Stay connected.
Stay safe.

Jaarverslag 2024 Skyleaf

CYBERWOLF
your digital bodyguard

spotit
YOUR SECURITY & NETWORK LAYER

Connecting you.

Het eerste jaarrapport van Skyleaf: een terugblik vol vertrouwen, een vooruitblik vol ambitie.

Sinds 2014 al werken we met passie en ambitie aan onze missie: mensen, bedrijven en machines met elkaar verbinden, steeds met een grote focus op veiligheid. Het is met spotit nooit ons doel geweest om de grootste te zijn in cybersecurity & networking, maar wel om de beste te zijn. Intussen is ons aanbod uitgebreid met Cyberwolf, een soort 24/7 digitale bodyguard van het privéleven. Beide bedrijven maken deel uit van de Skyleaf-holding.

In beide bedrijven werken we met topmensen, innovatieve technologieën en diensten die perfect aansluiten bij de behoeften van onze klanten. Stuk voor stuk zijn dat ondernemingen en organisaties die beseffen hoe essentieel het is om te investeren in kwaliteitsvolle oplossingen voor cybersecurity en netwerken. We gaan volop voor duurzame partnerships. We zien onszelf niet als een traditionele leverancier, maar als een echt verlengstuk van uw bedrijf of IT-afdeling. Iemand op wie u 200% kunt vertrouwen.

In ons allereerste jaarrapport van Skyleaf blikken we terug op 2024. We geven een overzicht van onze highlights, bundelen boeiende cijfers, zoomen in op ons vernieuwde Security Incident Response aanbod en geven tips voor uw cyberveiligheid.

Bedankt voor uw vertrouwen! We kijken ernaar uit om samen met u de volgende hoofdstukken van ons verhaal te schrijven - of dat nu met spotit is of met Cyberwolf. In een wereld waarin connectiviteit en beveiliging steeds belangrijker worden, kijken we alvast optimistisch naar de toekomst.

Steven Vynckier en Frederik Rasschaert,
Oprichters spotit en Cyberwolf

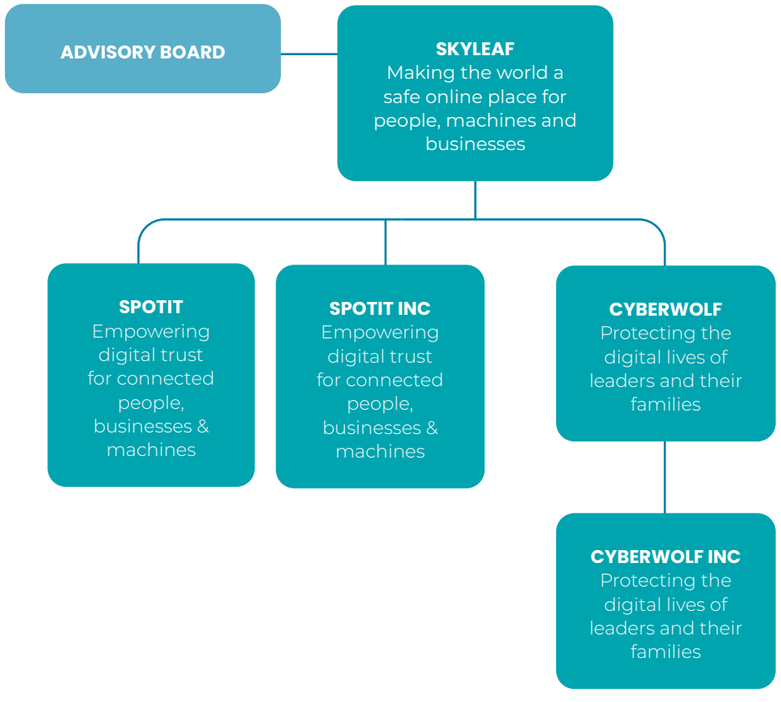
Protecting you.

Wie we zijn

Wie is **Skyleaf**?

Ons bedrijf werkt met een holdingstructuur, wat betekent dat er een moedermaatschappij (holding) is die toezicht houdt op verschillende entiteiten. De holding heet Skyleaf, met spotit en Cyberwolf als entiteiten.

Skyleaf heeft als duidelijke en belangrijke missie: de wereld een veilige online plek maken voor mensen, machines en bedrijven. In de onderling verbonden wereld van vandaag, waar digitale bedreigingen voortdurend in ontwikkeling zijn, streeft Skyleaf naar een veilige omgeving voor individuen en organisaties.



Wie is **Cyberwolf**?

Cyberwolf is een 24/7 digitale bodyguard voor het privéleven van VIPs, zoals C-suite, bestuurders, ministers, diplomaten en vermogende families wereldwijd. Net als spotit doet bij bedrijven, beschermen we toestellen, data, e-mail en accounts, monitoren we dreigingen, volgen we dark web-activiteiten en grijpen we in bij incidenten. Zo goed dat één van de grootste Amerikaanse banken ons tegenwoordig introduceert bij de meest vermogende families in zijn portfolio. We're only getting started!

Wie is **spotit**?

Onze missie
We creëren voor u peace of mind voor alles wat te maken heeft met beveiliging en connectiviteit. Als strategische partner zetten we sterk in op visie, expertise en vertrouwen.

Onze belofte
We maken het verschil met een high-level security- en netwerkaanpak op lange termijn. Uw security en netwerk zijn nu eenmaal een essentieel onderdeel van uw bedrijfsstrategie. Daarom vertrekken we van een actieplan met concrete doelstellingen. Naast standaardoplossingen (zoals switches, routers, firewalls en antivirussoftware), integreren we daarin ook high-tech kennis, 24/7 managed services, een projectaanpak en glasheldere rapportering.

Spotit in het kort

- Bouwt en beheert cybersecurity- en netwerkstrategieën
- Levert diensten in 80 landen op 5 continenten
- Heeft kantoren in Merelbeke, Herk-de-Stad en New York
- De groep (spotit en Cyberwolf) draaide 30 miljoen euro omzet in 2024 en telt 135 medewerkers
- Focust op bedrijven vanaf 150 medewerkers
- Is actief in alle sectoren met toonaangevende referenties in utilities, industrie, logistiek, farmatech en life sciences
- Oprichters Steven en Frederik hebben nog steeds alle aandelen in handen

Onze waarden

Trust

Vertrouwen is essentieel, en al zeker in cybersecurity. Logisch dus dat we extreem zorgvuldig omgaan met gevoelige gegevens, ons volledig bewust van het feit dat elke inbreuk ernstige gevolgen kan hebben. Ons geloof in vertrouwelijkheid, integriteit, betrouwbaarheid en eerlijkheid uit zich ook in het feit dat we leveren wat we beloven, dat we leren van fouten en dat we feedback ter harte nemen.

Human to Human

Bij spotit bouwen we aan échte connecties. We geloven dat mensen niet zomaar producten of oplossingen kopen, maar dat ze ook (willen) verbinden met anderen. Daarom plaatsen wij collega's, klanten, partners, ... centraal in elke interactie. Uitdagingen pakken we samen aan, met open communicatie en wederzijds respect. Elke dag werken we eraan om van ons bedrijf een betere versie van zichzelf te maken, met communicatie en respect als fundament.

Excel

Om onze klanten maximaal gelukkig te maken, willen we uitblinken. We streven naar topprestaties en nemen geen genoegen met middelmatigheid. Samen tillen we elkaar naar een hoger niveau. We blijven onszelf ook uitdagen om te verbeteren. Want excelleren is niet enkel een resultaat; het is een mentaliteit.

Entrepreneurship

Iedereen die bij ons werkt heeft een ondernemende ingesteldheid. Onze teamleden krijgen vrijheid en nemen verantwoordelijkheid. Ze handelen snel bij uitdagingen, nemen initiatief en werken samen aan oplossingen, ook als dat buiten hun comfortzone is. Samen gaan ze 'the extra mile' – en dat voelt u als klant.

We vierden onze 10de verjaardag

We pakten in 2024 uit met ons 10-jarig bestaan. We haalden heel wat pers en vierden natuurlijk ook feest. Op 8 juni kwamen medewerkers en partners samen in de idyllische Hottentothoeve in Bonheiden. De avond stond in het teken van 'back to the future' – van de uitnodiging en poster, tot de decoraties, drankjes en het cadeau. Er werd tot laat in de nacht gedanst...

