THOMAS MORE

PROJECTPLAN

STAGE RESILIX

Renzo Lemmens

2024 – 2025

Inhoud

1. Wat is Resilix?

“Bij Resilix richten we ons op het bieden van doelgerichte securityoplossingen, ontworpen vanuit een pragmatische aanpak om uw organisatie optimaal te beschermen tegen de complexe bedreigingen van vandaag. Als uw vertrouwde partner in cybersecurity streven we ernaar om nauw met u samen te werken, zodat we de beveiliging kunnen bieden die precies past bij de unieke behoeften van uw bedrijf.

Ons team van security experten met meer dan 15 jaar ervaring is toegewijd aan het creëren van een veiligere omgeving voor uw organisatie door te focussen op effectieve en efficiënte beveiligingsstrategieën. Wij willen uw eerste keuze zijn voor advies en ondersteuning in cybersecurity, door u te voorzien van de tools en kennis die nodig zijn om weerbaar te zijn tegen de digitale uitdagingen van nu en in de toekomst.”

Bron: https://www.resilix.be/more-info/about-resilix

2. Stageopdracht

Mijn stageopdracht bij Resilix richt zich op het ontwikkelen en implementeren van een geautomatiseerd systeem dat beveiligingsanalyses in Microsoft 365 vereenvoudigt en visualiseert. Momenteel maakt het team gebruik van verschillende tools voor security-audits, maar het afzonderlijk uitvoeren ervan en het bundelen van de resultaten (meestal in de vorm van een PPT) is omslachtig en inefficiënt.

Het doel van mijn opdracht is om dit proces te optimaliseren, zodat security-audits gestroomlijnd verlopen en er flexibiliteit is voor eigen aanpassingen. Dit kan variëren van het consolideren van bestaande tools in een geautomatiseerd script tot het gebruiken van een LLM (Large Language Model) om de output van deze tools te converteren naar een uniform formaat dat het opstellen van rapporten efficiënter maakt of zelfs een volledig eigen tool schrijven.

Hiernaast krijg ik de kans om hands-on ervaring op te doen bij klanten en werk ik nauw samen met het team, waarbij ik gebruikmaak van de expertise binnen Resilix op het gebied van beveiligingsmonitoring en -optimalisatie.

2.1. Wat is dan het probleem dat ik zal oplossen?

Voor Resilix:
Momenteel maakt Resilix gebruik van verschillende tools om security-audits uit te voeren binnen Microsoft 365. Dit zorgt voor een omslachtig en inefficiënt proces waarbij resultaten handmatig gebundeld moeten worden. Bovendien ontbreekt een gestandaardiseerde checklist, waardoor de focus per audit kan variëren (sommige tools richten zich op bepaalde aspecten, terwijl andere belangrijke risico’s mogelijk niet volledig belichten). Dit gebrek aan uniformiteit maakt het lastig om snel en gestructureerd inzicht te krijgen in de beveiligingsstatus van een klantomgeving.

Voor de klant:
Veel bedrijven hanteren een "het moet werken"-mentaliteit, waarbij security vaak niet de eerste prioriteit is. Beveiliging komt pas in beeld wanneer er specifieke compliance-eisen ontstaan of wanneer er twijfel rijst over de veiligheid van de IT-omgeving. Daarnaast is Microsoft-software standaard ingesteld op usability boven security, waardoor er risico’s ontstaan als beveiligingsinstellingen niet expliciet worden geoptimaliseerd.

2.2. Waarom bestaat dit probleem?

Geen geïntegreerd auditproces: Het ontbreken van een centrale tool leidt tot inefficiëntie en inconsistente resultaten.
Geen standaard checklist: Doordat er geen uniforme aanpak is, kunnen belangrijke beveiligingsrisico's over het hoofd worden gezien.
Security komt vaak op de tweede plaats: Bedrijven focussen primair op functionaliteit en productiviteit, terwijl security vaak pas later aandacht krijgt.
Microsoft's standaardinstellingen: De prioriteit ligt op gebruiksgemak, waardoor organisaties proactief maatregelen moeten nemen om security te verbeteren.

