G4S Academy

INTEGRATED SECURITY

G4S INTEGRATED SECURITY IS ONZE COMBINATIE VAN EXPERTISE, BEVEILIGINGSPROFESSIONALS, TECHNOLOGIE EN DATA-ANALYSES OM RISICO'S TE BEHEREN EN MEER WAARDE TE CREËREN VOOR ONZE KLANTEN

INHOUD

1. INLEIDING

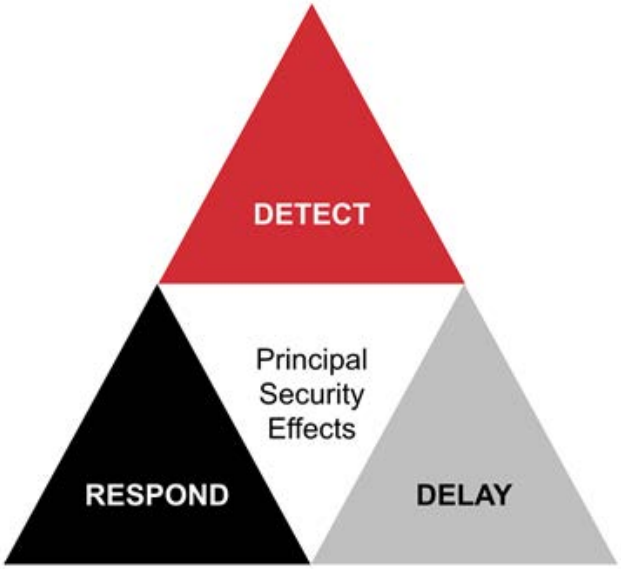
Integrated Security is het geheel van beveiligingsmaatregelen dat deel zou moeten uitmaken van uw beveiligingsoplossingen zodat u een optimaal beveiligingsprogramma kunt samenstellen.

Bij G4S beschrijven we Integrated Security als 'onze combinatie van expertise, beveiligingsprofessionals, technologie en data-analyses om risico's te beheren en meer waarde te creëren voor onze klanten'.

Om Integrated Security te ontwerpen, moet u eerst de verbanden tussen de belangrijkste veiligheidseffecten begrijpen. In de sector lopen de meningen nogal uiteen over wat nu precies de belangrijkste veiligheidseffecten zijn. Bij G4S zijn wij van mening dat 'detecteren, vertragen en reageren' de ruggengraat vormen van elk geïntegreerd beveiligingsprogramma.

Belangrijkste veiligheidseffecten hebben altijd bestaan en zijn in duizenden jaren tijd nooit veranderd. Wat wel voortdurend geëvolueerd en dus veranderd is, zijn de beveiligingsoplossingen.

Om te helpen bij het ontwerpen van Integrated Security programma's hebben wij het G4S Integrated Security Model ontwikkeld dat we in deze whitepaper zullen toelichten.



Afbeelding 1 - Principal Security Effects

2. BEVEILIGINGSRISICO'S

Een belangrijke stap in het ontwerpen van een Integrated Security programma is inzicht krijgen in de risico's van uw onderneming. Risico's worden gecreëerd door potentiële bedreigingen die kwetsbaarheden van activa uitbuiten en beveiliging heeft tot doel om maatregelen in te voeren die de potentiële bedreigingen tegengaan en de kwetsbaarheden inperken (dat noemen we tegenmaatregelen).

Aan de hand van een risicogebaseerde benadering kunt u de tegenmaatregelen efficiënter in kaart brengen. Onze risicogebaseerde benadering is gebouwd op drie fundamentele vragen:

De antwoorden op deze vragen reiken ons alle elementen aan om het risico te beperken. Als we alle elementen begrijpen, kunnen we het risico beter inperken door oplossingen te ontwerpen die de meest geschikte combinatie van tegenmaatregelen gebruiken.

Een goede beveiliging is intelligent en proportioneel. Met een ontoereikende beveiliging zijn vestigingen blootgesteld aan ontoelaatbare risico's, terwijl een overmatige beveiliging dan weer duur, hinderlijk en vaak niet effectief is. Op basis van uw risicobeperkende elementen moet u een reeks van beveiligingsoplossingen en tegenmaatregelen samenbrengen die samen een beveiligingsplan vormen. Deze oplossingen en maatregelen zijn het resultaat van de inzet van een aantal beveiligingscapaciteiten. Bij G4S zijn we ervan overtuigd dat Integrated Security gestuurd wordt door vier capaciteiten:

Afbeelding 2 - G4S Integrated Security capaciteiten

- **Risicoconsultancy** - De capaciteit om advies en ondersteuning te geven bij het beheer van beveiligingsrisico's.
- **Beveiligingsprofessionals** - De capaciteit om beveiligingsprofessionals in te zetten met ervaring inzake risico's, oplossingen en sectoren.
- **Technologie** - De capaciteit om technologie te ontwikkelen, selecteren, integreren, installeren en onderhouden.
- **Data-analyse** - De capaciteit om systematisch gegevens te verzamelen en verslagen, analyses en inzichten op te stellen.

Een Integrated Security programma moet een evenwicht vinden tussen een drang naar risico en, uiteraard, budgetten en bedrijfsstrategieën. Maar omdat bedreigingen voortdurend evolueren, is het belangrijk dat ook de oplossingen en tegenmaatregelen niet stilstaan. Daarom moet Integrated Security ook altijd een factor van voortdurende verbetering inhouden.

De input, in de vorm van Integrated Security, moet altijd leiden tot een zinvolle output die meer waarde biedt, risico's beheert en compliance verhoogt. Daarom leveren Integrated Security programma's een concurrentievoordeel op.

3. G4S INTEGRATED SECURITY

Bij G4S bekijken we Integrated Security aan de hand van een model en methodologie.