10

Het 2024 van Skyleaf

50+

Fier op onze NPS-score van 50+

Zou u spotit aanraden aan een collega of vriend? Dat is de kernvraag die we elk jaar opnieuw stellen aan onze klanten, via een uitgebreid Net Promoter Score-onderzoek door een externe partij. We willen op die manier dieper inzicht te krijgen in wat klanten echt denken over onze dienstverlening en verbeterpunten identificeren. In 2024 haalden we een knappe NPS-score van 51. Onze klanten noemden specifiek onze expertise, klantgerichtheid en betrouwbaarheid als kernsterktes.

x3

Cyberwolf groeit discreet verder en verdriedubbelde in 2024 in aantal leden.

Nieuwe talent recruitment website

De kwaliteit van onze dienstverlening staat of valt met ons team – daar zijn we ons van bewust. Om de kans op een perfecte match te vergroten, moeten we bij potentiële medewerkers natuurlijk een goed beeld scheppen van wie we zijn. Daarom lanceerden we in 2024 een gloednieuwe talent recruitment website. Op jobs.spotit.be vinden mogelijke sollicitanten de openstaande vacatures, maar ook achtergrondinfo over het bedrijf, onze Academy en ons wellbeingprogramma.

200.000

Zoveel schonken we de laatste 10 jaar al aan goede doelen. In 2024 doneerden we 10.000 euro aan de Zelfmoordlijn. Giving back to the community vinden we heel belangrijk.

10 bijkomende toptalenten

In 2024 verwelkomde spotit maar liefst 10 nieuwe collega's. Elk van hen versterkt ons engagement om klanten nog beter te bedienen – van presales tot facturatie. Met deze gerichte aanwervingen blijven we bouwen aan een excellente, persoonlijke service op elk contactpunt.

“Reddingslijn in geval van een cyberaanval”

HOTLINE

+32 (0)9 322 04 35

In 2024 breidden we de dienstverlening van ons Cyber Security Incident Response Team uit. Een hack, inbreuk, malware-infectie of andere cyberbeveiligingsbedreiging? Onze experts begeleiden u om uw organisatie zo snel mogelijk weer operationeel te maken, met minimale impact.

WE VERNIEUWDEN HET AANBOD VAN HET CYBER SECURITY INCIDENT RESPONSE TEAM

Vandaag krijgt meer dan 1 op de 8 Vlaamse ondernemingen te maken met een cyberincident. En uit een bevraging blijkt dat 39 procent van de Belgische bedrijven verwacht in het komende jaar slachtoffer te worden van een cyberaanval. Investeren in CSIRT is niet langer een ‘nice to have’ maar een absolute ‘must have’. Een cybersecurity-incident kan op gelijk welk moment plaatsvinden. Of het nu gaat om een cybercrimineel die via een succesvolle ransomware-aanval bitcoins opeist of om incidenten met (inter) nationale impact, onze emergency service garandeert een snelle reactie om de schade zo veel mogelijk te beperken.

Onze hotline is 24/7 bereikbaar. U komt er terecht bij een spotit incident responder die meteen de situatie evalueert en de impact in kaart brengt. Zo kan hij snel concrete actionable items adviseren om te anticiperen en meer schade te vermijden. Tegelijkertijd stellen we een multidisciplinair team samen met stakeholders van uw bedrijf én van spotit. Het team gaat het incident inperken, de hacker uit het netwerk verwijderen, en tijdens de recovery fase de omgeving op een veilige manier weer opstarten, zodat u verder kan focussen op business continuity.

Proactieve dienstverlening

Bij ons stopt het niet bij reactieve hulp na een incident. We bieden ook proactieve ondersteuning: we monitoren uw netwerk en grijpen in bij de eerste tekenen van verdachte activiteit. Hoe sneller we kunnen handelen, hoe groter de kans op een succesvolle aanpak. Daarom is een goede voorbereiding cruciaal. Met onze retainer service staan onze experts permanent paraat, kennen ze uw IT-omgeving door en door en kunnen ze meteen doeltreffend ingrijpen wanneer het nodig is.
Tijdens de onboarding wordt alle benodigde informatie verzameld over processen, de omgeving, rollen en verantwoordelijkheden. Daarna volgt een ‘Breach Readiness Assessment’. U krijgt zo een duidelijk zicht op de mogelijkheid van uw organisatie om cybersecurity-incidenten te identificeren, te onderzoeken, en erop te antwoorden. We installeren daarna een ‘honeypot warning system’ dat potentieel kwaadaardige activiteiten vroegtijdig detecteert, waardoor er snel op bedreigingen gereageerd kan worden. Deze service zorgt er ook voor dat alle relevante gegevens voor alle betrokken experts up-to-date worden gehouden. Een toegewijde servicemanager zal regelmatig updatevergaderingen plannen, gegevens en ‘lessons learned’ met u delen.

6 redenen waarom CSIRT een must is

1. **Onmiddellijke reactie:** een cyberaanval is als een medisch noodgeval voor uw organisatie. CSIRT biedt – net als artsen – onmiddellijke expertise wanneer u het meest kwetsbaar bent. CSIRT-teams zijn getraind om snel en efficiënt te reageren, waardoor de impact van de aanval wordt beperkt en de normale bedrijfsvoering zo snel mogelijk kan worden hervat.

2. **Expertise en specialisatie:** CSIRTs zijn de gespecialiseerde ‘artsen’ in de wereld van cybersecurity. Ze beschikken over de expertise die nodig is om de specifieke bedreigingen die uw bedrijf tegenkomt te diagnosticeren en te behandelen. Het team gebruikt geavanceerde tools en technieken om de bron van de aanval te identificeren, de schade te beoordelen en de meest effectieve strategie voor herstel te implementeren.

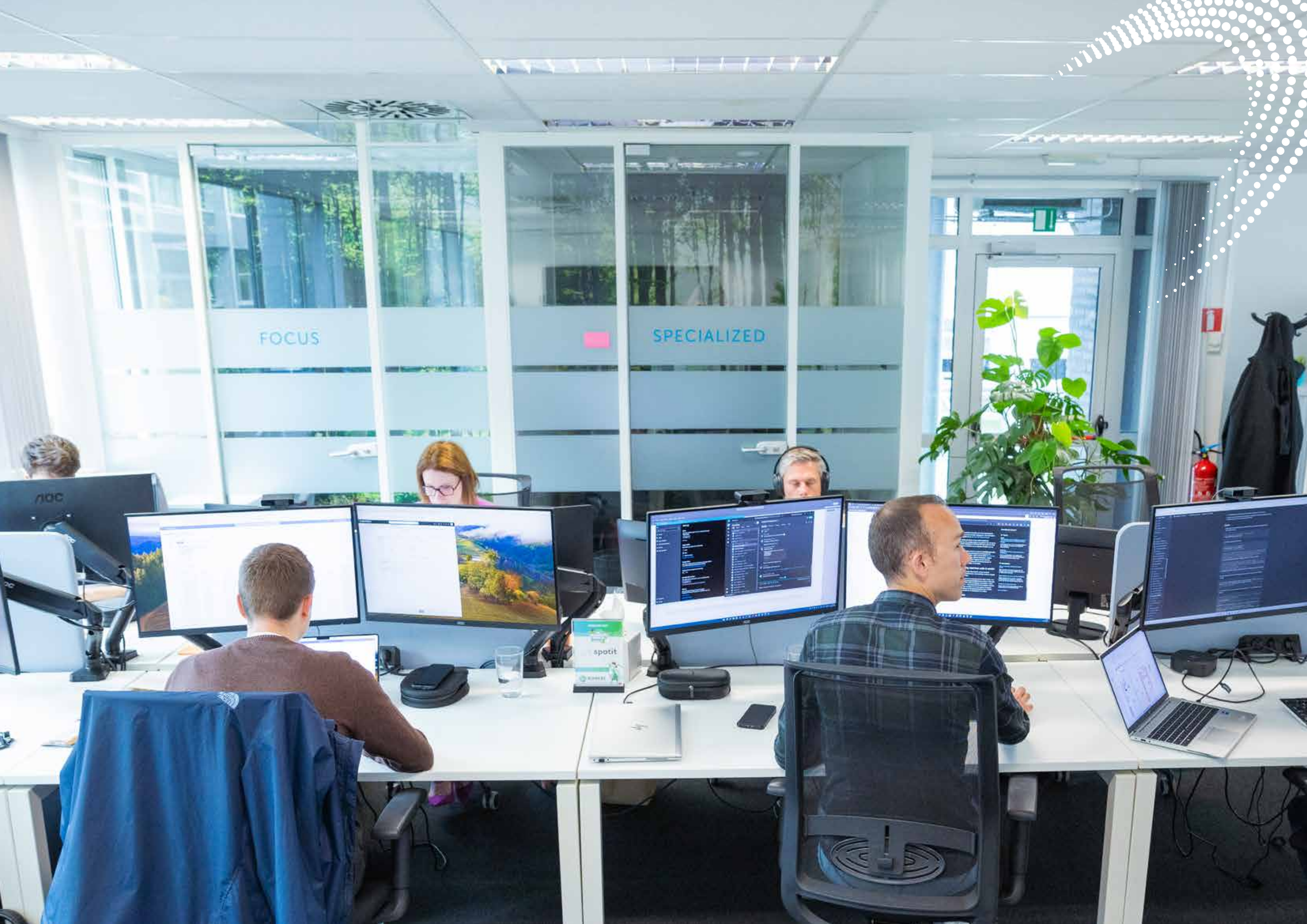
3. **Kostenbesparing:** hoewel het paradoxaal kan lijken, kan het inschakelen van een CSIRT leiden tot significante kostenbesparingen. Incidenten zoals datalekken en systeeminbraken kunnen enorme financiële lasten met zich meebrengen. Een CSIRT vermindert de risico’s en de daarmee samenhangende kosten significant.

