Verslag eerste begeleidingsgroepvergadering

9 maart 2023 hebben we een uiteenzetting van het project GAICIA gegeven. we gaven een presentatie om het project in te leiden, de doelstellingen te verklaren en onze algemene visie toe te lichten.
Ook waren er twee demonstraties voorzien om dit alles wat concreter en tastbaarder te maken. We verzamelden ook feedback over het project.

Agenda:

10.00 Inleiding: Korte inleiding en algemene visie van het project.

10.05 Doelstellingen project: De verschillende werkpakketten toegelicht. Een demonstratie van de testomgeving waarin we een fabrieksnetwerk nagebouwd hebben.

10.35 Aanvalsscenario 1: Een eerste aanvalsscenario werd uitgevoerd op onze testomgeving. Deze werd toegelicht.

10.50 ML-OT toolbox: Demonstratie van de ML-OT toolbox. De experimenten die we uitvoeren capteren we in een toolbox. Dit is een programmeerproject waarin de experimenten makkelijk gereproduceerd kunnen worden en makkelijk uitgebreid kunnen worden met nieuwe datasets.

11:15 Workshop en webinar topics: We bevraagden welke topics interessant zijn voor workshops en webinars via een digitale tool (wooclap). Zie pdf in de bijlage.

11.30 Verzamelen feedback en sturing: Feedback werd tijdens de gehele presentatie gecapteerd en hieronder verzameld.

12.00 Broodjeslunch

Feedback over de testomgeving:

- Op het netwerkniveau kan het busprotocol niet gecapteerd worden. Hierdoor kunnen aanvallers die fysieke toegang hebben tot PLC devices ongedetecteerd malicious acties uitvoeren. De vraag kwam om additionele informatie (buiten op netwerkniveau) te capteren om aanvallen met fysieke toegang ook te detecteren.
- BacNet en ethernet/IP is een protocol dat nog niet aanwezig is en graag teruggezien zou worden.

Feedback Workshops en webinars:
We stelden de vraag aan de begeleidingsgroep in welke topics er verder verdiept kan worden op een technische manier (workshops) of via een presentatie en Q&A (webinar).

- Na de demonstraties en uitleg was er interesse naar een workshop rond explainable AI toe.
  De mogelijkheid om ook context te geven aan voorspelling van een algoritme viel in de smaak bij de begeleidingsgroep aangezien er vaak sprake is van “Alarm Fatigue”. Deelnemers uit de industrie gaven mee dat per week in de grootteorde van 1000 alerts die hoogdringend zijn in de dashboard van een analyst terechtkomen. Vaak worden dan de meeste alerts genegeerd.
- Ook is er interesse naar een webinar performantie tuning van de algoritmes. Mogelijke subtopics hierbij zijn dan: wat zijn de geleerde lessen uit experimenten? Hoe schaalbaar zijn sommige algoritmes? Hoeveel False positives komen voor?

We stelden de vraag aan de begeleidingsgroep welke elementen in het project hun voornaamste interesse naar uit ging en of er nog additionele elementen aan bod moeten komen.

- Er is een groot probleem met False positives in de huidige monitorimplementaties. Dit betekent dat er vaak alerts worden gegenereerd wanneer er eigenlijk niks ernstig aan de hand is. Soms zal een technische werknemer apparaten herprogrammeren of op de infrastructuur zaken anders gaan instellen. Dit is op zich “nieuw” gedrag (= afwijken t.o.v. normale traffiek) maar niet een aanval. Hoe meer false positives of in andere woorden “vals alarm” hoe sneller analysten alert fatigue ervaren.
- Voor de integratie van de drie softwarecomponenten: log-extractie, algoritme en dashboard (we verwijzen naar de figuur op slide 17 in kader van werkpakket 4) was er interesse om voort te bouwen op software die al in de industrie bestaat. Specifiek was er interesse naar compatibiliteit van logs met bestaande tools zodat deze makkelijk met elkaar geïntegreerd kunnen worden. Hierbij werd het onderscheid gemaakt met de standaard informatie logs gegenereerd met tools zoals tshark of zeek en alert logs waarin de voorspellingen van algoritmes in terecht komen. Deze laatste types van logs kunnen we volledig zelf vormgeven. Servicenow werd als voorbeeld van software gegeven waarmee logs compatibel zouden kunnen zijn.

We stelden de vraag aan de begeleidingsgroep of iemand persoonlijk of een klant van hun zou openstaan voor een captatie van het netwerk om de mix en volume van netwerkprotocollen te capteren. Dit kan dan vergeleken worden met de testopstelling. De bedrijven stonden hiervoor open. Ook waren er contacten bij een universiteit van Singapore en een bedrijf dat ook binnen intelligente monitoring werk hadden gedaan. Deze contacten worden opgevolgd om te zien welke kennis gedeeld kan worden.

Tot slot werd er verduidelijking gevraagd wat een bedrijf concreet kan verwachten als output bij het delen van een netwerkcaptatie. Het gaat hier over een netwerkcaptatie waarin we het volume en mix van protocollen bekijken. Deze kan vergeleken worden met onze testomgeving. In de tweede jaarhelft testen we ook de schaalbaarheid van algoritmes uit. Door zo’n captatie bij een bedrijf uit te voeren kunnen we de kosten inschatten voor het maken van een intelligente monitoroplossing, nodige hardware voor data te capteren over de verschillende segmenten in het netwerk, nodige rekenkracht om algoritme op deze schaal in productie te zetten, … .

Met de input van de bedrijven gaan we aan de slag om de scope verder te verfijnen naar de nood van de industrie en de opportuniteiten voor het samenwerken met onze nieuwe contacten op te volgen.