Het G4S Integrated Security Model geeft ons inzicht in de verbanden tussen beveiligingsoplossingen. Zo krijgen we een beter beeld van beveiliging en hoe we oplossingen kunnen optimaliseren in overeenstemming met de Belangrijkste Veiligheidseffecten van G4S: detecteren, vertragen en reageren.

Het uitgangspunt van het model is het bewezen PPT-kader (proces, personeel, technologie) om processen te stroomlijnen en de efficiëntie te verbeteren. We hebben daar nog een vierde dimensie aan toegevoegd: data, want dit is de waarde die alle beslissingen ondersteunt. Het kader wordt nu dus PPTD. Dit kader noemen we de G4S Security Methodology.

Je zou de G4S Security Methodology kunnen vergelijken met een tafel met vier poten die op een oneffen ondergrond staat. Als een van de poten iets korter of langer is, zal de tafel niet langer in evenwicht zijn en kantelen. Dat geldt ook voor Integrated Security - de combinatie van oplossingen moet in evenwicht zijn - de optimale mix die de grootste ecologische, sociale en/of economische waarde oplevert is het ideale evenwichtspunt.

Het G4S Integrated Security Model en onze G4S Security Methodology zijn gebouwd op drie domeinen van beveiligingsdiensten:

PROCES = RISICODIENSTEN (EXPERTISE)

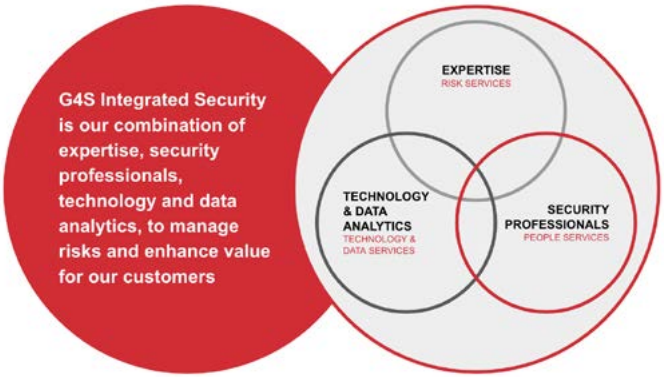
De output is bewustzijn, beleidsmaatregelen, procedures, gedrag, intelligentie, advies en ontwerp.

PERSONEEL = PERSONEELSDIENSTEN (BEVEILIGINGSPROFESSIONALS)

De output is interactie, aanwezigheid, preventie, reageren, beheren, communiceren, handelen en optimaliseren.

TECHNOLOGIE/DATA = TECHNOLOGIE- & DATADIENSTEN (TECHNOLOGIE & DATA-ANALYSE)

De output is systemen, producten, software, integratie, analyses, detecteren, vertragen, installeren en onderhouden.

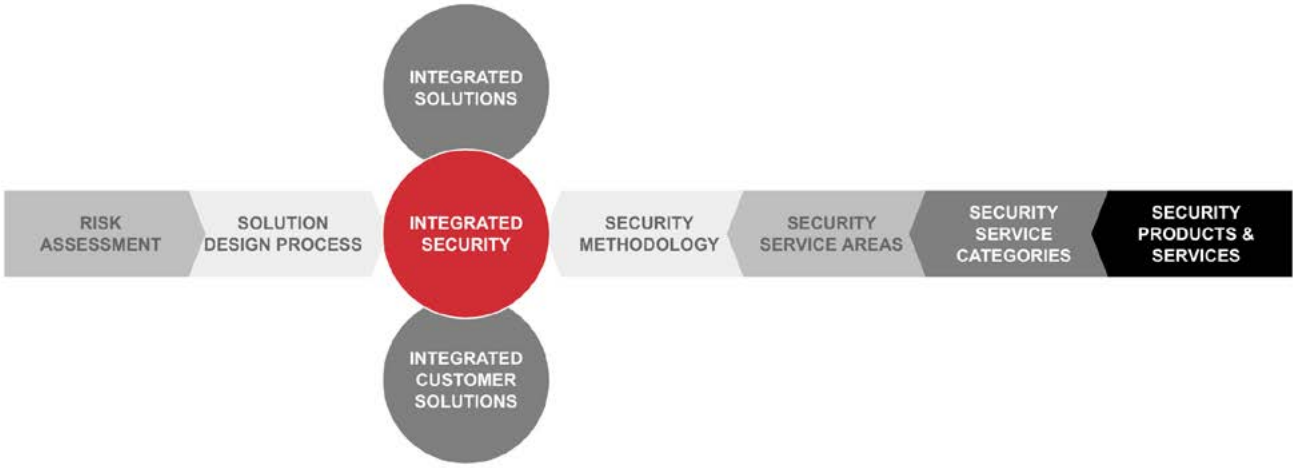


Afbeelding 3 - G4S Integrated Security

3.1 INTEGRATED SECURITY PRINCIPES

Zoals hieronder afgebeeld, begint het G4S Integrated Security Model met de klant, om te beginnen, met een risicoanalyse gevolgd door een proces om oplossingen uit te tekenen. Aan het andere uiteinde van het model, buiten de klant, begint het model met de duizenden beveiligingsproducten en -diensten die op de markt beschikbaar zijn. Bij G4S hebben we deze onderverdeeld in 25 categorieën van beveiligingsdiensten, die onder de drie domeinen van beveiligingsdiensten vallen, en uiteindelijk de vier capaciteiten van onze Security Methodology vormen.

Geïntegreerde oplossingen bestaan uit de ideale combinatie van beveiligingsproducten en -diensten uit 25 categorieën van beveiligingsdiensten die samengevoegd worden tot een volledig eenvormige oplossing om de veiligheidseffecten te bieden die u nodig hebt om uw risico's te beperken. Dit kan ook een combinatie van geïntegreerde oplossingen zijn, speciaal ontworpen voor een klant, en dan noemen we dit een Integrated Customer Solution. Dit wordt toegelicht in de onderstaande afbeelding 4 - G4S Integrated Security Principles.



