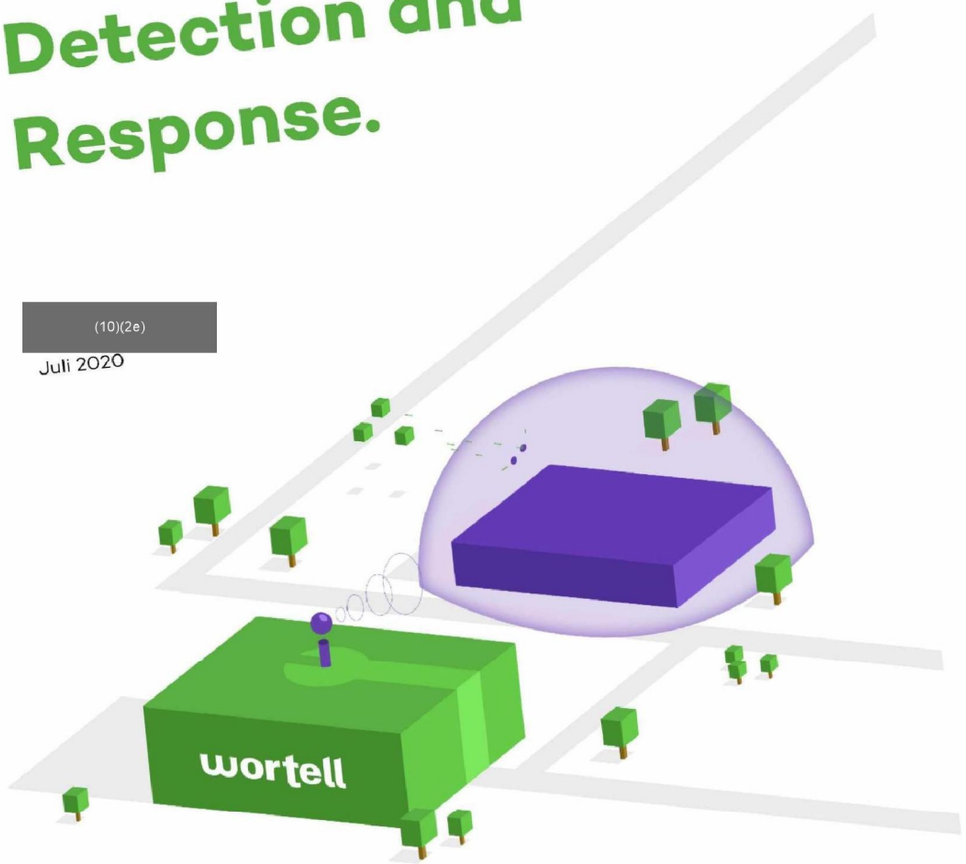
Ministerie van Volksgezondheid,
Welzijn en Sport

Managed Detection and Response.

(10)(2e)

Juli 2020



Samenvatting.

Het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) ontwikkelt op dit moment de landelijke COVID-19 app voor Android en iOS. De backend hiervan zal gehost worden bij de Belastingdienst in een Microsoft Azure omgeving. Voor deze Azure omgeving is 24x7 security monitoring nodig opdat onregelmatigheden danwel (poging tot) cyberinbraak kunnen worden gesignaleerd.

Wortell Enterprise Security biedt een 24x7 Managed Detection & Response (MDR) dienst voor Azure omgevingen vanuit haar Security Operations Center (SOC) in Gouda. Deze is gebaseerd op Azure Sentinel en sluit derhalve goed aan op cloud-native omgevingen.

VWS heeft Wortell Enterprise Security gevraagd te helpen met de inrichting van Azure Sentinel voor de COVID-19 app backend inclusief Use Cases (detectie logica) voor de verschillende onderdelen.