4. **Reactief én proactief:** een CSIRT werkt niet alleen reactief; het voert regelmatige controles en updates uit, waardoor veel aanvallen voorkomen kunnen worden. Die proactieve houding kan aanzienlijke kosten besparen en de continuïteit van uw bedrijf beschermen.

5. **Compliance:** de regelgeving rondom data en privacy wordt steeds strenger. Een CSIRT zorgt ervoor dat uw organisatie voldoet aan relevante wetten en normen, wat niet alleen boetes voorkomt, maar ook het vertrouwen van klanten en partners versterkt.

6. **Gemoedsrust:** weten dat er een expertenteam klaarstaat om in te grijpen, geeft rust. Weten dat de cybersecurity in handen is van professionals, stelt u en uw medewerkers in staat om zich te focussen op de kernactiviteiten van uw bedrijf.

FAQ CSIRT


FOCUS
SPECIALIZED
spotit

CASE

Ransomware attack bij Santens

Santens is een technische groothandel in bouwbeslag en -gereedschappen gericht op vakspecialisten, zoals schrijnwerkers, aannemers, technische diensten en openbare besturen. Het bedrijf met hoofdkantoor in Merelbeke-Melle werd het slachtoffer van een ransomware aanval, waardoor zijn systemen enkele dagen onbeschikbaar waren. Ze riepen de hulp in van de CSIRT-service van spotit.

De avond voor een verlengd weekend werd Santens opgebeld door de federale politie om te melden dat accountgegevens van Santens te koop werden aangeboden op het dark web. Het nieuws was het begin van een cyberaanval-nachtmerrie.

Santens richtte meteen een crisiscel op met interne medewerkers en externe professionals om de impact op de dagelijkse activiteiten te beoordelen. Het managementteam nam snelle en duidelijke beslissingen. Spotit evalueerde onmiddellijk na de aanval de situatie en impact. Het CSIRT-team isoleerde de geïnfecteerde systemen en kon voorkomen dat de ransomware zich verder verspreidde. Spotit zorgde voor zorgvuldige begeleiding en diepgaand advies bij het heropstarten van de systemen en implementeren van extra cybersecuritymaatregelen.

Dankzij de goede back-upsystemen die niet geïmpacteerd waren, slaagde Santens erin de schade te beperken en na een week al opnieuw op te starten. Santens tekende in op de Managed Detection & Response service met CSIRT inbegrepen. Spotit monitort nu actief de IT-omgeving op afwijkingen. Indien er toch een incident plaatsvindt, kan Santens rekenen op spotit-professionals om snel in te grijpen.

Voor de aanval leek een cyberattack eerder iets voor grote bedrijven. Door geconfronteerd te worden met een aanval en met andere bedrijven te praten, merkt Santens dat veel ondernemingen ermee in aanraking komen. Het bewustzijn voor cybersecurity staat nu hoog op de agenda. Santens zet volop in op actieve én blijvende bewustwording van de werknemers, zeker nu het verder blijft inzetten op digitalisering. Digitalisering en cybersecurity gaan hand in hand.

"De cyberaanval heeft het bedrijf een paar 100.000 euro gekost en de gederfde inkomsten lopen makkelijk op tot €2.000.000, een zeer zware impact voor een kmo zoals die van ons."

Bram Vande Walle, CEO Santens

10 TIPS

voor meer gemoedsrust in cybersecurity & networking

Zorg voor een sterke basis in beveiliging
Begin met een grondige beveiligingsaudit van je IT-omgeving. Identificeer kwetsbaarheden en los ze meteen op.

01

Implementeer multi-factor authenticatie (MFA)
Voeg een extra laag beveiliging toe door MFA te gebruiken voor toegang tot belangrijke systemen en applicaties.

06

Implementeer een zero trust-strategie
Vertrouw niemand binnen of buiten je netwerk zonder verificatie. Beperk toegang tot data en systemen tot enkel diegenen die het echt nodig hebben.

02

Gebruik een betrouwbare firewall en next-gen security-oplossingen
Bescherm je netwerk met geavanceerde firewalls en intrusion detection/preventionsystemen om ongewenste toegang te blokkeren.

07

Investeer in end-to-end encryptie
Bescherm gevoelige gegevens zowel in transit als in rust met sterke encryptieprotocollen.

03

Voer regelmatig penetratietests uit
Simuleer cyberaanvallen om te zien hoe goed je systemen bestand zijn tegen bedreigingen, en verbeter waar nodig.

08

Voer regelmatige updates en patch management uit
Zorg ervoor dat al je software, hardware en besturingssystemen up-to-date zijn met de laatste beveiligingspatches.

04

Monitor je netwerk 24/7
Gebruik een Security Operations Center (SOC) of geautomatiseerde tools om verdachte activiteiten en aanvallen in realtime te detecteren en te stoppen.

09

Bewustwording en training voor medewerkers
Medewerkers blijven de zwakste schakel in cybersecurity. Geef hen regelmatig training over phishing, social engineering en veilig online gedrag.

05

Stel een incident response plan op
Wees voorbereid op het ergste. Zorg voor een gedetailleerd plan dat beschrijft hoe je snel en efficiënt reageert op een beveiligingsincident.

10

Meer info? Contacteer ons!

“Onze drijfveer is helder: we willen de beste zijn”

Op 2 juni 2024 bestond spotit 10 jaar. In een decennium gebeurt natuurlijk heel wat – en al zéker in een sector als die van cybersecurity. Oprichters Steven Vynckier en Frederik Rasschaert, die nog steeds aan het hoofd staan van het bedrijf, blikten dan ook graag even terug én kijken vol goesting vooruit.

Hoe en waar is het voor jullie allemaal begonnen?
Steven: “We leerden elkaar kennen bij het IT-bedrijf waar we in dienst waren. Na een tijdje kwam Frederik in mijn team terecht en werkten we dus nauw samen. Het klikte en we beslisten om samen een eigen verhaal te schrijven. We hadden allebei het gevoel dat heel wat bedrijven die netwerk- en security-oplossingen aanboden compromissen sloten op het vlak van kwaliteit. Daarom was onze focus van in het begin: met goed opgeleide mensen topkwaliteit leveren en zo dé referentie worden op het vlak van connectivity en security.”
Frederik: “Een eigen zaak starten is natuurlijk wel een grote stap, maar het ondernemerschap zit ons in het bloed. Ik heb

“Dankzij onze aanpak beschouwen klanten ons niet als ‘gewoon een leverancier’, maar als echte partner en compagnon de route.”

me altijd graag verdiept in technologie, kreeg mijn interesse in IT mee van mijn vader, heb lang in de leiding van de jeugdbeweging gestaan en was sinds mijn 18de zelfstandige in bijberoep.”
Steven: “Mij is het ondernemerschap met de paplepel meegegeven. Mijn vader had een meubelbedrijf en mijn mama stond in de winkel. Ik heb van hen altijd veel vrijheid en autonomie gekregen. Tijdens mijn jeugd zat ik in de scouts en beoefende ik op een vrij hoog niveau atletiek. Dat typeert wel wat wie wij zijn.”