Afbeelding 4 - G4S Integrated Security principes

3.2 CATEGORIEËN VAN BEVEILIGINGSDIENSTEN

De drie domeinen van beveiligingsdiensten omvatten in totaal 25 categorieën van beveiligingsdiensten en een onbeperkt aantal producten en diensten in elke categorie.

RISICODIENSTEN (EXPERTISE)

De capaciteit om advies en ondersteuning te geven bij het beheer van veiligheidsrisico's

1. Vorming en opleiding - Aan de hand van gespecialiseerde vorming en opleiding, een ruime waaier van gestandaardiseerde en op maat gemaakte inhoud aanreiken die inspeelt op de vereisten van geaccrediteerde beveiligings- en veiligheidscertificaten, zoals evacuatiebeheer, risicobeperking of oplossingenontwerp.

2. Beveiligingsadvies en -ontwerp - Aan de hand van een adviserende benadering, beveiligingsoplossingen uitwerken voor een enkel gebouw of een groot bedrijfsterrein. Op basis van een risicogebaseerde en Integrated Security benadering, inzicht verkrijgen in unieke risico's, compliancebehoeften, bedrijfswaarden en beveiligingsuitdagingen.

3. Bedrijfsonderzoek - Aan de hand van deskundig advies met op maat gemaakte bedrijfsmodellen, onderzoeksmiddelen aanreiken. Van evaluatie over ontwerp tot levering, samenwerken met klanten om een ruime waaier van fraude- en onderzoeksoplossingen aan te bieden.

4. Risico-advies en -beheer - Aan de hand van diensten inzake risico-advies en -beheer, de sector, markten en personeelsdemografie van de klant grondig doorlichten om de risico's te beoordelen en evalueren en aanbevelingen te doen over mogelijke maatregelen.

PERSONEELSDIENSTEN (BEVEILIGINGSPROFESSIONALS)

De capaciteit om beveiligingsprofessionals in te zetten met ervaring inzake risico's, oplossingen en sectoren.

5. Mobiele beveiligingsprofessionals - Werken vanuit strategische locaties om klanten van dienst te zijn met regelmatig geplande inspecties, rondes en/of onmiddellijke reactie indien er zich een veiligheidsincident voordoet.

6. Beveiligingsprofessionals ter plaatse - Een cruciale aanvulling op het personeelsbestand van de klant. De beveiligingsprofessionals ter plaatse gaan proactief te werk om mensen, eigendommen en activa te beschermen door de allerbeste serviceprincipes te hanteren en toe te passen. De teams maken ook optimaal gebruik van ondersteunende technologieën om onmiddellijk in te grijpen indien er zich een incident voordoet.

7. Geavanceerde beveiligingsprofessionals - Op basis van hogere opleidingsniveaus of kwalificaties, bijkomende lagen van beveiliging aanreiken aan de klant en meer complexe taken uitvoeren uit een hele reeks van sectoren.

8. Interventie-beveiligingsprofessionals - Door Security & Risk Operations Centres naar de vestigingen van klanten gestuurd om alarmen te controleren en inspecties uit te voeren. Ze werken vanuit strategische hubs zodat ze een klant zo snel mogelijk kunnen bereiken indien er zich een beveiligingsprobleem voordoet.

9. Beveiligingsprofessionals voor transport - Beveiligde geleidediensten aanbieden aan klanten voor het transport van mensen en/of activa. Deze diensten geven de nodige gemoedsrust aan mensen die eventueel risico lopen of activa die tijdens het transport een risico kunnen opleveren.

10. Beveiligingsoperatoren en -analisten - Datagestuurde benadering om nauwkeurige incidentenverslagen en -informatie op te stellen zodat bedrijven een stap voor kunnen blijven naarmate de bedreigingen evolueren. Zo kunnen klanten hun beveiliging bijsturen waar nodig en gefundeerde bedrijfsbeslissingen nemen.

TECHNOLOGIE- & DATADIENSTEN (TECHNOLOGIE & DATA-ANALYSE)

De capaciteit om technologie te ontwikkelen, selecteren, integreren, installeren en onderhouden en de capaciteit om systematisch gegevens te verzamelen en verslagen, analyses en inzichten op te stellen.

11. Software voor alarmcontrole - Algemeen gebruikt in Security & Risk Operation Centres. De software waarschuwt indien er een alarm afgaat en de meldingen kunnen specifiek aangepast worden aan elke klant. De software wordt beheerd vanuit een centrale locatie en bevat informatie uit diverse beveiligingstoepassingen en -apparaten. Via deze software kunnen beveiligingsprofessionals snel en efficiënt ingrijpen.

12. Fysiek beheer van beveiligingsinformatie - Softwareplatform dat gegevens over gebeurtenissen verzamelt uit diverse beveiligingstoepassingen, -systemen en -apparaten. Aan de hand van deze gegevens kunnen beveiligingsprofessionals incidenten opsporen en proactief oplossen.

13. Toepassingen inzake incident- en casemanagement - Via managementsoftware kunnen klanten de informatie in real time bekijken en erop reageren. Software voor incidentmanagement verzamelt cruciale gegevens over incidenten voor verdere analyse en maatregelen en software voor systeemmanagement brengt verslag uit over de gezondheid van beveiligingssystemen en waarschuwt indien er een probleem opduikt.

14. Screeningsystemen - Goedkeuring van bezoekers of personeel aan de hand van een aantal criteria, zoals temperatuur en aanwezigheid van verdachte of verboden materialen. Dit kan gebeuren via een hele reeks verschillende toepassingen, zoals temperatuurtechnologie, röntgenfoto's, scanners en metaaldetectors.

