mbo digitaal

TLP: AMBER+STRICT

(SURF)SOC

SAMENWERKEN AAN CYBERVEILIGHEID IN HET MBO

11 december 2025

Ry Boxem

PROGRAMMA Cyberveiligheid

NETWERK Informatiebeveiliging en Privacy

MBO Raad

mbo digitaal

mbodigitaal.nl/cyberveiligheid

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:

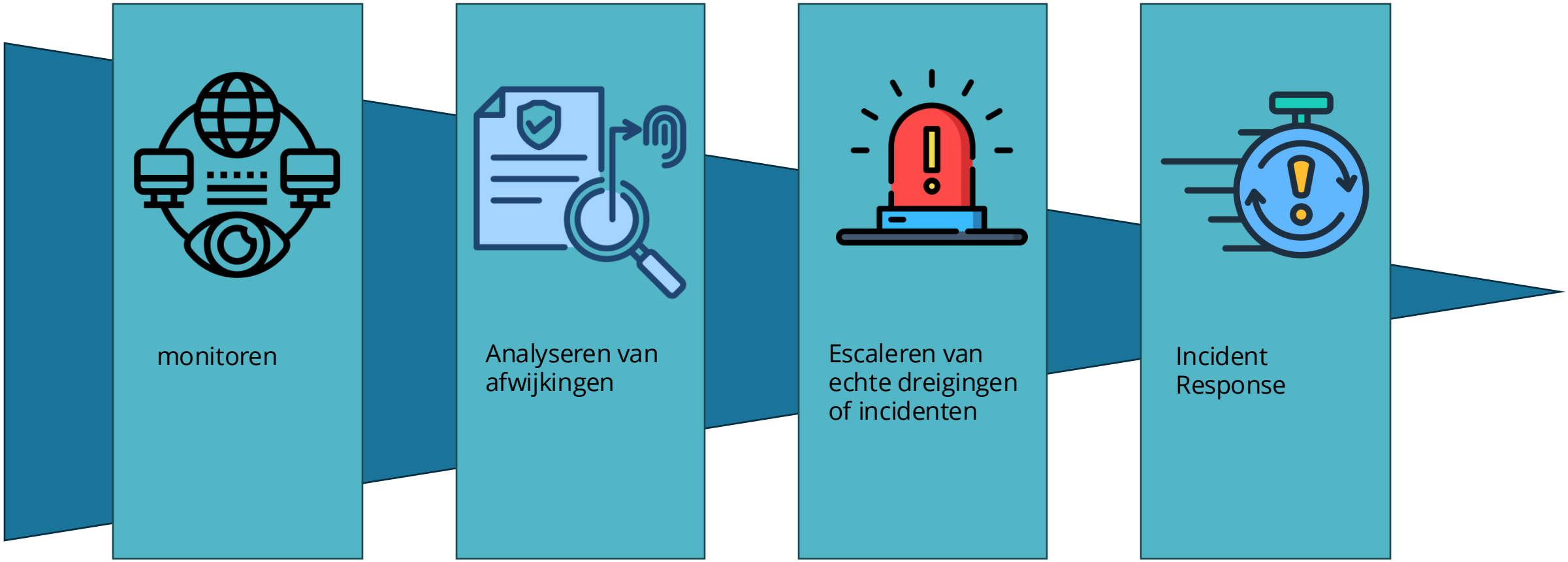
- dreigingen vroegtijdig te detecteren,
- incidenten snel te duiden, en
- gerichte respons te ondersteunen of uit te voeren.

• 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.