Hoe liep dat in het begin?
Steven: “We wilden niet de zoveelste – excuseer me voor de formulering – hardware-, software- en licentieboer zijn: vanaf dag één kozen we er expliciet voor een managed servicebedrijf te zijn. We starten een samenwerking altijd met een assessment van de bestaande situatie, bekijken wat beter kan, tekenen de visie uit en staan in voor de implementatie en het operationele beheer.”
Frederik: “We moesten niet van nul beginnen, want we hadden ondertussen al een mooi netwerk uitgebouwd. Bovendien hebben we het geluk gehad dat een aantal van onze relaties echt wel met ons wilden samenwerken. Zij geloofden in ons en hebben ons van in het begin gesteund, net als de technologiepartners met wie we werkten.”
Steven: “Om onze klanten volledig te ontzorgen, startten we tijdens die beginperiode meteen een NOC op, een network operations center. Al heel snel hadden we daarvoor de eerste klant binnen – een belangrijke mijlpaal. Kort nadien kregen we de kans om voor een zeer groot Vlaams nutsbedrijf te werken. Voor ons als kleine onderneming was dat een hele prestatie; dat toonde dat we de juiste competenties hadden.”

Hebben jullie leuke anekdotes uit die beginjaren?
Frederik: “Op het moment van het eerste NOC-contract hadden we nog geen eigen datacenter en bestond de cloud nog niet. We zijn toen vanuit mijn garage gestart met enkele PC’s. Wat we deden was wel veilig en professioneel, maar het materiaal waarmee we het moesten doen was beperkt. Zodra het financieel mogelijk was, hebben we geïnvesteerd in het datacenter in Oostkamp, dat we vandaag nog steeds gebruiken. Intussen is er ook eentje in Merelbeke bij gekomen.”
Steven: “Ook leuk te weten: de eerste 4 jaar zijn we 6 keer verhuisd. We zijn gestart in een bedrijvencentrum in Waregem en zijn daarna naar Merelbeke gekomen. Hier zijn we ook al enkele keren van plek veranderd en hebben we in de loop der jaren meer ruimte ingepalmd.”

Ik kan me voorstellen dat niet altijd alles van een leien dakje liep?
Frederik: “Hoe mooi ook, dat eerste grote project voor het nutsbedrijf in kwestie was zeker een uitdaging, aangezien we nog maar met 18 waren. De CIO heeft toen zijn nek uitgestoken voor ons, omdat hij zo sterk in ons geloofde. Na 3 jaar werden we bij de directie geroepen, die ons persoonlijk liet weten supertevreden te zijn. Het mooiste compliment dat we konden krijgen. We hebben die klant kunnen laten evolueren naar een stabiele omgeving zonder noemenswaardige incidenten, heel anders dan ze voordien gewoon waren. En die klant van het eerste uur is nog altijd zeer tevreden! Een andere uitdaging was het vraagstuk hoe we ons aanbod rond security operations in de markt moesten zetten. We hebben eerst geprobeerd om software te resellen met consultancy erbovenop. Op dat moment waren we daarmee te vroeg in de markt. De budgetten lagen veel te hoog en het issue stond nog niet hoog op de prioriteitenlijst. Daarna hebben we andere modellen uitgetest, tot we 6 jaar geleden geïnvesteerd hebben in een SOC. Zo’n security operations center detecteert anomalieën in het gedrag van mensen en machines, om op te sporen of er hackers aan het werk zijn en of er gaten zijn in de security. We hebben daarvoor ook de nodige mensen aangetrokken. Nu staat dat aanbod helemaal op punt.”
Steven: “Heel recent vormden de indexeringen van de lonen een hobbel in de weg. De lonen zijn onze grootste kostenpost. Logisch dus dat het geen evidentie is om zo’n indexering te verwerken als het economisch niet de beste tijden zijn. We zijn een gezond bedrijf dat winst maakt, maar we moeten wel gericht en slim kiezen waarin we investeren. We hebben geprobeerd in de VS een afdeling op te richten, maar die beslissing hebben we gedeeltelijk moeten terugschroeven. We ontginnen nog steeds die markt, maar nu op een lager pitje. Amerikaanse bedrijven zitten niet te wachten op een Belgische speler, hebben we gemerkt.”

Wat maakt spotit op vandaag zo bijzonder en uniek, volgens jullie?
Steven: “De reden waarom we spotit hebben opgericht en onze strategie zijn niet veranderd. We blijven focussen op netwerken en security, met kwaliteit als hoeksteen en altijd vanuit een langetermijnvisie. En dat werkt, zo blijkt, want onze klanten vinden dat we doen wat we beloven. Zij zijn echte ambassadeurs voor ons.”
Frederik: “We creëren echt waarde voor onze klanten – door onze technologie maar ook door mee te denken met ondernemingen. En we maken ook het verschil door te streven naar echte partnerschappen met onze klanten. In elke relatie is er wel eens een moment dat het minder gaat; het komt erop aan daar goed mee om te gaan. Dankzij die aanpak beschouwen klanten ons niet als ‘gewoon een leverancier’, maar als echte partner en compagnon de route.”

Wat is jullie grootste drijfveer?
Frederik: “Ik heb het altijd al plezant gevonden om waarde te creëren met technologie. Het geeft veel voldoening dat een klant resultaat boekt dankzij ons én dat apprecieert.”
Steven: “Ik krijg energie van het opstarten en uitbouwen van iets nieuws, en van mensen enthousiasmeren om samen voor een doel te gaan. We vinden het allebei ook leuk om maatschappelijk iets te betekenen. Dit jaar organiseerden we bijvoorbeeld al voor de tweede keer de ‘Tour de spotit’. De opbrengst gaat naar het goede doel.”

Hoe zijn de rollen eigenlijk verdeeld tussen jullie?
Steven: “We zijn zeer complementair. Ik ben verantwoordelijk voor sales, finance, legal en de internationale strategie, Frederik voor alles wat met technologie te maken heeft, ons portfolio, welke partnerships we moeten afsluiten,…”
Frederik: “We vinden van elkaar dat we allebei goed zijn in wat we doen en delen waarden als respect, eerlijkheid en positiviteit.”
Steven: “En we kunnen alles open met elkaar bespreken.”

Weerspiegelt zich dat ook in de bedrijfscultuur? Wat is het ‘spotit-DNA’?
Frederik: “Bij potentiële medewerkers vinden we het belangrijk dat er een match is op het vlak van onze 4 kernwaarden: expertise, human to human, ondernemerschap en vertrouwen. Dit is geen bedrijf waarin alles van a tot z geregeld wordt voor je. Mensen die zichzelf nieuwe kennis of skills kunnen aanleren, hebben dan ook een voetje voor. Die ‘getting things done-mentaliteit’ is doorslaggevend.”
Steven: “Mensen krijgen hier veel vrijheid, maar moeten ook verantwoordelijkheid kunnen opnemen. We verwachten ook dat ze met oplossingen komen voor problemen en dat ze beslissingen nemen. Onze slagzin is ‘gazze geven’.”
Frederik: “Dat merk je ook in onze vlakke organisatiestructuur. We hebben een managementteam met 4 personen: wijzelf, een head of operations en een head of finance. Daaronder heb je teams die zelf instaan voor de meer operationele zaken. Zij worden bijgestaan door een operations Chief of Staff, die een coachingrol heeft, en de hr coach. Wij zijn zelf ook heel aanspreekbaar: wie een idee heeft kan dat komen voorstellen in ons directiecomité, waar we snel beslissingen nemen. En we zetten ook sterk in op teamsfeer. We geven medewerkers elke maand updates over onze activiteiten, er is ieder kwartaal een teamevent, we organiseren drinks en sportactiviteiten,… Het zijn allemaal initiatieven om ervoor te zorgen dat mensen graag naar kantoor komen, elkaar beter leren kennen en dus beter kunnen samenwerken.”
Steven: “Onze mensen zijn onze belangrijkste assets. Zonder hen betekenen we niets. We zijn er fier op dat we de beste mensen in netwerk en security hebben. We hebben trouwens een eigen academy. Daar krijgen pas afgestudeerde IT’ers een half jaar opleiding in hard skills en soft skills.”

Hoe kijken jullie naar groei?
Steven: “Eigenlijk hebben we geen harde omzet- en winstambitie. We willen wel een gezond bedrijf zijn, maar willen vooral tevreden klanten hebben. Onze NPS-score is een belangrijke KPI voor de bonussen van medewerkers.”
Frederik: “Duurzame groei is veel meer dan alleen winst maken. Daarom hanteren we een visie die we niet op 1 of 2 jaar realiseren, maar op 5 tot 10 jaar.”

Is dat ook de reden dat jullie de enige aandeelhouders zijn?
Steven: “Ja, want als je een private equity-partner aan boord haalt, ligt de focus wel vaak eerder op korte termijn.”
Frederik: “Dan wordt er ook voortdurend over je schouder meegekeken naar targets. Dat creëert een bepaalde verwachting en beperkt de vrijheid.”
Steven: “We krijgen veel vragen om eens te gaan praten over samenwerkingen, maar staan daar niet voor open. We kiezen voor de vrijheid en onafhankelijkheid om onze eigen koers te bepalen.”

