Road to SIEM: stap voor stap naar een werkende SIEM-aanpak

Veel organisaties weten dat ze iets met SIEM moeten.

De echte vraag is:
waar begin je, zonder direct te veel complexiteit toe te voegen?

Wat we vaak zien, is dat organisaties wel voelen dat ze meer grip nodig hebben op security monitoring, maar nog geen logische route hebben om daar te komen. Road to SIEM maakt die route concreet. Door een gelaagde aanpak maken we helder wat er nodig is om SIEM straks echt waarde te laten opleveren. Het gaat dus niet alleen om de eindoplossing, maar juist om de weg ernaartoe: welke basis moet er liggen, wat moet eerst op orde zijn en hoe bouw je daarna gecontroleerd verder.

SMT
Data zonder gedoe

Veel organisaties willen een SIEM, maar missen de basis

In de praktijk zie je vaak:

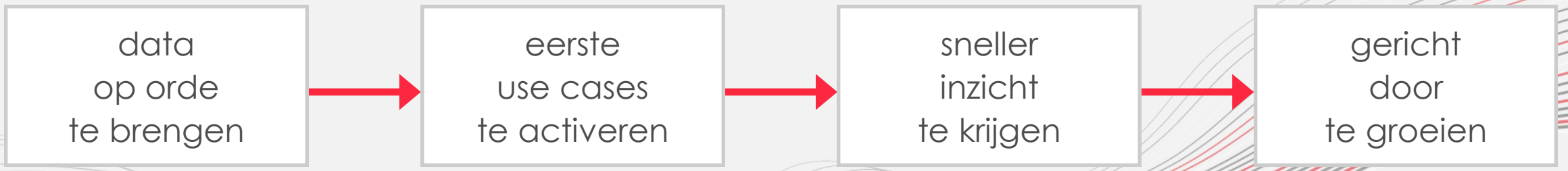
- basis nog niet op orde
- use cases nog niet scherp
- waarde nog niet zichtbaar

De behoefte aan een SIEM is vaak terecht, maar komt in de praktijk geregeld te vroeg op tooling uit. Terwijl de basis nog niet scherp is: welke data is relevant, wat wil je eigenlijk detecteren en onderzoeken en wat moet de omgeving straks kunnen dragen? Als je dat overslaat, wordt de stap naar een SIEM al snel een dure investering met beperkte opbrengst. SMT pakt dat anders aan. Niet door de wens vooreen SIEM kleiner te maken, maar door eerst te zorgen dat de route ernaartoe klopt. Daarmee wordt de investering beter onderbouwd en de kans groter dat het SIEM-platform straks ook echt doet wat het moet doen.

SMT
Data zonder gedoe

Niet sneller, wel slimmer naar een SIEM

Road to SIEM helpt om:



De kracht van onze aanpak zit in de volgorde. We trekken het gesprek weg van ‘welke tool kopen we?’ en brengen het terug naar ‘hoe zorgen we dat onze SIEM-aanpak straks echt werkt?’ Dat betekent: eerst de data die ertoe doet, dan de eerste use cases, dan meer inzicht en pas daarna verder opschalen. Zo blijft de route beheersbaar en wordt elke volgende stap beter onderbouwd. Het SIEM blijft dus nadrukkelijk het doel, maar wel op een manier die logisch is en die voorkomt dat er te vroeg te veel complexiteit wordt toegevoegd.

SMT
Data zonder gedoe

In drie stappen naar een werkende SIEM-aanpak

1. Basis op orde: data en eerste use cases
2. Verder uitbouwen: meer inzicht en meer context
3. Het SIEM opschalen: Enterprise Security en verrijking

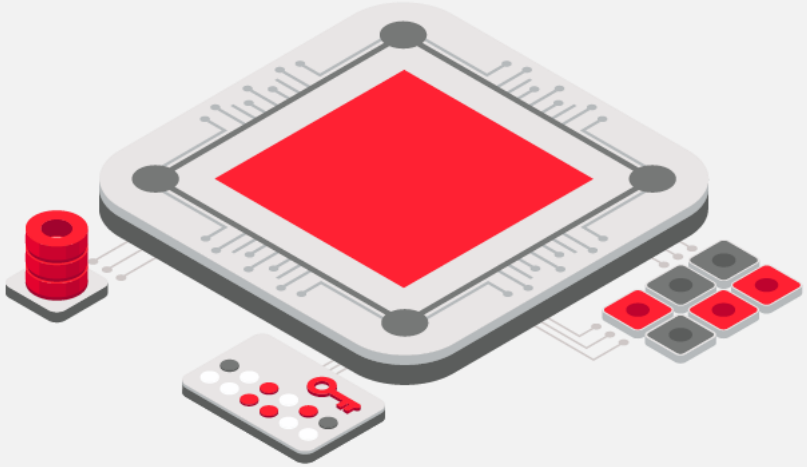
Road to SIEM is opgebouwd in drie duidelijke stappen. Eerst wil je de basis neerzetten, daarna ga je gericht verbreden en pas daarna wordt de stap naar zwaardere SIEM-functionaliteit logisch. Dat voorkomt dat je te vroeg te veel toevoegt en zorgt ervoor dat het SIEM-platform voortbouwt op een basis die al werkt. Het verhaal wordt daardoor technisch en inhoudelijk beter. Je maakt de route overzichtelijker, concreter en beter uitlegbaar aan klanten die wel weten dat een SIEM belangrijk is, maar niet precies weten hoe ze daar verstandig moeten komen.

