NETWORKING4ALL

LEADING IN CYBERSECURITY SOLUTIONS

CCV CYBER PENTEST

NIST National Institute of Standards and Technology

OWASP

CVSS

BEDRIJFSBROCHURE

+31 (0)20-7881030

info@networking4all.com

https://www.networking4all.com

Over Networking4all & Onze Certificeringen

Networking4all is een deskundige en servicegerichte leverancier van SSL/TLS certificaten & cybersecurity oplossingen. Wij bieden een uniek holistisch aanbod op het gebied van cybersecurity diensten met als doel ontzorgen. Onze diensten zijn gericht op de informatiebeveiliging pijlers mens, proces, techniek en monitoring.
Een juiste invulling van de pijlers; mens, proces, techniek en monitoring zal daadwerkelijk leiden tot een verlaging van de risico's.

- Train uw medewerkers
- Integreer cybersecurity in uw processen
- Beveilig en monitor uw bedrijfsomgeving | assets

Mede door onze flexibele en persoonlijke aanpak hebben wij altijd een passende oplossing voor uw behoefte. Wij leveren onze producten en diensten aan grote en kleine klanten uit diverse sectoren zoals detailhandel, zakelijke dienstverlening, ICT, industrie, gezondheidszorg, onderwijs en overheid.

U kiest voor Networking4all vanwege;

- 25 jaar expertise in online security
- 1-stop-shop voor al uw cybersecurity oplossingen/maatregelen
- Eigen ethische hackers, ISO consultants, security analisten en developers
- Unieke Risico Analyse t.b.v uw cybersecurity volwassenheid roadmap
- ISO 9001 & ISO 27001 gecertificeerd
- Bewezen partner in cybersecurity met 10k+ klanten

kiwa gecertificeerd ISO 9001

kiwa gecertificeerd ISO/IEC 27001

CCV CYBER PENTEST

Great Place To Work.®

CYBERSECURITY™ MADE IN EUROPE

Initiated by ECSO. Issued by Networking4all

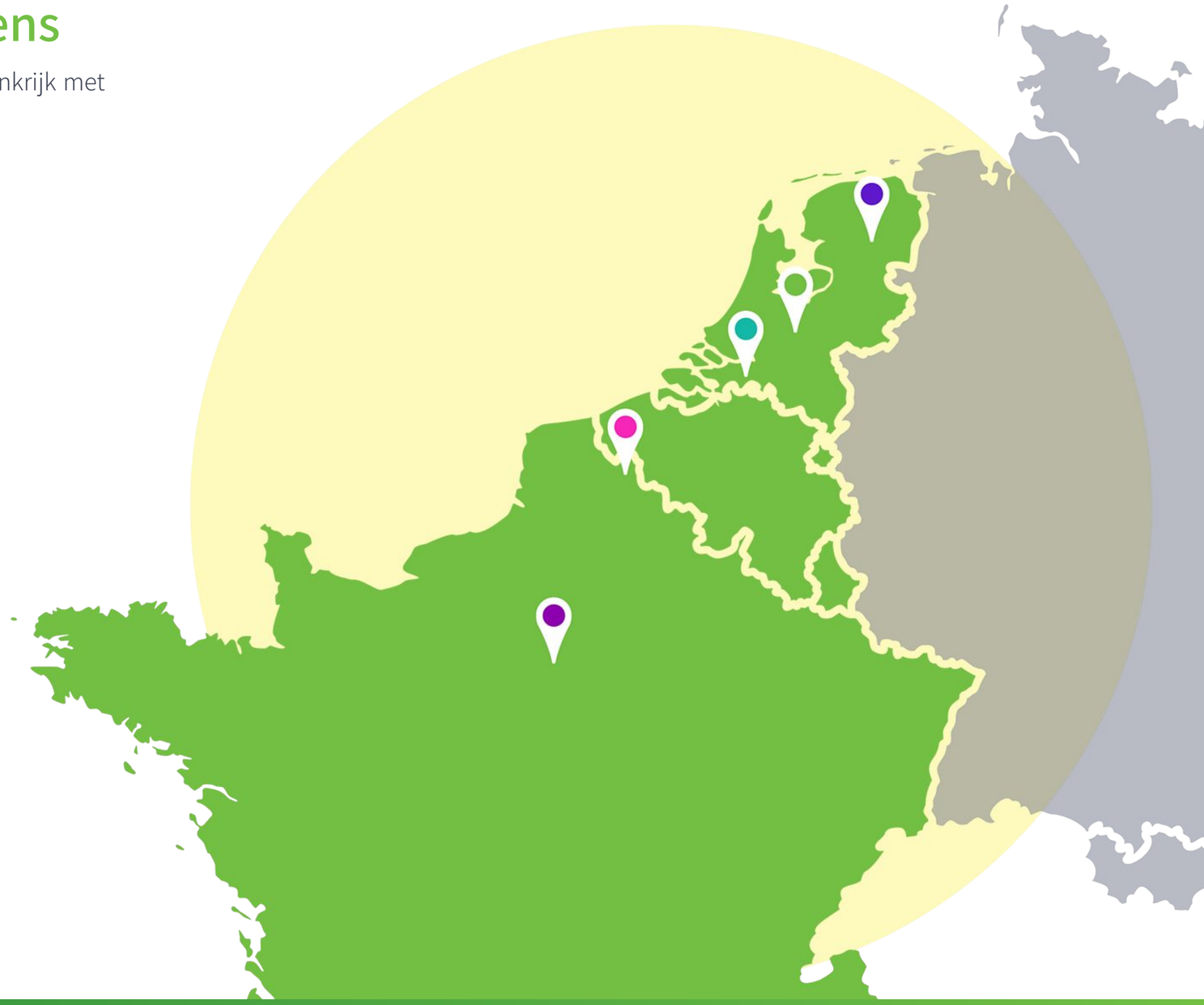
CYBERVEILIG NEDERLAND

Klik hier voor meer informatie over onze Certificeringen.

Europese kantoren & Contactgegevens

Networking4all bevindt zich op verschillende plekken in Nederland en Frankrijk met ons hoofdkantoor in Nederland te De Meern, Utrecht.

- **NL | Rijnzathe 4, 3454 PV Utrecht | Hoofdkantoor**
- **NL | Gildelaan 1, 4761 BA Zevenbergen**
- **NL | Overcingellaan 17, 9401 LA Assen**
- **FR | Parijs**
- **FR | Lille**



Contactgegevens

Telefoon
+31 (0)20 788 10 30

Email
info@networking4all.com

Kamer van Koophandel
Amsterdam, 20099481

BTW nummer
NL8112.78.888.B01

Evenwicht tussen Mens, Proces, Techniek en Monitoring

Beveiliging dient een evenwicht te zijn tussen technologie en organisatiecultuur. Onze producten en diensten zijn gericht op de informatieveiligheids pijlers mens, proces, techniek en monitoring.

Mens
Blijf uw medewerkers informeren over cyberbeveiligings vaardigheden en de gevaren van cyberaanvallen. Geef handvatten om adequaat te handelen. Houd Security Awareness top of mind middels diverse doorlopende awareness activiteiten.

Proces
Zorg voor een coherente structuur en werkwijze om risico's te beperken of bedreigingen in realtime aan te pakken. Dit door informatieveiligheid op te nemen in processen/de cultuur binnen de organisatie.

Technologie
Zorg voor de juiste technologische middelen om kwetsbaarheden in kaart te brengen en snel en adequaat te kunnen reageren op bedreigingen en aanvallen.

Monitoring
Continu observeren en analyseren van netwerken, systemen en activiteiten om verdachte gedragingen en potentiële beveiligingsincidenten te identificeren.

Een juiste invulling van de informatieveiligheid pijlers; mens, proces, techniek en monitoring zal daadwerkelijk leiden tot een verlaging van de risico’s.

Vraag naar de NUL-meting mogelijkheden op het gebied van Medewerker Awareness, IT-infra kwetsbaarheden en informatieveiligheid in uw processen.

Mens

Security Awareness
- Awareness as a Service
- Awareness E-learning | Networking4all
- Awareness E-learning | 2LRN4
- Awareness E-learning | KnowBe4
- Security Awareness Training Klassikaal
- Cybersecurity Event

Social Engineering
- Phishing | Email
- Vishing | Voice
- Smishing | SMS
- Mystery Guest
- USB drop

Educatie, Training en Opleiding
- OptiSec Pentest Professional (OSPP)
- Networking4all OptiSec Container Security (OSCS)
- Security Awareness Training Klassikaal
- Certified Ethical Hacker v12 (CEH)
- Certified Ethical Hacker Master Preparation
- Certified Incident Handler (ECIH)
- Certified SOC Analyst (CSA)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified in Cybersecurity (CC)
- Certified Cloud Security Professional (CCSP)
- Certified Information Systems Security Professional (CISSP)

Proces

Norm & Certificeringen
- Risico Analyse
- ISO 27001 Assessment
- ISO 27001 Begeleiding
- NEN 7510 Begeleiding
- NIS2 Compliance Assessment
- NIS2 Management Training

Business continuïteit
- Business Continuity Plan
- Emergency Response Plan
- Cybersecurity Calamiteitenoefening
- Back-up as a Service

Monitoring

Security Monitoring
- Managed Security Monitoring | 24/7 SOC SIEM
- Incident Response
- Digitaal Forensisch Onderzoek

Techniek

Ethisch Hacken
- Pentest
- Pentest as a Service
- Red Teaming
- Wifi | Bluetooth Audit

Vulnerability Scan & Management
- Nessus Vulnerability Scan
- Acunetix Web Application Scan
- WithSecure Exposure Management (VM)
- Qualys VMDR 2.0

