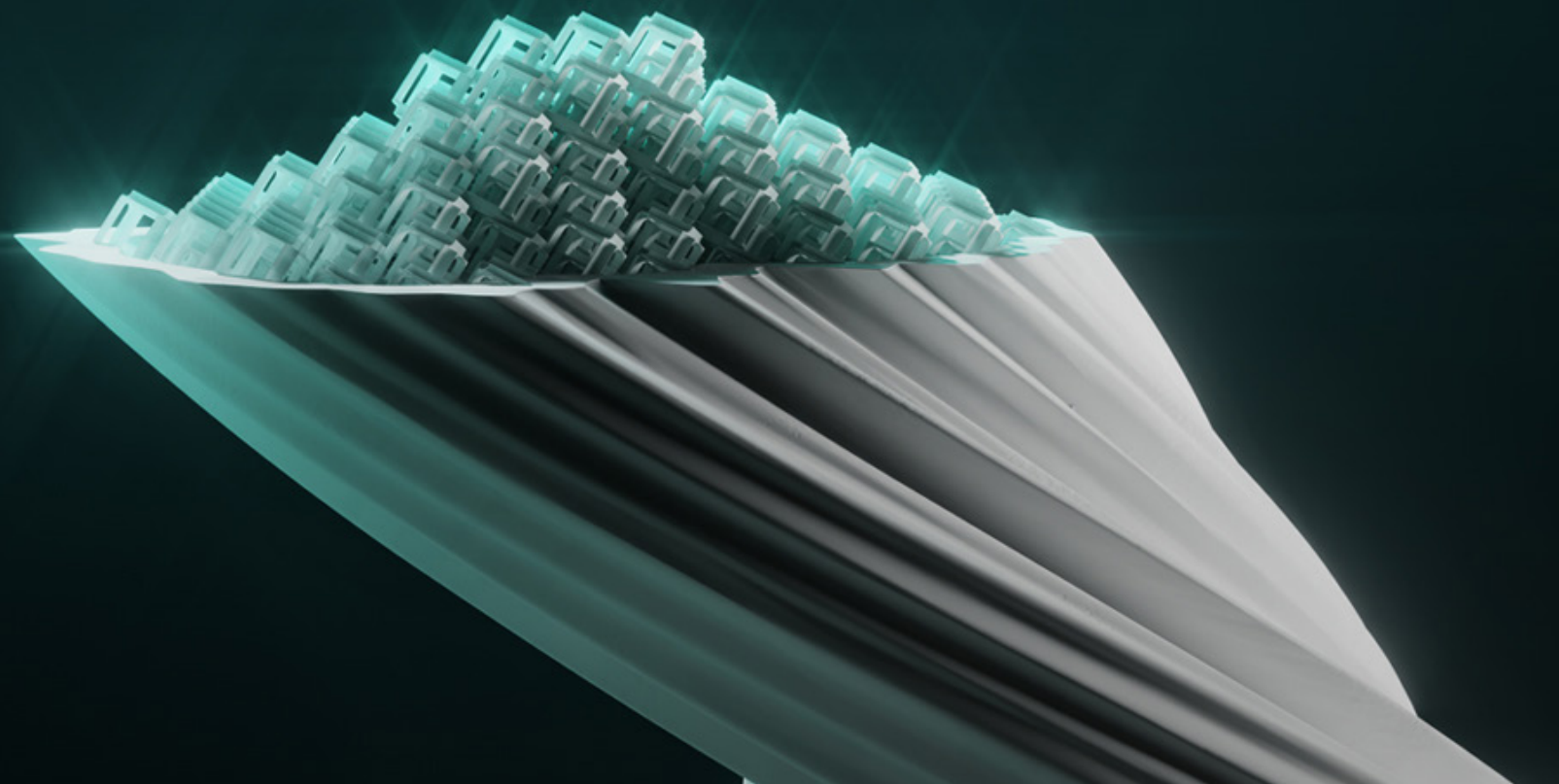
# DE TOP 5 VIJF SECURITY-UITDAGINGEN CHALLENGES VOOR CISO'S

Waar moet je op letten in het post-pandemie tijdperk?