SMT
Data zonder gedoe

Stap 1:
de juiste basis voor een SIEM

Focus op:

- waardevolle basisdata
- gebruikersactiviteit
- toegangscontrole
- wachtwoordbeheer
- eerste monitoring



In de eerste stap draait het om de data die direct nodig is om het SIEM-platform later goed te laten functioneren. De basis moet eerst staan. Dat houdt in dat niet alles in één keer wordt aangesloten, maar dat je begint met de data die snel inzicht geeft en direct relevant is voor security. Denk aan gebruikersactiviteit, toegangscontrole en wachtwoordbeheer. Dit is de fase waarin de eerste monitoring en eerste use cases werkend worden gemaakt. Daarmee leg je een fundament waarop later verder gebouwd kan worden, zonder dat de omgeving meteen onnodig zwaar of complex wordt.

SMT
Data zonder gedoe

Stap 2:
meer use cases, meer inzicht

In deze fase:

- meer use cases
- meer databronnen
- meer context
- zicht op kroonjuwelen
- meer awareness

Als de basis staat, kun je gericht verder bouwen. In deze fase voeg je extra databronnen toe, breid je use cases uit en krijg je scherper zicht op wat voor de organisatie echt belangrijk is. In de stukken wordt dat ook gekoppeld aan de kroonjuwelen van de organisatie: wat wil je echt beschermen, waar zit het grootste risico en welke signalen zijn dan het belangrijkst? Dat maakt de route naar een SIEM inhoudelijk sterker. Je bouwt dus niet breder om het breder bouwen, maar met meer grip op risico's, prioriteiten en context.

SMT
Data zonder gedoe

Stap 3:
klaar voor Enterprise Security

Wat ontstaat er nu?

- automatisering
- response
- threat intelligence
- risk intelligence
- user behaviour analytics

Pas in deze fase wordt de stap naar Enterprise Security echt logisch. Dan staat er al een basis, zijn use cases scherper en weet de organisatie beter wat relevant is. Daardoor wordt Enterprise Security geen te vroege investering, maar een gerichte versnelling. Dat is precies het verschil tussen zomaar naar een SIEM gaan en toewerken naar een SIEM-aanpak die echt iets oplevert. De geavanceerde laag krijgt daarmee ook een duidelijke plek: niet als startpunt, maar als vervolgstap op een platform dat al werkt.

SMT
Data zonder gedoe

Van eerste use cases naar een volledig SIEM-platform

Q1 basis operationeel

Q2 meer data en use cases

Q3-Q4 doorgroei naar volledig platform

Wat deze aanpak sterk maakt, is dat hij niet alleen logisch is, maar ook uitvoerbaar. In de stukken wordt de route gekoppeld aan een gefaseerde opbouw over het jaar: eerst de basis, daarna verdieping en daarna doorgroei naar een volledig functioneel SIEM-platform. Dat maakt Road to SIEM concreet. Voor klanten wordt zo zichtbaar dat het niet gaat om een abstract model, maar om een route in duidelijke stappen, met voortgang die ook in de tijd te volgen is.

SMT
Data zonder gedoe

Van implementatie naar run, improve en grow

Road to SIEM stopt niet na livegang.

- Run - beheer en continuïteit
- Improve - optimaliseren
- Grow - uitbreiden en doorontwikkelen

Een belangrijk onderdeel van de propositie is dat Road to SIEM niet ophoudt na de implementatie. Daarna begint juist het stuk waarin je zorgt dat de omgeving blijft draaien, dat use cases worden aangescherpt en dat de klant verder kan doorgroeien. Daarom hebben wij een 'Managed by SMT'- oplossing die ervoor zorgt dat het platform ook na de eerste implementatie optimaal blijft draaien. Wij zorgen ervoor dat het platform kan meebewegen met de organisatie. We ontwikkelen door op basis van nieuwe behoeften, nieuwe use cases en verdere groei.