2.3. Wat is de meerwaarde van mijn oplossing?

Voor Resilix:

- **Efficiëntere audits:** Door het proces te automatiseren en visualiseren, worden security-audits sneller en eenvoudiger uitvoerbaar. Dit resulteert in een aanzienlijke reductie van het aantal benodigde mandagen, wat direct bijdraagt aan een efficiënter gebruik van tijd en middelen.
- **Gestandaardiseerd en compleet inzicht:** Een uniforme checklist en geautomatiseerde rapportage a.d.h.v. een eigen standaard zorgen voor een vollediger overzicht van de beveiligingsstatus.
- **Schaalbaarheid:** De oplossing kan flexibel worden uitgebreid en aangepast aan de specifieke noden van klanten.

Voor de klant:

- **Sneller inzicht in security-status:** Met geautomatiseerde rapportages krijgt de klant direct inzicht in kwetsbaarheden en verbeterpunten.
- **Verbeterde beveiliging:** Door structurele monitoring en aanbevelingen kunnen beveiligingsrisico's vroegtijdig worden aangepakt.
- **Tijds- en kostenbesparing:** Doordat audits minder mandagen in beslag nemen, bespaart de klant niet alleen op auditkosten, maar kan hij ook sneller actie ondernemen om security-issues aan te pakken. Dit voorkomt potentiële schade en extra kosten door beveiligingsincidenten.
- **Gestandaardiseerd plan van aanpak:** Het assessment, dat steeds op maat is, wordt vertaald naar een Resilix-gestandaardiseerd plan van aanpak, wat zorgt voor een duidelijke en efficiënte opvolging van verbeterpunten.

2.4. Hoe kan ik zoeken naar een oplossing?

1. **Analyse van bestaande tools en methodes**
    - **Welke tools gebruikt Resilix momenteel?** Bekijk welke tools worden ingezet en waarom ze omslachtig zijn.
    - **Integratie van de Resilix-standaard:** Resilix hanteert al een eigen beoordelingsmethode, maar deze wordt momenteel niet automatisch verwerkt in de output van bestaande tools. Onderzoek hoe deze standaard direct geïntegreerd kan worden in de rapportage om handmatige aanpassingen te verminderen.
    - **Uitvoeren van een GAP-analyse:** Vergelijk de huidige werkwijze met de gewenste situatie om te identificeren waar de grootste knelpunten zitten. Deze analyse helpt bepalen welke functionaliteiten ontbreken in de huidige tools en hoe de Resilix-standaard optimaal geïntegreerd kan worden.
2. **Bepalen van vereisten en scope**
    - **Wat moet de oplossing kunnen?** Definieer de minimale functionaliteiten: automatiseren van security checks, visualisatie, rapportage, enz.
    - **Moet de oplossing bestaande tools combineren of een nieuwe oplossing zijn?** Een integratie van bestaande tools kan eenvoudiger zijn dan een compleet nieuwe tool ontwikkelen.
3. **Technologieonderzoek**
    - **Scripting en automatisering:**
        - Analyseren welke programmeertalen en automatiseringsmethodes geschikt zijn om security-audits efficiënter te maken.
        - Testen van verschillende benaderingen zoals API-integraties, command-line scripting en geautomatiseerde workflows.
    - **Security scanning tools:**
        - Evalueren van de huidige tools en testen hoe deze ingezet kunnen worden binnen de Resilix-methodologie.
        - Identificeren van beperkingen in de bestaande tooling en bepalen waar aanpassingen nodig zijn.
    - **Mogelijke integratiemethoden:**
        - Data-export vanuit bestaande tools en omzetting naar Resilix-standaard met scripts of een middleware-oplossing.
        - Directe aanpassingen in dashboards en rapportages om de Resilix-score op te nemen.
4. **Testen en itereren**
    - **Proof-of-Concept bouwen:** Begin met een script of tool die een klein deel van de audit automatiseert en breid uit.
    - **Validatie van de geïntegreerde scoremethode:** Controleer of de aangepaste output correct de Resilix-standaard reflecteert en volledig geautomatiseerd verwerkt wordt.
    - **Feedback vragen:** Test bij collega's binnen Resilix en kijk waar verbeteringen nodig zijn.

