

Klik op de parels voor een beschrijving.

Definitie:

Een parel is een regionaal of lokaal initiatief binnen de politie, waarin de aanpak of preventie van online criminaliteit tot stand komt. Een parel is op regionaal of lokaal niveau ontstaan, en is (nog) niet geïmplementeerd in alle eenheden. De parel heeft betrekking op online criminaliteit (brede definitie) en op het proces bij de politie, van aangifte tot opsporing, of de bredere inzet van de politie in de preventie of bestrijding van online criminaliteit. Er wordt van een parel gesproken indien het een niet-incidenteel initiatief betreft. Ten slotte worden alleen initiatieven die nog lopen (actief zijn) aangemerkt als parel, zodat er een actueel overzicht ontstaat van de ontwikkelingen binnen de politieorganisatie.

minder



EENHEDEN MET PARELS

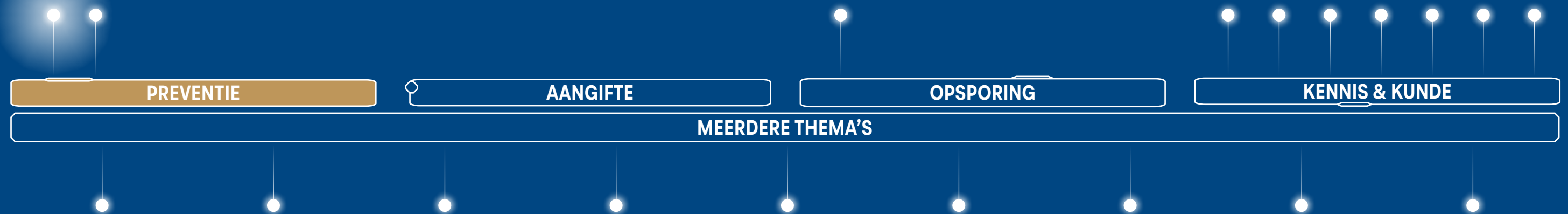
De politie-eenheden Noord-Holland en Oost-Brabant zijn niet opgenomen in dit overzicht, omdat er geen (geschikte) parels zijn aangedragen.

INTRODUCTIE

Online criminaliteit is onderdeel geworden van het dagelijkse werkaanbod van politiemedewerkers. Binnen de regionale politie-eenheden zijn allerlei initiatieven ontstaan op het gebied van de aanpak van online criminaliteit. Op dit moment ontbreekt echter zicht op al deze regionale en lokale initiatieven. In het onderzoek 'Parels bij de lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit' staan deze initiatieven daarom centraal.

Het rapport biedt een overzicht van veelbelovende regionale en lokale initiatieven op het gebied van online criminaliteit, zodat eenheden van elkaar kunnen leren, zodat initiatieven eventueel op grotere schaal kunnen worden ingezet, maar ook om inzicht te krijgen in eventuele knelpunten. De 19 geïdentificeerde parels worden in het rapport uitgebreid beschreven, ingedeeld aan de hand van verschillende fasen van het politiewerk: preventie, opsporing, kennis en kunde of meerdere fasen van het politiewerk.

Wil je snel oriënteren en kijken welke parels er zijn? Navigeer dan door deze infographic door te klikken op de parels in het schema hierboven.



BL@CKMAIL

Mobiele escaperoom bus: middel om met jongeren het gesprek aan te gaan over cybercrime en sextortion.

De escaperoom is met 3-4 personen binnen een kwartier uit te spelen en bestaat uit 4 spellen waarbij 4 codes moeten worden gevonden. Door slim te overleggen en goed te zoeken komen deelnemers in de bus tot de oplossing. Om het spel heen is een casus bedacht van een dame die wordt afgeperst met naaktbeelden. Het idee is dat als de deelnemers de 4 codes binnen de tijd vinden ze ervoor zorgen dat de foto's niet worden geüpload op internet.

Achteraf is er een briefing waarin wijkagenten, jeugdagenten of jongerenwerkers als begeleiders het gesprek aangaan met jongeren over dit onderwerp.

DOEL

Voorkomen van sextortion slachtoffers door het voeren van een preventiecampagne.

DOELGROEP

Jongeren van 14 tot 24 jaar oud

NIVEAU / TOEPASBAARHEID

Bus is van de eenheid Amsterdam, maar ook voor andere eenheden beschikbaar. Er wordt gekeken of de coördinatie onder het landelijke Mobiel Media Lab kan komen te vallen.



AMSTERDAM

Andere parels in Amsterdam:

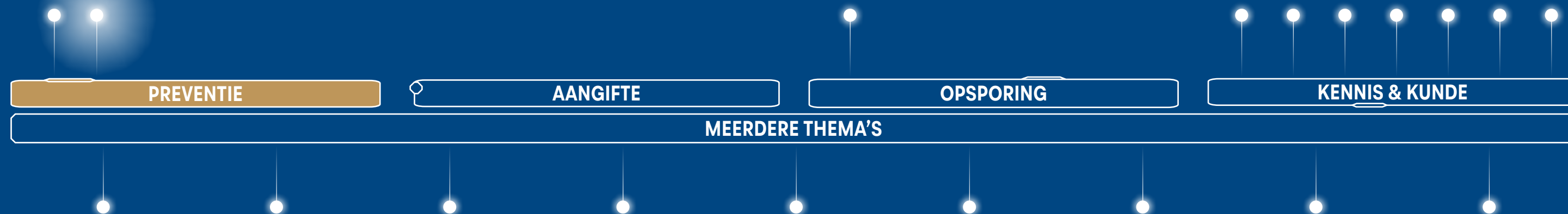
- [Cyber Support](#)
- [Workshop Cybercrime](#)
- [Cyberspecials](#)

SAMENWERKING

- Intern: Wijk- en jeugdagenten, communicatiemedewerker en de afdeling EPJO
- Extern: Openbaar Ministerie (OM), gemeenten, jongerenwerkers, scholen, Helpwanted en Level.

IMPLEMENTATIE

Wegens corona kon de bus in de proeffase niet op evenementen en festivals ingezet worden. Voor inzet op scholen was de 'capaciteit' (3-4 jongeren) aan de lage kant. Gekeken wordt naar inzet bij jongerenorganisaties.



RISK FACTORY

De Risk Factory is een initiatief van de veiligheidsregio Limburg-Noord, waarbij senioren en kinderen risico's beleven op het gebied van gezondheid en veiligheid en leren hoe in deze situaties te handelen.

Vanuit de politie is men een samenwerking aangegaan (in de vorm van een convenant), waarbij de politie meedenkt en helpt bij het ontwikkelen van scenario's.

Op het gebied van online weerbaarheid zijn twee scenario's ontwikkeld, die elk ongeveer 20-25 minuten duren:

1. Online oplichting /betaalverzoekfraude
2. Sexting

De ontwikkeling van online criminaliteit gaat snel. De politie monitort de actualiteit, zodat de (ontwikkeling van) scenario's hier goed op aansluit.

DOEL

Bijdragen aan preventie van cybercriminaliteit door bewustwording van risico's op het internet.

DOELGROEP

Ouderen (online oplichting) en kinderen uit groep 8 (sexting)

NIVEAU / TOEPASBAARHEID

Veiligheidsregio Limburg-Noord. Inmiddels zijn er ook overeenkomsten met seniorenorganisaties gesloten die actief zijn in heel Limburg.