Endpoint Beveiliging
- Mobile Device Management
- BlackBerry Cylance Endpoint
- BlackBerry Unified Endpoint Management
- WithSecure Endpoint Protection
- WithSecure Endpoint Detection and Response
- Keeper Password Manager
- Bitwarden

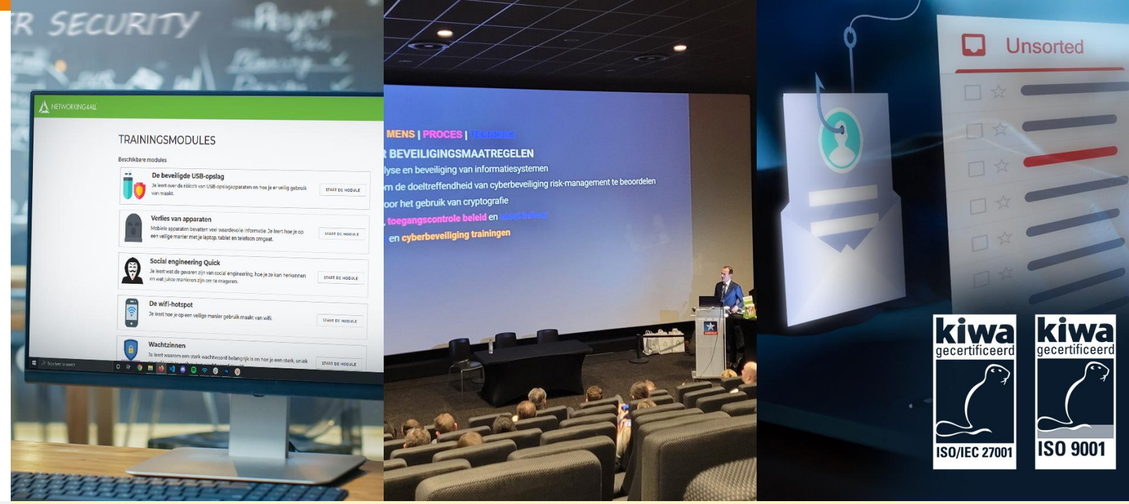
Webserver & Signing Certificaten

SSL
- SSL-TLS/SIGNING Certificaten
- SSL Beheer (Management Portal)
- SSL Automatiseren

Awareness as a Service

Een jaar lang security awareness bewustwordingsactiviteiten.

Mens | Security Awareness | Identify | Protect



Wat is Awareness as a Service?

Het doel van Awareness as a Service is het verhogen van de bewustwording onder de medewerkers op het gebied van informatiebeveiliging. Dit door uw organisatie een jaar lang te voorzien van security awareness bewustwordingsactiviteiten. Wij hebben een compleet pakket samengesteld met doeltreffende security awareness activiteiten voor uw medewerkers bestaande uit het **jaarprogramma**.

Hoe werkt Awareness as a Service?

Binnen Awareness as a Service bieden we meerdere activiteiten aan om medewerkers continu te prikkelen en zich bewust te maken en bezig te houden met security awareness.

- Awareness E-learning
- Security Awareness training klassikaal
- Phishing Simulatie

Jaarprogramma

- Doorlopende Awareness E-learning
- 2 Phishing Simulaties
- 1 of meerdere security awareness trainingen afhankelijk van het aantal deelnemers; klassikaal (online of op locatie)

Optioneel

- Privacy Box , dé giftbox tijdens uw security awareness traject
- Extra social engineering activiteiten
- Password Manager

Meer informatie nodig? Lees verder op onze website ➡

NETWORKING4ALL

Networking4all Awareness E-learning

Verhoog het veiligheidsbewustzijn, activeer de human firewall en bescherm uw organisatie tegen beveiligingsrisico's.

Mens | Security Awareness | Security Awareness E-learning | Identify

Wat is Awareness E-Learning?

Met E-Learning wordt een traject bedoeld waarin de werknemers van een organisatie digitale training ondergaan om zo hun bewustwording op het gebied van cyberveiligheid te verbeteren. Dit kan bijvoorbeeld door middel van praktijkvoorbeelden, interactieve games of het kijken van filmpjes door experts en slachtoffers. Deze trainingen worden vaak verdeeld over meerdere thema's en kunnen zo door het jaar heen gedaan worden. Zo worden uw werknemers niet overspoeld met informatie en blijft het beter hangen. Dit alles vanaf het apparaat van de deelnemer zodat zij zelf hun tijd kunnen indelen en niet afhankelijk zijn van specifieke tijden.

Waarom is Awareness E-Learning belangrijk?

In de beveiliging van een organisatie is de mens de zwakste schakel. Kwaadwillenden die ergens digitaal willen inbreken doelen daarom als eerst ook op de werknemers van een bedrijf, vaak door middel van phishing of social engineering, waarbij de aanvaller zich als iemand anders voordoet om de werknemers te manipuleren.Volgens de statistieken uit onderzoek van keepnet labs werd in 2020 30 procent van phishingberichten door gebruikers geopend, waarbij 12 procent ook daadwerkelijk op de schadelijke links werd geklikt.

Het doel van de Awareness E-learning:

- Bewustzijn verhogen en cybersecurity top of mind houden
- Vermindering van het risico op cyberaanvallen
- Verbetering van de beveiligingscultuur
- Reputatiebescherming

Werknemers kunnen:

- Phishing-e-mails beter herkennen en erop reageren.
- Sterke wachtwoorden kiezen en deze veilig gebruiken.
- De juiste procedures volgen in geval van een cyberaanval.
- Zich bewust zijn van de risico's van het openen van bijlagen of het klikken op links in e-mails van onbekenden.

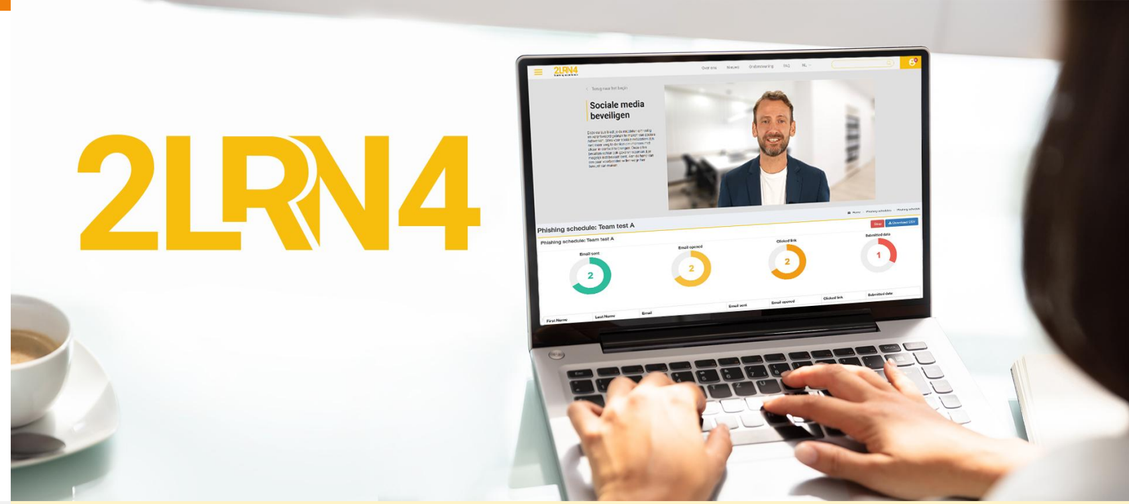
Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

2LRN4
Awareness E-learning

Verhoog het veiligheidsbewustzijn, activeer de human firewall en bescherm uw organisatie tegen beveiligingsrisico's.

Mens | Security Awareness | Security Awareness E-learning | Identify



Wat is 2LRN4 Awareness E-Learning?

2LRN4 is een flexibel, eenvoudig te gebruiken learning management platform (LMS), bedoeld om organisaties te helpen hun privacy- en veiligheidsbewustzijn te verbeteren. Het platform is zo ontwikkeld dat een organisatie alles zelf kan configureren en beheren. Zoals het bepalen van hun eigen toetsvragen of het invoegen van een eigen beleidsplan. Het is niet nodig om te configureren, u kunt tevens het normale programma volgen. Het platform wordt geleverd inclusief cursussen en is reeds geconfigureerd, zodat aanpassingen minimaal zijn.

Waarom is Awareness E-Learning belangrijk?

In de beveiliging van een organisatie is de mens de zwakste schakel. Kwaadwillenden die ergens digitaal willen inbreken doelen daarom als eerst ook op de werknemers van een bedrijf, vaak door middel van phishing of social engineering, waarbij de aanvaller zich als iemand anders voordoet om de werknemers te manipuleren. Volgens de statistieken uit onderzoek van keepnet labs werd in 2022 30 procent van phishingberichten door gebruikers geopend, waarbij 12 procent ook daadwerkelijk op de schadelijke links werd geklikt.

Het doel van de Awareness E-learning:

- Bewustzijn verhogen en cybersecurity top of mind houden
- Vermindering van het risico op cyberaanvallen
- Verbetering van de beveiligingscultuur
- Reputatiebescherming

Werknemers kunnen:

- E-learning cursussen over privacy- en online veiligheidsbewustzijn.
- U krijgt 12 nieuwe online cursussen (+/- 50 modules) per jaar.
- Een cursus bestaat in ieder geval uit twee instructievideo's, die het onderwerp introduceren vanuit een zakelijke en privé situatie, een e-learning die drie onderwerpen van het onderwerp toelicht en een toets, een zogenaamde challenge.
- De cursussen kunnen worden uitgebreid met eigen materiaal zoals webinars, enquêtes, documenten en video's.