ESET®

Digital Security
**Progress. Protected.**

CISO's weten dat cybersecuritytrends zich relatief langzaam over de jaren heen ontwikkelen. Er is zelden een blikseminslag van innovatie op het gebied van cybercriminaliteit die een radicale herstructurering van de strategie vereist. Maar de pandemie heeft dit uitgangspunt volledig veranderd.

Van de ene op de andere dag werden organisaties gedwongen om hun bedrijfsprocessen volledig te herzien, om massaal thuiswerken te ondersteunen en nieuwe manieren te creëren om hun klanten te bereiken. Bij ESET schakelden we honderden werknemers binnen enkele dagen om naar werken op afstand, ondanks de nodige VPN- en cloudknelpunten en hardware-uitdagingen.

Helaas hebben deze nieuwe digitale investeringen en werkwijzen in veel gevallen nieuwe mogelijkheden voor dreigingsactoren gecreëerd. De hoeveelheid phishing steeg exponentieel. Ransomware-actoren profiteerden van kwetsbaarheden in VPN's en verkeerd geconfigureerde RDP-verbindingen. Slecht beveiligde cloudapps werden een belangrijk aanvalsdoel. De dreigingspiek vertelde organisaties wat CISO's al wisten – dat het prioriteren van bedrijfscontinuïteit boven alles aanzienlijke risico's met zich meebrengt.

# 7.3%

Toename van kwaadaardige schadelijke e-mails in T2 2021, vergeleken met T1 2021

Bron: ESET Threat Report T2 2021

Digital Security
Progress. Protected.

"Werknemers, waarvan velen nog steeds thuiswerken, zijn gewend geraakt aan het elektronisch uitvoeren van veel administratieve taken – en cybercriminelen maken hier dankbaar misbruik van."

**Jiří Kropáč**

ESET Head of Threat Detection Labs

Bron: ESET Threat Report T2 2021

# **Hoe kunnen we**
# opkomende risico's beperken?

Nu we het ergste van de coronacrisis achter de rug hebben, moeten organisaties hun risicobereidheid en de gewenste balans tussen bedrijfsvoering en beveiliging opnieuw evalueren. De hybride werkplek waar de meesten voor kiezen zal een veranderlijkere, meer open omgeving zijn dan die van voor de pandemie. Voor velen moet de nadruk daarom nu liggen op risicobeperking die de productiviteit niet al te zeer beïnvloedt.

Hoewel organisaties weer een intensieve periode van verandering ingaan, blijven de best practices op het gebied van digitale beveiliging gelukkig net zo relevant als voorheen, en bieden nieuwe benaderingen innovatieve oplossingen voor opkomende uitdagingen. Dit handboek helpt CISO's in te schatten welke risico's het dringendst zijn en met welke maatregelen deze het beste kunnen worden beperkt.


eset
Digital Security
Progress. Protected.