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

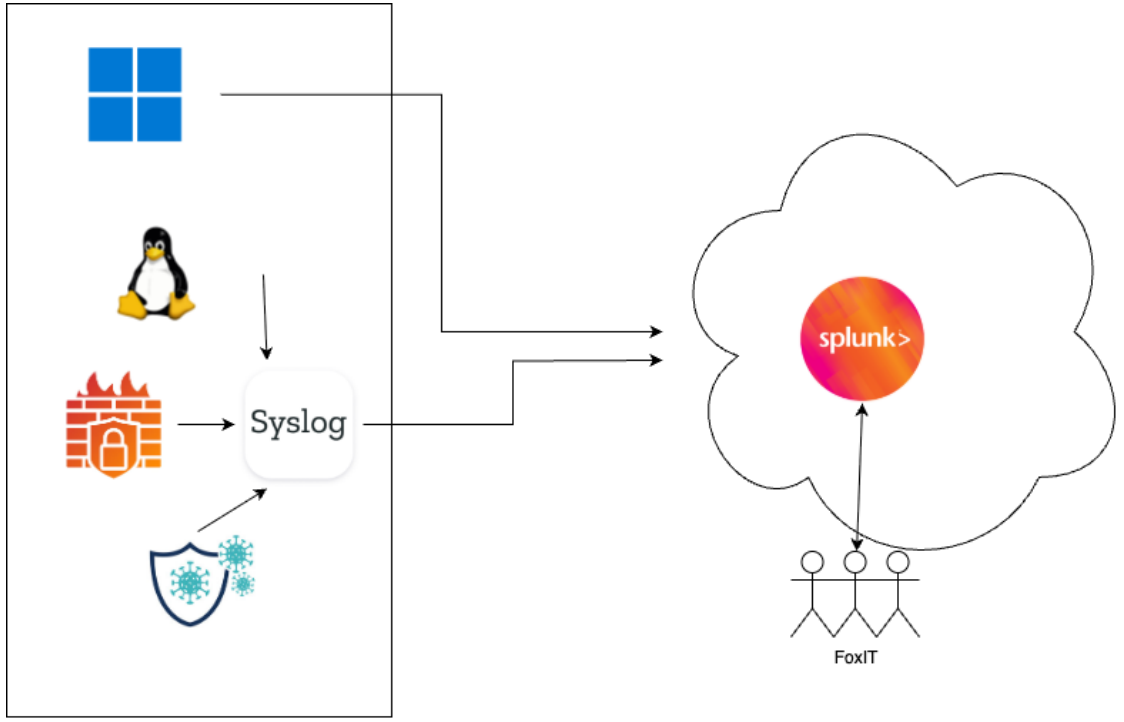
Uitzonderingen

- 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

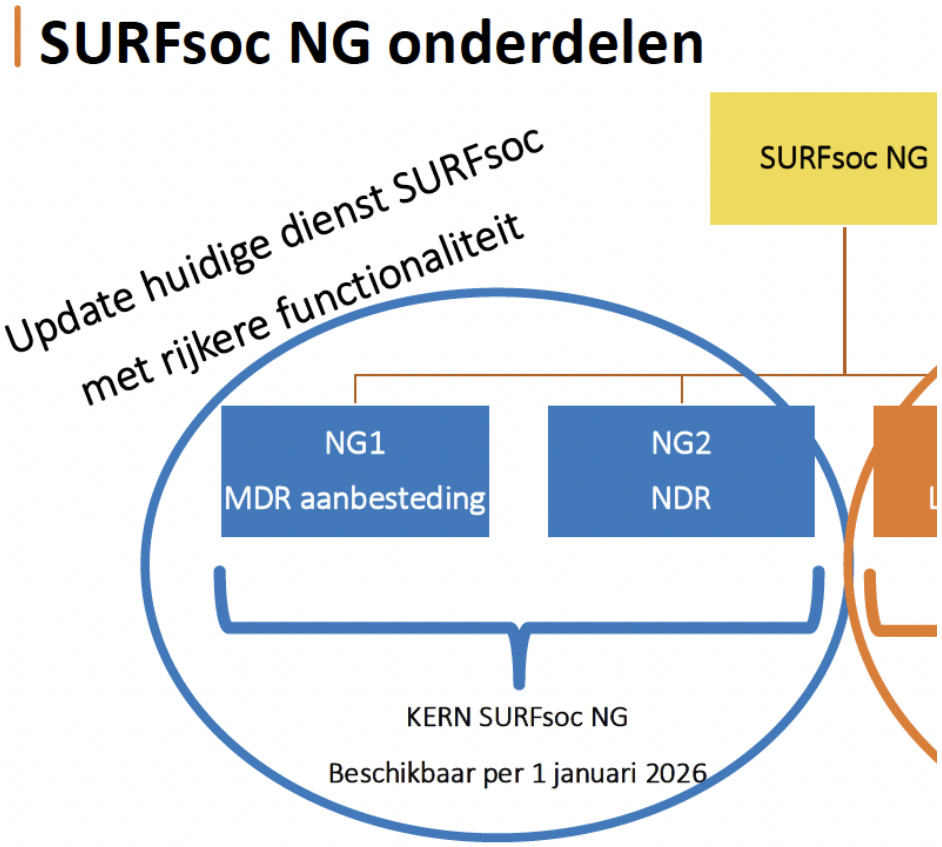
Het ‘oude’ SurfSOC - uitdagingen

- 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
- Fox IT was ook een van de partijen die had aangeboden om de dienstverlening voor SURFSOC-NG voort te zetten.