LIMBURG

Andere parels in Limburg:

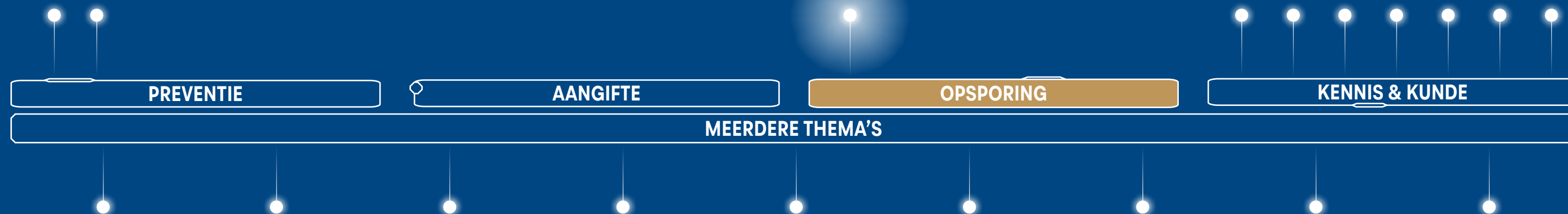
- [Kor3nwolf](#)
- [Dagelijkse Cyberquery](#)

SAMENWERKING

- Intern: Cybercrimeteam, analisten, wijkagenten, afd. zeden, afd. communicatie en leidinggevendenden
- Extern: Veiligheidsregio, vrijwilligers van de Risk Factory, universiteiten, IT-bedrijf, ouderenverenigingen, scholen, crisisbeheersing, provincie Limburg e.a.

IMPLEMENTATIE

N.a.v. bijvoorbeeld veranderende aangiftecijfers en/of nieuwe delicten kunnen nieuwe scenario's worden ontwikkeld en nieuwe doelgroepen worden bereikt.



DISTRICT CYBERTEAMS

Om cybercrime zaken te draaien zijn in Zeeland-West-Brabant cyberteams opgericht van minimaal 5FTE binnen de districtsrecherche.

De teams dragen ook bij aan de kennis en kunde, informatiepositie en olievlekwerking binnen het district rond het thema.

Er wordt gekeken of het thema breder geïntegreerd kan worden binnen de districtsrecherche. Financieel economische criminaliteit raakt bijvoorbeeld cybercriminaliteit en andersom.

DOEL

Reguliere opsporingsonderzoeken op cybercriminaliteit draaien, districtelijke feeling met het thema vergroten en een operationeel netwerk creëren voor samenwerking in de aanpak van cybercriminaliteit.

NIVEAU / TOEPASBAARHEID

De teams werken op districtelijk niveau. Omdat er meerdere teams zijn is er een dekking op eenheidsniveau.



ZEELAND-WEST-BRABANT

Andere parels in Zeeland-West-Brabant:

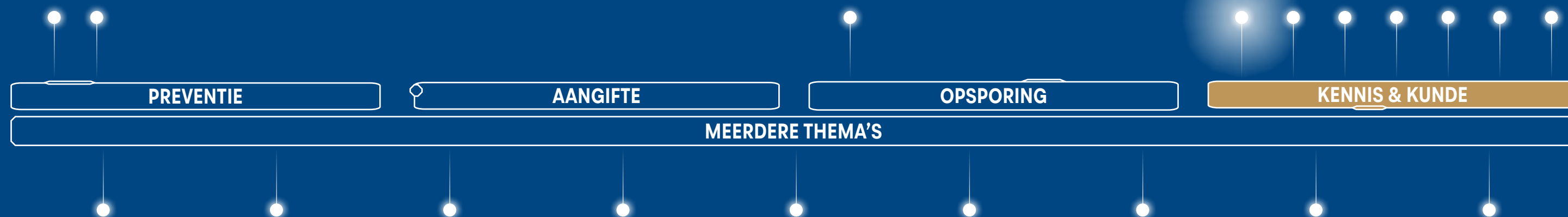
- [Cyber HQ](#)
- [Digikamers](#)
- [Digitaal weerbaar Breda](#)

SAMENWERKING

- Intern: 7-10 medewerkers. Afhankelijk van expertise die aanvullend nodig is in een onderzoek aanvulling met collega's van TDO of de financiële recherche. Daarnaast zijn liaisons vanuit het [Cyber HQ](#) team verbonden.
- Extern: overleg met ECTF, vermogenstraceerders van OM en publiek-private samenwerking

IMPLEMENTATIE

Het concept kan makkelijk worden toegepast in andere eenheden. Geschikt personeel vinden kan een uitdaging zijn: het thema wordt als ingewikkeld gezien.



CYBERCRISISOEFENING MET BT

De 'cybercrisisoefening met basisteam' is een sessie van 1,5-2uur waarbij een cybercrisisoefening de aanleiding vormt binnen om binnen basisteams het gesprek aan te gaan over cybercriminaliteit.

Tijdens de sessie geeft het lectoraat cybersafety van de Hogeschool Leeuwarden een presentatie over hoe de digitale en fysieke wereld elkaar raken. Vervolgens wordt een cybercrisisoefening uitgevoerd (een fictieve casus waarbij het lokale ziekenhuis door ransomware niet meer in patiëntendossiers kan). De oefening wordt nabesproken, er wordt gekeken of de medewerkers bekend zijn met de partners in de wijk op het gebied van cyber, ze maken kennis met het digitaal platform (het eerste aanspreekpunt voor een basisteam als kennis ontbreekt) en krijgen uitleg van een ziekenhuis over behoeften bij een cyberdrisis.

DOEL

Bewustwording op het gebied van cybercrime: laagdrempelige kennis-making met het thema en de rol van basisteams.

DOELGROEP

Basisteams binnen de politie

NIVEAU / TOEPASBAARHEID

Bewust is gekozen voor het basisteam, omdat zij een belangrijke rol hebben in acute ondersteuning tijdens of na een incident.



NOORD-NEDERLAND

Andere parels in Noord-Nederland:

- [Digitale vaardigheden Friesland](#)

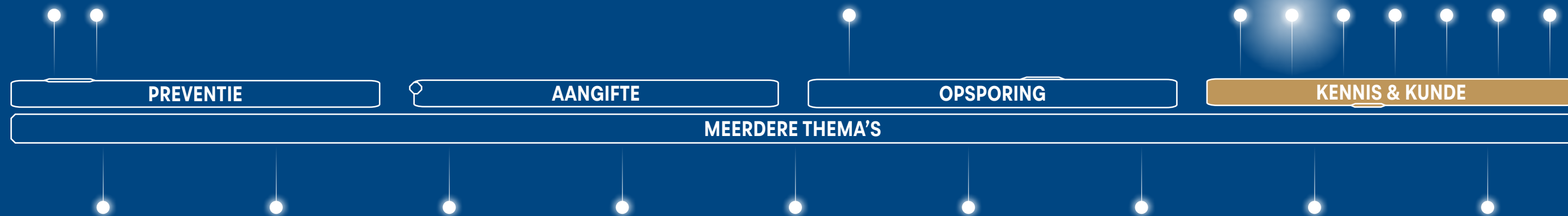
SAMENWERKING

- Intern: Basisteams, Digitaal platform
- Extern: Partners uit de wijk, Hogeschool Leeuwarden, studenten van de Hanze Hogeschool.