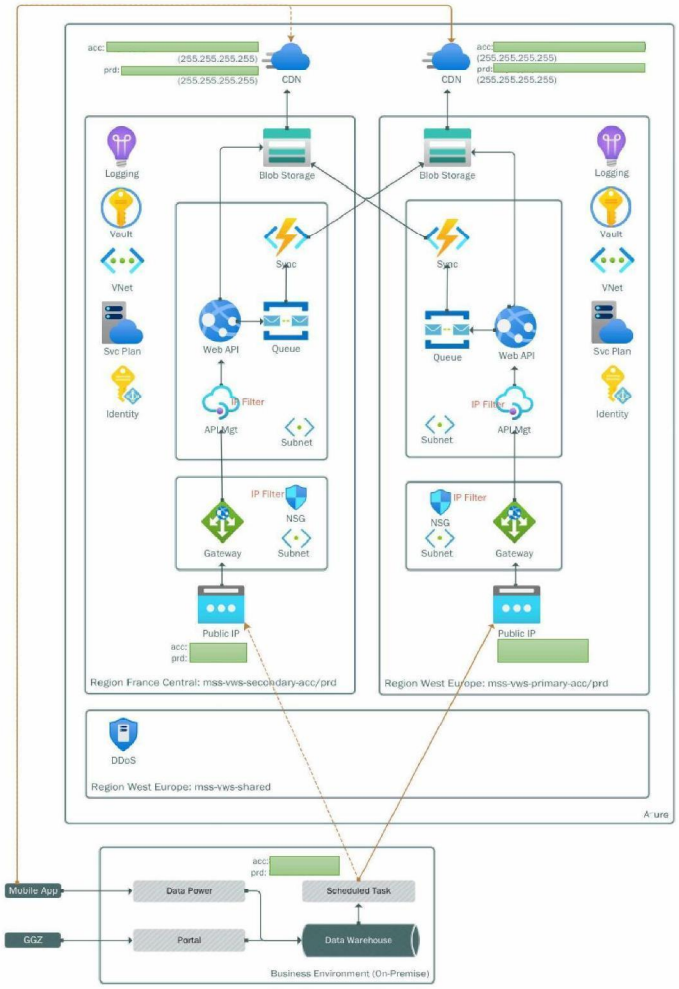
Voor de 'acceptatie' omgeving heeft Wortell Enterprise Security inmiddels de werkzaamheden aangevangen, waarbij Azure Sentinel inmiddels ingericht is en wordt er samengewerkt om Use Cases actief te maken. Deze offerte spitst zich toe op de 'productie' omgeving en de werkzaamheden en bewaking die daar benodigd zijn.

VWS heeft daarbij duidelijk gemaakt dat uiterlijk 3 augustus de werkzaamheden (voor onboarding en actief maken Azure Sentinel en Use Cases) afgerond dienen te zien, en de 24x7 monitoring aangevangen moeten zijn. Op verzoek van VWS heeft Wortell Enterprise Security de opzegtermijn verkort naar 1 maand, zodat ze keuzes kan maken om de oplossing te bestendigen of juist flexibel te beëindigen wanneer nodig.

Wortell Enterprise Security ziet er naar uit om VWS te ondersteunen en een bijdrage te mogen leveren in de lancering van deze belangrijke app voor de volksgezondheid.

COVID-19 APP.

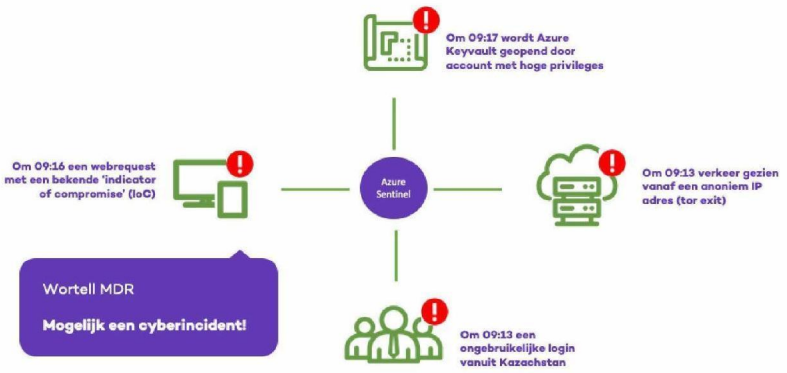
Op dit moment ontwikkelt VWS de landelijke COVID-19 app. Daarbij wordt een backend ontwikkelt op basis van Microsoft Azure die er grofweg alsvolgt uit ziet:



MANAGED DETECTION AND RESPONSE.

Managed Detection and Response is een Wortell Enterprise Security dienst welke (sommige) cyberdreigingen kan detecteren en indien nodig daar opvolging aan kan geven. Het detecteren en reageren gebeurt op 24x7 basis vanuit het Wortell Cyber Defense Center (CDC) in Gouda.