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

Resultaat aanbesteding

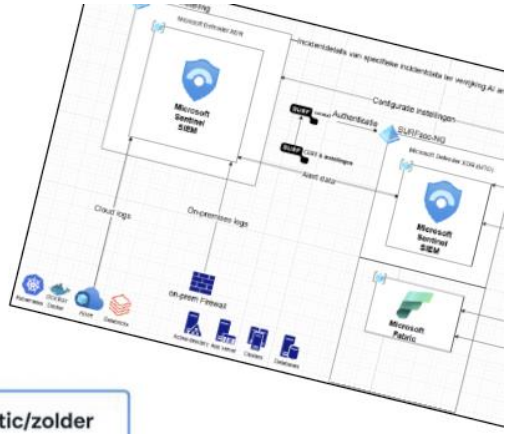
Architectuur

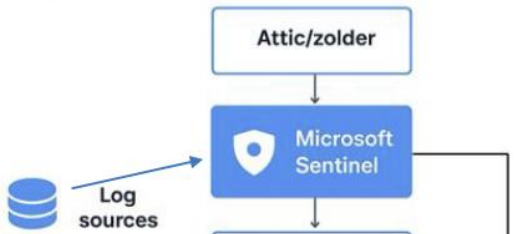
Decentraal instelling:

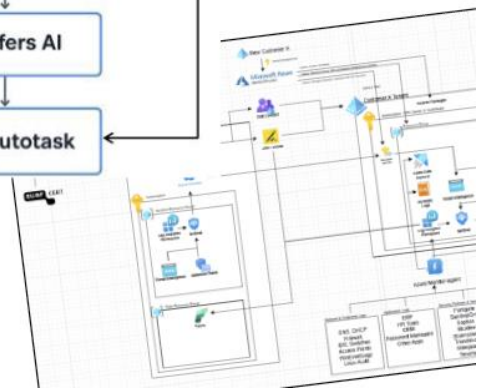
- Logbronnen van Instelling: cloud en on-prem
- Netwerksensor van SURF bij Instelling (additioneel)
- Sentinel (SIEM) van Instelling

Centraal:

- Ticketsysteem (Autotask)
- Koppeling ticketsysteem instelling mogelijk
- DTX/Computest+SURF Microsoft Sentinel







mbo digitaal

Resultaat aanbesteding

Automation

Voorbeelden

- Password reset
  - *Bij detectie van verdachte inlogpogingen of credential theft wordt via Sentinel een automation rule geactiveerd.*
  - *→ Azure ad (entra id) reset het wachtwoord direct en logt de gebruiker uit.*
- Multi-factor authenticatie (mfa)
  - *Wanneer afwijkend inloggedrag wordt vastgesteld, wordt op basis van conditional access policy MFA afgedwongen.*
  - *→ gebruiker moet direct mfa doorlopen.*
- Device isolatie
  - *Bij detectie van malware of laterale bewegingen activeert Sentinel een automation rule.*
  - *→ Microsoft Defender for endpoint plaatst het device in “isolation mode”, waardoor alleen beheercommunicatie mogelijk blijft.*