IMPLEMENTATIE

De sessie is in basisteams in Groningen gehouden en geëvalueerd.

Het is belangrijk ook goed aan te sluiten bij de behoeften van de basisteams zelf (hierop is de sessie aangepast). Ook is het goed het onderwerp terug te laten komen.



DIGITALE VAARDIGHEDEN FRIESLAND

Dit betreft een reeks initiatieven van het digitaal platform om de digitale vaardigheden van politiemedewerkers in het district te verbeteren.

Omdat binnen het district een grote diversiteit aan deskundigen werkt, zijn er specifieke activiteiten georganiseerd per doelgroep, zodat de inhoud optimaal aansluit bij wat medewerkers in de praktijk werkelijk tegenkomen.

DOEL

Digitale vaardigheden verbeteren van medewerkers binnen district Friesland: (1) begripkennis over definities en modus operandi van cyberdelicten, (2) digitale sporen veiligstellen, (3) aanhoudingen verrichten zonder dat digitale sporen verloren gaan, (4) juridische kennis bijbrengen op het gebied van cybercrime.

DOELGROEP

- intake en servicemedewerkers
- senior tactische opsporingsmedewerkers die aangiftes veredelen
- leidinggevers (operationeel experts)
- Basispolitiezorg
- Recherches

NIVEAU / TOEPASBAARHEID

Het project vond plaats door de hele eenheid bij verschillende afdelingen en lagen van het district Friesland. Ook is de escaperoom truck een keer ingezet op een landelijk evenement.



NOORD-NEDERLAND

Andere parels in Noord-Nederland:

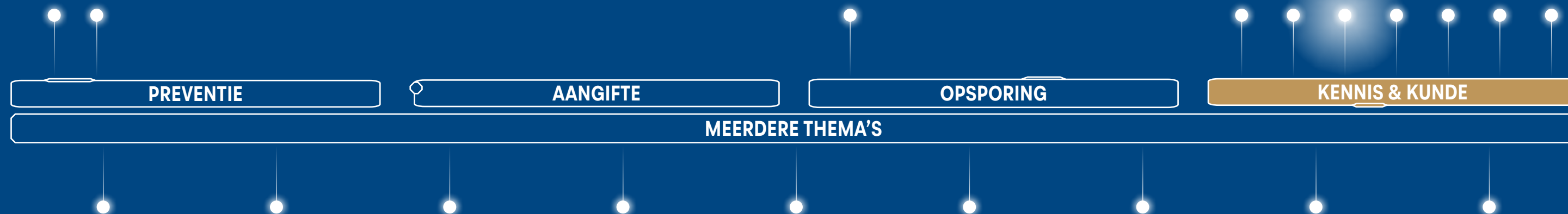
- [Cybercrisisoefening met BT](#)

SAMENWERKING

- Intern: Specialisten van het digitaal platform, de stuurlijn (leidinggevers)
- Extern: OM, studenten NHL Stenden.

IMPLEMENTATIE

Deelnemers waren enthousiast en maken reclame voor de initiatieven. Het spelelement in sommige activiteiten maakt dat het onderwerp laagdrempelig wordt aangeboden. Het project is goed toepasbaar in andere eenheden. Het zou goed zijn ook binnen de basisopleiding van de politie meer aandacht te geven aan digitale kansen en vaardigheden.



IT-COACHES DISTRICT TWENTE

Binnen district Twente zijn twee IT-coaches van buiten de organisatie aangesteld. Zij zetten verschillende middelen in die aansluiten bij de leervraag van politiemedewerkers op het gebied van digitalisering. Ook kijken zij naar kansen om de digitale wereld in te vlechten in het dagelijks politiewerk.

De coaches ontwikkelen de leermiddelen samen met een team binnen de politie (en evt. externe partners). Denk aan een workshop, 1 op 1 begeleiding en online tools. Op dit moment zijn ze bezig met een bewustwordingspilot met een VR-bril. Collega's worden door een IT-coach in een VR-omgeving geplaatst en krijgen hier klassieke of digitale opsporingsmogelijkheden (sporen) 'aangeboden' die ze moeten leren herkennen. Een ander voorbeeld is de bewustwordingsprikkel die de IT-coaches geven door een dagelijkse rapportages te verrijken met digitale aspecten.

DOEL

Het op gang brengen van een leerbeweging op het gebied van digitalisering.

DOELGROEP

Politiemensen in de basisteams en de districtsrecherche.

NIVEAU / TOEPASBAARHEID

Er is bewust gekozen voor het districtsniveau: om een groot bereik te creëren zonder dat de IT-coaches onvoldoende zichtbaar zijn (wat wellicht op eenheidsniveau zou zijn)



OOST-NEDERLAND

Andere parels in Oost-Nederland:

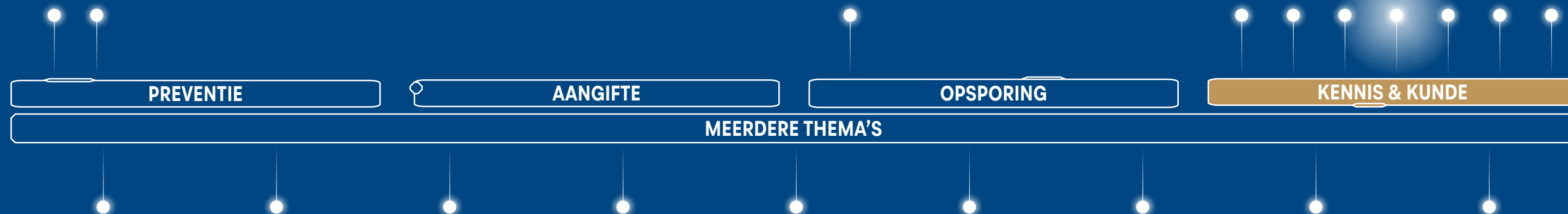
- Digitaal flexteam IJsselland
- Project Vriend in Nood-fraude

SAMENWERKING

- Intern: Basisteams, districts-recherche, regionale cybercrimeteam, TDO (Team Digitale Opsporing)
- Extern: Hogeschool Windesheim, NHL Stenden.

IMPLEMENTATIE

De ontwikkelfasen volgen elkaar op als beoogd, na 1,5 jaar vindt een meetmoment plaats. Het concept is goed toepasbaar in andere districten en eenheden. Communicatie over de IT-coaches is van belang om het project goed te laten landen.



DIGITAAL FLEXTTEAM IJSSELLAND

Er is een team opgericht van politiemedewerkers die het district digitaal vaardiger dienen te maken door verschillende projecten en activiteiten uit te voeren. Het Digitaal Flexteam bestaat op dit moment uit 5,6 FTE (wijkagenten, medewerkers van intake en service en personen met achtergrond in de recherche).

Ze richten zich op vier pijlers: (1) jeugd- en wijkagenten van basisteams, (2) opsporing, (3) intake en service en (4) sociale media en webcare. Per pijler worden verschillende projecten opgezet en activiteiten uitgevoerd. Een voorbeeld is het project 'Digitaal bewust' waarin collega's o.a. elke maand drie prikkels krijgen rond het thema. Bijv. het ophangen van een QR-code waarmee je in een virtuele doorzoeking komt met digital devices, een quiz en het verspreiden van malafide QR-codes.

