# PRAKTIJK 1: SECURITY OPERATION CENTER

## Oprichting van een SOC en de structurele verankering van cyberveiligheid in onze organisatie

Vera Celis, Glenn Molenberghs, Rob Lenaerts

08.03.22



TLP-AMBER

# INHOUD

1. Wat vooraf ging…
2. Gestructureerde aanpak
3. Organisatie van de SOC
4. Sitrep

# WAT VOORAF GING…

# WAT VOORAF GING…

## Cyberveiligheid verankeren

2020: Ongerustheid na de vele cyberaanvallen in het nieuws

Willebroek na de cyberaanval: “Gelukkig zijn er nog typemachines en typex”

Picanol zwa… cyberaanva… op te nemen

De gemeente Willebroek werd vrijdagnacht het slachtoffer van een cyberaanval. Het informaticasysteem werd gehackt en de hackers vroegen in ruil een som losgeld in bitcoins. Toch stonden de Willebroekse ambtenaren maandag paraat om de inwoners zo goed en zo kwaad als mogelijk verder te helpen.

GR+SC+MAT Geel

**Doen we als organisatie wel genoeg om cyberveilig te zijn?**

**Ja:**
**Veel geïnvesteerd in beveiliging**

**Nee:**
**Geen structurele opvolging binnen ICT**

# WAT VOORAF GING…

## Opvolging door SD geen goed idee….

### Opvolging door de ICT Service Desk



Opvolging door SD werkt niet:

- SD te druk met gebruikers meldingen
- SD hanteert ander prioriteiten- systeem:
  - incidenten eerst (storing),
  - preventie later…

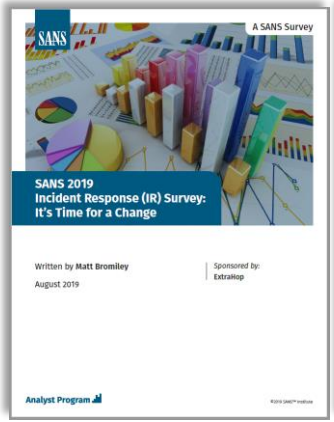
# WAT VOORAF GING…

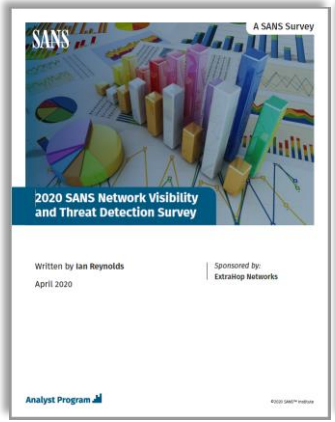
## Op zoek naar een oplossing

Op zoek naar manieren om:

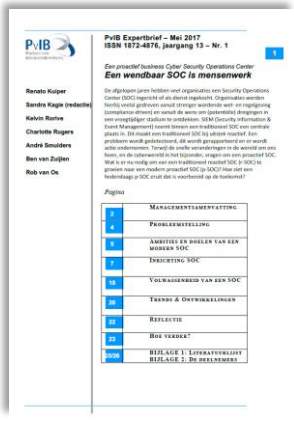
- Dreigingen en incidenten structureel op te volgen
- Cyberveiligheid structureel te veranker in de organisatie

  → eerste kennismaking met het begrip “SOC” (Security Operation Center)



