Zero Trust

- sådan kommer I godt fra start

Et stærkt forsvar baseret på Zero Trust er vejen frem
- og rejsen begynder her

Orange Cyberdefense

Indhold

Introduktion

Over hele verden øger virksomheder deres digitalisering for at blive mere konkurrencedygtige og mindre sårbare over for skiftende markedsvilkår. Det samme sker hos offentlige organisationer og myndigheder, som via nye digitale løsninger kan yde bedre service til deres borgere.

Men medaljen har en bagside: Øget digitalisering øger også risikoen for cyberkriminalitet. Alene i 2021 steg antallet af angreb med hele 21%, og international cyberkriminalitet er i dag en milliardforretning. Aldrig før har så mange cyberkriminelle været så velorganiserede, og aldrig har de haft så mange ressourcer til deres rådighed. Samtidig er risikoen for hybrid krigsførelse – herunder cyberkrig – også blevet markant større.

Mange virksomheder har erkendt, at traditionel firewallbeskyttelse ikke længere er nok. Deres perimeter ændrer sig hele tiden, så før eller siden vil de ydre forsvarsværker ikke længere beskytte godt nok. Det giver ikke længere mening at tale om "hvis vi bliver angrebet". Vi skal i stedet forholde os til "når vi bliver angrebet". Det er sådan, virkeligheden ser ud i dag.

Målet er, at kerneforretningen skal kunne køre videre – selv under angreb. Samtidig bliver medarbejderne mere mobile og har brug for fleksibel og sikker adgang til virksomhedens netværk og systemer, uanset hvor de befinder sig, og hvilke devices de anvender. **Den tilgang kaldes Zero Trust.**

Zero Trust er mere end en teknologi. Det er en tankegang, som bygger på, at trusler findes alle steder, og cyberangreb kan komme alle steder fra.

Tilbage til indhold

Zero Trust – en megatrend

Zero Trust er det største paradigmeskifte inden for cybersikkerhed i mange år, og som andre store forandringer tager det tid for den nye tankegang at slå rod.

Både Gartner og Forrester har anbefalet implementering af Zero Trust i over ti år, og mange organisationer er nu modne til at skifte deres traditionelle perimeter-forsvar ud med en mere tidssvarende løsning.

I takt med at vi bliver mere mobile og arbejder mere hybridt fra forskellige lokationer, har vi brug for sikker adgang til netværksressourcer, uanset hvor vi befinder os.

Sikkerhedsfolk har brug for større transparens og konstant indblik i, hvad der foregår i netværket.

Der er brug for bedre beskyttelse af forretningskritiske assets.

Over 80% af al internet-trafik foregår nu mellem maskiner via API'er, som bedre kan beskyttes med Zero Trust.

Tilbage til indhold

Hvorfor skifte til Zero Trust?

Er jeres cybersikkerhed gearet til at håndtere fremtidens avancerede trusler? Har I den rigtige strategi?

- **Hybridarbejdet er eskaleret, og der er sket en stor stigning i antallet af hjem-mearbejdspladser.**
- **Brugerne anvender stadig flere forskel-lige enheder.**
- **Brugen af IoT-enheder er i kraftig vækst.**
- **Øget migrering til cloud skaber større behov for sikker dataudveksling.**
- **Mange it-ressourcer går fra at være statiske til at være agile og dynamiske.**
- **Mangel på it-sikkerhedspecialister med rette erfaring og kompetencer øger behovet for automatisering.**

Tilbage til indhold

Hvad er Zero Trust?

Gartner definerer Zero Trust som:
"En tilgang hvor implicit trust fjernes fra al digital infrastruktur". En holistisk design-ideologi, hvor det antages, at cybertrusler kan komme fra hvor som helst – når som helst.

Grundtanken i Zero Trust er, at intet længere er tillidsbaseret, sådan som vi kender det fra traditionel perimetersikkerhed, hvor alt i netværket typisk er tilgængeligt for alle brugere, når de først er kommet forbi firewall'en.

Med Zero Trust opløses denne grænse. Der er ikke længere noget "indenfor" og "udenfor". I stedet følger sikkerheden hver enkelt bruger og tilrettelægges efter en riskovurdering af hvilke data og applikationer, der er mest forretningskritiske.

Samtidig deles alle netværk op i mikrosegmenter, som gør det langt sværere for cyberkriminelle at nå frem til forretningskritiske data og andre værdier, selvom de er trængt forbi det ydre forsvar.

"Zero Trust bryder den traditionelle og meget ressourcekrævende forbindelse mellem sikkerhed og fysisk infrastruktur. Når først alle digitale assets har fået de rette labels, som beskriver deres forretningsmæssige rolle og funktion, er det i princippet ligegyldigt, hvordan de fysiske netværk er bygget op."

