIX 365 SECURITY**.

Uit deze vergelijking bleek dat de geautomatiseerde aanpak een **halvering van de doorlooptijd** realiseert: van **6 dagen** naar slechts **3 dagen** per audit. Dit betekent een **besparing van meerdere mandagen per audit**.

De tijdswinst wordt vooral bereikt door het elimineren van repetitieve manuele stappen, het versnellen van de rapportgeneratie en het automatisch en gestructureerd ophalen van configuratie-informatie. Dit resulteert in een efficiënter auditproces met minder werklast en kortere doorlooptijd, zonder in te boeten aan kwaliteit of grondigheid.

4.2. Vooruitblik

Vooruitkijkend, hoop ik dat RESILIX de ontwikkelde tool verder blijft inzetten en verfijnen binnen hun interne werking. De tool biedt een sterke basis om Microsoft 365 Security Assessments efficiënter en consistenter uit te voeren, en kan op termijn bijdragen aan snellere en kwaliteitsvollere audits.

Mogelijk vormt RESILIX 365 SECURITY ook een meerwaarde in commerciële trajecten, bijvoorbeeld als demonstratie tijdens sales pitches of als onderscheidende factor in klantvoorstellen. Met verdere uitbreiding en onderhoud kan deze oplossing een kernonderdeel worden van de security-aanpak van RESILIX.

4.3. Terugblik

Terugkijkend op de oorspronkelijke doelstellingen van het projectplan, kan geconcludeerd worden dat deze in belangrijke mate zijn behaald:

- Er werd een duidelijke analyse gemaakt van de bestaande werkwijze en tooling;
- De ontwikkelde tool brengt efficiëntie, standaardisatie en reproduceerbaarheid in het assessmentproces;
- Het eindresultaat sluit nauw aan bij de noden van RESILIX en laat ruimte voor toekomstige uitbreidingen.

Tot slot blik ik met voldoening terug op deze opdracht. Het project gaf mij de kans om zelfstandig te werken aan een concrete uitdaging binnen een professionele omgeving, waarbij ik mijn technische vaardigheden, analytisch denkvermogen en oplossingsgerichtheid heb kunnen versterken. Het resultaat draagt niet alleen bij aan mijn persoonlijke groei, maar levert ook een directe meerwaarde op voor RESILIX.

4.4. Dankwoord

Bij het afronden van deze stage wil ik graag mijn oprechte dank uitspreken aan iedereen die heeft bijgedragen aan dit leertraject.

In het bijzonder wil ik mijn **stagementor(en)** bij RESILIX (**Hendrik Noben** en **Stephan Van Dyck)** bedanken voor de constructieve begeleiding, het vertrouwen en de waardevolle feedback tijdens het project. Ook dank aan het **hele team van RESILIX** voor de warme ontvangst, de inspirerende werkomgeving en de bereidheid om kennis te delen – dit maakte een wereld van verschil in mijn leerproces.

Daarnaast wil ik mijn **docent/stagebegeleider** aan **Thomas More Hogeschool in Geel** bedanken voor de begeleiding vanuit de opleiding en het mee bewaken van de kwaliteit van het project.

Tot slot ben ik dankbaar voor de kans om bij RESILIX te mogen meewerken aan een uitdagend en maatschappelijk relevant vraagstuk. Deze ervaring zal me zonder twijfel blijven inspireren in mijn verdere professionele loopbaan.

LITERATUURLIJST

Maester
https://maester.dev/docs/tests

Cammuray - ORCA
https://github.com/cammurray/orca/tree/master/Checks

CISA - ScubaGear
https://github.com/cisagov/ScubaGear/blob/main/baselines/README.md
https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

Semperis - Purple Knight
https://www.semperis.com/purple-knight/security-indicators/

Microsoft Learn
https://learn.microsoft.com/en-us/powershell/microsoftgraph/overview?view=graph-powershell-1.0

Bijlagen

1. *M365_Security_Tools_Technische_Vergelijking.xlsx*
   https://portfolio.renzo.me/assets/internship/M365_Security_Tools_Technische_Vergelijking.xlsx