Wat zijn jullie ambities voor de komende jaren?
Steven: “We gaan voor een gezonde groei met goeie mensen. We zijn daar klaar voor: onze nieuwe generatie SOC is écht af, is beschikbaar als open source- of als Microsoft-variant én klanten kunnen rekenen op onze service-meerwaarde. Dankzij die elementen zijn we in staat om de grote spelers te challengen. Wij willen de beste zijn, niet de grootste.”
Frederik: “We zijn voorzichtiger geworden dan vroeger om zeer ambitieuze uitspraken te doen, want de wereld verandert zo snel – niet alleen geopolitiek maar ook op het vlak van technologie.”
Steven: “Of we internationale aspiraties hebben? We zien wel kansen in Nederland, Scandinavië en Duitsland. Daar hebben we al klanten en is er een culturele fit. Mocht de vraag daar plots sterk stijgen of mocht daar een overname mogelijk zijn, kan onze business daar in een stroomversnelling komen.”

Er zijn ook veel mogelijkheden met jullie recente ‘product’ Cyberwolf? Wat is dat precies?
Steven: “Cyberwolf kan je zien als een soort 24/7 digitale bodyguard van het privéleven. Het is bedoeld voor C-level, board members, ministers, magistraten en vermogende mensen over de hele wereld. Eigenlijk doen we met Cyberwolf hetzelfde als wat we doen voor bedrijven: kwetsbaarheden identificeren, fraude opsporen, conversaties op het dark web traceren, de klant beschermen mocht er toch iets gebeuren. Voor een groot Amerikaans bedrijf – waarvan we de naam uiteraard niet mogen noemen – verzekeren we er al de cybersecurity mee van de volledige leadershipboard over de hele wereld. Het potentieel is echt enorm.”

Wie zijn Frederik en Steven?

Frederik Rasschaert (43) woont in Beveren Waas, houdt van lopen en fietsen (om daarna lekker te kunnen eten en drinken), reizen en afspreken met vrienden. In het weekend spendeert hij veel tijd op het voetbalplein om voor zijn 2 kinderen te supporteren.

Steven Vynckier (49) fietst graag (nadat hij noodgedwongen moest stoppen met lopen) en legt al eens een kaartje met vrienden en familie. Ook hij supportert graag voor zijn dochter, die danst, en zijn zoon, die pingpong speelt.

Tot slot: AI is momenteel een hot topic. Welke trends komen nog op ons af in de wereld van cybersecurity?
Frederik: “Artificiële intelligentie zal sowieso een shift veroorzaken in hoe we security in de toekomst zullen runnen. In alle technologieën die wij gebruiken, zit AI eigenlijk al ingebakken, maar er zijn nog veel kansen. Samen met KU Leuven en VUB doen we al enkele jaren research naar het inzetten van AI in cybersecurity, zodat we cybersecurity operations minder afhankelijk kunnen maken van mensen. Daarnaast delen we zogenaamde ‘threat intelligence’ met oa Centrum voor Cybersecurity Belgium. Naast AI is er natuurlijk nog steeds de cloud als enorme businessversneller, en meer en meer zijn bedrijven zich ook bewust van het belang van OT security (in productie-omgevingen). Er staat dus nog heel wat te gebeuren. Wij zijn er in elk geval klaar voor!”

€30.000.000

Omzet Skyleaf (Spotit + Cyberwolf)

MEEST POPULAIRE ASSESSMENTS IN 2024

- Pentest
- NIS2 Assessment
- Security & Network Assessment

10%

groei

FACTS &STATS

210

actieve klanten (in portefeuille)

4 SECTOREN WAAR WE HET MEEST ACTIEF ZIJN:

1. Utilities & Energy sector
2. Manufacturing & Process Industry
3. Logistics & Harbor
4. Pharmatech & Lifesciences

73% VAN DE RISICO'S VINDT ZIJN OORSPRONG IN 3 IT HOOFDDOMEINEN (BRON: UNIT 42)

- IT & BEVEILIGINGSINFRASTRUCTUUR
- DIENSTEN VOOR TOEGANG OP AFSTAND
- BEDRIJFSAPPLICATIES

TOP 3 VAN GROOTSTE BEDREIGINGEN IN BELGIË (BRON: CCB)

- RANSOMWARE
- ACCOUNT COMPROMISE
- DDOS

TOP 3 VAN AANVALLEN VOLGENS VOLUME IN HET SPOTIT SOC

- PHISHING
- MALICIOUS CODE
- INTRUSION (ATTEMPTS)

Inzichten in cyberdreigingen in 2024

HOE GERAKEN ZE BINNEN? DE MEEST GEBRUIKTE MANIEREN (BRON: SPOTIT CSIRT)

- EXPLOIT
- EXPOSED SECURITY INFRA
- MALWARE

TOP 3 VAN AANVALLEN VOLGENS VOLUME IN EUROPA (BRON: ENISA)

- DDOS
- RANSOMWARE
- DATADIEFSTAL

MEEST GEBRUIKTE AANVAL GELINKT AAN MOTIEF IN EUROPA (BRON: ENISA)

- RANSOMWARE – FINANCIEEL GEWIN
- DDOS – IDEOLOGIE
- MALWARE – SPIONAGE

Naast cijfers van het Centre for Cybersecurity Belgium zijn ook volgende rapporten interessante bronnen om te raadplegen.
Unit 42 Incident Response Report 2024 / Threat exposure Brucon 2024 / ENISA Threat Landscape 2024 / 2024 Report on the State of the Cybersecurity in the Union / Internet Organised Crime Threat Assessment IOCTA 2024 / Unit42 Attack Surface Threat Report / Verizon data breach report 2024

DE TRENDS EN UITDAGINGEN VAN 2024

Cybersecurity en connectiviteit vormen meer dan ooit een cruciaal duo in het hart van onze digitale maatschappij. Ondernemingen die digitaal verder willen groeien, zetten dan ook sterk in op die twee essentiële pijlers. Maar er zijn natuurlijk een aantal onomkeerbare trends en serieuze uitdagingen om rekening mee te houden. Ook in 2024 volgden we die nauwgezet.

1. De opkomst van artificiële intelligentie in cybersecurity
De inzet van artificiële intelligentie (AI) in cybersecurity is een gamechanger. AI-algoritmen worden steeds geavanceerder en zijn in staat om sneller dan menselijk mogelijk is bedreigingen te detecteren en erop te reageren. AI is zelfs tot 'predictieve analytics' in staat: het voorspellen van potentiële kwetsbaarheden.

2. De evolutie van edge computing
Edge computing is een revolutie voor connectiviteit, door gegevens dichter bij de bron te verwerken. Het is een verschuiving die de snelheid verhoogt en de betrouwbaarheid verbetert, maar die tegelijk ook nieuwe uitdagingen met zich meebrengt. Het beschermen van de grote verscheidenheid aan apparaten en gegevenspunten aan de 'rand' vereist dan ook innovatieve beveiligingsbenaderingen.

3. Zero trust-beveiligingsmodellen
Het concept van 'nooit vertrouwen, altijd verifiëren' vormt een hoeksteen van cybersecurity-strategieën. Nu het thuiswerken de grenzen van traditionele netwerkperimeters vervaagt, zorgen zero trust-modellen ervoor dat beveiliging niet afhankelijk is van de locatie, maar van continue verificatie van identiteit en toegangsprivileges.

4. De uitbreiding van 5G
De uitrol van 5G-netwerken maakt ultrahoge bandbreedte-connectiviteit alomtegenwoordig, waardoor een explosie van verbonden apparaten en applicaties mogelijk is. Dat opent echter ook nieuwe wegen voor cyberaanvallen. 5G-netwerken en verbonden apparaten beveiligen is dan ook van het grootste belang om hun volledige potentieel te benutten.

5. Regelgeving en privacy
Met de toenemende frequentie van datalekken voeren overheden wereldwijd strengere gegevensbeschermingsregels in. Bedrijven moeten door dat complexe regelgevende landschap navigeren om forse boetes en reputatieschade te vermijden, terwijl ze ook de privacy van de klant moeten beschermen. De recente NIS2 Directive is daar een concrete toepassing van en verplicht bedrijven en organisaties om meer te investeren in cyberveiligheid.

cybersecurity & netwerking

Wim Remes, Head of Operations bij spotit, beaamt uiteraard de naar voor geschoven trends van Gartner. Tegelijkertijd roept hij op tot de nodige nuchterheid. Zijn advies: start met de basics en groei stap voor stap in digitale maturiteit, met in elke fase de nodige aandacht voor first-class connectiviteit en verhoogde cyberveiligheid. Klinkt eenvoudig, maar is het niet altijd. Wim haalt alvast deze uitdagingen aan.