Klavs Thaarup

Senior Security Consultant
Orange Cyberdefense

Tilbage til indhold

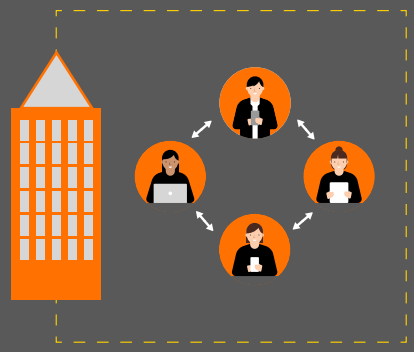
De vigtigste elementer i en Zero Trust-løsning er:

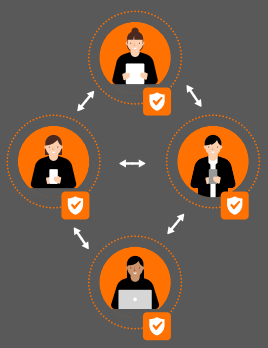
- **Stærk brugervalidering**
- **Policy-baseret fleksibel access**
- **Mikrosegmentering**
- **Automatisering**
- **Intelligence og AI**
- **Dataklassificering**

Zero Trust bygger på tre kerneprincipper

1. Alle brugere har kun adgang til de digitale ressourcer, der er nødvendige for deres funktion. (Concept of least privilege)
2. Det antages, at brud på sikkerheden er uundgåelige eller allerede sket.
3. Alle brugere og transaktioner overvåges og valideres 24/7.

Trust
Traditionel cybersikkerhed knytter sig til infrastrukturens ydre grænser, mens den indre sikkerhed er lav.





Zero Trust
I Zero Trust knytter sikkerheden sig til brugernes identitet, og sikkerheden er høj overalt – der er ingen "indenfor" og "udenfor" infrastrukturen.

"Zero Trust har især tre formål: Det første er at indkapsle og begrænse skaderne af de cyberangreb, som før eller siden vil finde sted. Det andet formål er at gøre sikkerheden helt fri af geografiske og netværksmæssige grænser. Og det tredje formål er at skille driften af sikkerhed og infrastruktur ad, så ændringer i det ene lag ikke påvirker det andet."

Ulrik Ledertoug

Director of Business Development and Services
Orange Cyberdefense

Tilbage til indhold

Fem myter om Zero Trust - og hvorfor de er forkerte

Klavs Thaarup, Senior Security Consultant hos Orange Cyberdefense, er en af Danmarks førende eksperter i Zero Trust. Gennem sin rådgivning af mange virksomheder og offentlige organisationer ved han, at der stadig hersker en del sejlivede myter om Zero Trust. Vi har bedt ham om at punktere de fem mest udbredte.

1 **"Zero Trust kræver, at vi har styr på alle assets i vores infrastruktur – og det har vi altså ikke."**

– Det er rigtigt, at Zero Trust kræver et komplet inventory. Dvs. overblik over al soft- og hardware man har kørende i netværket. Men det kan man forholdsvis hurtigt skanne sig til. Det er hverken særligt kompliceret eller tidskrævende, og så skaber fuldt inventory også mange andre sikkerhedsfordele.

2 **"Gartner skriver, det tager flere år at komme i mål med Zero Trust – så lang tid kan vi slet ikke vente."**

– Store forandringer tager tid. Men hvis man griber skiftet til Zero Trust rigtigt an, så bliver vejen til de første store fordele meget kortere. Fx bedre styring af identiteter. Implementering af Zero Trust er ikke nogen ørkenvandring, som først giver gevinst langt ude i fremtiden. Vi kan hjælpe med at bryde processen ned i overskuelige dele og gøre dem selvfinansierende.

3 **"Zero Trust er den rigtige vej at gå – men vores sikkerhed er ikke moden nok til det."**

– På afstand kan Zero Trust måske virke som om, man nærmest starte forfra med sin cybersikkerhed. Det er ikke rigtigt. De fleste virksomheder har allerede mange Zero Trust-egnede systemer implementeret, og de investeringer kan genbruges. Fx er cloud-teknologi forberedt til Zero Trust. Det er derfor, vi anbefaler at starte med et assessment. Det skaber overblik, så alle beslutninger kan træffes på et velinformeret grundlag.