2.5. Planning

2.5.1. **Week 1:** Inzicht in huidige werkwijze

- Het proces van Resilix begrijpen: welke tools en methoden worden nu gebruikt voor de security-audits?
- Opstellen van projectplan.

2.5.2. **Week 2-3:** Onderzoek en voorbereiding

- Bepalen van vereisten en scope: wat moet de oplossing kunnen?
- Onderzoeken van mogelijke scripting- en automatiseringsmogelijkheden (API-integraties, scriptingtalen, etc.).
- Verzamelen van informatie over beschikbare security scanning tools die ingezet kunnen worden.
- Een technische vergelijking (analyse) uitvoeren van alle tools die momenteel gebruikt worden voor M365-assessments, om knelpunten in de bestaande werkwijze te identificeren.

2.5.3. **Week 4-5:** Technologieonderzoek & Proof-of-Concept

- Testen van verschillende technologieën en benaderingen (zoals API-integraties, command-line scripting, geautomatiseerde workflows).
- Eerste tests uitvoeren met geëxporteerde data en verwerken naar de Resilix-standaard.
- Proof-of-Concept (PoC) bouwen voor de geautomatiseerde rapportage en integratie van de Resilix-standaard.

2.5.4. **Week 6-7:** Evaluatie & verfijning PoC

- Evalueren van de resultaten van het PoC en feedback verzamelen.
- Verfijnen van de PoC op basis van bevindingen: optimaliseren van processen en aanpakken van eventuele technische knelpunten.

2.5.5. **Week 8-9:** Integratie en uitbreiding

- Starten met de integratie van geautomatiseerde rapportage en dashboard-aanpassingen om de Resilix-score in de output te verwerken.
- Huisstijl van Resilix verwerken.

2.5.6. **Week 10-11:** Fine-tuning & testomgeving

- Validatie van de oplossing door deze uit te rollen in een testomgeving.
- Verzamelen van feedback van Resilix-medewerkers en klantgericht testen.
- Finetunen van het systeem om ervoor te zorgen dat het voldoet aan de vereisten.

2.5.7. **Week 12-13:** Documenteren & presenteren

- Documenteren van het ontwikkelde systeem, de gebruikte technologieën, en de implementatiestappen.
- Presenteren van de eindoplossing aan de opdrachtgever (Resilix) en eventueel betrokken medewerkers.

2.6. Deliverables

Aan het einde van de stage zal ik hopelijk de volgende resultaten kunnen opleveren:

- **Documentatie van het onderzoek**: Technische vergelijking van de huidige tools die door RESILIX gebruikt worden voor M365-assesments uit te voeren.
- **Demo van Proof-of-Concept:** Demonstratie van een werkende oplossing voor geautomatiseerde rapportage. In testomgeving of die van een werkelijke klant van Resilix (geanonimiseerd en vertoond aan de hand van screenshots, wegens non-disclosure van de source-code en klantengegevens).
    - **Bewijs van meerwaarde van de oplossing (realisatiedocument):** Door middel van een ‘benchmark’ bij een security audit wordt vergeleken hoeveel mandagen/uren worden bespaard. Hierbij wordt de efficiëntie en effectiviteit van de geautomatiseerde aanpak gemeten ten opzichte van de traditionele methode.

CONTACT

Renzo Lemmens | Student
r0931792@student.thomasmore.be

VOLG ONS

www.thomasmore.be
fb.com/ThomasMoreBE
#WeAreMore

THOMAS MORE