Wilt u graag eens sparren met Wim over de nieuwste trends en uitdagingen op het vlak van cybersecurity en connectiviteit? Neem vrijblijvend contact op met hem.

1. Taal
De directie en IT spreken nog te vaak een verschillende taal. Zorgen dat ze elkaar begrijpen – het 'standaardiseren' van die taal – is een belangrijke uitdaging zodat de juiste informatie naar de juiste mensen gaat. Zeker nu regulaties zoals NIS2 ervoor zorgen dat de directie aansprakelijk kan worden gesteld, is het noodzakelijk dat er klare en duidelijke taal wordt gesproken.

2. Mensen
Technologieën zijn een noodzaak en een handig hulpmiddel, maar mensen maken het echte verschil. Mensen met een bepaalde expertise en opgebouwde ervaring weten hoe ze op kritische momenten moeten handelen. Zorg dat mensen getraind blijven door bijvoorbeeld regelmatig table-top oefeningen te organiseren. Daardoor worden incidenten op een vlotte en gestructureerde manier afgehandeld, kent ook iedereen zijn plaats bij grote incidenten, en wordt er geen essentiële tijd verloren. Uiteraard is teamwork daarbij cruciaal.

3. Design
Vandaag moet het design van IT-infrastructuur 'Distributed', 'Immutable' en 'Ephemeral' zijn. Dat betekent dat vele losse componenten met elkaar moeten kunnen samenwerken, dat een verandering in een systeem gedetecteerd moet kunnen worden en gecontroleerd moet zijn, en dat we ervoor moeten zorgen dat volledige infrastructuren of hun onderdelen gemakkelijk en gecontroleerd vernieuwd kunnen worden. Als dat in orde is, kunnen bij de eerste indicaties van een cyberincident de activiteiten voortgezet worden met een betrouwbare infrastructuur. Die architectuurtransformatie is bij heel wat bedrijven vandaag nog niet (volledig) doorgedrongen.

4. Data
Data zijn voor veel organisaties een immense uitdaging. Gegevens zitten immers steeds meer verspreid en de hoeveelheid neemt gigantisch toe. Hoe en waar bewaar je die data en hoe geef je zin aan die data? Bij Security Operations zien we bijvoorbeeld een evolutie naar een 'data pipeline': een reeks processen die data van de ene locatie (de bron) naar een andere (het doel) verplaatst en transformeert. Het is een cruciaal onderdeel van data engineering en wordt vaak gebruikt in de context van big data, waar grote hoeveelheden gegevens continu moeten worden verwerkt en geanalyseerd.

5. Regelgeving
Nieuwe wetgevingen zoals NIS2 en DORA (voor de financiële wereld) komen op ons af. Pak dat pragmatisch aan. Bij NIS2 wordt Third Party Security Management – het identificeren van uw belangrijkste en meest kritische leveranciers – de belangrijkste uitdaging. Zorg dat u het proces onder controle hebt en samenwerkt met uw partners om samen de supply chain te beveiligen.

Bronnen: Cybersecurity Trends 2024 to Safeguard your Digital Assets | Gartner
Top Cybersecurity Trends and Strategies for Securing the Future | Gartner
The NIS 2 Directive: what does it mean for my organization? | Centre for Cyber security Belgium
NIS2 – an opportunity to focus on

“Cloudtechnologie heeft alles veranderd”

CTO FREDERIK OVER DE IMPACT VAN TECHNOLOGIE

11 jaar geleden zag de digitale wereld er heel anders uit. Mobiel internet stond nog in zijn kinderschoenen en social networking was veel minder aanwezig. Ondertussen is de digitalisering exponentieel gegroeid, wat zowel nieuwe kansen als nieuwe risico’s met zich meebrengt. Het aantal cyberaanvallen is sterk toegenomen, omdat er simpelweg meer mogelijkheden zijn om aan te vallen. Mensen bezitten nu meerdere toestellen (smartphones, tablets, laptops, smartwatches, …) en zijn continu online.

Toen spotit startte, waren de budgetten voor een Security Operations Center (SOC) enorm hoog, waardoor slechts een klein deel van de Belgische bedrijven daarin kon investeren. Vandaag zien we een ommekeer: cybersecurity staat nu bij elk bedrijf op de radar. Bovendien zijn de kosten voor een SOC door technologische vooruitgang aanzienlijk gedaald.

Cloudtechnologie heeft de manier waarop we werken fundamenteel veranderd. Waar vroeger alles in eigen datacenters draaide, is nu vrijwel alles in de cloud ondergebracht. Dat betekent dat de beveiliging niet langer rond één fysieke locatie draait, maar verspreid is over meerdere platformen en systemen.

De manier waarop aanvallers opereren, is sterk veranderd, en we zien steeds vaker gestructureerde en door staten gesponsorde cyberaanvallen. Tegelijk kunnen we met frameworks zoals MITRE ATT&CK tactieken van aanvallers beter in kaart brengen en linken aan specifieke groepen, zoals Rusland- of Noord-Korea-gesponsorde hackers. Die inzichten helpen ons om gerichter te verdedigen dan 10 jaar geleden.

Tot voor kort werd security binnen operationele technologie (OT) nauwelijks als prioriteit gezien. Bedrijven in deze sectoren stonden nauwelijks open voor bemoeienis van cybersecurityspelers. Vandaag is dat anders: door de groei van IoT en de digitalisering van industriële processen is OT-beveiliging een cruciaal aandachtspunt geworden.

Kunstmatige intelligentie speelt een steeds grotere rol in cybersecurity. Enerzijds helpt AI ons om systemen beter te beveiligen, bijvoorbeeld door sneller verdachte activiteiten te detecteren en security-analisten te ondersteunen. Anderzijds moeten AI-modellen zelf ook beveiligd worden. We helpen klanten bij het beschermen van hun AI-systemen tegen datalekken en misbruik. Daarnaast zetten cybercriminelen AI in om hun aanvallen te verbeteren.

Niet alleen bedrijven, maar ook personen zijn kwetsbaarder geworden. Alles is tegenwoordig digitaal: foto’s, documenten, e-mails, agenda’s, privégesprekken. Smartphones en laptops zijn altijd verbonden, waardoor de kans op afluisteren en spionage groter is. Dat betekent dat bepaalde groepen – zoals bedrijfsleiders, politici en andere hooggeplaatste professionals – extra risico lopen. Onze rol is om hen beter te beschermen.

Maatschappelijk verantwoord ondernemen

Environment

Afgelopen jaar hebben we verdere stappen gezet om onze ecologische voetafdruk te verkleinen. Door bewuste keuzes dragen we bij aan een duurzamere toekomst. Onze acties weerspiegelen onze verantwoordelijkheid voor het milieu en de generaties die na ons komen.

- **E-waste:** we werkten een policy uit om nodeloos of ondoordacht printen te vermijden
- **Elektrificatie wagenpark:** enkel full electric wagens maken deel uit van de car policy
- **Shared workspace en thuiswerk:** door het delen van middelen/ruimte en het verminderen van de uitstoot van woon-werkverkeer, minimaliseren we onze impact op het milieu.

Governance

Sterk bestuur en transparantie zijn voor spotit de sleutel tot duurzaam succes. In onze besluitvorming zijn langetermijnwaardecreatie, integriteit en stakeholderbetrokkenheid dan ook cruciaal.

Zo wordt onze vertrouwensband met klanten, partners en medewerkers nog sterker.

- **Externe adviseurs:** de Skyleaf-holding heeft een raad van advies waarin externe experts zetelen. Zij zorgen voor een frisse blik op onze strategie.
- **Organisatiestructuur geoptimaliseerd:** als groeiend bedrijf vinden we het belangrijk om onze organisatiestructuur te blijven bijsturen. Naast de twee CEO's en het directiecomité werd in 2024 met inspraak van de medewerkers een managementcomité ingevoerd.
- **Nauwe betrokkenheid van klanten:** we organiseren jaarlijks een kwalitatieve bevraging bij 50 tot 75 klanten. Tijdens een lunch brengen we onze ambassadeurs als eerste op de hoogte van toekomstplannen en nieuwigheden. Op de roadmap voor komend jaar staat ook de oprichting van een customer advisory board. Enkele klanten zullen daarin meedenken over onze strategische koers en bijdragen aan onze roadmap.