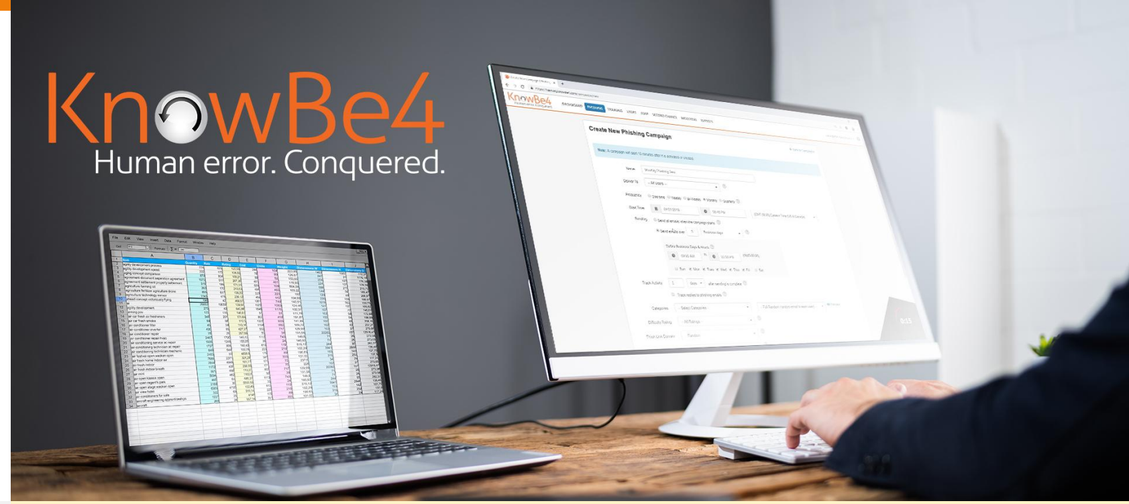
Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

KnowBe4 Awareness E-learning

Verhoog het veiligheidsbewustzijn, activeer de human firewall en bescherm uw organisatie tegen beveiligingsrisico's.

Mens | Security Awareness | Security Awareness E-learning | Identify



Wat is KnowBe4 Awareness E-Learning?

KnowBe4 is 's werelds grootste platform voor security awareness training gecombineerd met gesimuleerde phishing aanvallen. Zij bedienen meer dan 39.000 klanten om het voortdurende probleem van social engineering te beheersen. Het platform helpt organisaties om hun personeel te trainen in het herkennen, rapporteren en voorkomen van phishing-aanvallen, malware, CEO-fraude en andere vormen van cybercrime.

Waarom is Awareness E-Learning belangrijk?

In de beveiliging van een organisatie is de mens de zwakste schakel. Kwaadwillenden die ergens digitaal willen inbreken doelen daarom als eerst ook op de werknemers van een bedrijf, vaak door middel van phishing of social engineering, waarbij de aanvaller zich als iemand anders voordoet om de werknemers te manipuleren. Volgens de statistieken uit onderzoek van keepnet labs werd in 2022 30 procent van phishingberichten door gebruikers geopend, waarbij 12 procent ook daadwerkelijk op de schadelijke links werd geklikt.

Het doel van de Awareness E-learning:

- Bewustzijn verhogen en cybersecurity top of mind houden
- Vermindering van het risico op cyberaanvallen
- Verbetering van de beveiligingscultuur
- Reputatiebescherming

Werkwijze:

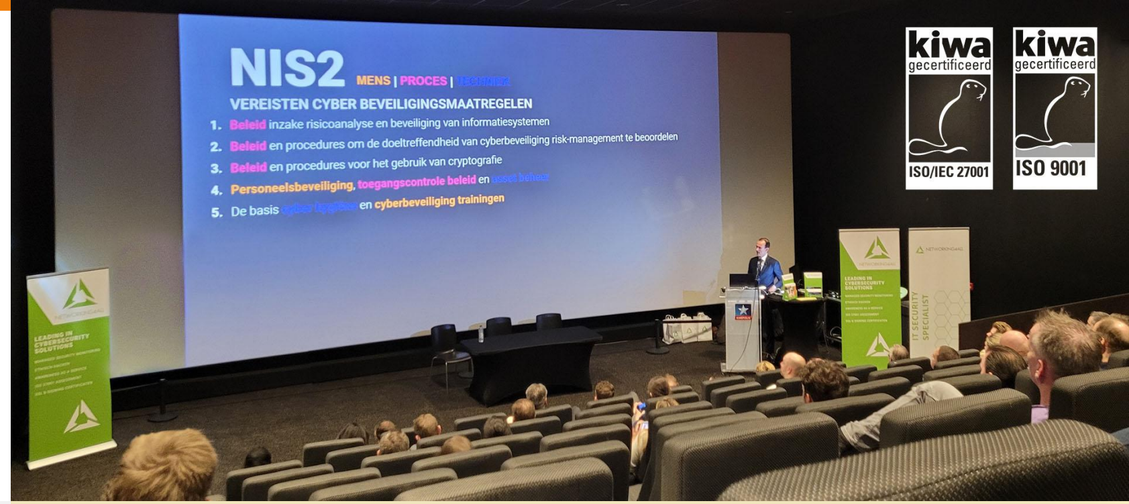
- Initiële test hoeveel medewerkers klikken op content van phishing
- Geautomatiseerde trainings campagnes met ingeplande reminders.
- Gesimuleerde phishing-aanvallen die geavanceerd en volledig geautomatiseerd zijn. Duizenden templates om uit te kiezen, onbeperkt gebruik.
- Zeer uitgebreide rapportages met statistieken en grafieken over trainings en phishing resultaten. Geeft direct duidelijkheid over de ROI. Klaar om aan de directie te laten zien.

Meer informatie nodig? Lees verder op onze website

Security Awareness Training Klassikaal

Uw medewerkers worden uitgedaagd om actief mee te denken over de verschillende thema’s.

Mens | Security Awareness | Identify | Protect



Wat is een security awareness training?

Naast onze e-learning bewustwordingstrainingen bieden wij ook trainingen in klassikaal verband aan. Medewerkers wordt in begrijpbare taal uitgelegd waar gevaren en risico’s liggen. Zo worden zij bewust gemaakt van de zwakke punten en behoed voor risico's die vooral op menselijk vlak voorkomen. Het gevolg hiervan is dat verantwoordelijkheden beter begrepen kunnen worden.

Een belangrijk doel van de security awareness training van Networking4all is medewerkers bewust maken van de grote en belangrijke rol die zij spelen in de beveiliging van een bedrijf. Het is belangrijk dat de risico's op menselijke fouten tot een minimum beperkt worden. Cybercriminelen maken geen kans door de hoogste standaarden in cyber security en IT-beveiliging te hanteren. Networking4all helpt u graag hieraan te voldoen. Met onze klassikale security awareness training zorgen wij ervoor dat uw medewerkers niet de zwakste schakel zijn in uw bedrijfsbeveiliging.

Het doel van awareness training:

- Stimuleer positieve gedragsveranderingen bij uw werknemers middels continue security awareness bewustwordingsactiviteiten.
- Bevorder een beveiligingscultuur om proactief te reageren op voortdurende cyberdreigingen.
  Dit door adoptie en verantwoordelijkheid van medewerkers op alle niveaus van de organisatie. Denk hierbij aan gerichte training.
- Verminder de risico's in de hele organisatie

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Cybersecurity Event

Hét security awareness event toegespitst op uw organisatie.

Mens | Security Awareness | Social Engineering | Ethisch Hacken | Protect

Wat is een Cybersecurity Event?

Wij merken dat steeds meer bedrijven behoefte hebben aan een organisatiebrede cybersecurity awareness impuls. Alle ogen dezelfde kant op m.b.t. het bewust zijn van en het handelen bij mogelijke security incidenten. Networking4all zet zich reeds 20 jaar in voor internetveiligheid. Wij organiseren en begeleiden uw Cybersecurity Event van A tot Z. Centraal staan de onderwerpen: privacy, informatiebeveiliging en cybersecurity. Uw Cybersecurity Event is volledig op maat en naar uw wens op te zetten. Ook in dit selectieproces denken wij graag met u mee. Wilt u een week, maand of voor een langere periode uw organisatie voorzien van een tal van cybersecurity, privacy en informatiebeveiliging activiteiten dan is het Cybersecurity Event de aangewezen dienst.

Hoe werkt een Cybersecurity Event?

Uw event is volledig op maat vorm te geven op het gebied van privacy, informatiebeveiliging en cybersecurity. Denk hierbij aan lezingen, workshops, games, phishing simulaties, Awareness E-learning. USB-drops en live hacking demo's. Maar bijvoorbeeld ook interactieve (Management) klassikale awareness trainingen.

Mogelijkheden Cybersecurity Event. O.a. :

- Kick-off Keynote
- Lezingen & Workshops
- Phishing simulatie
- USB drop op locatie of per post
- Awareness E-Learning
- Social Engineering
- Mystery Guest
- Vishing
- Smishing
- (Management) klassikale awareness trainingen
- NIS2

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Phishing | Email

Zijn uw medewerkers bestand tegen geraffineerde phishing methodes?

Mens | Social Engineering | Identify

Wat is een Phishing Simulatie?

Een phishing simulatie geeft inzicht in hoeverre medewerkers phishingmails openen, of zij doorklikken op links of bijlagen en of er gevoelige gegevens worden achtergelaten. Daarnaast is een phishing simulatie een perfect middel om cybersecurity bewustwording te creëren. Herkennen uw medewerkers een phishingmail? Zijn zij op de hoogte van de gevaren van een phishing mail? Met een phishing simulatie van Networking4all kunt u enerzijds uw medewerkers deze gevaren laten ervaren en anderzijds de huidige phishing kennis van uw personeel toetsen.