Indicatoren vanuit, maar niet beperkt tot, Microsoft security producten worden gecombineerd tot Use Cases. Deze meldingen en incidenten worden door het Managed Detection and Response team opgevolgd. Hieronder een voorbeeld van een Use Case:

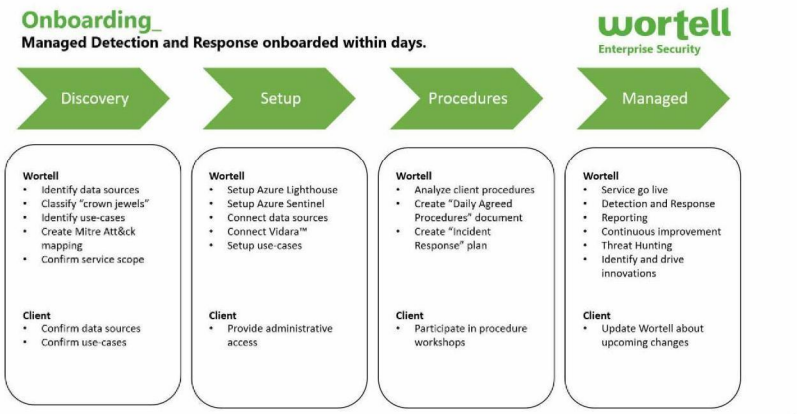


Verschillende logbronnen brengen gegevens naar Azure Sentinel, een cloud-native SIEM, die de individuele meldingen (events) combineert tot een integraal overzicht (incident), waarop het Wortell MDR team reageert.

AANSLUITEN.

Het leveren van de MDR dienst begint met het installeren en configureren van Azure Sentinel inclusief de juiste logbronnen. Omdat we gebruik maken van de bestaande Microsoft Azure omgeving kan dat eenvoudig en vlot. Een bijkomend voordeel daarvan is dat de data bij VWS cq de Belastingdienst blijft.

Daarnaast worden afspraken en processen vormgegeven. Dit doen we volgens een bewezen aanpak waarvan de stappen en activiteiten in onderstaande afbeelding zijn beschreven:



Zodra de activiteiten van de aansluitfase (Discovery, Setup, Procedures) zijn afgerond begint de "Managed" fase. Vanaf dat moment is de Service Level Agreement actief en worden incidenten conform verwachting opgevolgd.

INVESTERING.

Op basis van voorgaande komen we tot de volgende prijsstelling:

	Aantal	Stukprijs	Totaal
Managed Detection and Response.			
• Vidara™ Gold (24x7)	1	€ (10)(1c)	€ (10)(1c)
• Microsoft Azure			
○ Microsoft Azure Sentinel	1	€ (10)(1c)	€ (10)(1c)
○ Logbronnen	10	€ (10)(1c)	€ (10)(1c)
▪ Microsoft Azure CDN			
▪ Microsoft Azure Active Directory			
▪ Microsoft Azure DDOS protection			
▪ Microsoft Azure Log Analytics			
▪ Microsoft Azure Networking			
▪ Microsoft Azure Key Vault			
▪ Microsoft Azure Blob Storage			
▪ Microsoft Azure Event Hubs			
▪ Microsoft Azure Functions			
▪ Microsoft Azure API			
Maandelijkse kosten			€ (10)(1c)

De scope van deze prijsopgave is de productie omgeving van de COVID-19 app zoals beschreven op pagina 2.

Om bovenstaande dienstverlening te kunnen leveren is een eenmalige investering nodig voor het koppelen en configureren van de omgeving. Dit noemen wij aansluitkosten. De aansluitkosten zijn als volgt:

	Dagen	Stukprijs	Totaal
Aansluitkosten.			
• Klantomgeving aansluiten op MDR dienst	2	€ (10)(1c)	€ (10)(1c)
• Incident Response plan en procedures vaststellen	2	€ (10)(1c)	€ (10)(1c)
• Connecteren logbronnen	3	€ (10)(1c)	€ (10)(1c)
• Ontwikkelen Use Cases	7	€ (10)(1c)	€ (10)(1c)
Eenmalige aansluitkosten			€ (10)(1c)

Daarnaast is er een zogenaamde strippenkaart (retainer) nodig, opdat er direct uren beschikbaar zijn indien er opvolging (incident response) moet plaatsvinden. De kosten hiervoor zijn als volgt:

	Stuks	Stukprijs	Totaal
Incident Response.			
• Strippenkaart (retainer), saldo van 100 uur	1	€ (10)(1c)	€ (10)(1c)
			€ (10)(1c)

#WeKnowSecurity

Wortell Enterprise Security heeft als missie: "Bouwen aan een veiligere wereld, één bedrijf tegelijk". We focussen ons dan ook helemaal op Cloud & Security, met specialisatie op Microsoft technologie.

