mbo digitaal

(SURF)SOC

SAMENWERKEN AAN CYBERVEILIGHEID IN HET MBO

11 december 2025

Ry Boxem

mbo digitaal

Agenda

Introductie

Wat doet een SOC nou eigenlijk?

Is het effectief?

Uitdagingen ‘oude’ SURFSOC

Aanbesteding SURFSOC NG

Implementatieproces

mbo digitaal

Introductie

Na deze sessie weet je:

- Welke keuzes in SURFSOC Next Generation zijn gemaakt op basis van input uit het mbo.
- Wat een instelling concreet moet doen om SURFSOC succesvol te implementeren.
- Wat SURFSOC dagelijks voor je kan betekenen in termen van detectie, respons en risicobeheersing.
- Of en hoe SURFSOC past binnen jouw eigen planning, risico's en volwassenheidsniveau.

Wat is SOC:

Een Security Operations Center (SOC) is een gespecialiseerde dienst die **continu** (24/7) meekijkt met de digitale omgeving van jouw instelling, met als doel om:

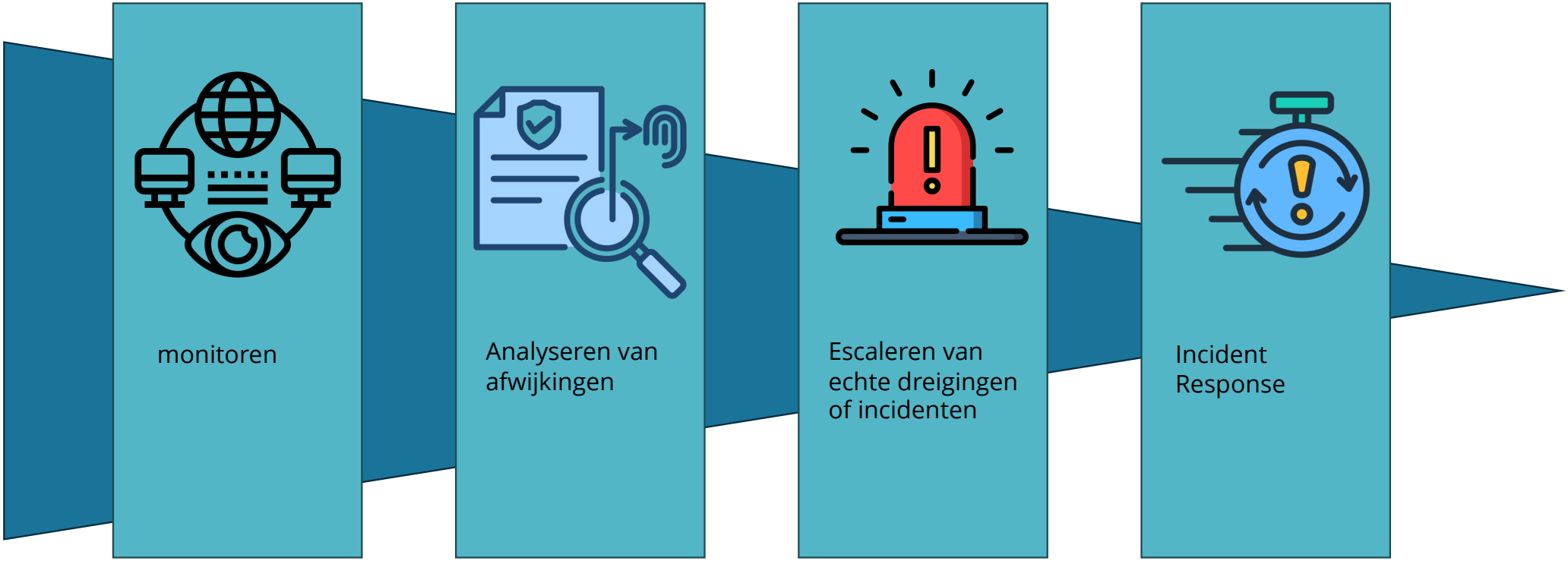
- dreigingen vroegtijdig te detecteren,
- incidenten snel te duiden, en
- gerichte respons te ondersteunen of uit te voeren.