# 1 Omgaan met de krappe arbeidsmarkt voor securityspecialisten

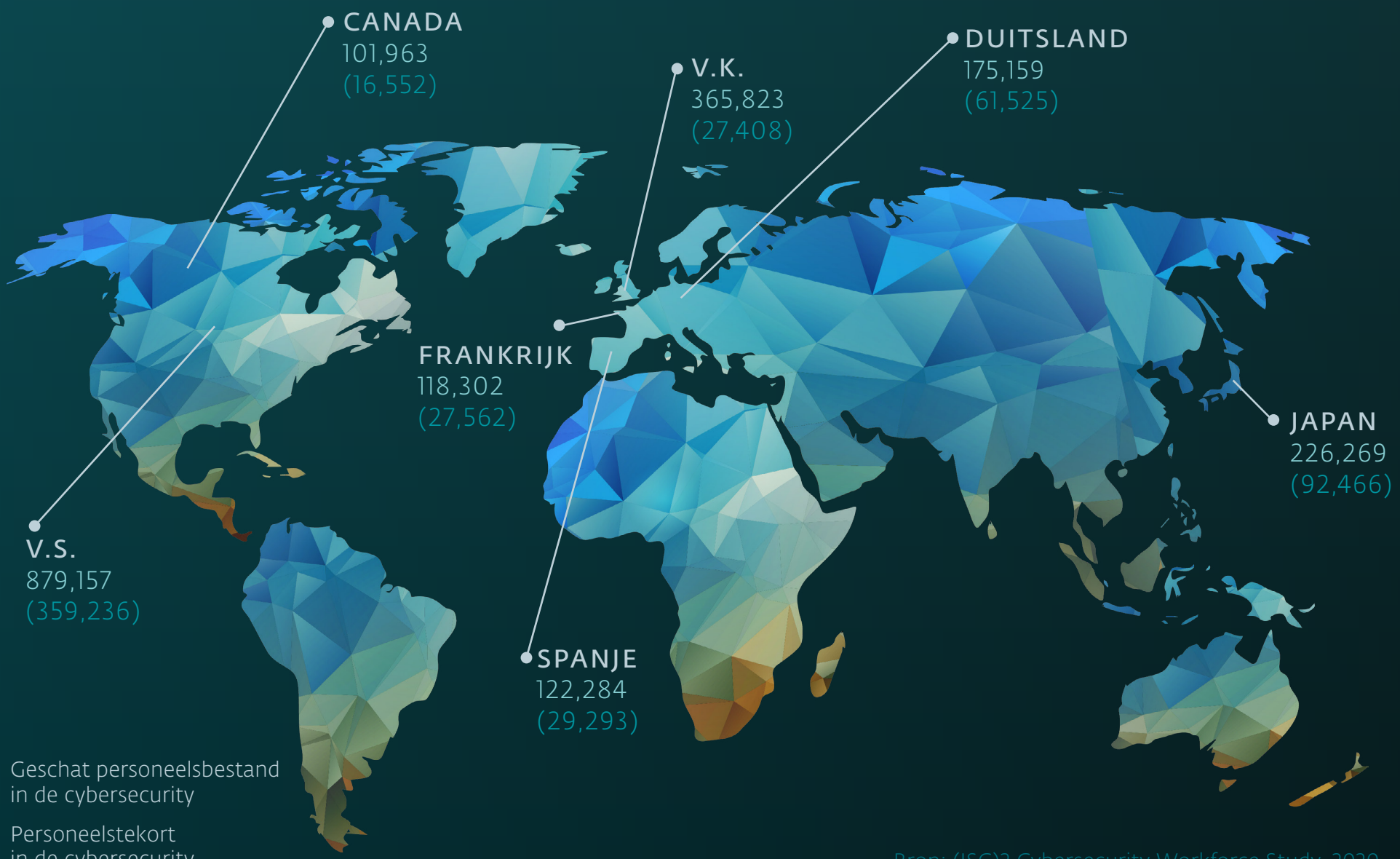
We weten allemaal dat het steeds moeilijker wordt om geschoolde securitytalenten te werven. Hoewel de personeelskloof in 2020 voor het eerst is gedicht, bedraagt het wereldwijde tekort aan gekwalificeerde professionals nog steeds meer dan drie miljoen. Door de snelle groei van cloud, IoT en andere digitale transformatieprojecten is de vraag naar securityvaardigheden veel groter dan het aanbod.

Naarmate deze investeringen doorzetten in het post-pandemietijdperk, zal dit tekort nijpender worden, vooral wanneer oudere professionals met pensioen gaan. Vooral de behoefte aan talent voor cloud security is bijzonder groot. De toename van misconfiguratie-incidenten benadrukt de potentiële impact voor bedrijven.

Regeringsplannen om meer studenten aan te moedigen te kiezen voor deze industrie moeten worden toegejuicht, maar zelfs als ze succesvol zijn, zal het jaren duren om hiervan de impact te merken. In de tussentijd zouden CISO's moeten proberen gebruik te maken van technologie en uitbesteding om de ergste effecten van de arbeidskrapte te beperken.