Wortell is een 100% Nederlands bedrijf, dat full-service veiligheid voor de Microsoft cloud biedt. Van advisering tot trainingen, van eigen software tot managed services. Met onze branche kennis van de (centrale en decentrale) overheid, de (financiële) dienstverleners en vele andere industrieën, maken we het verschil.

Microsoft Partner
Microsoft
Gold Cloud Platform
Gold Datacenter
Gold DevOps

Microsoft Regional Director

MVP Microsoft Most Valuable Professional

C|EH Certified Ethical Hacker

We hebben meerdere Microsoft Most Value Professionals (MVP), een Microsoft Regional Director (RD), een Certified Ethical Hacker (CEH) en nog vele andere collega's met diepgaande Microsoft (security) kennis en ervaring in dienst. Onze 20+ collega's staan voor u klaar.

Ook is Wortell maast liefst 10 keer Microsoft Gold Partner, en zijn we recent onderscheiden met de Azure Management Elite status; een kroon op ons werk rondom het veilig inrichten en veilig houden van (bedrijf kritische) Azure omgevingen.

En uiteraard hebben we ook de ISO 27001, ISAE 3402 en NEN 7510 certificeringen!

De kleine lettertjes.

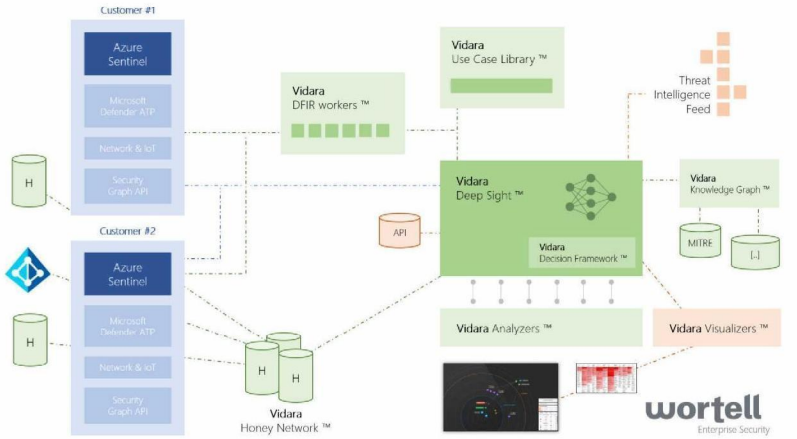
We zijn graag duidelijk over wat we met elkaar afspreken. Niets is zo vervelend als er achteraf discussie over krijgen. Daarom vatten we de belangrijkste zaken samen:

- *Deze opdracht wordt aangenomen door Wortell Enterprise Security B.V.; ons KvK nummer is 75218321.*
- *Op deze opdracht zijn onze algemene voorwaarden van toepassing; op verzoek sturen we u kosteloos een (digitaal) exemplaar toe.*
- *We benadrukken dat Wortell Enterprise Security BV niet aansprakelijk kan worden gesteld voor (directe of indirecte) schade als gevolg van een (cybersecurity) incident of aanval.*
- *Ministerie VWS gaat een samenwerking aan met Wortell waarbij Wortell het security beheer voor haar rekening neemt. Er is geen 100% garantie dat Wortell alle aanvallen (zowel intern als extern) kan voorkomen.*
- *De MDR (monitoring en detectie) dienst kost €* (10)(1c) *exclusief BTW per maand. Kosten voor incident opvolging, use case uitbreiding of ander werk cq wordt apart in rekening gebracht, het tarief hiervoor is €* (10)(1c) *exclusief BTW per uur.*
- *Ministerie VWS kan deze overeenkomst telkens per einde kalendermaand opzeggen. Dertig dagen daarna eindigt de dienst. Wordt deze niet opgezegd, dan loopt deze automatisch door.*
- *We sturen altijd een factuur op de 1e dag van de maand en brengen dan de kosten van de afgelopen maand in rekening; deze dient binnen 30 dagen na factuurdatum bij ons op de rekening te staan.*