DOEL

Het creëren van een digitaal vaardiger district.

DOELGROEP

Mensen binnen de politieorganisatie: basisteam(recherche) en andere teams als TDO. Maar ook ouderen en jongeren (preventie).

NIVEAU / TOEPASBAARHEID

Het Digitaal Flexteam richt zich vooral op de basisteams binnen het district en het onderwerp gedigitaliseerde criminaliteit.



OOST-NEDERLAND

Andere parels in Oost-Nederland:

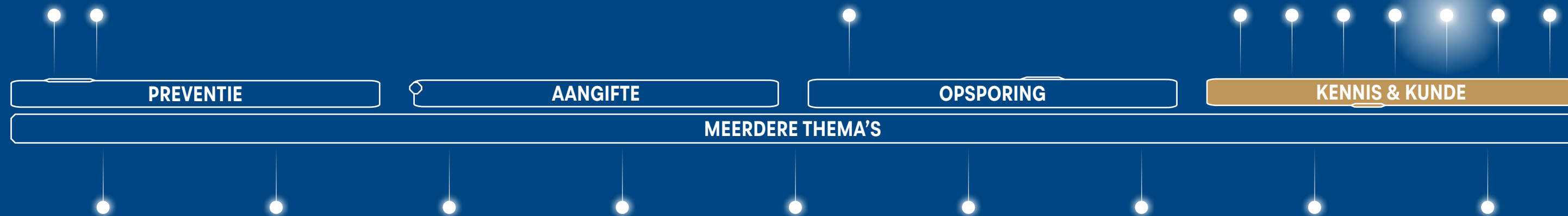
- [IT-coaches district Twente](#)
- [Project Vriend in Nood-fraude](#)

SAMENWERKING

- Intern: Intake en service, team digitale opsporing, regionale cybercrimeteam, expertisecentrum digitale opsporing, project intensivering aanpak cybercrime, district Twente en portefeuillehouder GGP.
- Extern: Scholen, gemeentes, jongerenwerk.

IMPLEMENTATIE

Het blijkt lastig teamleden vast te houden, mogelijk omdat het flexteam geen vaste contracten kan bieden. Mensen die opgeleid zijn in het team en goed functioneren worden naar andere teams overgeplaatst.



CYBER SUPPORT TEAM

Het cyber support team bestaat uit politiemedewerkers van het regionale cybercrimeteam (TDO) die een dag per week politiemedewerkers uit de districten ondersteunen op het gebied van cybercrime. De leden van het cyber support team hebben ervaring op het gebied van cybercrime doordat zij een IT-achtergrond hebben of al geruime tijd meedraaien in cybercrime opsporingsonderzoeken.

De leden zijn een aanspreekpunt voor de districten en organiseren activiteiten (op eigen initiatief) zoals een vragenuur, presentatie en/of ondersteuning bij opsporingsonderzoeken. Omdat ieder district in een andere ontwikkelingsfase zit op dit thema, ziet de ondersteuning er ook in ieder district anders uit.

DOEL

Een structuur die voorbereid is op de criminaliteit van de toekomst: cyber- en gedigitaliseerde criminaliteit.

DOELGROEP

Politiemedewerkers in de opsporing. In het kader van preventie ook basisteamcollega's, wijk- en jeugdagenten, operationele collega's.

NIVEAU / TOEPASBAARHEID

District wordt vanuit regio ondersteund richting zelfredzaamheid.



AMSTERDAM

Andere parels in Amsterdam:

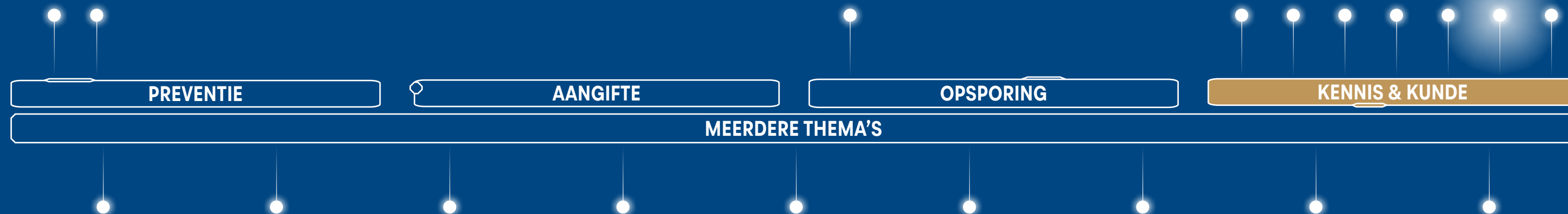
- [Bl@ckmail](#)
- [Workshop Cybercrime](#)
- [Cyberspecials](#)

SAMENWERKING

- Intern:
Het team wordt bemand door 5 leden van het regionale cybercrime-team een teamleider en tactisch coördinator. Zij werken samen met politiemedewerkers uit de district- en basisteams.

IMPLEMENTATIE

Het concept is afhankelijk van de behoeften goed toepasbaar binnen andere eenheden. Omdat veel regionale cybercrimeteams nog niet op volle sterkte draaien, is het de vraag of er capaciteit vrijgespeeld kan worden. Het bewaken van grenzen is ook belangrijk: ondersteunen is niet meedraaien.



WORKSHOP CYBERCRIME

De workshop is een kennismaking met cybercrime, waarin mensen cybercrime kunnen herkennen en de eerste stappen kunnen maken in het opsporingsproces. Veel collega's hebben nog onvoldoende kennis en kunde als het gaat om cybercrime. Er is behoefte aan praktijkervaring (learning on the job). Daarom is een workshop ontwikkeld op basis van 'serious gaming' met als casus sextortion. De workshop duurt ongeveer een dag. Elementen die in de workshop terugkomen zijn internetrechercheren, het opnemen van een goede aangifte en sporen veilig stellen.

De workshop bestaat uit een trainingsdeel, escape room en presentatie. Om zicht te krijgen op reeds aanwezige kennis en ontbrekende kennis, wordt voorkennis bevraagd, zodat de inhoud hierop kan worden afgestemd.

DOEL

Collega's handvatten bieden om cybercrime onderzoeken op te pakken en bewuster te maken van digitale (on)mogelijkheden.

DOELGROEP

Alle politiemedewerkers binnen de eenheid Amsterdam. Om beter aan te sluiten op de praktijk wordt deze opgedeeld in specifieke groepen.

NIVEAU / TOEPASBAARHEID

De workshop heeft deelnemers van alle niveaus en functies.