mbo digitaal

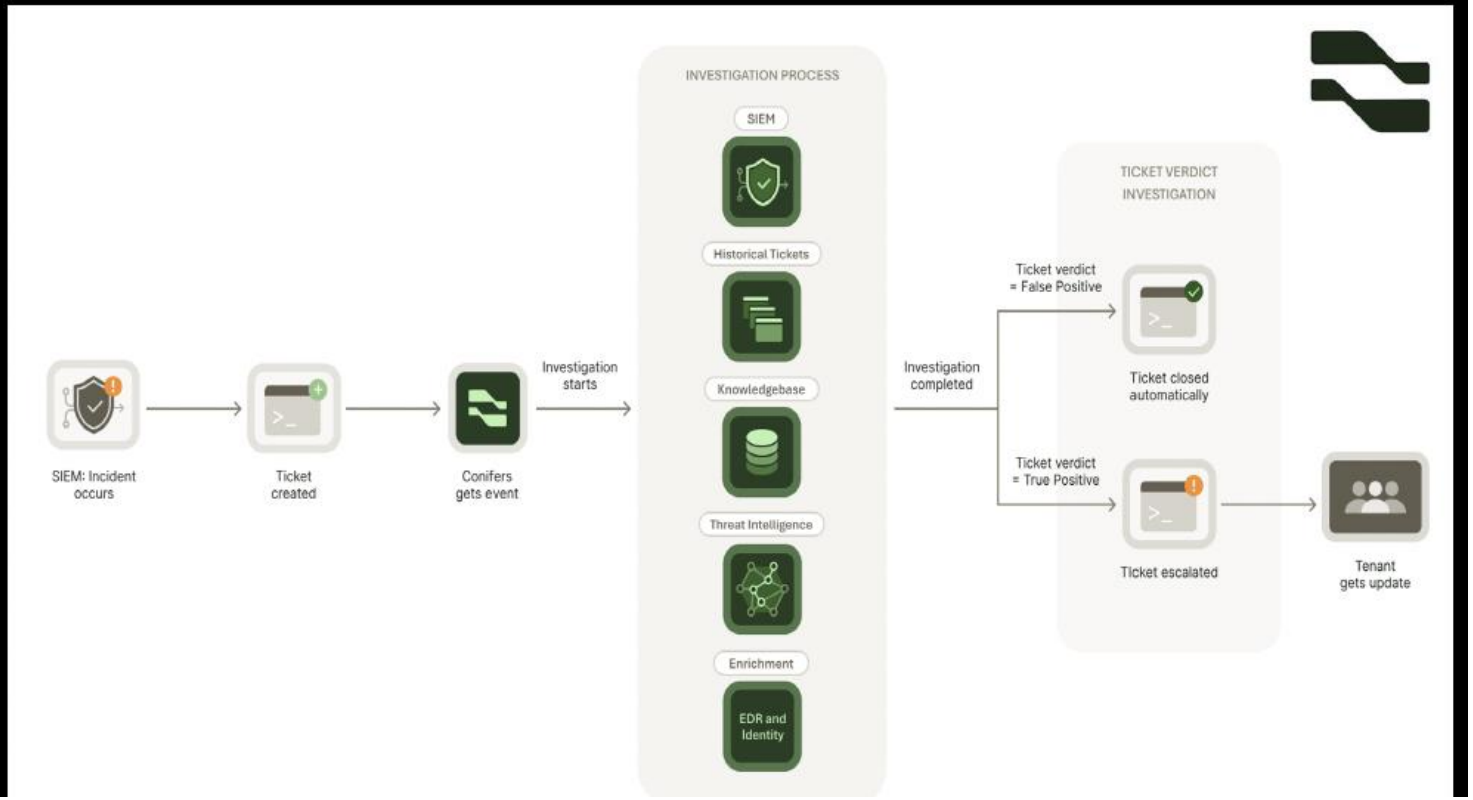
Resultaat aanbesteding

Gebruik van AI

Op beperkte set van use-cases: **Impossible Travel, Lateral Movement - Brute Force - Malware Execution - Phishing - Identity**

Wat doet Conifers.AI:

- **Per instelling een instance**
- **Vooraf afgetraind AI model**
- **Verrijkt en beoordeeld bepaalde use-cases die veel false-positives veroorzaken**
- **Analisten hebben tijd voor andere analyses**



