Stage IT/Dev: Automatisering van Beveiligingstesten voor Telemis Installaties

Telemis
Telemis is een bedrijf in medische apparatuur, gespecialiseerd in PACS/MACS-oplossingen, digitale pathologie en Business Intelligence voor de gezondheidszorg. De producten van Telemis helpen zorginstellingen, privé-praktijken, enzovoort, bij het efficiënt beheren van medische beeldvorming en gezondheidsgegevens. Bij Telemis heerst een hechte sfeer waar wederzijdse ondersteuning en spontane samenwerking de norm zijn.

Doelstelling van het Project
Het hoofddoel van deze stage is het ontwerpen, ontwikkelen en implementeren van een geautomatiseerd raamwerk voor beveiligingstesten. Dit raamwerk zal de beveiligingsstatus van onze webapplicaties en portalen die bij klanten (ziekenhuizen) zijn geïmplementeerd, continu beoordelen. Dit zorgt ervoor dat ze veilig zijn geconfigureerd en versterkt tegen veelvoorkomende kwetsbaarheden.

Context
Telemis levert kritieke softwareoplossingen aan de gezondheidszorg. Onze applicaties zijn geïnstalleerd in complexe IT-omgevingen binnen tal van ziekenhuizen. Het handmatig verifiëren van de beveiliging van elke unieke installatie is tijdrovend en is niet effectief op grote schaal.
Om ons beveiligingslandschap proactief te beheren, moeten we overschakelen van handmatige steekproeven naar een continu en geautomatiseerd validatieproces. De stagiair zal een oplossing bouwen die regelmatig een lijst met klant-URL's kan scannen op onjuiste beveiligingsconfiguraties en kwetsbaarheden, zoals die zijn geïdentificeerd tijdens onze interne penetratietesten.

Stage Doelstellingen (aangepast op basis van duur en vaardigheidsniveau)

- Zich vertrouwd maken met onze bestaande rapporten en documentatie over beveiligingstesten.

- Automatiseren van specifieke beveiligingscontroles. Voorbeelden zijn:
    - De geldigheid van TLS/SSL-certificaten en de sterkte van de codering verifiëren.
    - Blootgestelde administratieportalen of -diensten detecteren.
    - Controleren op informatielekken via foutpagina's, headers (bijv. serverversie) en stack-traces.
    - Zoeken naar standaard inloggegevens op bekende endpoints.
- Een kernmotor bouwen die een lijst met doel-URL's inneemt en de reeks testscripts systematisch op elk van hen uitvoert.
- Het raamwerk, de individuele testscripts en de procedure voor het uitvoeren van de scans en het interpreteren van de resultaten documenteren.
-

Wat de Stagiair uit deze Ervaring Zal Halen

- Praktische Cybersecurity Vaardigheden: Praktische ervaring opdoen in het identificeren en testen van reële beveiligingskwetsbaarheden in een bedrijfsomgeving.
- Automatisering & DevSecOps: Leren hoe beveiligingsautomatiseringstools van de grond af opgebouwd worden, een zeer gevraagde vaardigheid in het domein van DevSecOps (Development, Security, and Operations).
- Webapplicatiebeveiliging: Uw inzicht verdiepen in hoe webapplicaties worden aangevallen en, nog belangrijker, hoe ze worden beveiligd en versterkt.
- Inzicht in Zorg-IT: Waardevolle ervaring opdoen met het werken aan beveiligingsuitdagingen binnen de kritieke en streng gereguleerde sector van de gezondheidszorgtechnologie.

Profiel

- Momenteel bezig met een opleiding in Informatica, Cybersecurity, Informatietechnologie of een gerelateerd veld.
- Sterke scriptingvaardigheden, bij voorkeur in Python.
- Goed begrip van webtechnologieën en -protocollen (HTTP/HTTPS, API's, Cookies, Headers).