Maatwerk domein, email template en landingspagina

De phishing simulatie is volledig op maat. Op basis van de verkregen informatie over uw organisatie creëren wij een domein welke erg lijkt op het bedrijfsdomein. Vervolgens zal de email template als de lander dusdanig worden ingericht als een te verwachten mail behorende bij uw organisatie. Zo gaan de echte kwaadwillende immers ook te werk. Tevens bieden wij standaard templates waar u uit kan kiezen.

Phishing simulatie van Networking4all

- Phishing simulaties zoals in de praktijk
- Volledig maatwerk: unieke scenarios
  - Maatwerk email templates en landingspagina’s
  - Maatwerk domein
  - U kunt ook gebruik maken van onze standaard templates
- Uitleg waaraan de phishing herkend had kunnen worden
- Inclusief password check
- Gepersonaliseerde rapportage over de resultaten en verbeterpunten

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Vishing | Voice

Telefonische phishing | Hoe goed zijn uw medewerkers van vertrouwen?

Mens | Social Engineering | Identify

Wat is een Vishing Simulatie?

Zijn medewerkers te manipuleren? Telefonische phishing, ook wel vishing of voice phishing genoemd, wordt gebruikt om een gerichte aanval op een organisatie uit te voeren. De dienst staat ook bekend als Social Engineering Calls. Het kan ook gebruikt worden als voorbereiding op een toekomstige aanval. Bijvoorbeeld door specifieke informatie te achterhalen die gebruikt kan worden voor een spearphishing-aanval. In welke mate zijn de medewerkers binnen uw organisatie te manipuleren om gegevens prijs te geven?

Waarom een Vishing Simulatie?

Bij het telefonische phishing onderzoek wordt in kaart gebracht hoe weerbaar of kwetsbaar de organisatie en medewerkers zijn wanneer zij benaderd worden door de onderzoeker met de vraag om vertrouwelijke (persoons-)gegevens af te staan.Denk hierbij aan cliëntgegevens of inloggegevens. De onderzoeker kan verschillende rollen aannemen. Doorgaans doen wij ons voor als ICT-medewerker van een organisatie, thuiswerker of familielid van een cliënt. De exacte invulling en werkwijze wordt in overleg met de opdrachtgever bepaald.

Vishing simulatie van Networking4all

- Bewustwording vergroten
- Identificatie vaardigheden verbeteren
- Risicovermindering
- Opleiding en training
- Testen van reacties op incidenten

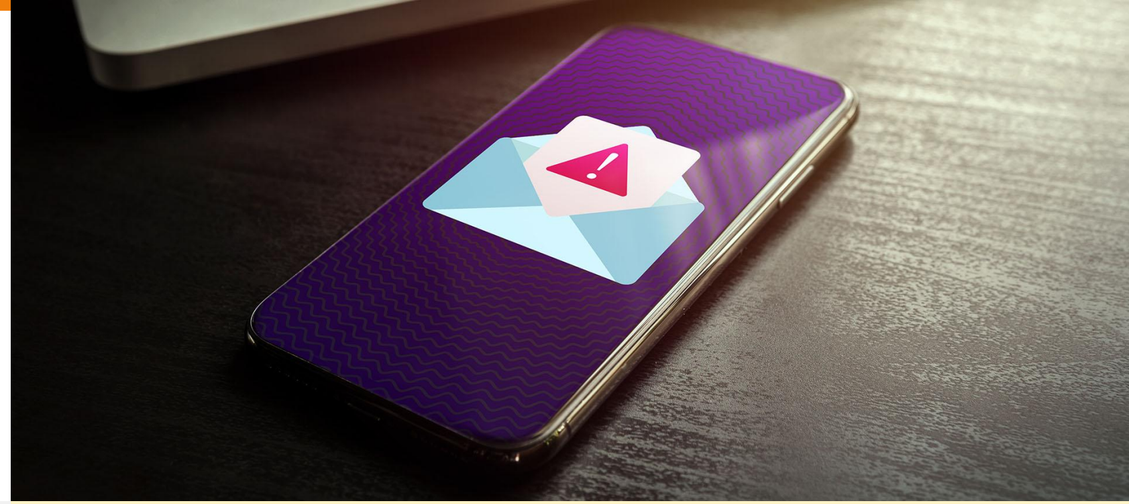
Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Smishing | SMS

Zijn de medewerkers binnen uw organisatie kwetsbaar voor phishing via SMS of Whatsapp?

Mens | Social Engineering | Identify



Wat is Smishing?

Smishing is een vorm van cybercriminaliteit waarbij aanvallers misleidende tekstberichten (SMS) gebruiken om slachtoffers te bedriegen. Deze berichten bevatten vaak links naar frauduleuze websites of verzoeken om persoonlijke informatie, zoals wachtwoorden of creditcardgegevens, te delen. Smishing is een samentrekking van "SMS" en "phishing," en het doel is om gevoelige gegevens te stelen of financiële schade aan te richten.

Waarom een smishing simulatie uitvoeren?

Het uitvoeren van een smishing simulatie geeft organisaties informatie waarmee zij hun beveiligingsmaatregelen kunnen versterken en werknemers bewuster maken van de gevaren van smishing-aanvallen. Door dergelijke simulaties kunnen bedrijven de zwakke punten in hun beveiliging identificeren en ervoor zorgen dat medewerkers getraind zijn om o.a. verdachte SMS-berichten te herkennen en er niet op te reageren.

Smishing simulatie van Networking4all

- Bewustwording vergroten
- Identificatie vaardigheden verbeteren
- Risicovermindering
- Opleiding en training
- Testen van reacties op incidenten

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Mystery Guest

Laat de organisatie infiltreren door een Mystery Guest gespecialiseerd in cybersecurity.

Mens | Social Engineering | Identify

Wat is een Mystery Guest?

Laat de organisatie infiltreren door een mystery guest gespecialiseerd in cybersecurity. Een onderzoeker doet zich voor als bijvoorbeeld een printermonteur of serviceprovider en probeert fysiek toegang te krijgen tot de organisatie. De term "mystery guest" wordt vaak geassocieerd met de horeca of de detailhandel, waar anonieme beoordelaars de kwaliteit van de dienstverlening beoordelen. In de wereld van cybersecurity verwijst een mystery guest echter naar een ethische hacker of beveiligingsexpert die de beveiligingsmaatregelen van een organisatie beoordeelt door zich voor te doen als een potentiële aanvaller.

Hoe werkt een Mystery Guest?

Mystery guests bootsen real-world aanvallen na, waardoor ze een realistisch beeld krijgen van hoe een aanvaller te werk zou gaan. Dit stelt organisaties in staat om gerichte maatregelen te nemen om zich te verdedigen en inzicht te krijgen waar het nog schort in de verdediging, het blue team. Hoe reageren medewerkers tijdens een mystery guest aanval? Hoe is het gesteld met de offensieve houding? Door kwetsbaarheden te identificeren, kunnen organisaties proactief reageren en deze zwakke punten versterken voordat ze worden uitgebuit.

Krijg inzicht in kwetsbaarheden zoals

- Ongeautoriseerde toegang tot het pand, (afgesloten) werkruimtes.
- Het zorgvuldig omgaan met fysieke informatie op bureaus.
- Het achterhalen van inloggegevens en andere vertrouwelijke info.
- Hoe reageert het personeel op de ontstane situatie?
- Hoe zijn de ruimtes binnen het pand beveiligd?
- Hoe gaat het personeel om met de middelen die door de mystery guest zijn achtergelaten?

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

USB drop

Vaak staat men niet stil bij de gevaren van een geïnfecteerde USB-stick.

Mens | Social Engineering | Identify

Wat is een USB drop?

Veiligheidsrisico's van het gebruik van mobiele datadragers zoals USB-sticks kunnen met diverse technische oplossingen beperkt worden. Toch blijven er risico's verbonden aan het gebruik. Dan komt het aan op de kennis, kunde en alertheid van medewerkers. Vaak staat men niet stil bij de gevaren van een geïnfecteerde USB-stick. Zijn de medewerkers op de hoogte van de regels omtrent mobiele datadragers van uw organisatie en handelen zij hiernaar? Een USB drop test toont aan hoe kwetsbaar uw organisatie is voor deze vorm van social engineering.

Hoe werkt een USB drop?

Tijdens de USB-drop prepareren wij USB-sticks die geautomatiseerde code uitvoeren op de werkstations waarin ze worden ingeplugd. Met behulp van deze code kunnen wij gegevens verkrijgen over het werkstation en kan de betreffende persoon aangesproken worden. Indien nodig is het vervolgens mogelijk om vervolgstappen te nemen om meer bewustzijn te creëren. Denk hierbij aan e-learnings, awareness trainingen en het blijvend uitvoeren van usb-drops.

USB drop simulatie van Networking4all

- Bewustwording vergroten
- Identificatie vaardigheden verbeteren
- Risicovermindering
- Opleiding en training
- Testen van reacties op incidenten

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Networking4all OptiSec Pentest Professional (OSPP)

OSPP verkort jouw voorbereiding op het OSCP-examen met maanden!

Mens | Security Awareness | Identify

Wat is Networking4all OptiSec Pentest Professional (OSPP) training?

Deze 5-daagse training is een unieke OSCP-preparation training in het Nederlands. Naast echte scenariolabs, waar vaardigheden ontwikkeld worden zoals penetratietesten, netwerkexploitatie en het identificeren van kwetsbaarheden, gaat OSPP dieper in op de materie en kijken we naar het “waarom en wanneer achter de praktische skills.

OSCP-preparation training

Dit scheelt maanden op je prep-time voor OSCP. Geen ‘try harder’, maar leer echt waar je mee bezig bent! Om deze training te volgen wordt minimaal het CEH-niveau verwacht van de cursist en een beheersing van commandline op Linux.