15. Brandpreventiesystemen - Brand- en rookmelders om de situatie in real time op te volgen. Bij een incident kunnen de systemen helpen om de brand in te dijken of, in bepaalde gevallen, te blussen door het gebruik van gassuppressie, schuimvorming of sprinklers. De systemen spelen een belangrijke rol om het gebouw en de bewoners te beschermen in geval van brand.

16. Alarmsystemen - Spelen een cruciale rol in de beveiliging door eventuele inbreuken in real time te detecteren. De alarmdetectie wordt omgezet in een signaal en/of sirene en onze beveiligingsprofessionals zullen ingrijpen volgens het met de klant overeengekomen protocol.

17. Systemen en software voor toegangscontrole - Activa beschermen door de in- en uitgang van locaties te controleren. Het platform controleert de personeelscapaciteit en bezettingsniveaus en stelt analyses op met behulp van software voor bezoekers- en identiteitsbeheer die gestuurd kan worden vanuit een centrale locatie.

18. Systemen en software voor videobewaking - Een platform om de gebouwen en/of activa van een klant in real time te bewaken en onmiddellijk in te grijpen als er iets gebeurt.

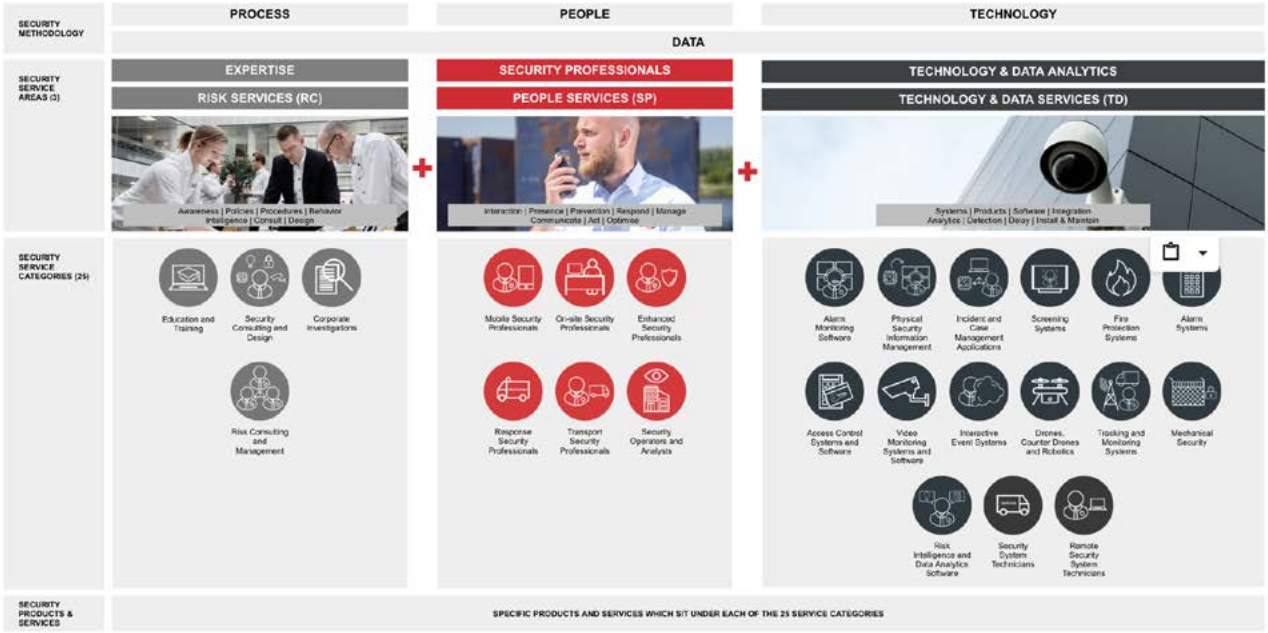
19. Interactieve eventsystemen - Een actieve vorm van preventieve beveiliging in de vorm van rook (mist) en/of onzichtbare inkt om activa te kunnen traceren.

20. Drones, afweerdrones en robotica - Met beveiligingsdrones, afweerdrones en robotica kunnen klanten terroristen, indringers, criminelen en rellen afweren op een veilige en efficiënte manier. Deze bewakingstechnologie kan ook een extra beveiligingslaag toevoegen, in combinatie met beveiligingsprofessionals, om de gebouwen en/of activa van een klant te controleren en te beschermen. Met nauwkeurige gegevens vanuit de lucht in real time kunnen agenten de beste beslissingen nemen om elke veiligheidssituatie aan te pakken.

21. Traceer- en controlesystemen - Klanten hebben zicht op afgezonderde werknemers, activa of voertuigen. Ideaal om waardevolle activa te beheren of voor werknemers die blootgesteld zijn aan gevaarlijke omgevingen. De systemen werken in real time zodat elke verdachte of gevaarlijke activiteit snel opgemerkt wordt.

22. Mechanische beveiliging - Opties voor mechanische beveiliging, zoals fysieke barrières en automatische deuren/poorten/hekken, kunnen de toegang tot een gebied vertragen. Op die manier kan de toegang voorkomen of aanzienlijk beperkt worden indien er zich een veiligheidsincident voordoet.

23. Software voor risico-informatie en data-analyse - Bruikbare en uitgebreide inzichten verkrijgen zodat klanten kunnen anticiperen en reageren op bedreigingen en deze kunnen opvolgen en melden vanuit een centrale locatie. In combinatie met door AI aangevulde gegevens met een uitgebreide globale voetafdruk en netwerken op het terrein. Dit levert



Afbeelding 5 - G4S Integrated Security bouwstenen

datagestuurde vooruitzichten op voor bedrijven, overheden en klanten die werken op complexe, onbekende of risicovolle markten.