AMSTERDAM

Andere parels in Amsterdam:

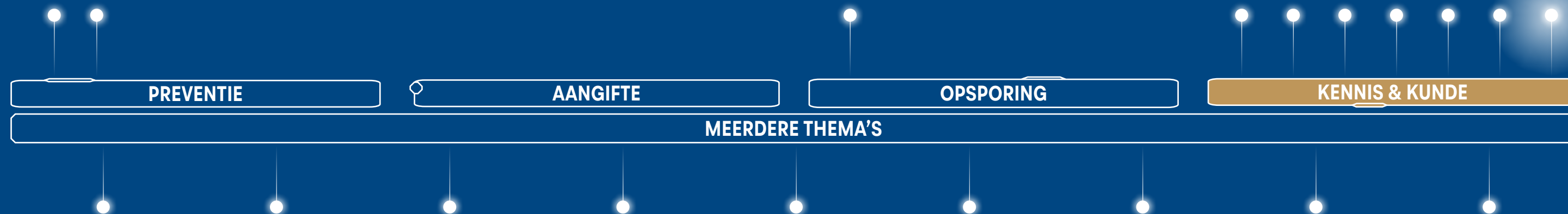
- [Bl@ckmail](#)
- [Cyber support team](#)
- [Cyberspecials](#)

SAMENWERKING

- Een vaste groep van 5-6 mensen uit de Opsporingsacademie.
- Een flexibele schil van ongeveer 8 docenten.
- 2 cybervrijwilligers die enkele keren het OSINT-deel van de workshop geven.

IMPLEMENTATIE

De escaperoom is goed toepasbaar in andere eenheden en tevens aan te passen aan andere doelgroepen (bijv. gemeente, OM). De escaperoom is tussentijds aangepast omdat deze te lastig bleek. Veel mensen wilden nog deelnemen aan de workshop: vaak organiseren zolang er animo is dus!



KOR3NWOLF

Kor3nwolf is een fictieve casus, opgebouwd op een CTF-platform. Dat is een omgeving waarin stapsgewijs, door het volbrengen van deeltaken, kennis en vaardigheden worden opgedaan.

De casus is bedoeld om collega's binnen de politieorganisatie digitaal bewust te maken. Tijdens de casus komt een melding binnen van een bedrijf dat digitaal wordt afgeperst en bitcoins moet betalen.

Spelenderwijs worden de deelnemers in groepen door de casus heen geholpen. Ze moeten bitcoin adressen opzoeken, open bronnen onderzoek verrichten en een PV van verdenkingen bijhouden. Andere onderwerpen waar men over leert zijn digitale sporen, inbeslagname van een telefoon en het indienen van vorderingen bij bijv. tech-bedrijven.

DOEL

Collega's op een laag-drempelige manier bekend maken met de digitale mogelijkheden binnen hun werk.

DOELGROEP

Politiemedewerkers binnen de opsporing. Voor andere doelgroepen kan de casus iets worden aangepast.

NIVEAU / TOEPASBAARHEID

De casus is gespeeld op het niveau van basisteams, districtrecherches en regionale rechterchies.



LIMBURG

Andere parels in Limburg:

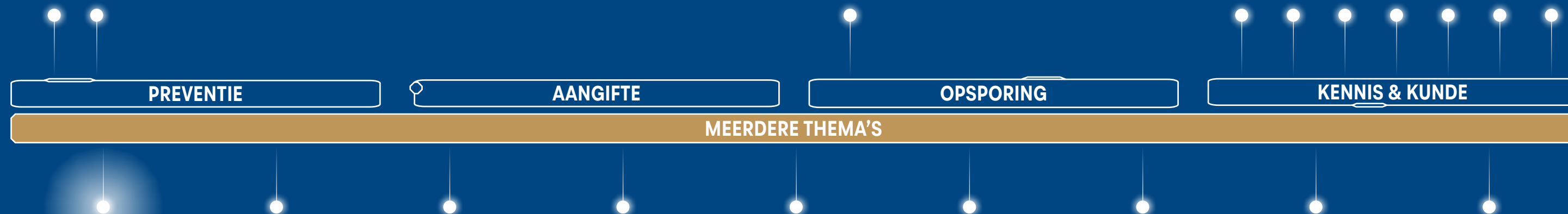
- [Risk Factory](#)
- [Dagelijkse Cyberquery](#)

SAMENWERKING

Voor de ontwikkeling van de casus is samengewerkt met diverse afdelingen binnen de politie-eenheid Limburg: o.a. het IBT-centrum, TDO, cybercrimeteam en innovatielab.

IMPLEMENTATIE

De casus kan (door bestanden over te dragen en uitleg te geven over de implementatie) rechtstreeks toegepast worden in andere eenheden. Wel zitten er enkele lokale elementen in verwerkt. Voor begeleiding van de casus moet capaciteit vrijgemaakt worden. En er is een technisch onderlegde collega nodig die de CTF op een server kan zetten en beveiligen.



PROJECT VRIEND IN NOOD-FRAUDE (VIN-fraude)

Bij VIN-fraude stuurt een fraudeur berichten naar een slachtoffer waarin hij/zij zichzelf voordoet als een bekende met het verzoek geld over te maken.

Dit project bestaat uit een centraal ingerichte werkwijze, waarin aangiften van VIN-fraude worden verrijkt met opsporingsindicaties, zodat basisteams de opsporingsonderzoeken verder kunnen afhandelen.

Er is o.a. een online aangiftesysteem ingericht, waar met behulp van automatisering opsporingsindicaties uit worden gefilterd. Ook is gebouwd aan een samenwerkingsstructuur met banken en telecomproviders.

DOEL

VIN-fraude strafrechtelijk aanpakken, meer inzicht krijgen in het fenomeen, barrières opwerpen en structuren hergebruiken.

DOELGROEP

Politiemensen in basisteams die relatief eenvoudige VIN-fraude zaken moeten oppakken en districtsrecherche voor grotere onderzoeken.

NIVEAU / TOEPASBAARHEID

Basisteam (zaak)
Regio (initiatief)
Landelijk (verdeling)



OOST-NEDERLAND

Andere parels in Oost-Nederland:

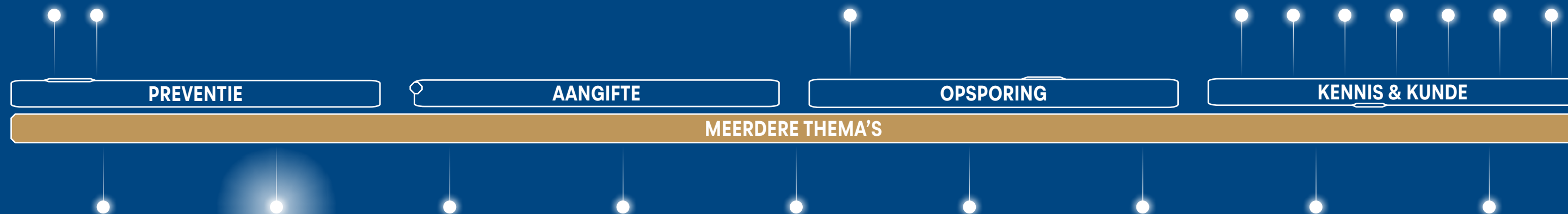
- [IT-coaches district Twente](#)
- [Digitaal flexteam IJsselland](#)

SAMENWERKING

- Intern: regionale cybercrime-team, districten en basisteams.
- Extern: Openbaar Ministerie, banken (en telecombedrijven).

IMPLEMENTATIE

Wegens juridische beperkingen moest men stoppen met bulk-vorderingen en -gegevens aanvragen bij banken en telecombedrijven. Dit omdat men uitkwam bij geldzels, waarvoor dit middel te zwaar is. Wel is het kennisdoel behaald en zijn structuren hergebruikt (er is ervaring opgedaan met automatisering en bulken).