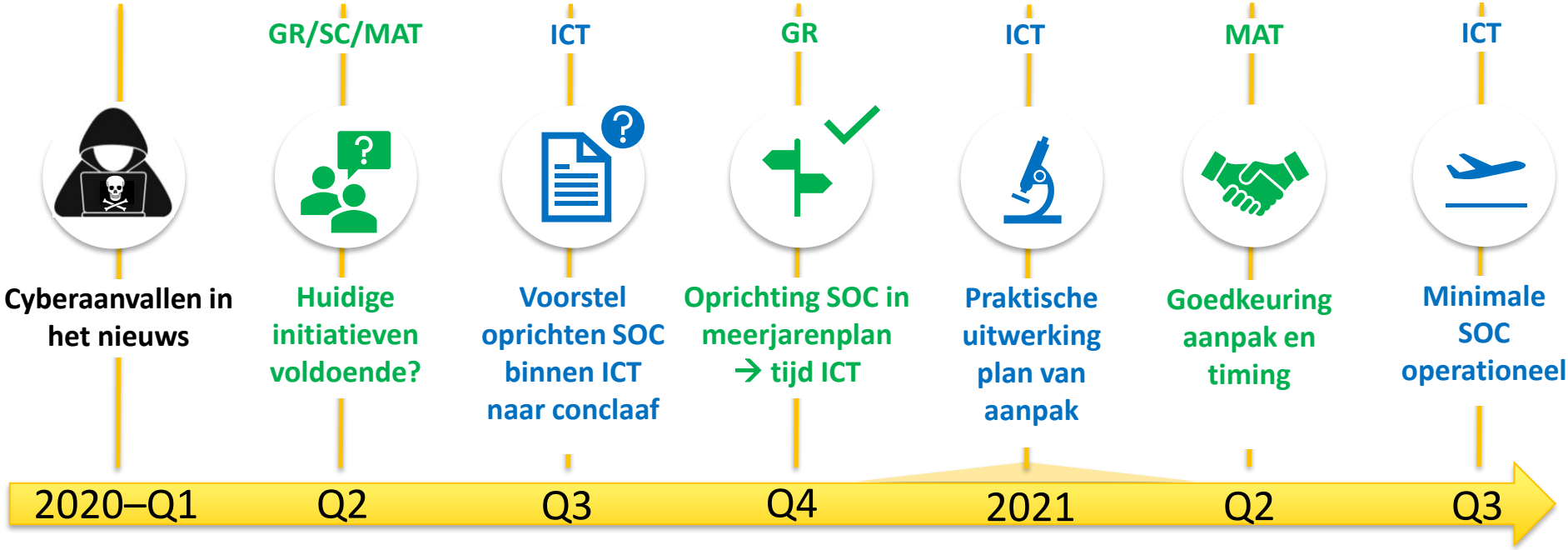







# WAT VOORAF GING…

## Op weg naar de SOC…



# EEN GESTRUCTUREERDE AANPAK



TLP-AMBER

## Doel van de SOC

Doel van de SOC is tweedelig:

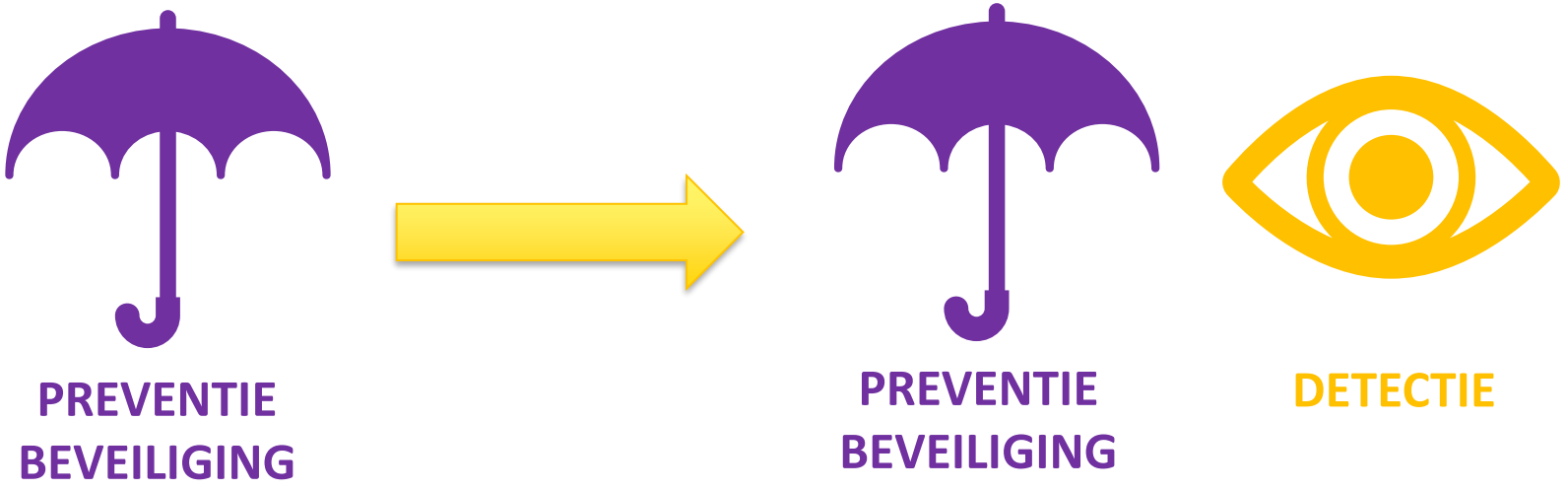
1 Praktische organisatie van de SOC
- permanente consequente opvolging van alle cybersecurity gebeurtenissen
- vastleggen verantwoordelijkheden, procedures, rapportering, …