4 **"Vi kan sagtens lave Zero Trust med de teknologier, vi allerede har."**

– Det kommer helt an på, om de er Zero Trust-egnede eller ej. Forsøger man fx at segmentere sit netværk med interne firewalls, vil man hurtigt opdage, at det bliver meget tungt at håndtere, og så går projekterne typisk i stå. Zero Trust kræver en høj grad af automatisering, og det er traditionelle teknologier som firewalls og VPN ganske enkelt ikke udviklet til.

5 **"Zero Trust er blot et spørgsmål om at købe og implementere de rette produkter."**

– Succes med ny teknologi bygger på de tre p'er: Products, people and processes – og det er Zero Trust en rigtig godt eksempel på. Det handler ikke bare om at bringe nye, smarte produkter i spil. Det er også derfor, at vi i et indledende assessment kigger grundigt på medarbejderkompetencer og processer.

Tilbage til indhold ▸

De fem risikosøjler i Zero Trust

Den optimale Zero Trust-løsning varierer fra virksomhed til virksomhed. Men det grundlæggende fundament består altid af disse fem risikosøjler, som integreres med hinanden ved hjælp af automatisering og monitorering.

Identitet

Konstant validering af alle brugere, applikationer og services.

Fuld monitorering af alle transaktioner.

Devices

Identificering og management af alle enheder – også mobile, IoT og OT.

Applikationer og API'er

Begrænset adgang til applikationer og workloads defineret efter hver medarbejders faglige behov.

Data

Kryptering af al data med de rette attributter, så de overføres og lagres sikkert i overensstemmelse med de forretningsmæssige behov.

Netværksmiljø

Kontrol, segmentering og løbende analyse på tværs af alle netværk, så trusler og angreb kan isoleres og håndteres effektivt, mens resten af infrastrukturen beskyttes – både on-site og i skyen.

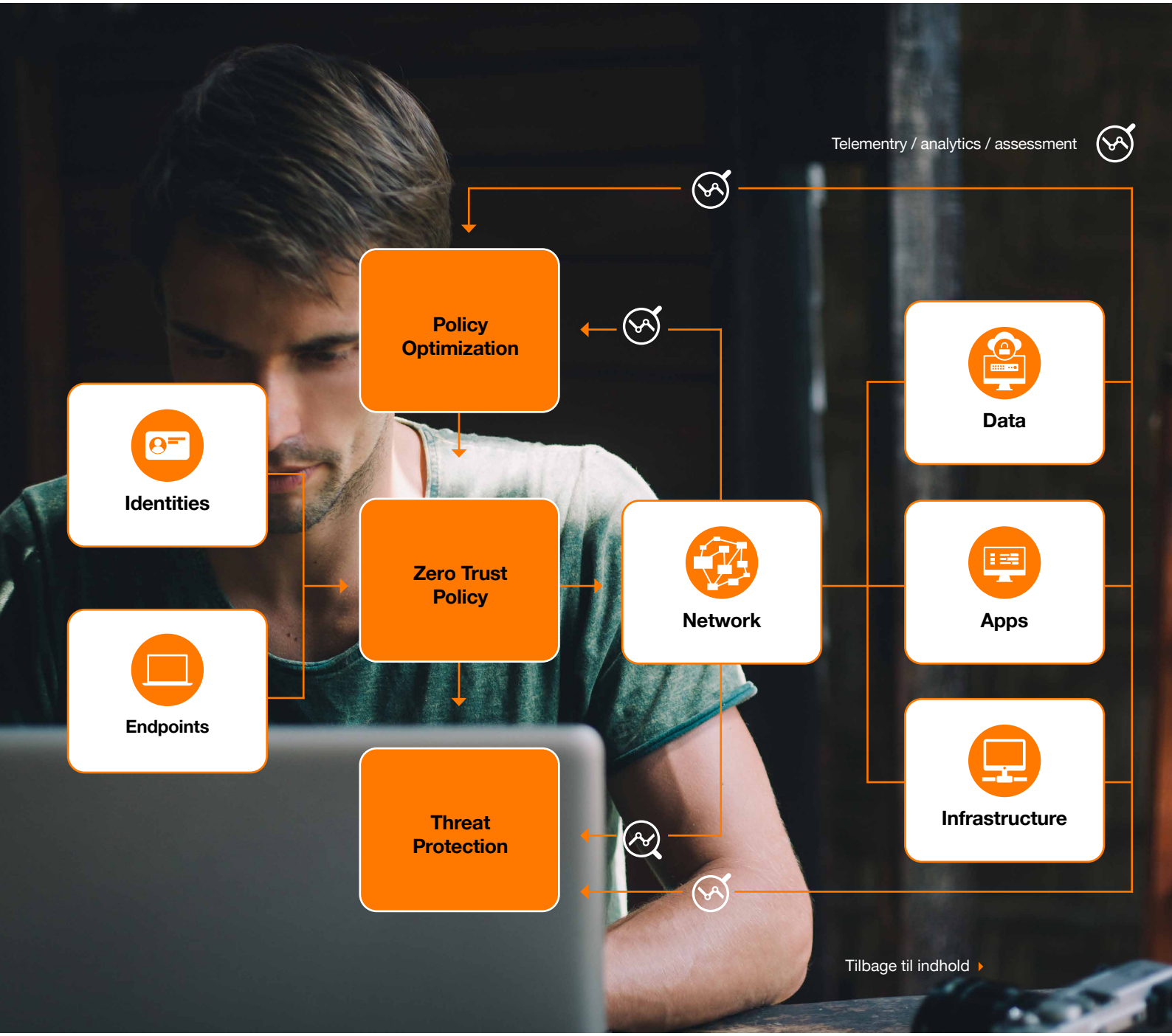
På tværs af de fem søjler er driften automatiseret og overvåget, så alt kan styres uden store investeringer i medarbejderressourcer, der er svære at skaffe.