Het OSCP-certificaat krijg je na het voltooien van een uitdagend 24-uurs praktijkexamen. Deze certificering is zeer gerespecteerd in de industrie. OSCP wordt erkend als een waardevolle aanvulling voor professionals die willen excelleren in de wereld van ethisch hacken.

De cursus behandelt:

- Penetratietesten
- Netwerkexploitatie
- Identificeren van kwetsbaarheden

Meer informatie nodig? Lees verder op onze website

Networking4all OptiSec Container Security (OSCS)

OSCS onthult geavanceerde inzichten en benadrukt optimalisatie van containersecurity.

Mens | Security Awareness | Identify

Wat is Networking4all OptiSec Container Security (OSCS) ?

Deze cursus biedt diepgaande kennis van container- en orchestratieconcepten, waardoor je effectiever advies kunt geven binnen de organisatie. Word bewuster van dreigingen en risico's, verbeter je advies- en samenwerkingsvaardigheden, en automatiseer beveiligingsmaatregelen volgens best practices uit de praktijk. Voor professionals gericht op compliance en auditing biedt de cursus inzicht in het behalen van beheersdoelstellingen in Agile en DevOps settings. Het overbrugt de kloof tussen traditionele IT-beveiliging en containeromgevingen. In een snel evoluerend technologisch landschap biedt OSCS toekomstbestendige vaardigheden en bevordert het begrip van verantwoordelijkheidsmodellen voor flexibiliteit in een veranderende organisatiestructuur.

De cursus behandelt:

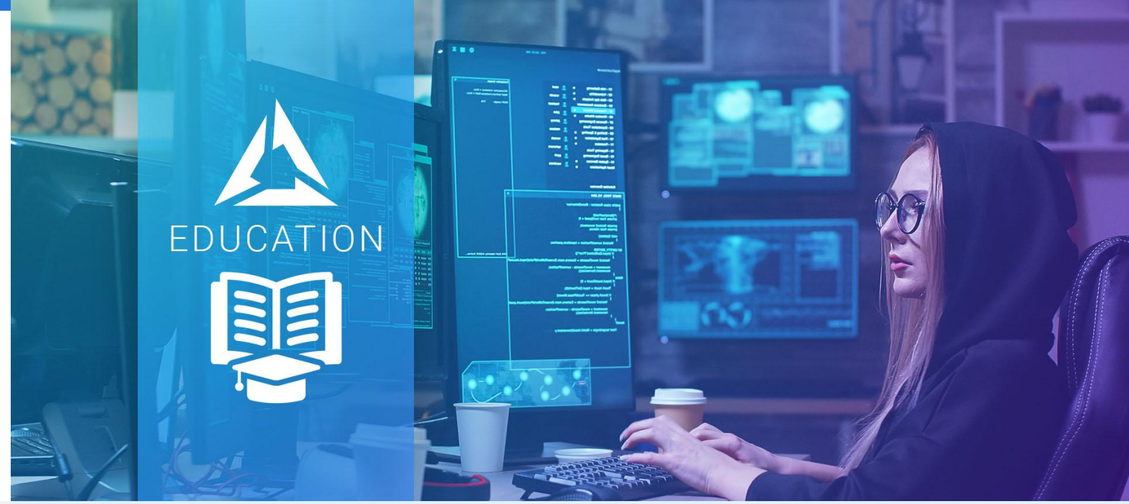
- Diepgaande kennis van container- en orchestratie concepten
- Word bewuster van dreigingen en risico's
- Verbeter je advies- en samenwerkingsvaardigheden
- Automatiseer beveiligingsmaatregelen
- Gericht op compliance en auditing
- Inzicht in het behalen van beheersdoelstellingen in Agile en DevOps.

Meer informatie nodig? Lees verder op onze website

Certified Ethical Hacker (CEH)

Erkende training, inclusief (her)examens, 6 maanden labtoegang en meer!

Mens | Security Awareness | Identify



Wat is Certified Ethical Hacker (CEH)?

De Certified Ethical Hacker (CEH) training van EC-Council is ontworpen om professionals op te leiden in ethisch hacken en cybersecurity. Deze intensieve cursus behandelt technieken die hackers gebruiken en leert deelnemers hoe ze systemen kunnen beveiligen tegen potentiële aanvallen. Het curriculum omvat onderwerpen zoals footprinting, scanning, enumeration, system hacking, malware-analyse, social engineering en meer. De training omvat praktische labs en hands-on ervaring om vaardigheden te versterken. Succesvolle afronding van het CEH-examen resulteert in certificering, die wereldwijd erkend wordt als bewijs van ethisch hacking competenties. CEH is een zeer waardevolle training voor als je wilt starten met het ethische hacken, maar ook voor bijvoorbeeld de security consultant om echt te begrijpen hoe de aanvallen werken en hoe te beschermen tegen deze.

De cursus behandelt:

- Footprinting
- Scanning
- Enumeration
- System hacking
- Malware-analyse
- Social engineering en meer.

Meer informatie nodig? Lees verder op onze website

Certified Ethical Hacker Master Preparation

Bewijs je praktische skills als erkend ethisch hacker.

Mens | Security Awareness | Identify

Wat is Certified Ethical Hacker Master Preparation?

De CEH Master training is het gevorderde niveau na de Certified Ethical Hacker (CEH) certificering. Deze opleiding richt zich op het verfijnen van praktische ethisch hacken vaardigheden en verdiepen van kennis op het gebied van cybersecurity. Toepassen van SQL Injections, vinden en uitbuiten van vulnerabilities. Toepassen van encryptie voor data exfiltratie en het gebruik van tools zoals WireShark. Deze training richt zich op het uitvoeren van de praktijk, waarbij de CEH training niet op elk onderdeel de ruimte biedt om de diepte in te duiken. Tijdens deze training staat de cursist in de rol van de ethische hacker en wordt verwacht minimaal het CEH niveau te beheersen.

De cursus behandelt:

- Het verfijnen van praktische ethisch hacken vaardigheden
- Het verdiepen van kennis op het gebied van cybersecurity
- Het toepassen van SQL Injections
- Het vinden en uitbuiten van vulnerabilities
- Het toepassen van encryptie voor data exfiltratie
- Het gebruik van tools zoals WireShark

Meer informatie nodig? Lees verder op onze website

Certified Incident Handler (ECIH)

Beman de eerste verdedigingslinie in cybersecurity.

Mens | Security Awareness | Identify

Wat is EC-Council Certified Incident Handler (ECIH) training?

De EC-Council Certified Incident Handler (ECIH) training biedt uitgebreide instructie aan professionals die betrokken zijn bij incident response en handling. Deze cursus behandelt incident detectie, rapportage, analyse en responsstrategieën. Deelnemers leren forensische technieken, malware-analyse en het beheren van beveiligingsincidenten.

Met nadruk op praktijkervaring via labs en scenario-oefeningen, rust de ECIH-training beveiligingsprofessionals uit met de vaardigheden om effectief te reageren op cyberincidenten. Het behalen van het ECIH-examen resulteert in certificering, waarbij professionals aantonen dat ze bekwaam zijn in het coördineren van een gestructureerde incident respons en het minimaliseren van schade.

De cursus behandelt:

- Incident Detectie
- Rapportage
- Analyse
- Responsstrategieën.
- Forensische technieken
- Malware-analyse
- Het beheren van beveiligingsincidenten

Meer informatie nodig? Lees verder op onze website

Certified SOC Analyst (CSA)

Klaar voor het werk in een Security Operations Center (SOC).

Mens | Security Awareness | Identify

Wat is Certified SOC Analyst (CSA)?

De Certified SOC Analyst (CSA) training van EC-Council is ontworpen om professionals te trainen in het beheer van Security Operations Centers (SOC). De cursus behandelt essentiële aspecten zoals SIEM-implementatie, incident response, threat intelligence en monitoring van beveiliging operaties. Met hands-on labs en praktische oefeningen leert deze training deelnemers doeltreffend reageren op en analyseren van beveiligingsincidenten.

Het CSA-certificaat, behaald na het succesvol afronden van het bijbehorende examen, erkent de vaardigheden van professionals in het proactief identificeren en mitigeren van beveiligingsrisico's, waardoor ze waardevolle bijdragen kunnen leveren aan SOC-teams.

De cursus behandelt:

- SIEM-implementatie
- Incident response
- Threat intelligence
- Monitoring van beveiliging operaties

Meer informatie nodig? Lees verder op onze website

Certified Information Security Manager (CISM)

Governance in cybersecurity.

Mens | Security Awareness | Identify

Wat is Certified Information Security Manager (CISM)?

De Certified Information Security Manager (CISM) training benadrukt expertise in informatiebeveiliging management. Met focus op strategische planning en beleidsvorming bereidt de cursus professionals voor op het beheren en leiden van organisatorische beveiligings initiatieven. CISM behandelt domeinen zoals informatiebeveiligingsbeleid, risicomanagement, incidentmanagement en governance. Het verwerven van dit certificaat bevestigt niet alleen een diepgaand begrip van beveiligingsconcepten, maar toont ook aan dat men in staat is om effectieve beveiligingsprogramma's te ontwikkelen en te onderhouden. CISM-certificering verhoogt de geloofwaardigheid van beveiligingsprofessionals en is waardevol voor diegenen die een leidende rol willen spelen in het beheren van informatiebeveiliging binnen organisaties.

De cursus behandelt:

- Informatiebeveiligingsbeleid
- Risicomanagement
- Incidentmanagement
- Governance

Meer informatie nodig? Lees verder op onze website

Certified Information Systems Auditor (CISA)

CISA is een must-have voor auditors.

Mens | Security Awareness | Identify

Wat is Certified Information Systems Auditor (CISA) ?