2 Cybersecurity verankeren in de werking
- zorgen dat we “genoeg” doen voor cybersecurity
- mosterd halen in bestaande raamwerken of standaarden

# EEN GESTRUCTUREERDE AANPAK

## Sleutelopmerking

Bescherming niet meer voldoende, uitbreiding met detectie nodig



# EEN GESTRUCTUREERDE AANPAK

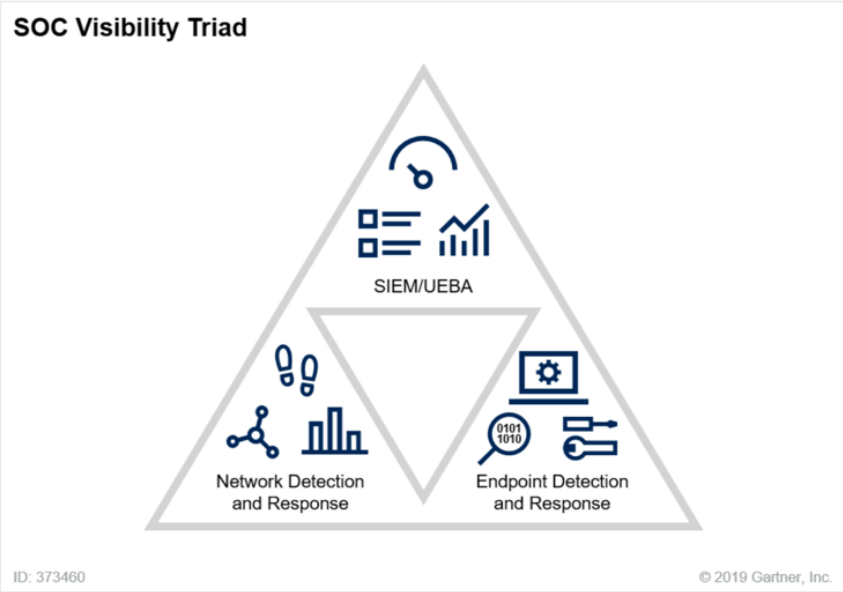
## Geelvoordeel

Voordeel ICT stadbestuur Geel: technisch al redelijk geëquipeerd

“SOC Visibility Triad”:
3 beveiligingsmechanismes

- NDR: visualiteit op het netwerk
- EDR: visualiteit op de endpoints
- SIEM: centraliseren van alle alarmen

→Realisatie makkelijker haalbaar
→Meer gemotiveerd



# GESTRUCTUREERDE AANPAK

## Standaarden & raamwerken

Voor structuur van de SOC gingen de mosterd halen bestaande standaarden:

- veel keuze
- keuze eenvoudig – zeer uitgebreid
- moeilijk in te schatten welke standaard voor ons interessant was

Leerrijke video over de soorten standaarden & raamwerken:


Raamwerken te verdelen in 3 groepen met elk hun eigen focus:

- Controle raamwerken: wat?
  - middelen, mensen, …
- Programma raamwerken: hoe?
  - combineren controls
- Risico raamwerken: veerkracht
  - technologische vooruitgang, dreigingen, …

# GESTRUCTUREERDE AANPAK

## Soorten raamwerk

Raamwerken per soort:

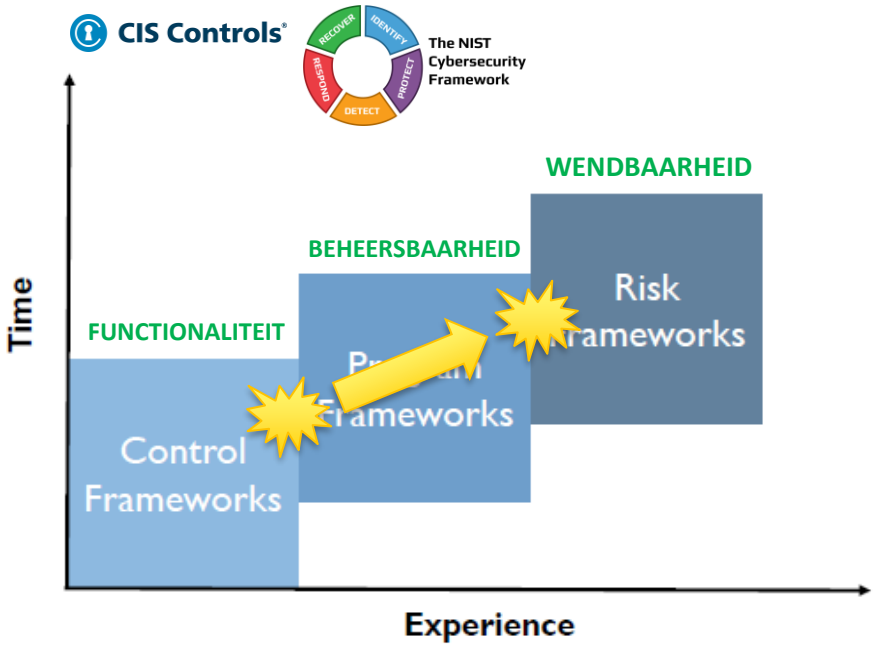
- Control Frameworks

Evaluatie huidige systemen

- Program Frameworks

Organisatie SOC

- Risk Frameworks
  - NIST 800-39, 800-37, 800-30
  - ISO 27005
  - FAIR



Tips & tricks:

- Neem niet klakkeloos over, gebruik enkel wat nodig is
  - Meten en rapporteren van huidige status en vorderingen
  - Programma raamwerk als inspiratie voor een SOC handleiding
- Rapporteer “top-level” naar het management maar gebruik praktijk voorbeelden of situaties als ondersteuning
- Zet in op 2 paarden:
  - Snel paard: snelle verwezenlijkingen binnen het ICT team (praktisch: SOC)
  - Trager paard: dient overschrijdende afspraken m.b.t. cyberveiligheid (noodplanning, databeleid, …) → niet uitstellen!

# DE ORGANISATIE VAN DE SOC



TLP-AMBER

# ORGANISATIE VAN DE SOC AANPAK

## Mogelijke rollen

# ORGANISATIE VAN DE SOC AANPAK

ANALYSE

DETAILANALYSE

CENTRALISEREN ALARMEN

MITIGATIE

KWETSBAARHEDEN & DREIGINGEN INDENTIFICEREN

SOC WERKING ORGANISEREN

BELEID & RAPPORTAGE

**BEURTROL: CYBERSECURITY ANALIST (ALLE 9 ICT'ERS)**

Security Analyst

PERMANENTIE

ESCALATIE GEBEURTENIS SPECIALIST IS BACKUP ANALIST

**ROL: STEDELIJKE CERT (CRISISCEL CYBERINCIDENT)**

Geel · VTC · GBA Gegevensbeschermingsautoriteit · Politie Geel - Laakdal - Meerhout · CERT.be The Federal Cyber Emergency Team · EXTERNE PARTNERS

ZWAAR CYBERINCIDENT

**ROL: CYBERSECURITY SPECIALIST (ICT CERT): 1 OF 2 ICT'ERS**

Senior Security Analyst · SIEM Engineer · Threat Intel Researcher (F) · Red Team Specialist (F) · Forensics Specialist (F)

Incident Handler · Threat Hunter · MITRE ATT&CK · Vlaamse overheid · Politie · FCCU · EXTERNE PARTNERS · howest · EXTERNE PARTNERS

OPERATIONELE FEEDBACK MANAGER IS BACKUP SPECIALIST

**ROL: CYBERSECURITY MANAGER: 1 ICT'ER**

UITWERKEN STRATEGIE ORGANISATIE SOC

SOC Lead · SOC Manager

PARTNERS: Geel · VVSG · IOK

BRONNEN: NIST National Institute of Standards and Technology U.S. Department of Commerce · SANS · Cyber Competence Network · CENTRE FOR CYBER SECURITY BELGIUM · enisa · CIS Center for Internet Security