• Belang van een SOC:

Een SOC is je vangnet. Wanneer andere beveiligingsmaatregelen falen — en dat gebeurt vroeg of laat — zorgt het SOC ervoor dat je de aanval toch op tijd ziet en kunt handelen.

mbo digitaal

Wat doet een SOC eigenlijk?



mbo digitaal

Monitoren

Monitoren vormt de basis van het SOC. Hierbij wordt continu gekeken naar activiteiten binnen jouw netwerk, systemen, endpoints en identiteiten. Alle relevante log- en telemetrygegevens worden verzameld zodat afwijkingen, patronen of ongebruikelijke gebeurtenissen zichtbaar worden. Het doel van monitoren is om volledig en actueel inzicht te hebben in wat er in de digitale omgeving gebeurt — 24/7 en zonder onderbreking. Alleen met goede monitoring ontstaat het fundament waarop detectie en beveiliging kunnen steunen.

mbo digitaal

Analyseren

Analyseren is het proces waarbij binnenkomende signalen worden beoordeeld om te bepalen of ze normaal gedrag of een potentiële dreiging vertegenwoordigen. SOC-analisten gebruiken daarbij context, correlatie en kennis van aanvalspatronen om verdachte activiteiten te duiden. Door deze interpretatie ontstaat onderscheid tussen ruis en relevante gebeurtenissen, en wordt duidelijk welke signalen aandacht verdienen. Analyseren geeft betekenis aan de data en maakt zichtbaar wát er werkelijk aan de hand is.

mbo digitaal

Escaleren

Escaleren is het moment waarop een geverifieerde dreiging wordt doorgezet naar de organisatie omdat er daadwerkelijk actie nodig is. Alleen meldingen die een reëel risico vormen worden gedeeld, voorzien van duidelijke informatie over wat er is gezien en waarom het relevant is. Zo ontvang je geen ruis, maar alleen waarschuwingen die ertoe doen. Escaleren zorgt ervoor dat mogelijke incidenten tijdig onder de aandacht komen van de juiste mensen binnen de instelling.

mbo digitaal

Response

Response is het nemen van concrete maatregelen om een dreiging in te dammen, te beperken of volledig te stoppen. Zodra een incident is vastgesteld, is het essentieel dat er direct handelingsadvies beschikbaar is: welke systemen moeten worden geïsoleerd, welke accounts geblokkeerd, en welke stappen moeten worden genomen om verdere schade te voorkomen.

Omdat aanvallen niet wachten op kantooruren, is snelle response — óók ’s nachts of in het weekend — van groot belang. Cyberincidenten kunnen zich binnen minuten uitbreiden, waardoor directe containment het verschil maakt tussen een klein incident en een grote verstoring. Response zorgt ervoor dat er altijd een duidelijk handelingsperspectief is, op elk moment van de dag.

mbo digitaal

Is een SOC effectief? - Detectietesten

SURF en MBO digitaal hebben in het verleden bij 10 mbo instellingen detectietesten uitgevoerd.

- Doel:
  - Checken of de sensoren correct zijn ingeregeld
  - Zien hoe (snel) detectie op gang komt
- Bevindingen:
  - Aannames versus werkelijkheid
  - Zonder DPI-sensor worden initiële (discovery) attacks vaker gemist
  - Netwerksensor = belangrijk
  - Defender for Identity is handig voor detectie
  - Leermoment (Fox-IT vs. externe SOC-diensten)
  - Inmiddels een vast onderdeel van SURFsoc

mbo digitaal

Pentesten/Red teams

Bij recente pentesten/red teams die zijn uitgevoerd onder toezicht van mbo-digitaal werden de aanvallers allemaal gedetecteerd.

