SBIR Cyber Security

Projecttitel:	**Real-time monitoring & adaptieve cyber intelligence**
Bedrijf:	**BusinessForensics BV**
In samenwerking met:	**TNO, TU Delft, Texar Data Science, Microsoft, Rapidminer, OpenAnalytics, FuzzyLogix en Data Science Innovation.**

Probleemstelling

Vitale infrastructuren zijn in hoge mate afhankelijk van ICT, waarbij ketenuitval zelfs tot ontwrichting van de maatschappij kan leiden. De doelstelling van ons project betrof het real time detecteren en adaptief kunnen onderzoeken van onbekende bedreigingen binnen het Cyber domein.

De vraag die we ons gesteld hebben, luidde: hoe kunnen we, vertrekkende vanuit het huidige product van BusinessForensics voor de financiële industrie, de cyber analist behoeden voor een overkill aan waarschuwingen, hoe kunnen we zijn beslissingen ondersteunen met waardevolle informatie en hoe kunnen we de kennis van deze specialist betrekken bij de preventie en detectie van potentiele bedreigingen?

Projectsamenvatting

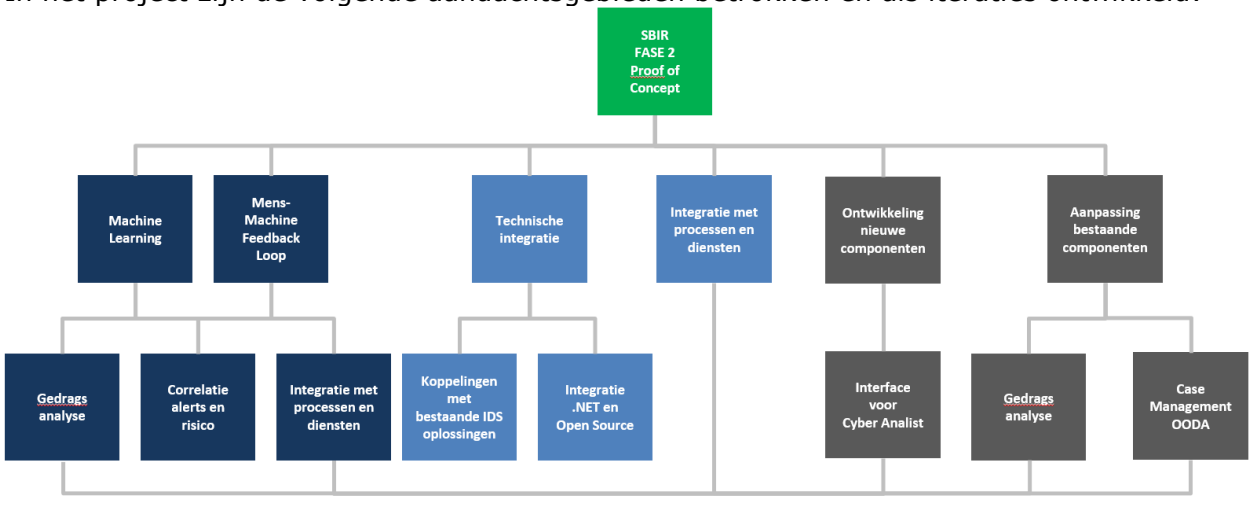
BusinessForensics heeft een aantal innovaties gerealiseerd die ertoe hebben geleid dat haar bestaande platform breder kan worden toegepast: naast financial crime prevention ook voor cyber security. Het concrete resultaat van het project is een werkende oplossing (software product) die in real time kritische infrastructuren op holistische wijze kan monitoren en hieruit mogelijke bedreigingen kan onderkennen op basis van een combinatie van detectiemechanismen, en een zorgvuldig opgezette interactie tussen mens en machine om de bedreigingen te onderzoeken en te (her)classificeren. De interactie van gebruikers met het systeem levert metadata op die door hetzelfde systeem kan worden onderzocht op afwijkende patronen.

Centrale gedachte is dat de analisten en operators zowel worden geëxploiteerd als ontlast. Om te kunnen bepalen of de technologie de kwaliteit en werkdruk ten goede komt vindt er een continue evaluatie plaats van zowel de gedetecteerde bedreigingen als de activiteiten van de cyber operators. Tot slot zijn de veelheid en diepgang van profileringsmogelijkheden van ons huidige systeem uitgebreid met vooral in de academische wereld beschikbare algoritmen. Onderwijl de privacy waarborgend van zowel gebruikers als van individuen die onderworpen zijn aan monitoring routines.