## Consolidatie rollen

CRISISBEHEER OP ORGANISATIEVLAK

DREIGINGSINFORMATIE VERZAMELEN

PEN-TESTEN

DIGITAAL FORENSISCH ONDERZOEK

# ORGANISATIE SOC AANPAK

## Tips & tricks

- Betrek hele ICT dienst erbij
  - Beurtrol “SOC analist”
  - Sommige taken zijn van toepassing op de hele dienst / organisatie
- Indien mogelijk: zet er een eigen projectleider op
- Kleine ICT omgevingen → combineer SOC/NOC
- Neem verantwoordelijkheden/rollen op in functieprofielen
- Gericht rapporteren MAT:
  - Gedurende ontwikkeling (eerste 2-3 jaar): per kwartaal
  - Eenmaal verankerd: jaarlijks

# SITREP

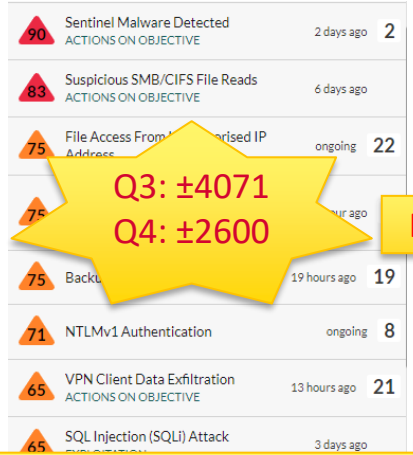


TLP-AMBER

# SITREP

## Gebeurtenissen afvinken en registeren

### Eerste triage: afvinken in SIEM systeem

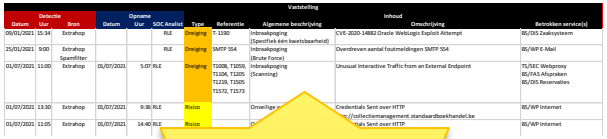



Q3: ±4071
Q4: ±2600

Filteren

### Registratie: op te volgen gebeurtenissen

**INDIVIDUELE GEBEURTENISSEN**

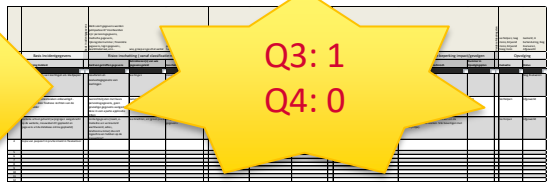


**DOORLOPENDE RISICO'S**

Q3: ±100
Q4: ±25

Escaleren

### Escalatie IVC: enkel grote incidenten/risico's



Q3: 1
Q4: 0

Gebeurtenissen

SOC Register

Incidentenregister IVC

Tijdsinvestering voor elk niveau:

## OPERATIONEEL

- Security analist
- Dagelijkse opvolging
- Effort
  - Niet ervaren: 1 tot 3 uur / dag
  - Ervaren: 30 tot 60 min / dag

## PROJECT

- SOC Manager
- Organisatie SOC
- Toepassing raamwerken
- Effort
  - 2021: 85 dagen
  - 2022: 85 dagen

Kosten:

# SITREP

## Kwartaalrapportage MAT

- Vorderingen werking
- Detecties door SOC
- Initiatieven:
  - Ethisch hacken
  - VPAM Project (toegang leveranciers)
  - Digitale nachtklok
- Thema's:
  - Netwerksegmentatie
  - IoT/OT
  - Cybersecurity ratings

Geel



# SITREP

## Bezig: functiewaardering

## Hoe discrepantie op vlak werkdruk wegwerken?

Basistaken

Proces-rollen

**TOEGEWEZEN SERVICES**

**KENNIS + VAARDIGHEDEN**

Basistaken ICT taken:
- Dagelijks beheer
- Ondersteuning
- Onderhoud
- Projecten
- Organisatie

ISM Rollen:
- Incident manager
- Change manager
- …

SOC Rollen:
- Security analist
- Security specialist
- SOC manager

| ICT TECHNICUS | JUNIOR ICT | SENIOR ICT | ICT ADVISEUR | ICT MANAGER |
|---|---|---|---|---|
| Praktisch | | Organisatorisch | | Strategisch |
| Verantwoordelijkheid # services | | | | |
| Basiskennis | | Specifieke kennis | | Overkoepelend |
| Verantwoordelijke services | | | | |
| Aantal ISM/SOC Rollen | | | | |

# VRAGEN?

Geel

Je komt er, je blijft er