“Met slechts 12 bevindingen en geen volledig compromittering in drie weken tijd, is duidelijk dat de organisatie al een sterke basis heeft om de systemen te beveiligen. Daarnaast is het ook gelukt om de aanvallers te detecteren en was het daarmee gelukt om de aanvallers de toegang tot het netwerk te ontzeggen. ”

mbo digitaal

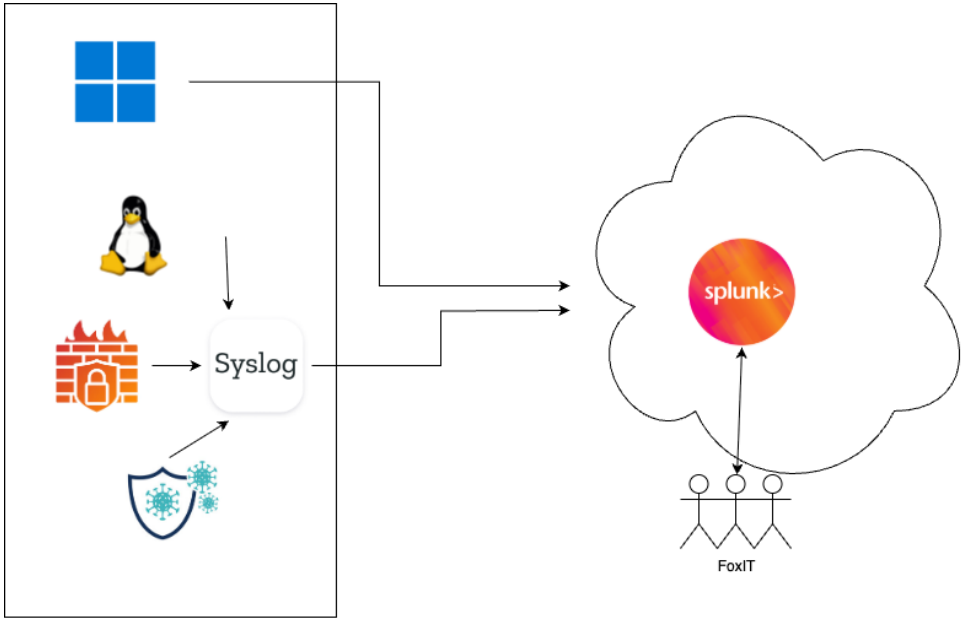
Uitzonderingen

- Als logging niet op orde is
  - Missende logging (hele log source of deel van de hosts)
  - Verkeerde audit settings
- Als adviezen van het SOC niet opgevolgd worden of processen niet duidelijk zijn.
  - Feedbackloop is van belang voor het op peil houden van de dienstverlening
  - Onduidelijke processen of ontbreken van kaders kunnen zorgen voor het niet of vertraagd uitvoeren van incident response stappen.
- Als basisbeveiliging ontbreekt (patching, IAM, MFA)
  - SOC overspoelt met incidenten, inperkende maatregelen zijn dan als dweilen met de kraan open.

mbo digitaal

Het ‘oude’ SurfSOC

- Dienstverlening SURFsoc sinds 2021, mede na aanleiding security incidenten bij instellingen (UM)
- Vanuit aanbesteding (2020) is partnerschap met marktpartij (Fox-IT) uitgevoerd