mbo digitaal

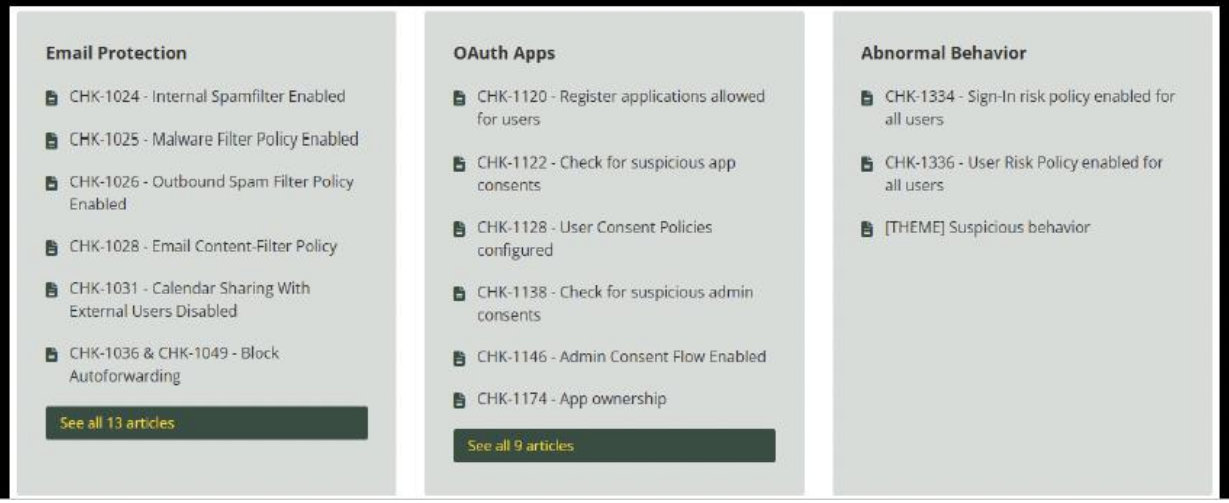
Resultaat aanbesteding

Samenwerking met Attic security

Inzet naar keuze van instelling

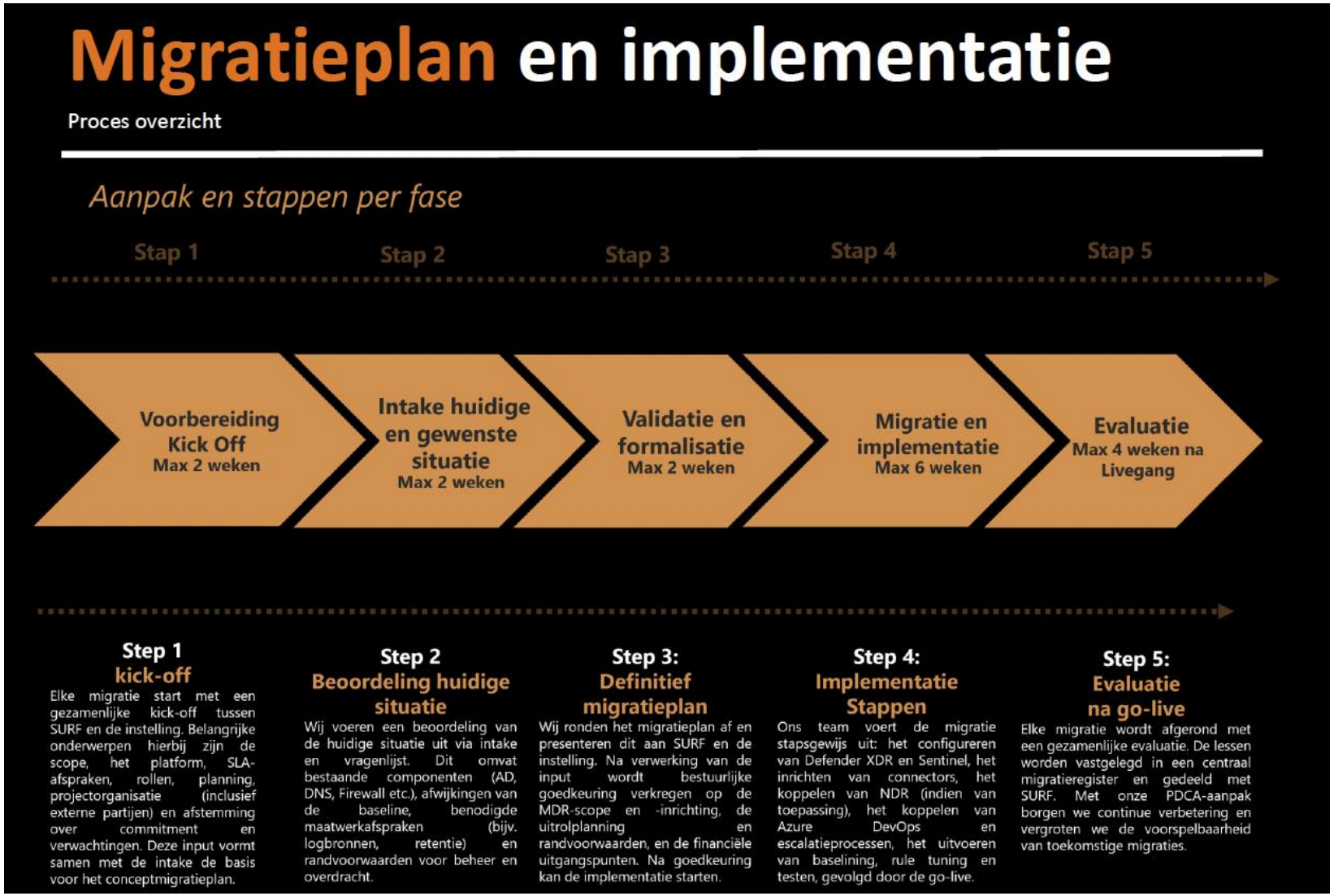
- Attic voert meer dan 100 beveiligingschecks uit op de Microsoft 365-omgeving van de instelling. En dat niet één keer, maar continu. Zo wordt gecontroleerd of de 365 omgeving goed is geconfigureerd en of er iets veranderd is wat risico oplevert.