Dat betekent: machine learning en automatisering inzetten om bepaalde werkzaamheden als accountbeheer, beleidsoptimalisatie, code-audits en Threat Detection & Response over te nemen. Er is een groeiend aanbod van Managed Detection & Response (MDR)-diensten die CISO's nieuwe mogelijkheden bieden om het beheer van EDR- en XDR-oplossingen uit handen te geven. Dit helpt niet alleen om de uitdagingen op het gebied van personeel te verlichten, maar verlegt deze taken ook naar getrainde deskundigen, die hun expertise en brede inzicht in de sector kunnen inbrengen.

# Geschat wereldwijd personeelsbestand
## en -tekort op het gebied van security




Bron: (ISC)2 Cybersecurity Workforce Study, 2020

Voor IT-bedrijven is er ook een belangrijke rol weggelegd. Door het opzetten van IT-hubs, onderwijsprogramma's en andere activiteiten, waaronder vrijwilligerswerk (zoals veel ESET-medewerkers doen), kunnen zij helpen met het stimuleren van het cyberbewustzijn en de belangstelling voor dit vakgebied onder scholieren. Een lokaal initiatief, dat gesteund wordt door ESET in Nederland, is HackShield Future Cyberheroes: een spel voor kinderen tussen de 8 en 12 jaar, dat hen (online) skills leert om zich te wapenen tegen cybercriminaliteit.

Ook awarenesstrainingen zijn van groot belang voor iedereen, om meer te leren over veelvoorkomende vormen van digitale criminaliteit en deze te herkennen. ESET's gratis cybersecuritytraining behandelt onder meer veilig internetten, malware, phishing en goede wachtwoordhygiëne.

**67%**

van de bedrijfsleiders begrijpt het belang van beveiliging in remote werkomgevingen. Gebrek aan bewustzijn bij het bestuur heeft echte impact op teams.

Bron: (ISC)2 Cybersecurity Workforce Study, 2020


ESET MANAGED DETECTION &
RESPONSE-DIENSTEN
Voorkom. Reageer. Voorspel.
Maak gebruik van de vaardigheden van onze
eersteklas IT Security-onderzoeksteams
Ontdek meer
eset
Digital Security
Progress. Protected.


eset
Digital Security
Progress. Protected.

# 2 Beheer third-party risico's

Tijdens de pandemie werd er scherper gekeken naar de distributieketens. Dat is een goede zaak. Veel bedrijven vinden het zo vanzelfsprekend dat ze niet eens weten hoeveel externe leveranciers ze gebruiken om essentiële producten en diensten te leveren. Helaas kunnen de partijen die jouw organisatie contracteert ook een groot cyberrisico vormen, vooral als ze toegang krijgen tot bedrijfsnetwerken en -middelen. Sommige organisaties, zoals bleek uit een onderzoek uit 2018, beschouwen medewerkers en contractanten als 'de zwakste schakel' in de beveiligingsketen. Zij worden potentieel verantwoordelijk gehouden voor datalekken, phishingaanvallen en ransomware-compromissen. Wij vinden echter dat het onjuist is om deze verantwoordelijkheid volledig bij medewerkers zelf neer te leggen: zij moeten niet de schuld krijgen van het feit dat aanvallers vandaag de dag geraffineerde manieren vinden om hen via (spear)phishing te bereiken. In eerste instantie ligt de verantwoordelijkheid bij de organisatie, om de juiste beveiligingsoplossingen in te zetten en medewerkers de basismaatregelen bij te brengen, om zo medewerkers op securitygebied zoveel mogelijk te ontzorgen.

CISO's willen idealiter dat hun leveranciers hetzelfde of een beter beveiligingsniveau hebben als hun eigen organisatie. Om dit te bereiken is continue evaluatie nodig, bijvoorbeeld op basis van vragenlijsten die voortkomen uit intern beleid en normen.