DIGITAAL DISTRICT

Het Digitaal District wordt omschreven als de motor van de aanpak van cybercrime en gedigitaliseerde criminaliteit in de eenheid Midden-Nederland.

Enerzijds is het digitaal district een operationeel centrum waar onderzoeken gedraaid worden, anderzijds zit er een projectgroep om de beweging in de districten en basisteams aan te jagen. Hiervoor worden kennissessies georganiseerd, zijn inloopspreekuren gepland waar mensen met hun casus terecht kunnen en wordt een opleidingsaanbod gecreëerd rondom het thema. Ook worden een aantal recherchekundigen van de DRR voor twee jaar in het Digitaal District geplaatst, zodat zij digitale kennis meenemen in de reguliere opsporing voordat zij terug worden geplaatst in de DRR.

Het Digitaal District is een omgeving waar nieuwe initiatieven worden ontwikkeld.

DOEL

Aanjagen van vernieuwing op het gebied van gedigitaliseerde criminaliteit en cybercrime.

DOELGROEP

Hele eenheid met alle lagen en functies.



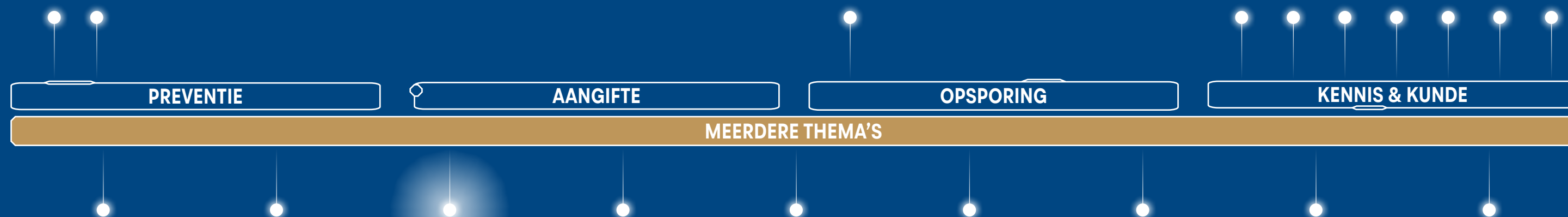
MIDDEN-NEDERLAND

SAMENWERKING

- Ca. 50 medewerkers (voormalig regionaal cybercrimeteam en een projectteam).
- Extern consultancy bureau is betrokken bij de vormgeving en evaluatie.
- Samenwerking vindt plaats met medewerkers uit basisteams en districten.

IMPLEMENTATIE

Er is een plek gecreëerd met meer mogelijkheden om initiatieven te starten op het thema cybercrime en digitalisering. Door structurele onderbezetting in de eenheid is het lastiger een nieuw thema te adresseren.



CYBERSPECIALS

In dit project worden gespecialiseerde politie cybervrijwilligers (Cyber Specials) ingezet om ondersteuning te bieden binnen de eenheid op het thema cybercrime. Er zijn ca. 30 Cyber Specials in de eenheid Amsterdam. De naam 'vrijwilliger' wordt bewust gemeden, omdat binnen de politie bij het woord 'vrijwilliger' snel wordt gedacht dat ze onvoldoende gekwalificeerd zijn. Vrijwilligers komen van buiten de politieorganisatie, dienen te beschikken over een IT-achtergrond en/of hebben affiniteit met cyber en willen de politie verder helpen.

De achtergrond van de vrijwilligers is erg divers. Ze werken 2-12 uur per week en worden op alle paden van de cybercrime strategie ingezet. Denk aan het vergroten van kennis en kunde (lesgeven, doceren) en het vergroten van bewustwording.

DOEL

Door inzet van cyber-vrijwilligers sneller vooruitgang boeken in het versterken van de aanpak.

NIVEAU / TOEPASBAARHEID

Er is binnen de politie inmiddels een landelijke ambitie om het op te zetten.



AMSTERDAM

Andere parels in Amsterdam:

- [Bl@ckmail](#)
- [Cyber support team](#)
- [Workshop cybercrime](#)

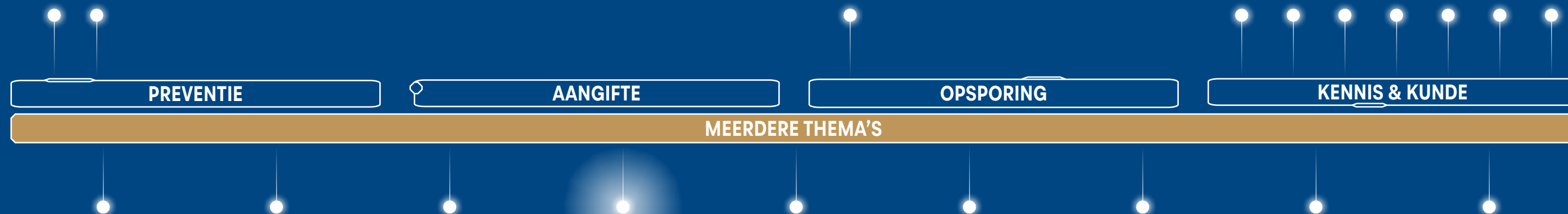
SAMENWERKING

Er zijn vijf stakeholders:

- (kandidaat) cyber-vrijwilligers
- Team Coördinatie Politievrijwilligers (TCP)
- De inlener
- De matchmaker, recruiter of coördinator
- Landelijk Programma

IMPLEMENTATIE

Verder opschalen is goed mogelijk. Belangrijke succesfactoren zijn (1) het hebben van een ervaren goed draaiend TCP (2) voor de komende 4-5 jaar een vrijgemaakte coördinator om het van wal te krijgen.



CYBERDRIEHOEK

De cyberdriehoek bestaat uit structurele overleggen tussen de burgemeester (regionaal portefeuillehouder cybercrime), de politiechef van de eenheid en de hoofdofficier van justitie van arrondissement.

Het is een overleg dat geen gezag heeft, maar wel kan stimuleren dat bepaalde zaken worden geagendeerd en dat er bewustwording wordt gecreëerd op het thema. De agenda wordt bepaald aan de hand van actiepunten uit het vorige overleg en door input vanuit beleidsondersteuners. Voorbeelden van agendapunten die eerder zijn besproken zijn: 'landelijke ontwikkelingen', 'smart cities' en 'informatievoorziening van de Vereniging van Nederlandse Gemeenten (VNG) over de informatie samenleving'. Vanuit het cybercrimeteam wordt input geleverd voor de cyberdriehoek en meegedacht over beleidsvorming.

DOEL

Lokale bestuur meer betrekken bij de aanpak van cyber en bewustwording binnen en buiten de organisaties.

NIVEAU / TOEPASBAARHEID

De cyberdriehoek vindt plaats op regionaal niveau, maar wel op het hoogste ambtelijke niveau, waardoor er ook landelijk een link wordt gelegd.