Desuden er Zero Trust-overvågningen så effektiv, at menneskelig styring let kan skabe flaskehalse.

Tilbage til indhold ›

Sådan fungerer et Zero Trust-forsvar

Et typisk eksempel på en Zero Trust-løsning hvor eksisterende systemer er bygget sammen med automatiseret, policy-baseret styring af sikkerheden.



Tilbage til indhold

Vores erfarne specialister

"Med Zero Trust opnår virksomheder ikke alene en meget stærk beskyttelse mod cyberkriminalitet. Det giver også fleksibel og sikker adgang til flere kunder, partnere og dataleverandører – uanset hvor de befinder sig."

Ulrik Ledertoug

Director of Business Development and Services
Orange Cyberdefense

"Hvis en indbrudstyv kun kan få adgang til ét rum i dit hus, så er det jo stærkt begrænset, hvad der kan stjæles. Det er derfor software-baseret mikrosegmentering en essentiel del af enhver Zero Trust-løsning."

Martin Christensen

Security Consultant / Ethical Hacker / Pentester
Orange Cyberdefense

"Zero Trust er et fuldstændig grundlæggende skifte i vores måde at tænke sikkerhed på – det er som at gå fra VHS til Netflix."

Klavs Thaarup

Senior Security Consultant
Orange Cyberdefense

Tilbage til indhold

Zero Trust-rejsen i syv skridt

Et skifte til Zero Trust kan inddeles i syv delprocesser, som ikke nødvendigvis behøver at ligge i forlængelse af hinanden. Der er gode muligheder for at udvikle og implementere dem parallelt, så de bliver selvfinansierende, længe før skiftet til Zero Trust er fuldt gennemført.

Vejen til succes med Zero Trust

1 Kortlæg jeres infrastruktur
Hvad kan I tåle at miste i tilfælde af, at I bliver ramt af et hackerangreb? Og hvad kan I absolut ikke tåle at miste? Hvordan interagerer jeres enheder med hinanden?

2 Definér jeres enheders rolle og vigtighed
Tildel hver enhed, system, compliance og forretningsmæssige roller, benyt labels.

3 Etablér automatisk monitorering af brugere, data og netværkstrafik
I en Zero Trust-løsning er der to vigtige funktioner: Policy decision point (PDP) og Policy enforcing point (PEP). Konstant, automatiseret monitorering danner grundlag for valg af policies (PDP). Zero Trust-løsningen styrer sikkerheden (PEP) ud fra statiske policies kombineret med monitorering af hver enkelt enhed.

4 Implementér stærk brugervalidering
Gør multifaktor brugervalidering og session risk detection til kernen i jeres access-strategi, så risikoen for misbrug af jeres brugeres identiteter minimeres.

5 Implementér fleksibel policy-baseret access
Definér sikre access policies for alle netværksressourcer, og håndhæv dem med konsekvente sikkerheds-policies, som øger jeres kontrol og indsigt.

6 Implementér mikrosegmentering
Kombinér traditionel beskyttelse af netværkets ydre grænser med software-defineret mikrosegmentering, som gør det langt sværere for cyberkriminelle at bevæge sig rundt i netværket.

7 Integrér PDP og PEP
Den mest afgørende opgave på Zero Trust-rejsen er at integrere Policy decision point (PDP) og Policy enforcing point (PEP) ved hjælp af automatisering.