24. Technici gespecialiseerd in beveiligingssystemen - Hoogopgeleide technici die diensten inzake installatie, onderhoud en herstelling aanbieden zodat cruciale beveiligingssystemen met zo weinig mogelijk storingen kunnen werken.

25. Technici gespecialiseerd in beveiligingssystemen op afstand - Hoogopgeleide technici die werken binnen strikte service level agreements om diagnose-advies te geven en problemen met beveiligingssystemen te troubleshooten. Zo kunnen klanten rekenen op de continue service die nodig is om de systemen operationeel te houden.

3.3 NIEUWE ONTWIKKELINGEN

Er worden voortdurend nieuwe producten en diensten ontwikkeld op het vlak van beveiliging, de sector staat nooit stil. Drones, afweerdrones en robotica, het zijn maar enkele voorbeelden van meer recente categorieën van beveiligingsdiensten die de voorbije jaren op de markt zijn gebracht. Daarnaast zijn er duizenden producten en diensten in de 25 categorieën van beveiligingsdiensten.

Het is dan ook belangrijk om te beseffen dat beveiliging voortdurend evolueert en nooit zal stilstaan. En dat geldt ook voor de bedreigingen. Daarom moeten we de beveiligingssector professionaliseren en onze kennis delen.

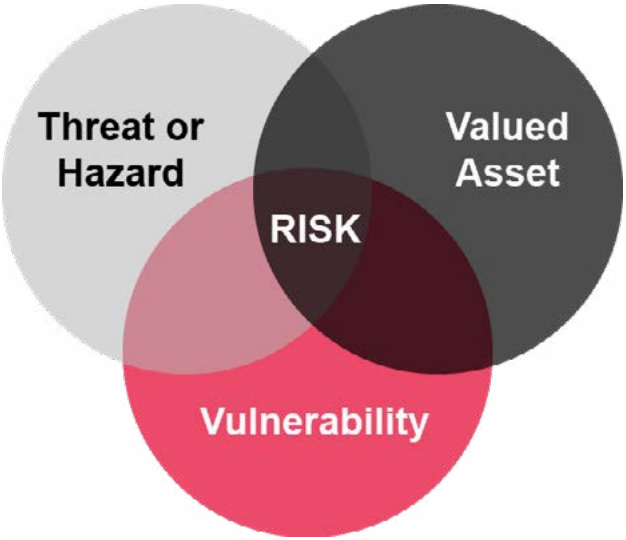
3.4 DE COMBINATIE

Om meer inzicht te krijgen in de belangrijkste veiligheidseffecten en Integrated Security, doorlopen we een scenario.

Stel u voor: u legt een baar goud in een open veld. Die baar goud is voor u uiteraard heel waardevol en u wilt niet dat die gestolen wordt.

Er is een dief in de buurt die op zoek is naar goud. U beschermt het goud op geen enkele manier en verbergt het niet. Hoewel de dief niet precies weet waar uw goud zich bevindt, is de kans groot dat het goud gestolen wordt.

Risico is het resultaat van een bedreiging die of gevaar dat een actief bereikt door een kwetsbaarheid en schade veroorzaakt, het actief vernietigt of de toegang ertoe ontzegt.



Afbeelding 6 - Het opstellen van beveiligingsrisico's

In het bovenstaande diagram stelt het goud uw waardevol actief voor. De bedreiging is de dief die op zoek is naar goud. De kwetsbaarheid is het gebrek aan eender welke bescherming. Deze drie elementen creëren risico.

We kunnen het risico beperken door de kwetsbaarheid van het goud te beperken. Om te achterhalen hoe we deze kwetsbaarheid kunnen beperken, moeten we de laatste vraag van de risicogebaseerde benadering beantwoorden, 'Hoe kunt u uw activa zo efficiënt mogelijk beschermen?'. Daarbij gaan we op zoek naar de meest efficiënte oplossingen om de risico's te verkleinen. Zo zal de kwetsbaarheid verminderen en daarmee ook het risico.

We weten instinctief dat we het risico dat het goud gestolen wordt kunnen beperken door dit op een of andere manier te beschermen. In de veronderstelling dat u het goud niet kunt verplaatsen, kunt u het volgende doen:

BENADERING 1 (VOORWERP)

- Gegevens opzoeken en analyseren over de bedoelingen en capaciteiten van de dief (risico-advies en -beheer)
- Het goud in een kluis bewaren (technologische beveiliging)
- De kluis vergrendelen en van een alarm voorzien (vorming en opleiding)
- Het alarm controleren (alarmsystemen)
- De kluis in de gaten houden met videobewakingssystemen (systemen en software voor videobewaking)

BENADERING 2 (CEL)

- Een veilige ruimte rond de kluis bouwen (mechanische beveiliging)
- Een interactief eventsysteem in de veilige ruimte installeren (bv. mist) (interactieve eventsystemen)
- De toegang tot de veilige ruimte strikt controleren (vorming en opleiding)
- De veilige ruimte vergrendelen en van een alarm voorzien (vorming en opleiding)
- Het alarm controleren (alarmsystemen)
- Een beveiligingsprofessional aan de deur van de veilige ruimte plaatsen (beveiligingsprofessionals ter plaatse)
- De ingang van de veilige ruimte in de gaten houden met videobewakingssystemen en -software (systemen en software voor videobewaking)
- De gegevens van de toegangscontrole en de videobewakingsbeelden van de veilige ruimte verzamelen en analyseren om de beveiliging en de beveiligingsactiviteiten te verbeteren (vorming en opleiding)

BENADERING 3 (GEBOUW)