De Certified Information Systems Auditor (CISA) training richt zich op audit- en beveiligingsprofessionals die betrokken zijn bij informatiesystemen. Met een nadruk op auditing, controle en beveiliging, dekt CISA essentiële domeinen zoals informatiesysteem acquisitie, ontwikkeling en implementatie, informatiebeveiliging management en IT-operaties. Het curriculum voorziet deelnemers van kennis over internationale standaarden en best practices. Het behalen van het CISA-certificaat bevestigt niet alleen een grondig begrip van auditprincipes, maar ook de bekwaamheid om risico's te evalueren en effectieve controlemaatregelen te implementeren. CISA-certificering vergroot de professionele geloofwaardigheid en is waardevol voor diegenen die zich willen specialiseren in informatie systeemaudits en -beveiliging.

De cursus behandelt:

- Informatiesysteem Acquisitie
- Ontwikkeling en implementatie
- Informatiebeveiliging Management
- IT-operaties

Meer informatie nodig? Lees verder op onze website

Certified in Cybersecurity (CC)

Erkende ISC² CC training inclusief (her)examen en ISC² licentie.

Mens | Security Awareness | Identify

Wat is Certified in Cybersecurity (CC)?

Het ISC² Certified in Cybersecurity-certificaat bevestigt je grondige begrip van de fundamenten van informatiebeveiliging. Dit snel opkomende en bekroonde certificaat wordt steeds meer erkend door bedrijven, waardoor het waardevol is voor je arbeidskansen en een fundamentele eerste stap naar security. Het certificaat dient als uitstekende voorbereiding op officiële CISSP- of CCSP-trainingen, waarbij CISSP de nummer één gevraagde certificering wereldwijd is in het domein van Cyber Security. CC behandelt Security Principles, Business Continuity, Access Control, Network Security en Security Operations. Het formele examen, af te leggen bij Pearson VUE, leidt tot certificering, en de bekroning van "Best Professional Certification Program" in 2023 versterkt de erkenning van deze training.

De cursus behandelt:

- Security Principles
- Business Continuity
- Access Control
- Network Security
- Security Operations

Meer informatie nodig? Lees verder op onze website

Certified Cloud Security Professional (CCSP)

Erkende ISC² CCSP training van een erkend trainer.

Mens | Security Awareness | Identify

Wat is Certified Cloud Security Professional (CCSP)?

De Certified Cloud Security Professional (CCSP) training van ISC² is gericht op professionals die betrokken zijn bij cloud security. CCSP biedt een diepgaand inzicht in de complexiteiten van beveiliging in cloud omgevingen. Deelnemers verwerven vaardigheden om cloud risico's te beoordelen, beveiligingsbeleid te ontwikkelen en beveiligingscontroles te implementeren. Het CCSP-certificaat erkent expertise op het gebied van cloudbeveiliging en benadrukt het vermogen van professionals om gegevens en systemen effectief te beschermen in een cloudomgeving.

De cursus behandelt:

- Cloud-architectuur
- Data security
- Identity and access management
- Compliance en legal issues

Meer informatie nodig? Lees verder op onze website

Certified Information Systems Security Professional (CISSP)

Erkende ISC² CISSP training van een erkend trainer.

Mens | Security Awareness | Identify

Wat is Certified Information Systems Security Professional (CISSP)?

De Certified Information Systems Security Professional (CISSP) training, aangeboden door ISC², is een toonaangevende certificering voor informatiebeveiliging. Deze uitgebreide cursus behandelt acht domeinen, waaronder beveiliging en risicomanagement, communicatie- en netwerkbeveiliging, toegangsbeheer en meer.

Ontworpen voor ervaren beveiligingsprofessionals, streeft CISSP naar een holistische benadering van informatiebeveiliging waarmee dit certificaat ook wel als de gouden standaard wordt beschouwd. Deelnemers verwerven diepgaande kennis en vaardigheden, inclusief ethische normen en beleidsvorming. Het certificaat toont aan dat de professional in staat is om complexe beveiligings uitdagingen te begrijpen en effectieve oplossingen te implementeren. Het CISSP-certificaat is wereldwijd erkend en benadrukt de competentie van beveiligingsexperts.

De cursus behandelt:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Meer informatie nodig? Lees verder op onze website

Risico Analyse

In welke cybersecurity bewustzijnsfase zit jouw organisatie?

Proces | Security Awareness | Certificaat Diensten | NIS2 | Identify

In welke cybersecurity bewustzijnsfase zit jouw organisatie?

Door regelmatig het cybersecurity-bewustzijn van de organisatie te evalueren, kunnen stappen worden ondernomen om het bewustzijn te vergroten en risico's te verlagen. Networking4all heeft een model ontwikkeld om te bepalen in welke fase van cybersecurity bewustzijn uw organisatie zich bevindt. Welke maatregelen de organisatie reeds heeft toegepast en welke maatregelen nog kunnen worden uitgevoerd om tot een hogere cultuur van veiligheid te komen met als doel risico's verlagen.

- Heeft de organisatie de basis maatregelen op orde?
- Domeinen: Mens, Proces, Techniek, Fysiek, Juridisch en beheer maatregelen
- Op welk domein(en) dienen er risico verlagende maatregelen te worden genomen?
- Welke (type) maatregelen zijn benodigd om de volgende stap te zetten?
- Mapping met ISO 27001, NIS2 en DORA
- Ook voor resellers/partners. Whitelabel inzetbaar in uw huisstijl!

Bewustzijnsfasen

- level 1 Onbewustheid
- level 2 Bewustwording
- level 3 Plan de Cybercampagne
- level 4 Implementatie
- level 5 Consolidatie
- level 6 Integrale Cyberpreventie
- level 7 Cultuur van Veiligheid

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

ISO 27001 Assessment

Dé voorbereiding voor uw ISO 27001 audit.

Proces | Security Awareness | ISO Diensten | Identify

Wat is een ISO 27001 Assessment?

Als u op het punt staat om een certificeringstraject voor de ISO 27001 in te gaan, is een goede voorbereiding van groot belang. Zorg ervoor dat u inzicht hebt in alle belangrijke zaken omtrent informatiebeveiliging voor een optimale voorbereiding op uw ISO 27001 audit!

Nulmeting

Het ISO 27001 Assessment geeft inzicht in welke controls binnen de ISO 27001 standaard in uw organisatie nog aandacht behoeven. Middels een ISO 27001 Assessment weet de organisatie hoe het gesteld is met de informatiebeveiliging en wat u moet doen om zwakke plekken te versterken. Wij controleren alles conform de richtlijnen van de ISO standaard, waaronder ook uw kwaliteitsmanagement systeem.

Het ISO 27001 Assessment traject:

- Voorbespreking
- Interviews
- Review documenten
- Rapportage & Roadmap
- Nabespreking

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

ISO 27001 Begeleiding

Begeleiding door ervaren specialisten tijdens uw ISO 27001 Auditing traject.

Proces | Security Awareness | ISO Diensten | Identify

Wat is ISO 27001?

De ISO 27001 norm is een internationale norm voor informatiebeveiliging. Deze norm helpt u om uw bedrijfsrisico's te begrijpen en op basis daarvan passende maatregelen te nemen. Het resultaat is bedrijfskritische informatie die optimaal beschikbaar, veilig en van hoge kwaliteit is. De ISO 27001 certificering zorgt ervoor dat de informatiebeveiliging van uw organisatie goed geregeld is en uw organisatie voldoet aan de eisen en verwachtingen van klanten en leveranciers op het gebied van informatiebeveiliging.

Wat is ISO 27001 Begeleiding?

Als u wilt beginnen aan de voorbereiding voor uw ISO 27001 audit kan dit een zorgelijk proces zijn. Wat houdt de norm precies in en hoe moet ik alle processen m.b.t. informatiebeveiliging correct inrichten binnen mijn organisatie? Door de bovenstaande vragen en daarnaast de complexiteit van de voorbereiding op een ISO audit is het verstandig om dit proces met een ISO expert te doorlopen Met de ISO 27001 Begeleiding van Networking4all bent u verzekerd van deskundig advies tijdens het gehele traject door ervaren ISO specialisten!

Het doel van de ISO 27001 Begeleiding:

- Begeleiding bij verbeteren controls t.b.v informatiebeveiliging
- Begeleiding en ondersteuning tijdens het ISO 27001 traject
- Voorbereiding op uw jaarlijkse controle-audit
- Assessment en deskundig advies door ervaren ISO experts
- Bevorderen van compliance (bijv. AVG, ISO27001)
- ISO Service Abonnement

Meer informatie nodig? Lees verder op onze website ➟

NETWORKING4ALL

NEN 7510 Begeleiding

Begeleiding door ervaren specialisten tijdens uw NEN 7510 Auditing traject.

Proces | Security Awareness | Certificaat Diensten | Identify

Wat is NEN 7510?

NEN 7510 is een Nederlandse norm die specifiek gericht is op het waarborgen van de beveiliging van persoonsgegevens in de gezondheidszorg. Deze norm biedt een raamwerk voor het opzetten, implementeren, onderhouden en verbeteren van beveiligingsmaatregelen met betrekking tot de verwerking van persoonsgegevens in de zorgsector. Het is gebaseerd op de internationale norm ISO 27001, maar is aangepast en uitgebreid om specifiek te voldoen aan de behoeften en vereisten van de Nederlandse gezondheidszorg.

Waarom is NEN 7510 belangrijk?