- Elke melding is voorzien van een duidelijke uitleg. Zodat direct wat het probleem is, waarom het belangrijk is én wat te doen om het op te lossen.



mbo digitaal

Implementatie



mbo digitaal

Voorbereiding – stap 1

- Introductie van de onboarding
- Benodigde rechten
- Logging strategie

mbo digitaal

Voorbereiding – stap 2
checklist Microsoft security producten

Advies	A3 Beschikbaarheid	A5 Beschikbaarheid
Microsoft Defender for Identity sensor installeren op alle domeincontrollers	❌ Niet inbegrepen	✅ Volledig inbegrepen
Attack Surface Reduction (ASR) regels configureren via Microsoft Intune	✅ Inbegrepen via MDE P1	✅ Volledig inbegrepen via MDE P2
Microsoft Defender for Endpoint met EDR in block mode activeren	❌ Niet beschikbaar	✅ Volledig inbegrepen
Automatic Attack Disruption configureren in Microsoft Defender XDR	❌ Niet beschikbaar	✅ Volledig inbegrepen
Cloud-delivered protection en real-time protection inschakelen	✅ Basis functionaliteit	✅ Volledige functionaliteit
Conditional Access policies configureren voor apparaat compliance	✅ Basis functionaliteit	✅ Volledige functionaliteit
Microsoft Defender for Office 365 Safe Links en Safe Attachments activeren	❌ Niet inbegrepen	✅ Volledig inbegrepen
Tamper Protection inschakelen via Microsoft Intune	✅ Inbegrepen via MDE P1	✅ Volledig inbegrepen via MDE P2
Device discovery op 'Standard' niveau configureren in Defender for Endpoint	⚠️ Beperkte functionaliteit	✅ Volledig inbegrepen
Audit logging inschakelen voor alle kritieke services	✅ Basis audit logging	✅ Advanced audit logging
Microsoft Defender for Cloud Apps connector configureren	✅ Cloud App Discovery	✅ Volledige Cloud App Security
Multi-Factor Authentication (MFA) verplicht stellen voor alle accounts	✅ Security defaults MFA	✅ Geavanceerde MFA opties
Conditional Access policies configureren voor verhoogde sign-in risico's	❌ Niet inbegrepen	✅ Volledig inbegrepen
Controlled Folder Access inschakelen voor ransomware bescherming	✅ Inbegrepen via MDE P1	✅ Volledig inbegrepen via MDE P2
Network Protection inschakelen in Microsoft Defender	✅ Inbegrepen via MDE P1	✅ Volledig inbegrepen via MDE P2
Microsoft Defender SmartScreen configureren	✅ Basis SmartScreen	✅ Geavanceerde SmartScreen
Endpoint security baseline policies implementeren via Intune	✅ Basis security baselines	✅ Volledige security baselines