Social

Mensen vormen de kern van ons succes. In 2024 hebben we dan ook verder ingezet op de ontwikkeling en het welzijn van onze medewerkers. Door samen te werken en te verbinden met andere organisaties zoals het hoger onderwijs, creëren we een positieve impact binnen én buiten onze organisatie. Daarnaast ondersteunen we ook goede doelen.

- **Tweede editie van Tour de spotit:** Op zaterdag 27 april organiseerden we onze tweede editie van Tour de Spotit. Maar liefst 83 vrienden, familieleden en medewerkers zetten hun beste beentje voor en fietsten in totaal 6.300 kilometer. We haalden 10.000 euro op voor het goede doel De Zelfmoordlijn.
- **Levenslang leren:** onze spotit Academy toont aan hoeveel aandacht we hechten aan opleiding en coaching. Pas afgestudeerde jongeren kunnen via een traineeship van een half jaar opleiding volgen bij interne en externe coaches. Naast theoretische lessen doen ze ook heel wat praktijkervaring op. Ze leren trouwens niet alleen de nodige IT-technische skills, maar ook soft skills zoals planning en communicatie. Uiteraard staat het thema opleiding en voortdurend bijscholen hoog op de agenda voor onze meer ervaren medewerkers.
- **Kennis delen met scholen:** we partneren al enkele jaren samen met KU Leuven en VUB, met wie we werken aan projecten rond AI in cybersecurity.
- **Aandacht voor diversiteit en inclusie:** in een sector als de onze is het niet evident om een gelijke verdeling tussen mannelijke en vrouwelijke medewerkers te bekomen, maar het is een thema waarvoor we heel bewust aandacht hebben. Op dit moment zijn 17% van onze medewerkers vrouwen. En nog een leuk weetje: we hebben niet alleen Belgische medewerkers in ons team, maar ook mensen uit de VS en Italië.

Spotits 360° evaluatiecyclus

DE KRACHT VAN FEEDBACK

Bij spotit geloven we dat groei ontstaat uit eerlijke en constructieve feedback. Daarom hanteren we een 360° evaluatiecyclus die verder gaat dan de klassieke top-down evaluaties. In onze aanpak telt ieders stem: teamleads evalueren medewerkers, collega's geven waardevolle feedback aan elkaar, en medewerkers krijgen de kans om hun mening te geven over hun teamlead.

Die holistische methode bevordert een cultuur van vertrouwen, transparantie en samenwerking, en zorgt ervoor dat iedereen een duidelijk zicht krijgt op zijn of haar sterktes en groeipunten. Door feedback van iedereen met wie je samenwerkt, willen we mensen versterken, teams laten groeien en samen uitblinken. Want bij spotit is groei geen soloreis, maar een teamprestatie.

Meerdere perspectieven aan tafel

Elk jaar in oktober starten we onze jaarlijkse evaluatiecyclus met peer feedback. Die collega's kunnen rechtstreekse teamgenoten zijn, of mensen uit andere teams met wie is samengewerkt aan een specifiek project. Medewerkers mogen zelf 3 tot 5 collega's kiezen om waardevolle inzichten te krijgen over hun vaardigheden, communicatie en samenwerking. Daarna volgt de feedback van hun teamlead. Die beoordeelt hen op een reeks professionele en soft skills, en op basis van onze spotit-waarden. Medewerkers krijgen ook de kans om hun teamlead te evalueren. Goed leiderschap begint immers met luisteren en feedback meenemen.

Alle informatie wordt opgeslagen in hun profiel in onze evaluatietool, die we ook gebruiken om doelen op te volgen. Daar kunnen medewerkers steeds hun evaluaties en doelstellingen raadplegen.

Al die input wordt besproken tijdens een gesprek met de manager. Het ideale moment om verwachtingen helder te krijgen, kansen te verkennen en samen een persoonlijk groeipad uit te werken.

CASE

Belgische Federatie van Voedselbanken

Sinds kort beschikt de Belgische Federatie van Voedselbanken over een volledig **nieuw, veilig en performant netwerk**. Daardoor verloopt de verdeling van voedselpakketten aan de minstbedeelden vandaag veel efficiënter, tot grote tevredenheid van de voedselbankvrijwilligers.

Sinds COVID-19 en de energiecrisis was het volume van voedselpakketten zo sterk gestegen dat het voor de vrijwilligers van de Belgische Federatie van Voedselbanken niet meer haalbaar was om voorraden manueel te tellen. Via een geautomatiseerd systeem met barcodescanners kunnen zij efficiënter werken, daalt de foutenmarge en is een correcte rapportering naar de overheid gegarandeerd. Om dat systeem te realiseren, was er nood aan **een stabiel en veilig netwerk.**

Cisco doneerde netwerkmateriaal, maar die hardware moet uiteraard ook geïnstalleerd, **beheerd en 24/7 gemonitord** worden. De spotit Security & Network Engineers rolden nieuwe netwerken uit in de magazijnen en implementeerde ze in het spotit NOC. Daardoor kunnen ze snel reageren en ingrijpen wanneer bepaalde alerts van netwerk devices binnenkomen. Voedselbank Limburg beschikt nu over een professioneel netwerk met 15 access points die het volledige magazijn voorzien van stabiele en veilige wifi. Ook extra devices, zoals inbraakalarmen en bewakingscamera's, werden aangesloten op het netwerk.

"Spotit is een aanrader!
Daar moeten we niet over twijfelen. Ze gaan zeer goed om met hun klanten, en blijven steeds waakzaam."

Bart Buckinx, Afgevaardigd Bestuurder
bij Voedselbank Limburg vzw

“De spotit Academy geeft je een echte headstart”

DEELNEMER EMILE TRENSON

Sinds de opstart van de Spotit Academy 5 jaar geleden, studeerden al meer dan 30 jonge professionals af, waarvan 85% nog steeds bij spotit aan de slag is. In het traineeship van zes maanden krijgen beloftevolle talenten opleidingen door interne en externe coaches. Emile Trenson, vandaag actief in het spotit SOC, getuigt over de meerwaarde.

Wat is jouw achtergrond?
“Ik heb aan hogeschool Odisee Elektronica-ICT gestudeerd, met de afstudeerrichting infrastructuur. Op een jobbeurs kwam ik met spotit in contact. Veel bedrijven proberen je daar te lokken met flashy standen, maar dat was niet waar ik naar op zoek was. Toen ik met de mensen van spotit ging praten, voelde ik meteen een klik qua aanpak en cultuur. Zo groeide mijn interesse.”

Je nam in 2019-2020 deel aan de spotit Academy. Wat is dat precies?
“Omdat spotit merkte dat het moeilijk was om medewerkers met ervaring te vinden, besliste het zélf nieuwkomers op te leiden. Schoolverlaters of mensen die een carrièreswitch maken, kunnen solliciteren voor de Academy. Niet alleen hun voorkennis, maar vooral hun motivatie en de fit met het bedrijf zijn doorslaggevend. Als ze worden toegelaten, start een traject van zes maanden waarin hun kennis van IT naar een hoger niveau getild wordt. De eerste twee à drie maanden focussen volledig op theoretische kennis. Daarna worden stageopdrachten en labo-oefeningen toegevoegd. Zo kunnen deelnemers hun kennis in de praktijk testen, onder begeleiding van een mentor. Een onderdeel is bijvoorbeeld dat ze leren om van nul een netwerk op te bouwen, in plaats van enkel bestaande systemen aan te passen.

Naast technische training zijn er ook soft skills opleidingen, zoals timemanagement en klantgericht communiceren.”

Hoe blik je terug op je deelname?
“Heel positief. Je krijgt in de Academy de kans om in korte tijd veel kennis op te doen, iets wat je anders heel wat meer tijd zou kosten. Veel bedrijven geven pas geleidelijk verantwoordelijkheid aan nieuwkomers, terwijl ik bij spotit echt werd klaargestoomd en snel aan de slag kon. Een echte headstart! Er zijn volgens mij maar weinig deelnemers die spijt hebben; vaak blijven ze ook een hele tijd bij spotit werken. Sinds een drietal jaar ben ik zelf ook betrokken bij de organisatie van de Academy. Vanuit mijn ervaring als security analyst help ik nieuwe deelnemers met hun traject. Ik begeleid bijvoorbeeld de labo-oefeningen.”

Tot slot: hoe zou je de spotit Academy samenvatten?
“Een unieke kans waarvoor je veel terugkrijgt! Met de Academy investeert het bedrijf echt in jong talent. Dat is niet vanzelfsprekend. Het toont aan dat je hier vertrouwen krijgt.”