De gezondheidszorg verwerkt enorme hoeveelheden gevoelige persoonsgegevens, variërend van medische dossiers tot patiëntinformatie. Het lekken of compromitteren van deze gegevens kan verstrekkende gevolgen hebben, niet alleen voor individuele patiënten maar ook voor de integriteit van de zorginstellingen zelf. NEN 7510 biedt een gestructureerde aanpak om de vertrouwelijkheid, integriteit en beschikbaarheid van deze gegevens te waarborgen, waardoor zorginstellingen kunnen voldoen aan hun wettelijke verplichtingen en het vertrouwen van patiënten kunnen behouden.

Het doel van de NEN 7510 Begeleiding:

- Waarborgen beveiliging persoonsgegevens in de gezondheidszorg
- Gestructureerde aanpak
- Risicobeheer
- Compliance met wet- en regelgeving

Meer informatie nodig? Lees verder op onze website ➟

NETWORKING4ALL

NIS2 Compliance Assessment

Wat betekent de NIS2-richtlijn voor jouw organisatie?

Proces | Security Awareness | Certificaat Diensten | NIS2 | Identify

Hoe uw organisatie kan voldoen aan de NIS2 richtlijnen?

De NIS2 richtlijn stuurt aan op een hoog volwassenheidsniveau van informatiebeveiliging. Dit zorgt ervoor dat al voordat de richtlijn is omgezet naar nationale wetgeving de mogelijke invulling van de NIS2 vereisten kan worden geschetst. Deze invulling moet natuurlijk in lijn zijn met dat hoge informatiebeveiliging volwassenheidsniveau dat wordt nagestreefd binnen de EU. NIS2 compliance kan ongetwijfeld een uitdaging vormen voor uw organisatie. Het waarborgen van een robuuste cyberbeveiliging en het voldoen aan de steeds veranderende normen vereisen zorgvuldige planning en uitvoering.

Met onze uitgebreide expertise en toewijding aan informatiebeveiliging, bieden we begeleiding, consultancy en security oplossingen die uw organisatie helpen om NIS2 compliance te bereiken en uw digitale activa te beschermen. We kijken ernaar uit om met u samen te werken aan een veilige digitale toekomst.

Het doel van de NIS2 Compliance Assessment:

- Risicobeoordeling
- Incidenten Behandeling
- Bedrijfscontinuïteit
- Beveiliging toeleveringsketen
- Beveiliging netwerk en informatiesystemen
- Effectiviteit Cybersecurity maatregelen
- Cyber Hygiëne & Opleiding
- Cryptografie
- Fysieke beveiliging
- Multifactor-authenticatie

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

NIS2 Management Training

Wat betekent de NIS2-richtlijn voor jou als bestuurder?

Proces | Security Awareness | Certificaat Diensten | NIS2 | Identify

NIS2 Wetgeving voor bestuurders

De norm schrijft voor dat bestuurders dienen te beschikken over de benodigde kennis en vaardigheden om cybersecurity risico's te beoordelen, beveiligingsplannen kritisch te evalueren, besluiten te bespreken, standpunten te formuleren, en beleid en oplossingen te beoordelen die de bedrijfsmiddelen van hun organisatie beschermen. Bij gebrek aan adequaat risicobeheer kunnen zowel bedrijven als individuele functionarissen en bestuurders aansprakelijk worden gesteld.

Waarom NIS2 Management Training?

Verkrijg een grondige kennis en diepgaand inzicht in informatiebeveiliging. Behoud controle over cybersecurity binnen uw organisatie. Verbeter uw begrip en communicatie met collega's op het gebied van cybersecurity. Voldoe aan de eisen van NIS2 gericht op bestuurders.

Het doel van de NIS2 Compliance Assessment:

- Risicobeoordeling
- Incidenten Behandeling
- Bedrijfscontinuïteit
- Beveiliging toeleveringsketen
- Beveiliging netwerk en informatiesystemen
- Effectiviteit Cybersecurity maatregelen
- Cyber Hygiëne & Opleiding
- Cryptografie
- Fysieke beveiliging
- Multifactor-authenticatie

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Business Continuity Plan

Goed voorbereidt zijn zodat de impact op de organisatie beperkt blijft

Proces | Informatie Beveiliging | Security Awareness | Certificaat Diensten | NIS2 | Identify

Wat is Business Continuity Plan?

Een Business Continuity Plan (BCP) is een strategisch document dat de noodzakelijke stappen en processen beschrijft om bedrijfsactiviteiten tijdens en na onverwachte verstoringen te waarborgen. Het doel van een BCP is niet alleen het beperken van operationele stilstand, maar ook het beschermen van essentiële bedrijfsmiddelen, zoals systemen, data, infrastructuur en werknemers.

Waarom Business Continuity Plan?

Tegenwoordig zijn wij steeds afhankelijker van technologie en wereldwijde toeleveringsketens. Hierdoor kunnen onverwachte verstoringen aanzienlijke schade veroorzaken.
Zonder een effectief BCP kunnen bedrijven te maken krijgen met:

- Financiële verliezen door operationele stilstand of verloren klanten.
- Reputatieschade die het vertrouwen van klanten, partners en investeerders ondermijnt.
- Boetes of sancties wegens het niet naleven van regelgeving zoals de NIS2-richtlijn.

Belangrijke onderdelen van een BCP zijn:

- Risicoanalyse: Identificeren van potentiële bedreigingen (natuurrampen, cyberaanvallen, uitval van leveranciers).
- Impactanalyse: Het vaststellen van de gevolgen van verstoringen voor cruciale bedrijfsprocessen.
- Herstelstrategieën: Duidelijke plannen om binnen een minimale hersteltijd weer operationeel te zijn.
- Testen en evalueren: Regelmatige simulaties om ervoor te zorgen dat het plan in de praktijk effectief is.

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Emergency Response Plan

Hoe effectief is uw noodresponseplan?

Proces | Security Awareness | Identify

Wat is een Emergency Response Plan begeleidingstraject?

Een Emergency Response Plan (ERP) begeleidingstraject is een proces waarbij een organisatie wordt ondersteund bij het ontwikkelen, implementeren en verbeteren van een effectief Emergency Response Plan. Het doel van een ERP-begeleidingstraject is om ervoor te zorgen dat een organisatie goed voorbereid is op noodsituaties en in staat is om snel en adequaat te reageren om schade te minimaliseren, de veiligheid van medewerkers te waarborgen en de bedrijfscontinuïteit te behouden.

Het identificeren en evalueren van potentiële noodsituaties en risico's waarmee de organisatie kan worden geconfronteerd, zoals brand, natuurrampen, chemische lekkages, terroristische aanslagen, enz. Het regelmatig evalueren van het Emergency Response Plan, het identificeren van zwakke punten en het implementeren van verbeteringen op basis van lessen uit eerdere noodsituaties, feedback van medewerkers, veranderingen binnen de organisatie, enz. Het ERP-begeleidingstraject wordt vaak uitgevoerd met de hulp van interne teams en externe consultants of adviesbureaus die expertise hebben op het gebied van noodplanning en -beheer.

Het doel van de Emergency Response Plan:

- Voorbereiden op noodsituaties
- Identificeren zwakke plekken
- Waarborgen bedrijfscontinuïteit
- Veiligheid van medewerkers
- Schadebeperking
- Snellere respons en betere coördinatie

Meer informatie nodig? Lees verder op onze website

Cybersecurity Calamiteitenoefening

Bent u voorbereid op een cyberaanval?

Proces | Security Awareness | Identify

Wat is een Cybersecurity Calamiteitenoefening?

Een Cybersecurity Calamiteitenoefening is een geplande en gestructureerde oefening die is ontworpen om de reactie van een organisatie op een cybersecurity-incident te testen, evalueren en verbeteren. Het is een simulatie van een daadwerkelijke cyberaanval of een andere vorm van cybersecuritycalamiteit, waarbij verschillende aspecten van de organisatie en haar betrokken teams worden getest. Tijdens een cybersecurity calamiteitenoefening wordt een scenario gecreëerd dat lijkt op een echte cyberaanvalssituatie. Dit kan bijvoorbeeld het binnendringen van een netwerk, een ransomware-aanval, een phishing-campagne of een datalek omvatten.

Het doel is om te zien hoe de organisatie reageert op het incident en om de effectiviteit van de cybersecurity maatregelen, procedures en reactieplannen te evalueren. De oefening betrekt vaak verschillende teams en belanghebbenden binnen de organisatie, zoals IT-personeel, beveiligingsteams, communicatie teams, managementteams en juridische afdelingen. Elk team heeft zijn eigen rollen en verantwoordelijkheden bij het omgaan met een cyberincident, en de oefening biedt de gelegenheid om de samenwerking tussen deze teams te verbeteren.

Het doel van de Emergency Response Plan:

- Response Vaardigheden ontwikkelen
- Samenwerking bevorderen
- Evalueren van bestaande plannen
- Minimaliseren van impact

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Back-up as a Service

Verzekerd van uw data.

Techniek | Recover

Wat is Back-up as a Service?

Het doel van de back-up is een kopie van gegevens te maken welke kan worden hersteld in geval van een storing in de primaire gegevens. Storingen in de primaire gegevens kunnen het gevolg zijn van hardware- of softwarefouten, gegevenscorruptie, of een door mensen veroorzaakte gebeurtenis, zoals een kwaadaardige aanval (virus of malware), of het per ongeluk verwijderen van gegevens, maar ook na bijvoorbeeld een brand in het bedrijfspand.

Bij onze oplossing wordt het geheel uit handen genomen en regelen wij in samenwerking met Infradax alles. Beheer en onderhoud van de noodzakelijke apparatuur, applicaties, processen en beheer in het eigen datacenter in Nederland. Zo bent u voor een vast bedrag per maand verzekerd van een managed back-up-omgeving en betaalt u simpelweg voor deze service, in plaats van dat u zelf moet investeren in een back-up-omgeving en die vervolgens ook moet beheren.