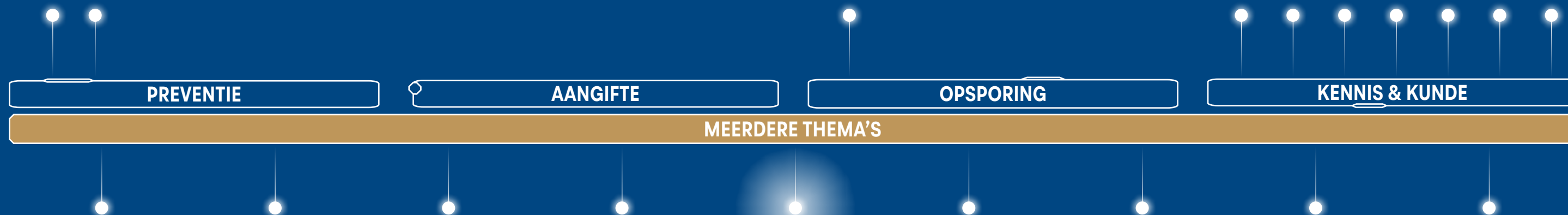
DEN HAAG

SAMENWERKING

- Intern:
Eenheidschef Den Haag, adviseur van de eenheidschef, regionaal cybercrimeteam.
- Extern:
Regionaal samenwerkingsverband Integrale Veiligheid, gemeente Katwijk (burgemeester, afd. Openbare Orde en Veiligheid, afd. Economische Zaken), Openbaar Ministerie (Hoofdofficier van Justitie).

IMPLEMENTATIE

Gezien de ontwikkelingen op het gebied van digitale veiligheid zou de cyberdriehoek vaker kunnen plaatsvinden.



AANPAK GELDEZELS

Het project 'aanpak geldezels' is een werkwijze die bestaat uit drie onderdelen:

1. het aanstellen van aanspreekpunten binnen districtsrecherches en basisteams,
2. het oppakken van geldezelzaken
3. de afhandeling van geldezelzaken.

Onderzoeken worden gedraaid in nauwe samenwerking met ketenpartners. De kern van het project zijn de gezamenlijke actiedagen. De geldezel wordt eerst verhoord door de politie, gaan dan in gesprek met de reclassering of het ETF, waaruit een advies komt voor de Officier van Justitie, die een afdoening op maat geeft waarvan gedacht wordt dat de geldezel er het meest baat bij heeft. Er worden nog steeds (taak)straffen opgelegd, maar ook schadevergoeding of voorwaarden om verplicht een hulpverleningstraject te volgen.

DOEL

Aantal open geldezelzaken naar beneden brengen; preventie; maatwerk en een eenduidige werkwijze.

DOELGROEP

Geldezels: naïeve jongeren, kwetsbare jongeren, ouderen met uitzichtloze situatie.

NIVEAU / TOEPASBAARHEID

Het project vindt plaats op eenheidsniveau, waar districten en basisteams verantwoordelijk worden gemaakt voor het oppakken van zaken.



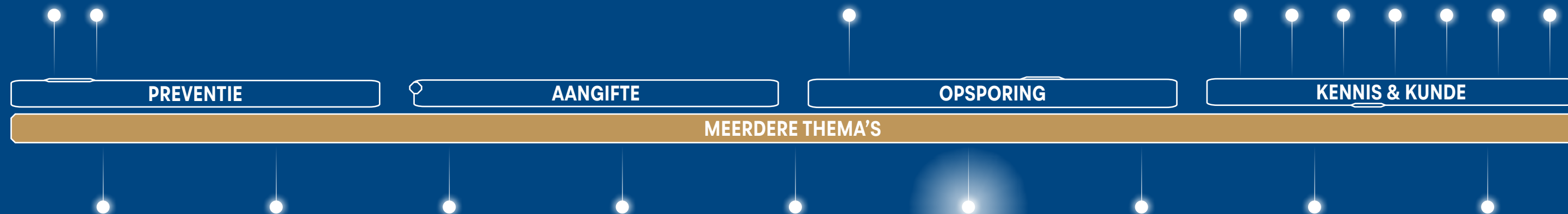
ROTTERDAM

SAMENWERKING

- Intern: District recherche en basisteams.
- Extern: Reclassering Nederland, Humanitas, team ETF van gemeente R'dam, OM.

IMPLEMENTATIE

Van te voren was nooit gedacht dat het project zou uitgroeien tot de huidige aanpak.



CYBER HQ

Het project 'Cyber HQ (headquarters)' betreft de vorming van een multidisciplinair team - bestaande uit politiemedewerkers vanuit tactiek, specialisme en intel – op regionaal niveau dat zich richt op drie hoofdpijlers in de aanpak van cybercriminaliteit:

1. Operatie: uitvoeren van onderzoeken en interventies
2. Crisis management
3. Specialisatie op het thema phishing.

De informatiepositie op het gebied van phishing is inmiddels sterk verbeterd en er lopen op omvangrijke publiek-private projecten op het thema. Men heeft periodiek een intelligence beeld en de houtskoolschets van de opsporing wordt in werking gebracht. Men wil continue blijven doorontwikkelingen en op zoek gaan naar verbeteringen.

DOEL

Toekomst bestendig maken van de eenheid door te intensiveren op het gebied van digitale criminaliteit.

DOELGROEP

-

NIVEAU / TOEPASBAARHEID

Het Cyber HQ is een team op regionaal niveau, maar door overleggen als het LOCO en ROCO ook landelijk en districtelijk ingebed.



ZEELAND-WEST-BRABANT

Andere parels in Zeeland-West-Brabant:

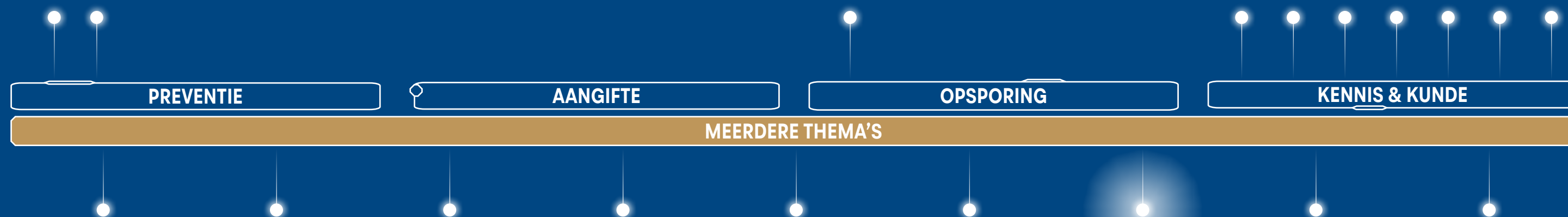
- [District cyberteams](#)
- [Digikamers](#)
- [Digitaal weerbaar Breda](#)

SAMENWERKING

- Intern (Cyber HQ): oude cybercrimeteam (ca. 20FTE), intelligence (7FTE)
- Extern (buiten Cyber HQ): teamchef kolom specialistische opsporing; sectorhoofd DRR, sectorhoofd intelligence.

IMPLEMENTATIE

Cyber HQ is grotendeels vormgegeven als beoogd. Het fundament staat (vlieg-wiel, motorblok, energie creëren) en mensen en middelen zijn aanwezig. De fysieke huisvesting liet op zich wachten vanwege corona.