SMT
Data zonder gedoe

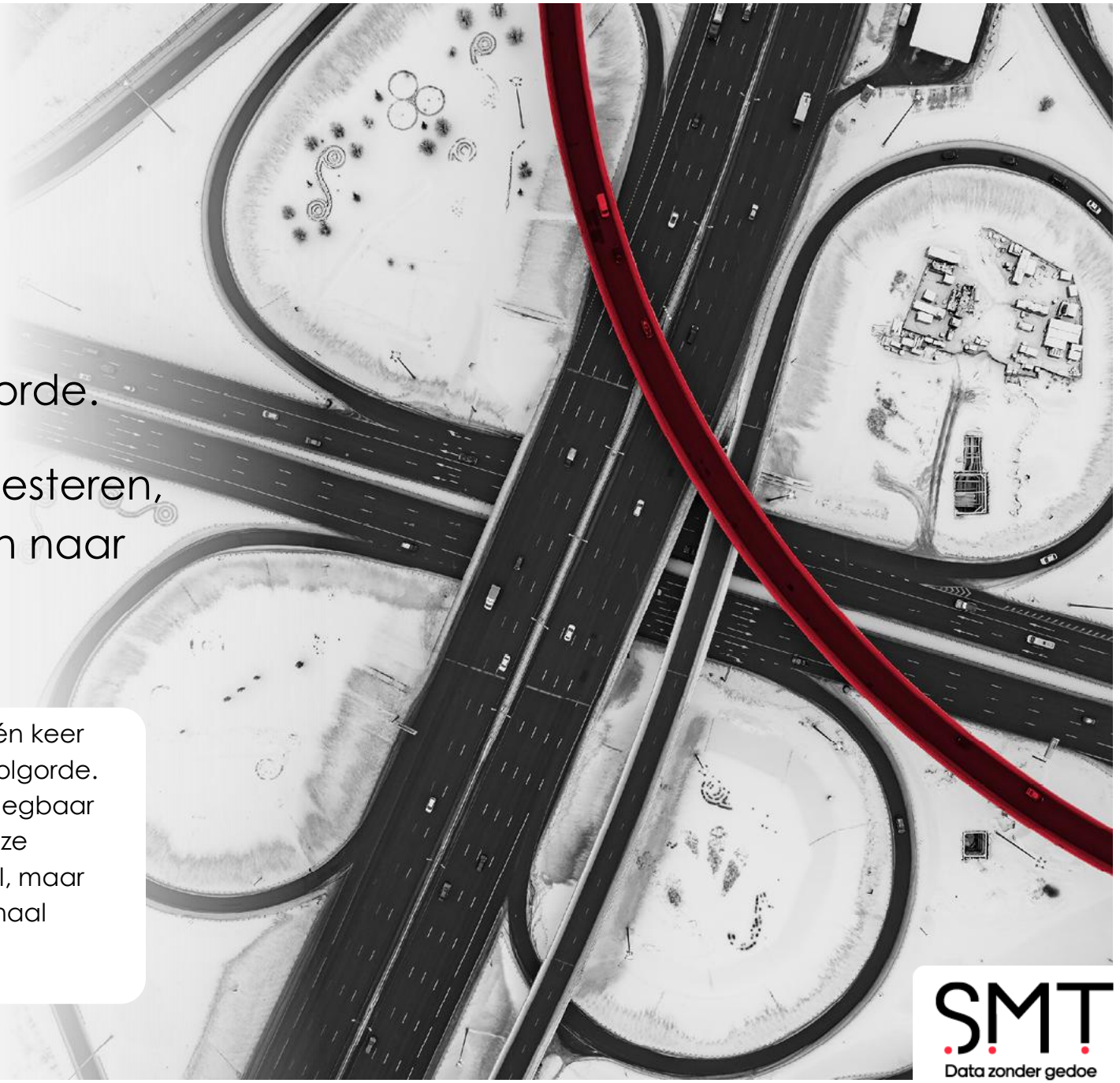
Road to SIEM houdt de route beheersbaar

Niet alles tegelijk.

Wel de juiste stappen in de juiste volgorde.

Zo helpt SMT klanten om gericht te investeren, meer grip te krijgen en door te groeien naar een SIEM-platform dat werkt.

De kern van Road to SIEM is beheersbaarheid. Niet alles in één keer willen, maar zorgen dat je de juiste stappen zet in de juiste volgorde. Daardoor wordt de route naar een SIEM concreter, beter uitlegbaar en beter vol te houden. En precies daar zit de kracht van deze propositie: klanten krijgen niet alleen een technisch einddoel, maar een route om daar verstandig te komen. Dat maakt het verhaal sterker, geloofwaardiger en beter toepasbaar in de praktijk.



SMT
Data zonder gedoe