mbo digitaal

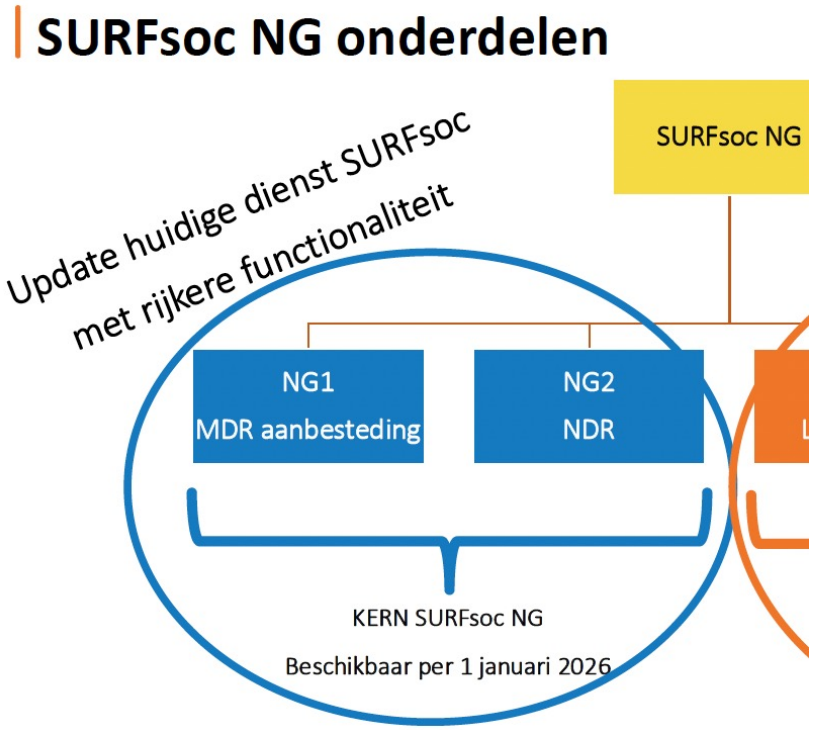
Het ‘oude’ SurfSOC - uitdagingen

- Scoping van ‘aanbesteding 2020’ past niet meer voldoende
- Meer flexibiliteit nodig mede ivm de grotere variatie in deelnemende instellingen

mbo digitaal

Aanbesteding SURFSOC NG

- Goede basis dienstverlening, waaronder automatisch ingrijpen
- Gericht/geschikt op standaardisatie (Microsoft security stack)



mbo digitaal

Aanbesteding SURFSOC NG

Situatie instellingen	Kenmerken	Match met SURFsoc NG1
Deelnemer huidige Multi-Tenant SURFsoc	Voornamelijk gebruik makend van Microsoft-stack (gericht op standaardisatie)	Ja
	On-prem servers Linux, Cloud AWS etc.	Ja
	Aanvulling netwerksensor nodig	Ja, analyse opgenomen, daarnaast levering netwerksensor vanuit NG2-NDR
	Andere (niet-Defender) EDR	Nee, beperkt (idem huidige situatie)
	Complexere heterogene IT-omgeving: VMWare, Kubernetes	Nee, beperkt. Meer eigen analyse nodig. Voor die delen mee doen met NG2-SIEMunlimited
	Specials: SAAS, Webserver	Nee, hooguit beperkt (idem huidige situatie)
Deelnemer huidige Single-Tenant SURFsoc	Voornemend om gebruik te maken van Microsoft-stack (grotendeels standaardisatie)	Ja
	Niet mogelijk om gebruik te maken van Microsoft-stack On-prem is vereiste andere hoge/bijzondere eisen	Eigen of dedicated oplossing uit de markt Wachten op/meedoen met NG2-SIEMunlimited
Eigen SOC/SIEM	Complexere heterogene IT-omgeving, eigen detectieregels	Nee Wachten op/meedoen met NG2-SIEMunlimited
Uitbesteed aan marktpartij	Indien kenmerken vergelijkbaar huidige Multi-Tenant situatie	Ja
Geen SOC/SIEM	Indien kenmerken vergelijkbaar huidige Multi-Tenant situatie	Ja

mbo digitaal

Aanbesteding SURFSOC NG – mbo's!

Situatie instellingen	Kenmerken	Match met SURFsoc NG1
Deelnemer huidige Multi-Tenant SURFsoc	Voornamelijk gebruik makend van Microsoft-stack (gericht op standaardisatie)	Ja
	On-prem servers Linux, Cloud AWS etc.	Ja
	Aanvulling netwerksensor nodig	Ja, analyse opgenomen, daarnaast levering netwerksensor vanuit NG2-NDR
	Andere (niet-Defender) EDR	Nee, beperkt (idem huidige situatie)
	Complexere heterogene IT-omgeving: VMWare, Kubernetes	Nee, beperkt. Meer eigen analyse nodig. Voor die delen mee doen met NG2-SIEMunlimited
	Specials: SAAS, Webserver	Nee, hooguit beperkt (idem huidige situatie)
Deelnemer huidige Single-Tenant SURFsoc	Voornemend om gebruik te maken van Microsoft-stack (grotendeels standaardisatie)	Ja
	Niet mogelijk om gebruik te maken van Microsoft-stack On-prem is vereiste andere hoge/bijzondere eisen	Eigen of dedicated oplossing uit de markt Wachten op/meedoen met NG2-SIEMunlimited
Eigen SOC/SIEM	Complexere heterogene IT-omgeving, eigen detectieregels	Nee Wachten op/meedoen met NG2-SIEMunlimited
Uitbesteed aan marktpartij	Indien kenmerken vergelijkbaar huidige Multi-Tenant situatie	Ja
Geen SOC/SIEM	Indien kenmerken vergelijkbaar huidige Multi-Tenant situatie	Ja