Tilbage til indhold ▸

Zero Trust er en ny og meget anderledes måde at tænke it-sikkerhed på

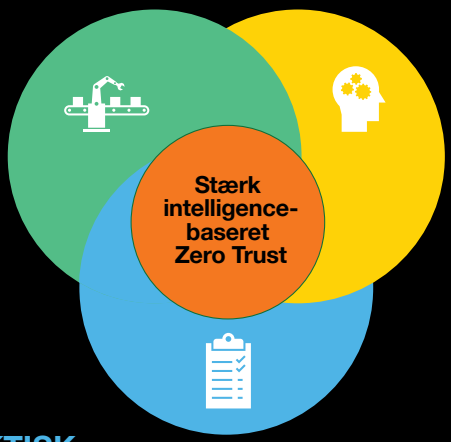
Vores specialister har arbejdet med Zero Trust i mange år og er derfor i stand til at yde kompetent rådgivning i alle faser.

Zero Trust kræver fokus på både operativt, taktisk og strategisk niveau.

OPERATIVT

- Centralisering
- Monitorering / automatisering
- Detection / respons

Vores specialister kan hjælpe med at implementere den monitorering og automatisering, der "limer" hele jeres Zero Trust-løsning sammen.



STRATEGISK

Planlæg og implementér den rigtige Zero Trust helt fra starten gennem:

- Uddannelse af medarbejdere
- Tildeling af så få brugerprivilegier som muligt
- Antagelse af at angreb er uundgåelige eller allerede har fundet sted
- Validering og godkendelse af alle transaktioner

TAKTISK

- Multi-faktor brugervalidering
- Policy-baseret adgangskontrol
- Mikrosegmentering

Få eksperthjælp til at planlægge og opbygge alle taktiske funktioner.

Start med vores Zero Trust Assessment

Som det første skridt på rejsen mod Zero Trust anbefaler vi en grundig gennemgang af jeres sikkerhedsmiljø for at afdække, hvilke muligheder I har før det store skifte. Det sikrer, at I får maksimalt udbytte af de sikkerhedsinvesteringer, I allerede har gennemført. En assessment giver også et solidt grundlag for at planlægge de forskellige delfaser, så de bliver selvfinansierende og skaber ekstra stort afkast på den lange bane.

Tilbage til indhold

Gode huskeråd om Zero Trust

Fælles forståelse
Start med en fælles forståelse af, hvad Zero Trust er. I Orange Cyberdefense følger vi standarden NIST SP 800-207 – på linje med Gartner og Forrester. Det er den forståelses-ramme, vi anbefaler at lægge til grund for en god Zero Trust-strategi.

Monitorering og automatisering
Læg vægt på monitorering og automatisering.

Få hjælp ude fra
Vælg en stærk sikkerhedspartner, som råder over konsulenter med stor erfaring inden for Zero Trust.

Gevinster i processen
Et skifte til Zero Trust tager typisk adskillige år at gennemføre – men vær opmærksom på, at der er mange gode gevinster at hente under-vejs, men der kan høstes mange store fordele undervejs.

Mange veje til målet
Opbygning af en Zero Trust-løsning behøver ikke at foregå fra A til Å. De fleste delprocesser kan udføres parallelt og uafhængigt af hinanden.

Grundstenene i Zero Trust
Komplet inventory, høj transparens og grundig klassificering er blandt de vigtigste grundelementer i en stærk Zero Trust-løsning.

Tilbage til indhold

Orange Cyberdefense

- **Orange Cyberdefense** er en af Europas ledende it-sikkerhedsleverandører med mere end 25 års erfaring inden for cybersecurity og Managed Security Services. Vores kompetencer spænder over alt fra overvågning, pentesting, analyse, rådgivning og sparring til implementering, drift og administration af kundernes strategiske it-sikkerhedsløsninger.
- **Orange Cyberdefense** er eksperter i at analysere virksomheders, myndigheders og organisationers it-sikkerhed og rådgive om, hvordan man bedst prioriterer de nødvendige indsatsområder i forhold til det aktuelle trusselsbillede.
- **Orange Cyberdefense** råder over 250 af branchens bedste analytikere fordelt på 17 SOCs, 13 CyberSOCs og 4 CERTs i hele verden. De indsamler og analyserer data fra over 500 informationskilder 24/7, hvilket giver markedets bedste intelligence-baserede billede af, hvordan det globale trusselsniveau udvikler sig.
- **Orange Cyberdefense** har et stort og internationalt white hat hacker-team, som består af 150 etiske hackere, hvoraf +25 sidder i Norden.

Kontakt os, hvis du har brug for rådgivning eller har spørgsmål til Zero Trust – og hvordan du kommer i gang.

Send e-mail

Tilbage til indhold