- Een gebouw rond de veilige ruimte bouwen (mechanische beveiliging)
- Het gebouw vergrendelen en van een alarm voorzien (vorming en opleiding)
- Het alarm controleren (alarmsystemen)
- De toegang tot het gebouw controleren (systemen en software voor toegangscontrole)
- De ingang van het gebouw in de gaten houden met videobewakingssystemen en -software, alsook de binnen- en buitenkant van het gebouw (systemen en software voor videobewaking)
- De gegevens van de toegangscontrole en de videobewakingsbeelden van het gebouw verzamelen en analyseren om potentiële afwijkingen op te sporen (vorming en opleiding)
- Beschikken over beveiligingsprofessionals ter plaatse en geavanceerde beveiligingsprofessionals binnen en buiten het gebouw (beveiligingsprofessionals ter plaatse/geavanceerde beveiligingsprofessionals)

BENADERING 4 (PERIMETER)

- Een hek optrekken rondom uw gebouw (mechanische beveiliging)
- Alarmsystemen installeren op uw hek (alarmsystemen)
- Het hek in de gaten houden met videobewakingssystemen en -software (systemen en software voor videobewaking)
- Systemen voor toegangscontrole installeren om de toegang tot uw site te beheren (systemen en software voor toegangscontrole)
- Uw systemen en software voor videobewaking aanvullen met risico-informatie en data-analyse (software voor risico-informatie en data-analyse)
- Alle beveiligingstoepassingen sturen vanuit een systeem voor fysiek beveiligingsinformatiebeheer (fysiek beveiligingsinformatiebeheer)
- Interventie-beveiligingsprofessionals paraat houden als versterking indien nodig (interventie-beveiligingsprofessionals)
- Mobiele beveiligingsprofessionals opstellen buiten het hek (mobiele beveiligingsprofessionals)
- De locatie van uw beveiligingsprofessionals traceren en volgen (traceer- en controlesystemen)
- Beschikken over een programma voor bijscholing en opleiding om de veiligheidscultuur van uw werknemers te verbeteren en te behouden (vorming en opleiding)

Enzovoort ... De bovenstaande lijst is een voorbeeld van wat u zou kunnen doen. Elke situatie is anders en elk veiligheidsplan moet intelligent en proportioneel zijn.

Laten we eens bekijken waar het hier echt om gaat. De bovenstaande lijst gaat uit van het actief en geeft een overzicht van mogelijke tegenmaatregelen, vertrekkende vanuit het goud tot aan de perimeter van het terrein. Maar laten we nu eens vertrekken vanuit het standpunt van de bedreiging, in plaats van uit te gaan van het actief. Laten we eens bekijken welke effecten we creëren vanuit het standpunt van de bedreiging en naar binnen toe werken. Vanaf de perimeter van het terrein worden de bedreigingen geconfronteerd met het volgende:

DETECTEREN - We hebben tegenmaatregelen ingevoerd om de bedreiging te detecteren. In ons voorbeeld doen we dit door:

- Vorming en opleiding
  (Beschikken over een programma voor bijscholing en opleiding om de veiligheidscultuur van uw werknemers te verbeteren en te behouden)
- Traceer- en controlesystemen
  (De locatie van uw beveiligingsprofessionals traceren en volgen)
- Mobiele beveiligingsprofessionals
  (Mobiele beveiligingsprofessionals opstellen buiten het hek)
- Fysiek beveiligingsinformatiebeheer
  (Alle beveiligingstoepassingen sturen vanuit een systeem voor fysiek beveiligingsinformatiebeheer)

- **Software voor risico-informatie en data-analyse**
  (Uw systemen en software voor videobewaking aanvullen met risico-informatie en data-analyse)
- **Systemen en software voor toegangscontrole**
  (Systemen voor toegangscontrole installeren om de toegang tot uw site te beheren)
- **Systemen en software voor videobewaking**
  (Het hek in de gaten houden met videobewakingssystemen en -software)
- **Alarmsystemen**
  (Alarmsystemen installeren op uw hek)

VERTRAGEN - De volgende tegenmaatregelen zorgen voor een vertraging in de voortgang van de bedreiging:

- **Mobiele beveiligingsprofessionals**
  (Mobiele beveiligingsprofessionals opstellen buiten het hek)
- **Interventie-beveiligingsprofessionals**
  (Interventie-beveiligingsprofessionals paraat houden als versterking indien nodig)
- **Systemen en software voor toegangscontrole**
  (Systemen voor toegangscontrole installeren om de toegang tot uw site te beheren)
- **Mechanische beveiliging**
  (Een hek optrekken rondom uw gebouw)

