1. Business Case

Achtergrond

Baloise Belgium nv is een verzekeringsmaatschappij die deel uitmaakt van de Zwitserse Baloise Group. Het bedrijf streeft naar duurzame samenwerkingen en optimale verzekeringsoplossingen. Publieke webapplicaties spelen een cruciale rol in de dienstverlening van Baloise, maar vormen tegelijkertijd een potentieel doelwit voor cyberaanvallen.

Probleemstelling

Momenteel ontbreekt een geautomatiseerd systeem voor het monitoren en beveiligen van publieke webapplicaties. Baloise voert al vulnerability scans uit, maar wil een extra beveiligingslaag door middel van redundantie en automatisering. Verschillende scanners leveren verschillende resultaten op, en door meerdere scanners te vergelijken, kan een beter inzicht worden verkregen in kwetsbaarheden.

Doelstelling

Het implementeren van een geautomatiseerd monitoringsysteem en het integreren van een geschikte vulnerability scanner die periodiek rapporteert over kwetsbaarheden. Dit draagt bij aan de beveiliging van publieke en interne webapplicaties en vermindert manuele inspanningen.

2. Scope

Projectomvang

Het project omvat:

- Het analyseren van de bestaande webapplicaties en hun kwetsbaarheden.
- De implementatie van een geautomatiseerde monitoringsoplossing.
- Het integreren en configureren van een geschikte vulnerability scanner.
- Het automatiseren van het scanproces met een CI/CD-pipeline in Azure DevOps.
- Documenteren van het proces en resultaten voor toekomstige optimalisatie.

Niet binnen scope

- Het volledig vervangen van bestaande securityprocessen.
- Handmatige penetratietests.

3. Werkwijze & Methodologie

Agile Werkwijze

Het project wordt uitgevoerd volgens een Agile-aanpak, waarbij iteratief gewerkt wordt en tweewekelijks sprints worden gehouden. Dit zorgt voor flexibiliteit en snelle feedbackloops.

Gebruik van Azure DevOps

- Sprint planning en backlogbeheer.
- CI/CD-integratie om de vulnerability scanner periodiek te laten draaien.
- Automatisering van rapportage voor securityteams.

4. Planning en Mijlpalen

Fase	Activiteit
Week 1	Onderzoek naar oplossingen en risico’s
Week 2 - 4	Implementatie van monitoringfunctionaliteit
Week 5 - 8	Opzetten en testen van de vulnerability scanner
Week 9 - 11	Automatiseren van scanning en integratie met Azure DevOps
Week 12 - 13	Evaluatie, documentatie en optimalisatie

5. Risicoanalyse & Mitigatie

Risico	Impact	Mitigatie
Schade aan webapplicaties door scanning	Hoog	Configuratie van veilige scaninstellingen en testen in gecontroleerde omgevingen
Overbelasting van servers	Middel	Instellen van rate limiting en tijdslimieten voor scans
Overvloed aan meldingen	Middel	Fijn afstemmen van scanparameters en prioriteren van kritieke kwetsbaarheden
Compliance en privacyrisico’s	Hoog	Toestemming vragen en scoping definiëren met securityteam

6. Succescriteria

Het project wordt als succesvol beschouwd als:

- De vulnerability scanner geautomatiseerd draait en rapporten oplevert in Azure DevOps.
- Webapplicaties gemonitord worden met minimale false positives.
- Het scanproces niet leidt tot prestatieproblemen op productieomgevingen.
- Het proces goed gedocumenteerd is voor overdracht en verdere optimalisatie.

7. Conclusie

Door dit project te realiseren, versterkt Baloise de beveiliging van zijn webapplicaties door proactief kwetsbaarheden te identificeren en te beheren. De geautomatiseerde aanpak en integratie met Azure DevOps zorgen voor een efficiënter en veiliger securitybeheer, zonder handmatige inspanningen te verhogen.