mbo digitaal

Voorbereiding – stap 3
Best practices configuratie Microsoft security producten

Policy Name	DTX	Default value
<klantnaam> - Default DFE AV Settings (Windows)	Microsoft Defender Antivirus	
<klantnaam> - Default DFE AV Settings (MacOS)	Antivirus	
<klantnaam> - Default Security Experience settings	Windows Security Experience	
Policy: <klantnaam> - Default DFE AV Settings (Windows)		
Allow Archive Scanning	Allowed. Scans the archive files.	
Allow Behavior Monitoring	Allowed. Turns on real-time behavior monitoring.	
Allow Cloud Protection	Allowed. Turns on Cloud Protection.	
Allow Email Scanning	Allowed. Turns on email scanning.	
Allow Full Scan On Mapped Network Drives	Not allowed. Disables scanning on mapped network drives.	If you disable or don't configure this setting, mapped network drives won't be scanned.
Allow Full Scan Removable Drive Scanning	Allowed. Scans removable drives.	
Allow Intrusion Prevention System (Deprecated)	Allowed.	
Allow scanning of all downloaded files and attachments	Allowed.	
Allow Realtime Monitoring	Allowed. Turns on and runs the real-time monitoring service.	
Allow Scanning Network Files	Not configured* (kan klant-specifiek zijn, default is disabled)	If you enable this setting or do not configure this setting, network files will be scanned.
Allow Script Scanning	Allowed.	
Allow User UI Access	Allowed. Lets users access UI. * (kan klant-specifiek zijn, default is allowed)	
Avg CPU Load Factor	40	If you disable or don't configure this setting, CPU utilization won't exceed the default value. The default value is 50.
Check For Signatures Before Running Scan	Enabled	
Cloud Block Level	High	
Cloud Extended Timeout	50	
Days To Retain Cleaned Malware	7	
Disable Catchup Full Scan	Not configured	
Disable Catchup Quick Scan	Not configured	
Enable Low CPU Priority	Enabled	If you disable or don't configure this setting, not changes will be made to CPU priority for scheduled scans.
Enable Network Protection	Enabled (block mode)	
Excluded Extensions (WPK)	- (klant-specifiek, eerst auditen)	
Excluded Extensions (SRV)	- (klant-specifiek, eerst auditen)	
Excluded Paths (WPK)	- (klant-specifiek, eerst auditen)	
Excluded Paths (SRV)	- (klant-specifiek, eerst auditen)	
Excluded Processes (WPK)	- (klant-specifiek, eerst auditen)	
Excluded Processes (SRV)	- (klant-specifiek, eerst auditen)	
PUA Protection	PUA Protection on. Detected items are blocked. They will show in history along with other threats.	
Real Time Scan Direction	Monitor all files (bi-directional).	If you disable or don't configure this setting, monitoring for incoming and outgoing files will be enabled.
Scan Parameter	Quick scan	
Schedule Quick Scan Time	600	If you disable or don't configure this setting, daily quick scan controlled by this config won't be run. This policy setting allows you to specify the time of day at which to perform a daily quick scan. The time value is represented as the number of minutes past midnight (00:00)
Schedule Scan Day	Every day	If you disable or don't configure this setting, a scheduled scan will run at a default frequency. Never (default).
Schedule Scan Time	840	This policy setting allows you to specify the time of day at which to perform a scheduled scan. The time value is represented as the number of minutes past midnight (00:00). By default, this setting is set to a time value of 2:00 AM. If you disable or don't configure this setting, a scheduled scan will run at a default time.
Signature Update Fallback Order	Not configured	
Signature Update File Shares Sources	Not configured	
Signature Update Interval	1	If you disable or don't configure this setting, checks for security intelligence updates will occur at the default interval. De default value is 8 (hours).
Submit Samples Consent	Send all samples automatically.	Default value: Send safe samples automatically.
Disable Local Admin Merge	Disable Local Admin Merge	Default value: Enable Local Admin Merge.
Allow On Access Protection	Allowed.	If you enable or don't configure this setting, monitoring for file and program activity will be enabled.
Remediation action for Severe threats	Quarantine. Moves files to quarantine.	Changes to this setting are not applied when tamper protection is enabled. Apply action based on the update definition. This is the default value.
Remediation action for Moderate severity threats	Quarantine. Moves files to quarantine.	Changes to this setting are not applied when tamper protection is enabled. Apply action based on the update definition. This is the default value.
Remediation action for Low severity threats	Quarantine. Moves files to quarantine.	Changes to this setting are not applied when tamper protection is enabled. Apply action based on the update definition. This is the default value.
Remediation action for High severity threats	Quarantine. Moves files to quarantine.	Changes to this setting are not applied when tamper protection is enabled. Apply action based on the update definition. This is the default value.

mbo digitaal

Voorbereiding – stap 4
Defender for Endpoint Intune policies

Voor de configuratie van werkplekken die via Microsoft Intune worden uitgerold, zijn aanvullende beveiligings- en configuratie-instellingen beschikbaar gesteld in de vorm van JSON-policybestanden. Deze bestanden bevatten vooraf gedefinieerde configuraties die aansluiten op de gewenste security baseline en zorgen voor een uniforme en compliant inrichting van alle beheerde endpoints.

mbo digitaal

Intake document

Aan te leveren:

- TenantID
- SubscriptionID
- Domeinnamen
- Microsoft licenties (medewerkers, studenten)
- Additionele Microsoft licenties
- Aantal endpoints/servers

mbo digitaal

Intake document

(Technische) randvoorwaarden:

- Toegang tot Azure tenant (door instelling)
- Geactiveerde Microsoft licenties (A3/A5)
- Defender agents uitgerold
- Overzicht van overige logbronnen en compliance eisen tav logging
- Contactgegevens van enkele beheerders