Akkoord,	Akkoord,
Ministerie VWS	**Wortell Enterprise Security B.V.**
_____	Danny Burlage — *CEO*
	Maarten Goet — *CTO*
Datum:	

Appendix: Vidara™

Vidara™ is een platform ontwikkeld door Wortell en wordt ingezet om de Managed Detection and Response dienst te kunnen leveren op basis van Azure Sentinel, en deze tevens functioneel aan te vullen met additionele features:



Een architecturaal overzicht van Vidara™

Vidara™ Deep Sight

Vidara™ Deep Sight is de kern van het Vidara™ platform en zorgt voor de integratie met de Azure Sentinel omgeving van de Opdrachtgever. Vidara™ maakt het voor Wortell mogelijk om op incidenten en meldingen te reageren. Daarnaast biedt Vidara™ de mogelijkheid voor centraal beheer en het genereren van rapportage van klantomgevingen.

Het Decision Framework ™ zorgt er voor dat incidenten geclassificeerd kunnen worden aan de hand van de door Wortell getrainde modellen en gekoppelde bronnen.

Vidara™ DFIR Workers

DFIR staat voor "Digital Forensics & Incident Response" en wordt ingezet voor het identificeren, onderzoeken en mitigeren van schade als gevolg van een cybersecurity aanval.

Vidara™ DFIR Workers beperkt zich tot de technische middelen welke worden ingezet voor het forensisch onderzoek. Zoals de middelen welke nodig zijn om te kunnen "Threat Hunten" en het uitvoeren van triage op indicatoren. Het isoleren van een geïnfecteerde omgeving behoort ook tot de rol van de DFIR workers.

Vidara™ use-case Library

Individuele meldingen of bedreigingsinformatie is niet voldoende om een aanval goed te begrijpen. Het is belangrijk om zoveel mogelijk meldingen te correleren om tot de kern van de aanval te komen en te begrijpen hoe een aanval zicht heeft ontwikkeld. Het correleren van verschillende systemen om tot een mogelijke situatie te komen noemen we "use-cases".

De Vidara™ use-case Library is een verzameling van vooraf gedefinieerde use-cases voor bekende kwetsbaarheden en aanvallen. Daarnaast worden klantspecifieke use-cases bewaard in de use-case library en gedeeld met alle andere klanten van de Managed Detection and Response dienst bij Wortell. Zo profiteert elke klant van de Managed Detection and Response dienst van elkaars investeringen en bouwen we samen aan een veiligere omgeving.

Vidara™ Knowledge Graph

De Vidara™ Knowledge Graph maakt het mogelijk te integreren met externe databronnen zoals het "MITRE ATT&CK framework". Door incidenten te koppelen aan het MITRE ATT&CK framework wordt het process van de aanval inzichtelijk gemaakt. Door de technieken en methodes van de aanval te begrijpen kan een juiste reactie worden gegeven en eventuele vervolgschade worden voorkomen.

Vidara™ Honey Network

Het Vidara™ Honey Network bestaat uit applicaties en/of apparaten om organisatiespecifieke bedreigingsinformatie te verzamelen. Deze bedreigingsinformatie kan worden gebruikt om gerichte beveiliging toe te passen. Daarnaast geeft de informatie inzicht in het soort aanvallen waar organisaties mee geconfronteerd worden en de data waar hackers op uit zijn.

Vidara™ Dashboards

Bedreigingsinformatie en beveiligingsincidenten welke zijn gedetecteerd en geregistreerd in Vidara™ zijn zichtbaar in de Vidara™ dashboards. Deze dashboards worden door de Wortell security experts gebruikt maar zijn ook toegankelijk voor de klant. De status van incidenten en de relatie tot de Service Level Agreement worden in het dashboard getoond. Deze informatie kan worden geëxporteerd naar (management)rapportages.