Certificeringen van leveranciers kunnen ook nuttig inzicht geven in de invoering van controles en sommigen kunnen automatisch worden geëvalueerd. Sterker nog, automatisering in de vorm van Vendor Risk Management (VRM)-tools is altijd nuttig om publieke gegevens te controleren en het security-volwassenheidsniveau van leveranciers op verschillende gebieden in te schatten. Sommige leveranciers zetten zelfs eigen honeypots in om op aanvallen te controleren. Organisaties moeten zich eerst afvragen wat hun prioriteiten zijn met VRM en op basis van deze antwoorden een strategie ontwikkelen.


Breid uw security intelligence uit van lokale netwerken naar de wereldwijde cyberspace, met ESET Threat Intelligence-rapporten en feeds.
Ontdek meer
eset
Digital Security
Progress. Protected.

**66%**
van de bedrijfsleiders zegt te overwegen kantoorruimte te herinrichten.

**73%**
van de werknemers wil flexibel blijven in hun werkmogelijkheden.

**67%**
van de werknemers wil ook meer samenwerking op locatie.

Digital Security
Progress. Protected.

Bron: Microsoft 2021

# 3 De nieuwe realiteit van de hybride werkplek

Hybride werken is een kans om het beste van twee werelden te hebben: voldoen aan nieuwe verwachtingen van werknemers rondom de balans tussen werk en privéleven, en het stimuleren van innovatie door face-to-face interactie. Maar het stelt organisaties ook bloot aan de risico's van werken op afstand: afgeleide gebruikers, ongepatchte endpoints en infrastructuur voor externe toegang, zwakke accountwachtwoorden en foutief geconfigureerde cloudinstanties.

Bovendien is er een verhoogd risico op verloren of gestolen apparaten, meekijkers en onbeveiligde wifinetwerken die gevolgen hebben voor werknemers nu ze weer kunnen reizen.

CISO's moeten het securitybeleid van hun organisatie herzien met het oog op dit nieuwe landschap. Dat kan betekenen dat er MFA wordt uitgerold en strengere toegangscontroles en microsegmentatie worden geïmplementeerd als onderdeel van Zero Trust. Het kan ook leiden tot het uitbesteden van threat detection en -response via MDR, en het opzetten van nieuwe (awareness-)trainingen voor werknemers. Het belangrijkste is dat het gaat om een combinatie van mensen, processen en technologie op basis van best practices, zoals degenen die hiernaast worden genoemd.

**Lees meer over hoe u werknemers die op afstand werken kunt beveiligen**

# 10 STAPPEN NAAR CYBERVEILIGHEID

Waarop moet u zich richten als u uw bedrijf effectief wilt beschermen?


Bron: NCSC 2021


eset
Digital Security
Progress. Protected.