Wat is de spotit Academy?

Beloftevolle talenten kunnen gedurende zes maanden een traineeship volgen, gevuld met opleidingen door interne en externe coaches. Naast theoretische lessen staat ook praktijk op het programma. We leren deelnemers niet alleen de nodige IT-technische skills aan, maar focussen ook op soft skills, zoals planning en communicatie. Ideaal om een succesvolle carrière te starten binnen security & netwerken, en om op lange termijn te evolueren binnen spotit. In september 2025 start de zevende editie.

Straffe prestaties dankzij een sterk team

Elke dag bouwen onze medewerkers mee aan de toekomst van onze organisatie én onze klanten. Maak kennis met onze verschillende teams:

MANAGED SERVICES

- **SOC-team:** ons Security Operations Center bewaakt en beschermt 24/7 de IT-omgevingen van klanten tegen bedreigingen, met realtime detectie en respons.
- **CSIRT:** apart team dat snel en deskundig reageert op beveiligingsincidenten om schade te minimaliseren.
- **NOC-team:** beheert en optimaliseert netwerkprestaties en uptime, met een proactieve en probleemoplossende aanpak.

DOMAIN EXPERTS

- **OT-team:** richt zich op de beveiliging en connectiviteit van industriële systemen, met expertise in unieke OT-uitdagingen.
- **Offensive-team:** voert ethische hacktests en kwetsbaarheidsanalyses uit om systemen te versterken tegen mogelijke aanvallen.
- **Consulting-team:** helpt organisaties risico's te beheren, compliance te waarborgen en een sterke beveiligingsstrategie te ontwikkelen.

TECHNOLOGY

- **Internal IT Operations-team:** zorgt dat onze medewerkers over toptools beschikken om productief en kwaliteitsvol werk af te leveren.
- **Service Excellence-team:** combineert ontwikkeling en operationele expertise om snelle, betrouwbare en schaalbare oplossingen te leveren. Het team bestaat uit **DevOps** (automatiseren repetitieve processen en taken ten voordele van de klant of spotitcollega), **Data Science** (doen analyse van bestaande data (klanten of spotit) en verwerken deze tot nuttige rapportering) en **Platformation** (richten het IT-ticketingsysteem in en kijken voor continue verbetering bij de afhandeling van tickets).

OPERATIONS

- **Architecten-team:** vertaalt de Netwerk- en security-uitdagingen naar technologische oplossingen op maat
- **Projects & Service Management-team:** implementeert maatwerkoplossingen voor complexe IT-projecten, van start tot finish met een focus op kwaliteit.
- **Security Engineering-team:** voor de meest complexe securityvraagstukken kan u bij dit team terecht

SALES & MARKETING

- **Presales, Sales & Marketing, Service Development-team**: verbindt klantbehoeften met spotit oplossingen, met een klantgerichte aanpak en overtuigende communicatie.

STAFF

- **HR-team:** zet zich in om talent aan te trekken, te ontwikkelen en te ondersteunen, met een focus op een stimulerende en positieve werkcultuur.
- **Finance & Orders-team:** waarborgt financiële stabiliteit en groei met nauwkeurige planning, analyses en strategisch beheer.
- **Legal:** goede afspraken (op papier) maken goede vrienden.
- **Facilities & Reception:** zorgt voor een piekfijne kantoorruimte en steeds een warm ontvangst.

Ons Partner Ecosysteem

If you want to go fast, go alone. If you want to go far, go together. En wij willen vooral samen ver geraken. We investeren dan heel wat tijd en resources in het opzetten en behouden van sterke, duurzame partnerships.

Onze strategische technologiepartners

Wij geloven in de kracht van samenwerking. Daarom kiezen we bewust voor technologiepartners die tot de top van hun sector behoren. Stuk voor stuk merken die innovatie en kwaliteit combineren en die, net als wij, gaan voor duurzame oplossingen. Met deze strategische allianties bouwen we aan langetermijnrelaties die onze klanten ten goede komen – vandaag en morgen.

Onze academische partners, sectorfederaties en netwerkorganisaties

Als specialist in cybersecurity en netwerking nemen we onze rol in het bredere ecosysteem ernstig. Via ons lidmaatschap van organisaties blijven we niet alleen op de hoogte van technologische en beleidsmatige evoluties, maar leveren we ook actief onze bijdrage aan de toekomst van de sector. Zo bouwen we mee aan een sterk, innovatief en veerkrachtig ondernemingsklimaat.

Onze fijne klanten

Heel wat ondernemingen in België doen een beroep op ons. En daar zijn we trots op! Hieronder een selectie:

Bekijk enkele van onze referenties

Klaar om uw netwerk- en beveiligingsbehoeften te bespreken?

Wij zijn steeds beschikbaar. Aarzel niet om ons te contacteren voor een vrijblijvend gesprek en een lekkere koffie. Bezoek ons in een van onze kantoren, of plan een gesprek met een expert.

www.spotit.be
+32 (0)9 322 04 44
info@spotit.be

Speerpunten voor de toekomst

Sterkere focus op governance, risk & compliance
Governance, risk management en compliance (GRC) zijn al jaren een vaste waarde binnen onze dienstverlening. Met een **ervaren team van specialisten** ondersteunen we klanten in uiteenlopende sectoren. Vandaag wint GRC snel aan belang, zeker met de komst van NIS2 en steeds strengere regelgeving. Daarom investeren we gericht in de verdere uitbouw van onze GRC-activiteiten. Zo blijven we een betrouwbare partner voor bedrijven die hun risico's willen beheersen, hun compliance willen versterken en klaar willen zijn voor de toekomst.

Gemoedsrust dankzij ons 100% Belgische SOC én NOC
Al tien jaar onderscheiden we ons met een **unieke combinatie van SOC (Security Operations Center) en NOC (Network Operations Center)**. Waar veel partijen zich enkel op cybersecurity focussen, bieden wij ook de **onderliggende netwerkexpertise** die cruciaal is voor een sterke beveiligingsaanpak. Want echte veiligheid begint bij een stabiel, performant netwerk. Bovendien zijn al onze diensten **100% Belgisch**. In tijden van geopolitieke onzekerheid is dat voor veel klanten een geruststellende factor én een bewuste keuze.

Versnelling hoger voor OT Security & Networking
Operational technology is het kloppend hart van sectoren zoals logistiek, industrie, nutsvoorzieningen en farma/life sciences. Toch krijgen OT-netwerken vaak niet de aandacht die ze verdienen. Om daar verandering in te brengen, **zetten we volop in op OT Security & Networking** met een aparte businessunit. Zo bieden we onze klanten de gespecialiseerde kennis, aanpak en technologie die nodig zijn om hun operationele systemen toekomstbestendig én cyberveilig te maken.

Sterke groei in de publieke sector
Tot voor kort waren we minder zichtbaar in de publieke sector, maar daar komt snel verandering in. We zetten volop in op **samenwerking met overheden en organisaties in de zorg- en onderwijswereld.** Een belangrijke mijlpaal daarin is ons partnership met Shield vzw, een samenwerkingsverband dat instellingen in de gezondheidszorg en het hoger onderwijs ondersteunt bij het opzetten en beheren van een performante en veilige cybersecurity-architectuur. Met onze oplossingen en expertise bouwen we actief mee aan een digitale en weerbare publieke sector.

Snelle en doeltreffende ondersteuning bij cybercrisissen
Met ons CSIRT-team (Cyber Security Incident Response Team) staan we paraat om bedrijven te ondersteunen bij digitale incidenten en crisissituaties. Maar we gaan nog een stap verder. **We breiden ons aanbod uit met offensive security**, waarbij we – steeds in overleg met de klant – doelgerichte aanvallen simuleren. Zo brengen we kwetsbaarheden aan het licht vóór echte hackers dat doen. Voor deze nieuwe businessunit hebben we een ervaren expert aangesteld, zodat we onze klanten ook proactief kunnen wapenen tegen cyberdreigingen.

Cyberwolf versnelt internationaal
Cyberwolf bouwde de voorbije jaren een sterke klantenportefeuille uit in zowel Noord-Amerika als Europa. Die **internationale groei** willen we nu verder versnellen. Tot nu toe werkten we bewust onder de radar. Maar de volgende stap is duidelijk: onze zichtbaarheid vergroten, zonder onze kenmerkende discretie te verliezen. Cyberwolf blijft een stille kracht – maar wel één die steeds meer impact maakt.


spotit
YOUR SECURITY & NETWORK LAYER