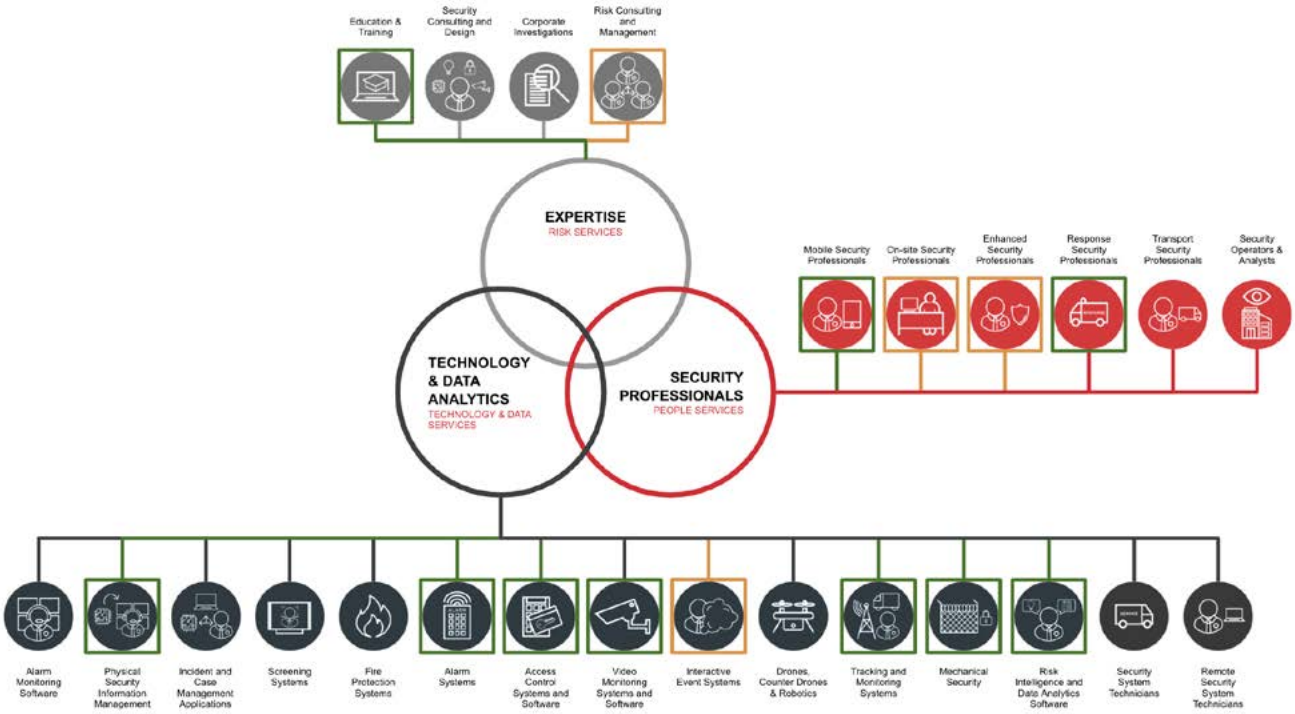
REAGEREN - Het laatste effect is reageren. Dit kan gebeuren door een van de volgende elementen:

- **Vorming en opleiding**
  (Beschikken over een programma voor bijscholing en opleiding om de veiligheidscultuur van uw werknemers te verbeteren en te behouden)
- **Traceer- en controlesystemen**
  (De locatie van uw beveiligingsprofessionals traceren en volgen)
- **Mobiele beveiligingsprofessionals**
  (Mobiele beveiligingsprofessionals opstellen buiten het hek)
- **Interventie-beveiligingsprofessionals**
  (Interventie-beveiligingsprofessionals paraat houden als versterking indien nodig)
- **Interactief eventsysteem**
  (om het actief te hullen in mist als dit aangevallen wordt)

Na de perimeter van het terrein (benadering 4) staat de bedreiging voor het gebied tussen de perimeter en het gebouw, dan de gevels van het gebouw (benadering 3), dan de cel/kluis (benadering 2) en tot slot het voorwerp/de safe (niveau 1). Dit zijn allemaal bijkomende lagen en elke laag bestaat uit functies van detecteren, vertragen en reageren. De combinatie van de categorieën van beveiligingsdiensten (en de beveiligingsproducten en -diensten) creëert de optimale Integrated Securitysoplossing voor het goud.

Op die manier realiseren we ook een heel diepgaande beveiliging, hoe meer diepgang, hoe meer lagen de bedreiging moet doorboren en zo daalt ook de kans dat het doel (het goud stelen) bereikt wordt.

In afbeelding 7 geven de groene kaders de categorieën van beveiligingsdiensten weer die gebruikt werden in benadering 4, de oranje kaders geven de bijkomende categorieën van beveiligingsdiensten weer die werden gebruikt in benadering 3, 2 en 1. Zoals we zien, werden in dit voorbeeld de meeste categorieën gebruikt uit het volledige spectrum van de 25 categorieën van beveiligingsdiensten.



Afbeelding 7 - Integrated Security - categorieën van beveiligingsdiensten

3.5 HET OPTIMALE INTEGRATED SECURITY PROGRAMMA

De meest optimale en 'juiste' combinatie van oplossingen voor u wordt bepaald door hoe cruciaal uw activa zijn en welk type van bedreigingen aangetrokken wordt door uw activa. Andere factoren die vorm geven aan uw oplossing zijn uw individuele (bedrijfs)strategie, de output van de vereiste ecologische, sociale en/of economische waarden, uw risico's en het vereiste complianceniveau.

Bij G4S beschrijven we Integrated Security als 'onze combinatie van expertise, beveiligingsprofessionals, technologie en data-analyses om risico's te beheren en meer waarde te creëren voor onze klanten'. De belangrijkste woorden in deze definitie zijn de laatste drie: 'voor onze klanten'. Op verzoek zal G4S bij het ontwerp van uw Integrated Security een klantgerichte benadering hanteren en wij raden u aan om hetzelfde te doen vanuit een bedrijfsgericht standpunt.

Om Integrated Security te ontwerpen, moet u eerst de verbanden tussen de functies vertragen, detecteren en reageren begrijpen.

Bijvoorbeeld:

Hoeveel vertraging zal de goudsafe in het bovenstaande voorbeeld opleveren? Wanneer zal de aanval worden gedetecteerd? En hoe snel kan de interventiefunctie ter plaatse zijn?

Maar er is meer: wat is het bedreigende element, welke tools zullen er gebruikt worden, hoeveel bedreigende elementen zullen er zijn? (dus inzicht hebben in hun waarschijnlijke capaciteit en bedoeling).

Om deze vragen te beantwoorden, moet u een risicobeoordeling en -analyse uitvoeren en daarna dan bepalen welke risico's u zult dekken en welke u zal moeten aanvaarden als resterende risico's. Om Integrated Security te ontwerpen en implementeren, moet u bovendien inzicht hebben in uw onderneming, uw risico's en de veiligheidsmaatregelen waarover u beschikt. Dit betekent dat u technische ondersteuning nodig hebt om de oplossing te vinden die perfect bij u past. Schuif bepaalde opties niet te snel opzij en gebruik een holistische strategie, ga op zoek naar een partner of partners met een volledig overzicht van alle 25 categorieën van beveiligingsdiensten en de capaciteit om de duizenden beveiligingsproducten en -diensten die op de markt beschikbaar zijn uit te pluizen en te vergelijken.