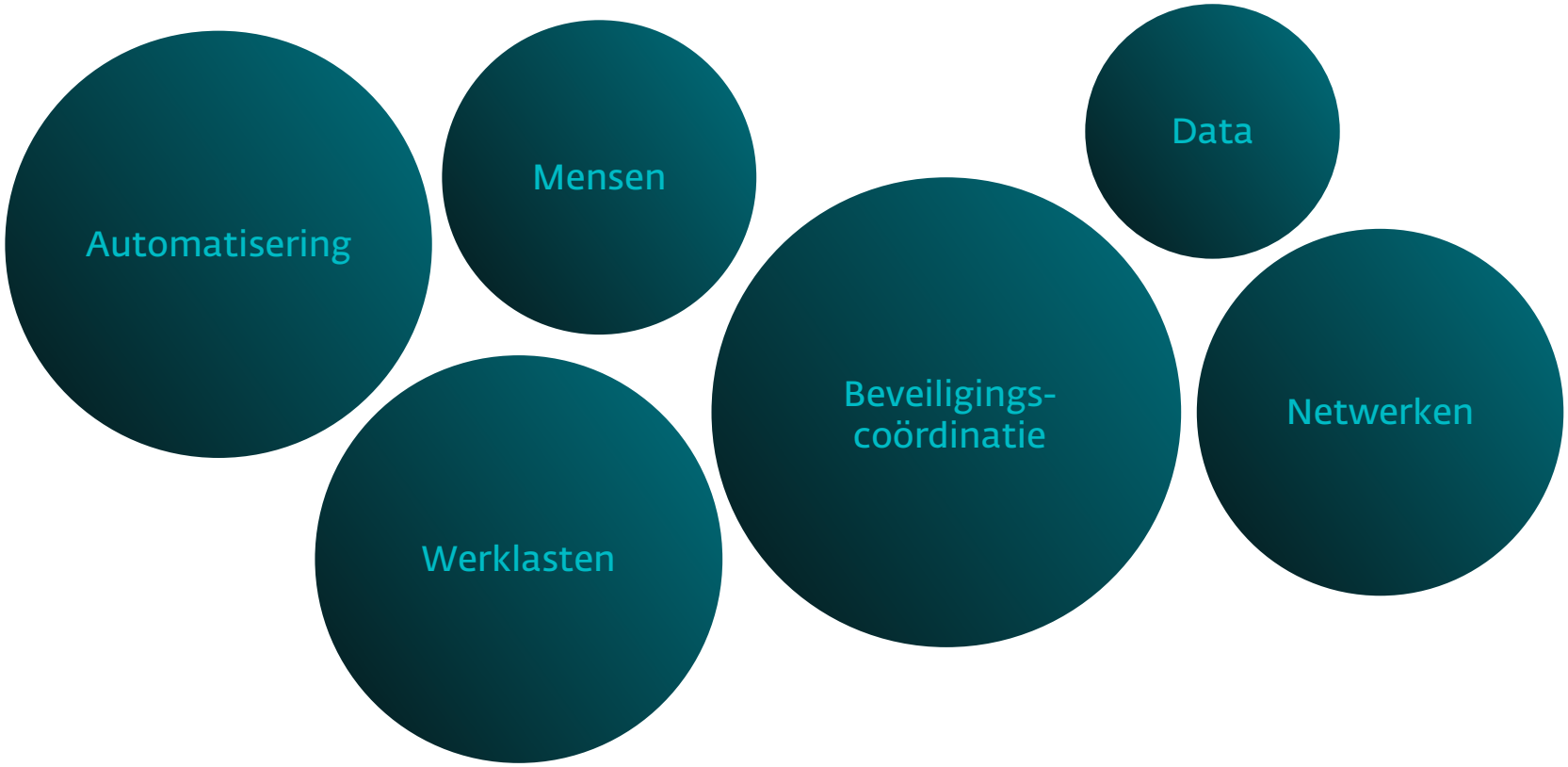
# 4 Overweeg een Zero Trust-benadering

De hybride werkplek wordt gekenmerkt door Bring Your Own Device (BYOD), hybride cloudomgevingen en regelmatige verplaatsing van werknemers in en uit de traditionele bedrijfsomgeving. Dat soort complexiteit is een ongelooflijke uitdaging om te beheren met behoud van productiviteit en een naadloze gebruikerservaring. Hiervoor is Zero Trust ontwikkeld.

Het werd meer dan tien jaar geleden voor het eerst beschreven en is gebaseerd op het principe "Vertrouw nooit, verifieer altijd", om de impact van inbreuken te beperken. Dat betekent dat alle netwerken als niet-vertrouwd moeten worden gezien en dat gebruikers en apparaten voortdurend moeten worden geverifieerd, dat het principe van de minste rechten moet worden toegepast en dat ervan moet worden uitgegaan dat er al inbreuk is gepleegd.

Het goede nieuws is dat veel van de stappen die nodig zijn om Zero Trust te stimuleren, zoals multifactorauthenticatie, microsegmentatie, EDR, host-based firewalls, gegevensversleuteling en vulnerability management misschien al deel uitmaken van uw set-up.