DIGIKAMERS

De digikamer is een instrument om bekwaamheid op digitaal politiewerk realiseren. Het is een fysieke locatie met verschillende middelen en functies. Het is:

- een werkkamer voor de digitale wijkagent.
- een werkplek waar telefoons uitgelezen kunnen worden (door de aanwezigheid van een UFED).
- een plek waar OSINT-onderzoeken uitgevoerd kunnen worden.
- een plek waar met een beeldtafel (groot scherm) geografische kaartlagen met data over elkaar gelegd kunnen worden.
- een geschikte plek voor 'scrumsessies'

De digikamer faciliteert de gewenste beweging. Het jaagt het proces van de digitalisering van het politiewerk aan door mensen enthousiast te maken en te prikkelen om hiermee aan de slag te gaan. Collega's lopen bijvoorbeeld langs en gaan vragen stellen.

DOEL

Digitalisering breed binnen de politieorganisatie vormgeven.

DOELGROEP

Medewerkers binnen de basisteams.

NIVEAU / TOEPASBAARHEID

Digikamers zijn ingericht op het niveau van basisteams en richten zich op meerdere onderdelen van het politiewerk: van communicatie tot preventie en opsporingsonderzoek.



ZEELAND-WEST-BRABANT

Andere parels in Zeeland-West-Brabant:

- [District cyberteams](#)
- [Cyber HQ](#)
- [Digitaal weerbaar Breda](#)

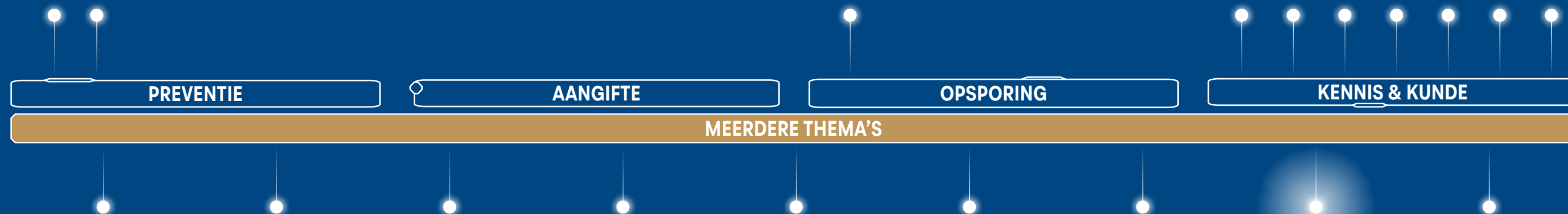
SAMENWERKING

Er wordt samengewerkt met een grote hoeveelheid personen binnen de politieorganisatie. Er is een vast team van ondersteuning met 8 collega's van de afd. communicatie, control, bedrijfsvoering, HRO, thema jeugd, bestuur ondersteuning en sociale media.

IMPLEMENTATIE

Er wordt een voorstel opgesteld om digikamers als standaard op te nemen in de inrichting van basisteams.

In andere eenheden zijn vergelijkbare concepten opgezet.



DIGITAAL WEERBAAR BREDA

Het project kan worden gezien als een ecosysteem, waarin verschillende vitale partnerorganisaties met elkaar samenwerken op het gebied van cyberveiligheid. Het is een samenwerking op basis van vertrouwen, zonder hiërarchie of organisatie die centraal staat.

Initiatieven die voortkomen uit de bijeenkomsten van Digitaal Weerbaar Breda zijn bijv. de ontwikkeling en presentatie van een incident response plan door een van de partners. Ook verzocht de gemeente de groep na te denken over de cyberveiligheid rond de gemeenteraadsverkiezingen. Verder deelt de politie informatie over werkwijzen van criminelen, zodat partnerorganisaties hierop kunnen inspelen.

DOEL

Door informatie met elkaar te delen, elkaar in positie brengen om de digitale weerbaarheid te vergroten.

NIVEAU / TOEPASBAARHEID

Digitaal weerbaar Breda vindt lokaal plaats.



ZEELAND-WEST-BRABANT

Andere parels in Zeeland-West-Brabant:

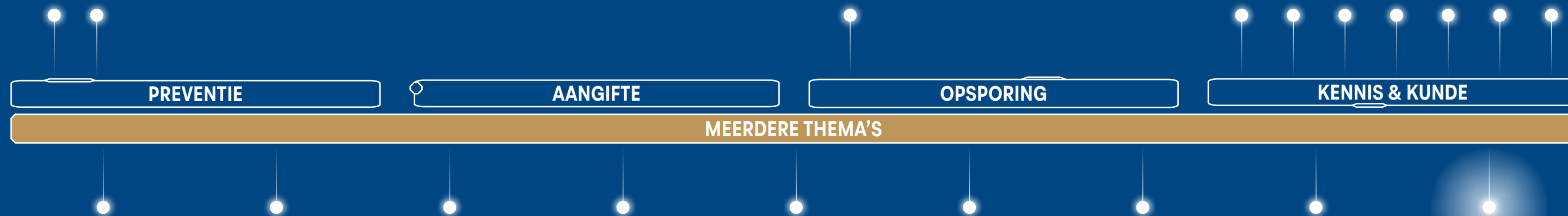
- [District cyberteams](#)
- [Cyber HQ](#)
- [Digikamers](#)

SAMENWERKING

- Amphia Ziekenhuis
- Brabant Water
- Essent
- Landelijke telecomprovider
- ICT-bedrijf
- Gemeente Breda
- Politie

IMPLEMENTATIE

De samenwerking vindt plaats o.b.v. intentieverklaring. Men wil vaker bij elkaar komen, omdat er tussen de bijeenkomsten veel gebeurt en incidenten plaatsvinden.



DAGELIJKSE CYBERQUERY

Het initiatief 'dagelijkse cyberquery' betreft het duiden en scoren van aangiften cybercrime door medewerkers van de Dienst Regionale Informatie Organisatie (DRIO), zodat basisteams concrete aanwijzingen krijgen over aangiften die opgepakt dienen te worden. De aangiften die de DRIO scoort en duidt zijn aangiften die uit de cybercrime query naar voren komen. Groen betekent dat basisteams het advies krijgen om de aangifte geen prioriteit te geven; oranje dat er een interessante opsporingsindicatie aanwezig is en rood dat de zaak met prioriteit opgepakt moet worden vanwege heterdaad mogelijkheden.

De case-screener kan afwijken van het advies van de DRIO. Uiteindelijk wordt elke dag een overzicht gestuurd met de veredelde aangiften naar een grote lijst politiemedewerkers.

DOEL

Kennispositie verbeteren op cybercriminaliteit; uniformiteit in de verwerking van aangiften cybercriminaliteit; in stelling brengen van basisteams bij het oppakken van zaken.

DOELGROEP

Case-screeners en leidinggevenden van basisteams.

NIVEAU / TOEPASBAARHEID

Het project vindt plaats op eenheidsniveau. De dagelijkse cyberquery wordt gebundeld per basisteam.



LIMBURG

Andere parels in Limburg:

- [Risk Factory](#)
- [KOR3NWOLF](#)

SAMENWERKING

- Intern: Vanuit de DRIO en het cybercrimeteam zijn vier collega's betrokken bij de dagelijkse veredeling van zaken.
- Extern: Het OM leest mee en gaat een richtlijn schrijven voor het oppakken van zaken.

IMPLEMENTATIE

Door de veredeling wordt heel concreet aangegeven aan basisteams welke opsporingskenmerken er zijn en met welk autorisatieverzoek en welke vragen zij bijv. naar een bank moeten. De intensiteit (dagelijks) is hoog, maar nodig.