mbo digitaal

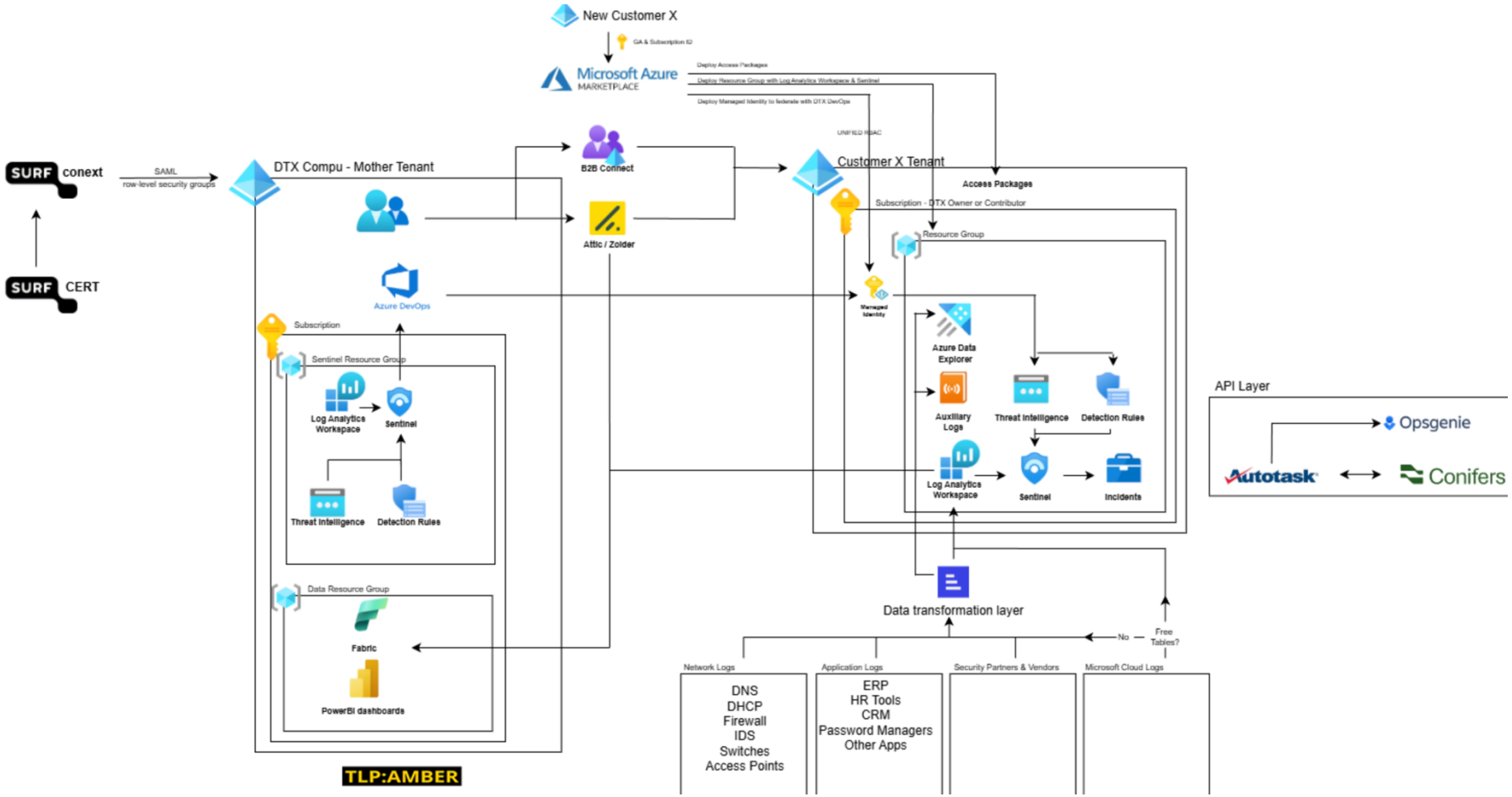
Intake document

(Technische) randvoorwaarden:

- Toegang tot Azure tenant (door instelling)
- Geactiveerde Microsoft licenties (A3/A5)
- Defender agents uitgerold
- Overzicht van overige logbronnen en compliance eisen tav logging
- Contactgegevens van enkele beheerders

mbo digitaal

Technisch aansluiten



mbo digitaal

Tuning

De tuningfase zorgt ervoor dat het SOC niet alleen werkt, maar effectief werkt.

- SOC-detecties aansluiten op de specifieke infrastructuur en risico's van jouw instelling.
- False positives te verminderen, zodat er minder ruis is en meldingen relevant blijven.
- Zorgt dat belangrijke signalen niet worden gemist doordat detecties worden aangescherpt en afgestemd.
- Maakt gebruik van jouw gebruikerspatronen en systemen om onderscheid te maken tussen normaal en afwijkend gedrag.
- Verhoogt de kwaliteit en betrouwbaarheid van SOC-meldingen.
- Leidt tot snellere, beter onderbouwde escalaties en daardoor een effectiever incidentresponsproces.

mbo digitaal

Procesafspraken

Escalatiepaden

Contacten

Ticketing

(SURF)SOC

Voor vragen:

m.deben@mbodigitaal.nl

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.