## De belangrijkste gebieden waarop CISO's actie kunnen ondernemen




Bron: Brian Kime, Forrester – senior analist en gastspreker bij ESET World


OPLOSSINGEN VOOR IDENTITEITS- & GEGEVENSBESCHERMING
Ontdek ESET's volledig gevalideerde encryptie-oplossingen en de krachtige multifactorauthenticatie-oplossing. Met deze oplossingen worden de gegevens van uw organisatie effectief beschermd, in overeenstemming met compliancevereisten.
Ontdek meer
eset
Digital Security
Progress. Protected.


eset
Digital Security
Progress. Protected.

# 5 Het is tijd voor proactieve beveiliging

CISO's begrijpen instinctief dat het beperken van cyberrisico's goedkoper en gemakkelijker is wanneer dit vooraf gebeurt, met proactieve maatregelen. De uitdaging is om voldoende middelen te vinden en te weten waar ze moeten worden ingezet, zodat ze de meeste waarde hebben. De omvang van die uitdaging lijkt overweldigend.

Pentesting is een nuttige manier om kwetsbaarheden, die uitgebuit zouden kunnen worden, in de organisatie te vinden en kan helpen bij het prioriteren van patching-inspanningen, hoewel een gebrek aan integratie met deze tools in de development- of operationele processen de snelheid van het herstel kan vertragen. Geautomatiseerde, op risico gebaseerde patchingoplossingen zijn de beste optie om organisaties te helpen bij het prioriteren van het enorme aantal CVE's waarmee ze elke week worden overspoeld.

Een andere stap is het inzetten van EDR en XDR, om proactief en snel verborgen dreigingen te identificeren door middel van correlatie en analytics die bepaalde activiteiten aan het licht brengen die menselijke ogen mogelijk missen. Hier vind je nuttig advies. Wat betreft misconfiguratie -- gegevensversleuteling, geautomatiseerde controles op beleidsconfiguratie vroeg in de ontwikkelingscyclus, en continue controle via Cloud Security Posture Management (CSPM)-tools kunnen allemaal helpen de risico's te beperken.

En bovenal, naarmate uw organisatie blijft veranderen en het bedrijfsmodel evolueert, is het belangrijk om ervoor te zorgen dat de beveiligingsstrategie en -cultuur evenredig meegroeien. Dat betekent niet alleen het inzetten van extra maatregelen naarmate de IT-omgeving groter en complexer wordt, maar ook het formaliseren van processen via een goed governancekader. Dat is het soort organisatorische volwassenheid dat uw bedrijf nodig heeft, en waar CISO's zich op moeten richten, nu het een nieuwe periode van post-pandemische groei ingaat.

## MEER DAN 18.000 CVE'S

werden bekendgemaakt in 2020 -
meer dan in enig ander jaar.

## MEER DAN 17 MILJARD

geschonden records in 2019 waren te wijten
aan vermijdbare configuratiefouten.

Bron: Redscan NIST Vulnerability Analysis, 2020


Op zoek naar een goed startpunt voor Extended Detection & Response?
ESET's XDR biedt uitstekende zichtbaarheid, incident response en herstelmaatregelen.
Ontdek meer
Digital Security
Progress. Protected.

Digital Security
**Progress. Protected.**

Al meer dan 3 decennia ontwikkelt ESET® toonaangevende IT-beveiligingssoftware en -diensten voor het leveren van uitgebreide, meerlaagse bescherming tegen cyberdreigingen voor bedrijven, kritieke infrastructuur en consumenten wereldwijd. Inmiddels is ESET uitgegroeid tot het grootste IT-security bedrijf uit de Europese Unie met oplossingen variërend van endpoint en mobile security, tot encryptie en tweefactorauthenticatie. ESET is sinds haar oprichting pionier op het gebied van machine learning en cloudtechnologieën die malware voorkomen, detecteren en erop reageren. ESET is een particulier bedrijf dat wereldwijd wetenschappelijk onderzoek & ontwikkeling bevordert.