In veel bedrijven legt de verzekeraar ook beperkingen op met specifieke beveiligingsvereisten in overeenstemming met lokale, regionale of internationale beveiligingsnormen. Andere zijn gebonden aan complianceregels met betrekking tot ISO-normen, FDA-normen en/of soortgelijke voorschriften. In bepaalde bedrijven zijn specifieke voorschriften (bv. cruciale infrastructuur) van toepassing die gevolgd moeten worden. Uw optimale Integrated Security programma moet ook rekening houden met deze regels, voorschriften en beperkingen.

Tot slot moet een optimaal Integrated Security programma ook trachten om zo toekomstbestendig mogelijk te zijn, digitalisering is een realiteit. Bij de samenstelling van uw Integrated Security programma moet u beveiligingsmaatregelen kiezen die aansluiten bij deze digitalisering en bij de meest recente technologische ontwikkelingen. Het gebruik van videobewakingssystemen met geavanceerde AI en/ of toegangscontrolesystemen in combinatie met biometrie zijn twee voorbeelden van toekomstgerichte beveiligingsmaatregelen. Deze systemen kunnen u bovendien helpen om het ideale evenwicht te vinden tussen kosten en bescherming door recurrente kosten af te wegen tegen investeringskosten.

4. POSTSCRIPTUM

Deze whitepaper werd opgesteld door de G4S Academy.

Deze whitepaper kan vooruitblikkende verklaringen bevatten, waaronder verklaringen over onze bedoelingen, overtuigingen of huidige verwachtingen met betrekking tot de fysieke beveiligingsbedrijven en -activiteiten. Lezers worden gewaarschuwd niet te veel te berusten op deze vooruitblikkende verklaringen.

Deze whitepaper heeft niet tot doel om een volledig en allesomvattend beeld te schetsen van Integrated Security, maar om meer informatie te geven en kwalitatieve inzichten te verschaffen van G4S-experts om u aan het denken te zetten over hoe de beveiligingstoekomst van uw organisatie er zal uitzien.

De informatie die G4S in deze whitepaper geeft, is enkel bedoeld voor algemene informatieve doeleinden. We geven geen enkele voorstelling of garantie, uitdrukkelijk of impliciet, over de nauwkeurigheid, gepastheid, geldigheid, betrouwbaarheid, beschikbaarheid of volledigheid van de informatie. In geen enkel geval kunnen wij aansprakelijk gesteld worden voor eender welke verliezen of schade als gevolg van het gebruiken van of het vertrouwen op eender welke informatie verschaft in deze presentatie.

Aansluitend bij de benadering 'Knowledge Created Together' en 'Value Created Together' van onze G4S Academy horen wij graag uw feedback en mening over deze gids. Samen weten we meer. U kunt uw meningen, positieve en negatieve opmerkingen doorsturen naar g4sacademy@be.g4s.com.

Deze whitepaper en eventuele geschillen of vorderingen (inclusief niet-contractuele geschillen of vorderingen) die voortvloeien uit of in verband met de whitepaper of de inhoud of opstelling ervan worden beheerst door en geïnterpreteerd volgens de wet van België. De Nederlandstalige rechtbanken van Brussel zijn als enige bevoegd om te beslissen over eventuele geschillen of vorderingen (inclusief niet-contractuele geschillen of vorderingen) die voortvloeien uit of in verband met dit document of de inhoud of opstelling ervan.

G4S

G4S is de grootste beveiligingsonderneming ter wereld. We bieden een brede waaier van beveiligingsdiensten, geleverd op basis van een enkele dienst, meerdere diensten of een geïntegreerd pakket, op zes continenten.

Onze groeiende focus op geïntegreerde, door technologie mogelijk gemaakte oplossingen levert bijkomende voordelen inzake beveiliging en efficiëntie op voor onze klanten. Op die manier kunnen wij het aanbod van G4S op de beveiligingsmarkt ook beter onderscheiden en dat draagt dan weer bij tot onze doelstelling om onze winstgevendegroei te versnellen.

Onze activiteiten zijn onderverdeeld in drie kerndiensten: Secure Solutions, Risk Consulting Services en Care and Justice Services.

G4S ACADEMY

De G4S Academy is een platform binnen G4S dat ons in staat stelt om nauwer samen te werken met onze klanten, leveranciers, partners en andere belanghebbenden om zo samen kennis en waarde op te bouwen.

De G4S Academy heeft als doel om kennis te creëren en te delen op basis van onze globale expertise zodat wij voor nog betere veiligheid en beveiliging kunnen zorgen en waarde kunnen creëren voor onze klanten. Beveiliging en veiligheid zijn uitgegroeid tot een fundamenteel onderdeel van de bedrijfsactiviteiten. Bij veel van onze traditionele klanten komt de focus nu meer te liggen op een sterkere bedrijfsgroei in plaats van het beheer van veiligheid en beveiliging. Dat is een van de grootste uitdagingen waar bedrijfsleiders in de beveiligingssector vandaag mee te maken krijgen en zo worden we allemaal gedwongen om op een heel andere manier te communiceren over onze waarde.

Via de G4S Academy kunnen we een cultuur creëren die traditionele ideeën over beveiliging in vraag stelt, die openstaat voor technologische veranderingen en die anticipeert op toekomstige beveiligingsvereisten door onze kennis en expertise te benutten en te delen met beveiligingsprofessionals. Wij zetten ons in om relevante, actuele inhoud te verschaffen via alle mogelijke media.

Meer informatie over de G4S Academy vindt u op www.g4s.be/academy

VALUE CREATED TOGETHER

CONTACT

NEEM CONTACT OP MET HET G4S TEAM – CHECK WWW.G4S.BE

V1 MEI 2021