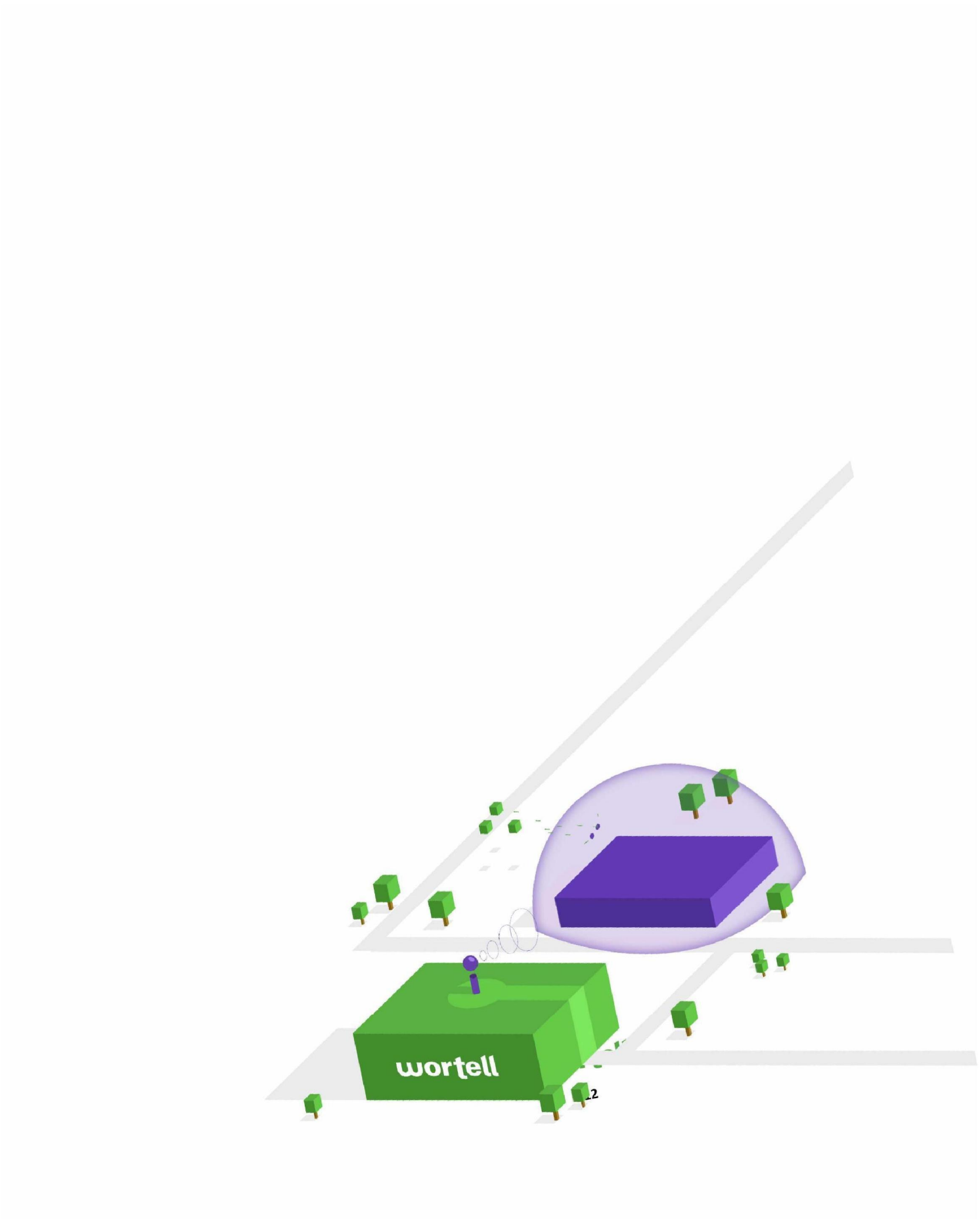
Vidara™ Threat Hunting

Threat Hunting is het pro-actief zoeken naar dreigingen welke niet zijn gedetecteerd door de detectieproducten. Threat Hunting is een door mensen geleid process als aanvulling op de bestaande detectie en reactie middelen. Risico's worden geïdentificeerd, verstoord en gemitigeerd bij detectie van actieve dreigingen.

Vidara™ Incident Response Plan

Beveiligingsincidenten zijn geen technisch probleem zijn maar een bedrijfsprobleem. Een Incident Response Plan is een set van instructies om een organisatie te ondersteunen bij de reactie op beveiligingsincidenten. Het plan beschrijft scenario's voor problemen zoals dreigingen, datalekken en onbeschikbaarheid van bedrijfskritische applicaties.

Hoe een organisatie reageert op een incident heeft een enorme impact op de uiteindelijke schade van een beveiligingsincident. In sommige gevallen, wordt schade als gevolg van een beveiligingsincident, niet gedekt door verzekeraars omdat bepaalde procedures niet gevolgd zijn.


wortell