Het doel van deze oplossing is een systeem dat daadwerkelijk de informatiestress voor operators reduceert, de kwaliteit van detectie verbetert en de reactiesnelheid verhoogt.

In het project betrokken aandachtsgebieden

In het project zijn de volgende aandachtsgebieden betrokken en als iteraties ontwikkeld:



Deze aanbesteding volgt de Small Business Innovation Research (SBIR) methode. SBIR benut en ontwikkelt kennis, creativiteit en innovatiekracht van het bedrijfsleven voor innovaties die een passend antwoord geven op maatschappelijke opgaven.

SBIR Cyber Security

Projecttitel:	**Real-time monitoring & adaptieve cyber intelligence**
Bedrijf:	**BusinessForensics BV**
In samenwerking met:	**TNO, TU Delft, Texar Data Science, Microsoft, Rapidminer, OpenAnalytics, FuzzyLogix en Data Science Innovation.**

Deze aandachtsgebieden zijn aangepast ten opzichte van het oorspronkelijke projectplan. De belangrijkste verschillen zijn als volgt te verklaren:

- De ontwikkelingen aan de feedback loop hebben een duidelijkere positie gekregen en zijn daarom als separaat aandachtsgebied gedefinieerd
- Er is een duidelijker onderscheid gemaakt tussen de aanpassingen in processen & diensten binnen de applicatie en de aanpassingen die buiten de applicatie moeten worden geïmplementeerd (dus in de operationele organisatie of werkzaamheden buiten het systeem).
- De aanpassingen aan de bestaande componenten ten behoeve van de cyber analist blijken dermate vergaand te zijn dat er een aparte client omgeving is ontwikkeld waarbinnen de interface volledig op maat kan worden geconfigureerd. Naast de aanpassingen aan de bestaande componenten is er dus een nieuwe component aan de product suite van BusinessForensics toegevoegd.

Belangrijkste project resultaten

Bij het ontwerpen van de doelarchitectuur t.b.v. de technische integratie is nadrukkelijk rekening gehouden met de afnemerswens voor een onderhoudsarm platform. Als gevolg daarvan is aanvullend onderzoek gedaan naar alternatieve oplossingen en zijn extra partners bij het project betrokken. Uiteindelijk is een doelarchitectuur ontworpen en gerealiseerd die onderhoudsarm, flexibel en innovatief is.

Gezien de specifieke materiedeskundigheid die is verbonden aan het toepassen van individuele ML algoritmen hebben we besloten ook eigen expertise te ontwikkelen. Dit laatste heeft geleid tot aanvullende arbeidsplaatsen binnen BusinessForensics.

Tevens zijn er contacten gelegd met een juridisch advieskantoor om de organisatorische positionering van het systeem t.a.v. privacy te borgen. Dit heeft er toe geleidt dat het autorisatiemodel zoals dat in de applicatie wordt gehanteerd (functionele en data rechten) volledig is aangepast en is voorbereid op de nieuwe EU privacy regelgeving.

Prototype en andere deliverables

Het concrete resultaat van het project is een werkend prototype dat in real time de cyber security aspecten van kritische infrastructuren op holistische wijze kan monitoren. Hieruit kunnen mogelijke bedreigingen worden onderkend op basis van een combinatie van detectiemechanismen. Tevens vindt een zorgvuldig opgezette interactie tussen mens en machine plaats om de bedreigingen te onderzoeken en te (her)classificeren. Het doel van deze oplossing is een systeem dat daadwerkelijk de informatiestress voor operators reduceert, de kwaliteit van detectie verbetert en de effectiviteit van de opvolging verhoogt.

De resultaten zijn door ons op basis van het prototype gemeten. Dit betreft zowel de detectieresultaten als de usability. Als dataset hebben we een logbestand van een intrusion detectie systeem gebruikt dat alle verdachte handeling binnen een uitgebreid honeypot netwerk heeft vastgelegd.

Een aantal deelresultaten zijn reeds in gebruik genomen bij bestaande klanten van BusinessForensics, waaronder de interactie tussen mens en machine, de binnen het project nieuw ontwikkelde client interface en de aanpassingen in de work flow configuratie voor de case management module. Voor het einde van dit kalenderjaar wordt ook het nieuwe autorisatiemodel ten behoeve van de privacybescherming in gebruik genomen.