mbo digitaal

Aanbesteding SURFSOC NG - geen mbo's

Situatie instellingen	Kenmerken	Match met SURFsoc NG1
Deelnemer huidige Multi-Tenant SURFsoc	Voornamelijk gebruik makend van Microsoft-stack (gericht op standaardisatie)	Ja
	On-prem servers Linux, Cloud AWS etc.	Ja
	Aanvulling netwerksensor nodig	Ja, analyse opgenomen, daarnaast levering netwerksensor vanuit NG2-NDR
	Andere (niet-Defender) EDR	Nee, beperkt (idem huidige situatie)
	Complexere heterogene IT-omgeving: VMWare, Kubernetes	Nee, beperkt. Meer eigen analyse nodig. Voor die delen mee doen met NG2-SIEMunlimited
	Specials: SAAS, Webserver	Nee, hooguit beperkt (idem huidige situatie)
Deelnemer huidige Single-Tenant SURFsoc	Voornemend om gebruik te maken van Microsoft-stack (grotendeels standaardisatie)	Ja
	Niet mogelijk om gebruik te maken van Microsoft-stack On-prem is vereiste andere hoge/bijzondere eisen	Eigen of dedicated oplossing uit de markt Wachten op/meedoen met NG2-SIEMunlimited
Eigen SOC/SIEM	Complexere heterogene IT-omgeving, eigen detectieregels	Nee Wachten op/meedoen met NG2-SIEMunlimited
Uitbesteed aan marktpartij	Indien kenmerken vergelijkbaar huidige Multi-Tenant situatie	Ja
Geen SOC/SIEM	Indien kenmerken vergelijkbaar huidige Multi-Tenant situatie	Ja

mbo digitaal

Aanbesteding SURFSOC NG

- Managed Detection & Response (MDR) dienstverlening
  - Beproefde oplossing uit de markt, kostenefficiënt
  - Optimaal voor standaardisatie Microsoft-stack, daarnaast voldoende flexibel

- 27/7 SOC – monitoring en analyse
- XDR/SOAR – ondersteunen MS stack
- Automatisch mitigeren
- Validatie:
  - Aantoonbare dekking
  - Inzicht in kwaliteit
  - Transparantie

mbo digitaal

Verloop aanbesteding

- 8 partijen hebben aangeboden op de aanbesteding
- Reviews vanuit verschillende ‘sectoren’
  - Mbo
  - Hbo
  - Wo
  - Onderzoek/medisch

mbo digitaal

Resultaat aanbesteding

Uitbestede MDR:

- 24/7 monitoring en analyse
- Integratie met Microsoft security suite (Defender, Sentinel)
- Portal en rapportages per instelling + sectorbreed
- Detectie op basis van Mitre Att&ck use-cases
- Kennisdeling en gezamenlijke incidentrespons met SURFcert
- Inzet van Netwerksensoren van SURF voor vroegtijdige detectie
- Playbooks voor automatisch ingrijpen

mbo digitaal

(SURF)SOC

Voor vragen:

r.boxem@mbodigitaal.nl

MBO Digitaal is een platform van de MBO Raad voor samenwerking aan digitalisering in het mbo. MBO Digitaal werkt samen met alle mbo-instellingen en heeft sterke banden met MBO Voorzieningen, Kennisnet en SURF.