Het doel van de Back-up as a Service:

- Uw data gegarandeerd in Nederland
- Disaster Recovery
- Beveiligd en beheerbaar
- Snelle RPO en RTO tijden
- Managed backup, zowel op eigen locatie als in de cloud
- Standaard 4 weken retentie
- Monitoring & Alerting (kantooruren)
- Actualisatie & Patch management
- Anti-virus & Anti-malware
- Incident Management
- Back-up Hardening
- Installatieservice & Servicedesk

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Pentest

Zijn uw gegevens veilig? Laat ons u hacken!

Techniek | Ethisch Hacken | Identify

Wat is een penetratietest (pentest)?

Bij een penetratietest, ook wel pentest genoemd, gebruiken onze ethical hackers allerhande middelen om toegang te verkrijgen tot uw systemen, websites en/of losse apparaten door middel van kwetsbaarheden. De kwetsbaarheden worden blootgelegd waarbij vooraf is bepaald welke systemen in de pentest zijn opgenomen. Dit noemen wij de scope. De kwetsbaarheden, bevindingen en adviezen vatten we samen in een uitgebreid rapport. De duur van een pentest is afhankelijk van de grootte van uw website, netwerkomgeving, applicaties enz.

Waarom een pentest?

Een pentest levert inzichten waarmee uw organisatie de informatiebeveiliging kan versterken. Zo kan een pentest de kwetsbaarheden van nieuwe en/of bestaande servers, webapplicaties/websites of een compleet netwerk in kaart brengen. In andere gevallen kan het waardevol zijn om een goed beeld te verkrijgen van het algehele beveiligingsniveau van uw organisatie.

Het doel van de pentest:

- Hackers een stap voor zijn
- Inzicht in kwetsbaarheden
- Risico's beheren
- Bevorderen van compliance (bijv. AVG, ISO27001)
- Overtuigend rapport voor uw klanten of leveranciers

Alternatieve producten:

- Pentest as a Service
- Nessus Vulnerability Scan
- Acunetix Web Application Scan

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Pentest as a Service

Een pentest service in abonnementsvorm waarbij u de frequentie en doorlooptijd bepaalt.

Techniek | Ethisch Hacken | Identify

Wat is Pentest as a Service?

Naast onze standaard pentest bieden wij ook Pentest as a Service aan. Pentest as a Service is een pentest service in abonnementsvorm waarbij u de frequentie en doorlooptijd bepaalt. Dit is interessant voor klanten die graag regelmatig pentesten willen laten uitvoeren om de algehele veiligheid van hun omgeving continu te testen. Vanwege de verschillende pentest strategieën die mogelijk worden toegepast kunt u afwisselen tussen een pentest gericht op algehele veiligheidscontrole en bijvoorbeeld gericht op een webapplicatie. Dit is volledig naar eigen wens in te vullen. Ook voor klanten welke B2B oplossingen aanbieden waarbij potentiële eindklanten bewijs van penetratietesten eisen alvorens over te gaan tot zakendoen, is deze dienst interessant omdat u ten alle tijden een recent rapport kan aanbieden.

Waarom een Pentest as a Service?

Een pentest geeft hier zekerheid. Het pentesten van uw systemen is een betrouwbare manier om de netwerkbeveiliging en systeem kwetsbaarheden van uw organisatie te controleren. Om aan deze vereisten te voldoen, moeten de systemen die door een organisatie worden gebruikt of beheerd, aan specifieke beveiligingsnormen voldoen.

Het doel van de pentest as a Service:

- Regelmatig infrastructuur testen op kwetsbaarheden
- Hackers een stap voor zijn
- Inzicht in kwetsbaarheden
- Risico’s beheren
- Bevorderen van compliance (bijv. AVG, ISO27001)
- Overtuigend rapport voor uw klanten of leveranciers

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Red Teaming

Zijn uw bedrijfsgeheimen echt geheim? Er is maar één manier om daar veilig achter te komen.

Techniek | Security Awareness | Social Engineering | Ethisch Hacken | Identify

Wat is Red Teaming?

Vind de zwakke punten, voordat iemand anders het doet. Stel uw organisatie op de proef met een levensechte aanval en leg de gevoelige punten van uw infrastructuur bloot met ons Red Team. Dit kan zowel fysiek als digitaal. Bij fysiek kunt u denken aan camera's die zijn opgehangen, of het binnendringen van een gebouw doordat een medewerker de deur openhoudt voor ons omdat wij ons voordoen als een postbezorger met volle handen. Red Teaming kan u een unieke kijk bieden in de security van uw organisatie en infrastructuur. Het kan gevoelige plekken openbaren die u nooit had verwacht.

Waarom een Red Teaming?

Red Teaming is een simulatie waarmee u exact te weten kunt komen hoe een kwaadwillende zou opereren om in te breken in uw netwerk, systeem of applicatie, zowel fysiek en sociaal als technologisch. Tijdens een Red Teaming operatie probeert ons security team gevoelige informatie in handen te krijgen die zij alleen van uw netwerk zouden kunnen hebben achterhalen, of een vlag te planten binnen uw bedrijf, systemen of applicaties.

U kunt uit de volgende onderdelen een keuze maken:

- Pentest
- Wifi Audit
- Bluetooth Audit
- Phishing
- Vishing (telefonisch) SE calls
- USB Drop
- Mystery Guest
- Tailgating (fysieke controle van uw gebouw / kantoor)
- Dumpster Diving
- Vulnerability scans
- Web Applicatie scans
- Open Source Intelligence onderzoeken

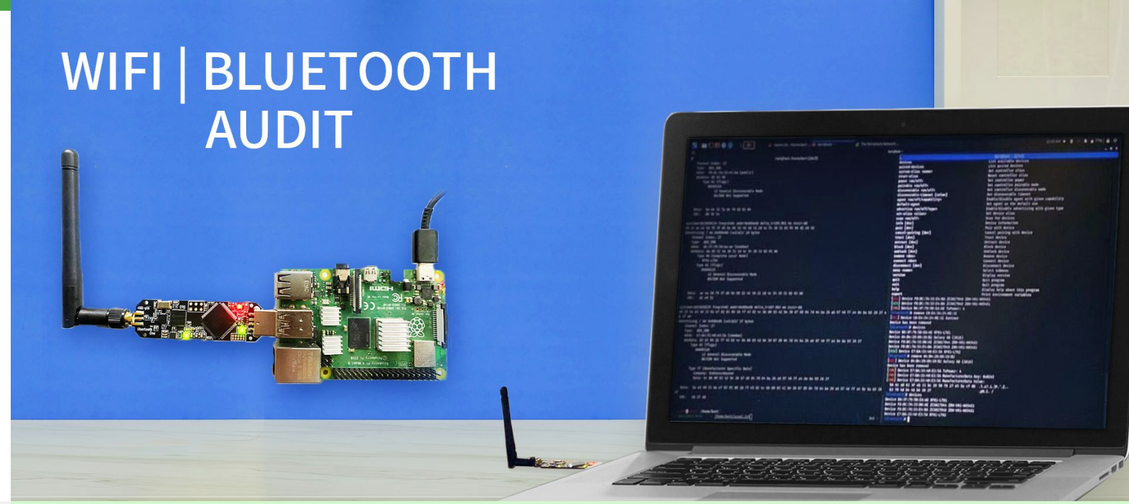
Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Wifi | Bluetooth Audit

Een onveilige configuratie maakt u kwetsbaar.

Techniek | Ethisch Hacken | Identify



Wat is een Wifi | Bluetooth Audit?

Nu overal draadloze netwerken worden gebruikt, is het auditen van wifi-netwerken een veelgevraagde dienst. Een onveilige configuratie maakt deze erg kwetsbaar, waarbij aanvallers van op afstand toegang kunnen krijgen tot netwerken en deze kunnen exploiteren. Dit is al mogelijk door bijv. een aanvaller die met zijn auto naast uw pand komt te staan. Door de groei van draadloze netwerken en mobiele apparaten zijn draadloze netwerken een belangrijk doelwit geworden voor cybercriminelen.

Het doel van een draadloos netwerk is eenvoudige toegang te bieden aan gebruikers, maar dit kan een open deur worden voor aanvallers. Een wifi audit zorgt ervoor dat u deze deur gesloten houdt. Bovenstaande geldt ook voor Bluetooth verbindingen. Bij simpele pairing is het mogelijk om bepaalde characteristics (functies) uit te lezen, te wijzigen en te verwijderen. Niet alleen telefoons en speakers maken gebruik van Bluetooth, maar bijvoorbeeld ook industriële sensoren. U kunt zich voorstellen, zodra dit soort apparaten gehackt worden, dat het enorme (imago)schade en financiële schade kan veroorzaken. Bij het auditen van draadloze netwerken evalueren wij de daadwerkelijke beveiliging, effectiviteit en prestaties om een overzicht te krijgen van de toestand van het netwerk.

Mogelijke risico's van een onveilig wifi-netwerk:

- Datalekken
- Man-in-the-Middle aanvallen
- Malware verspreiding
- Malicious hotspots
- Evil Twin aanvallen
- Zwakke wachtwoorden
- Zwakke tot geen encryptie
- Geen gescheiden netwerken (Gast / Zakelijk)

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Nessus Vulnerability Scan

Scan uw netwerk en infrastructuur (IP adressen) op kwetsbaarheden.

Techniek | Vulnerability Scan & Management | Identify

Wat is een Nessus Vulnerability Scan?

De Vulnerability Scan is een uitgebreide scan die scant op kwetsbaarheden via een volledig geautomatiseerd proces op basis van bekende beveiligingsfouten. U kunt hiermee uw interne en/of externe netwerk en infrastructuur (IP adressen) laten scannen. De scan houdt daarbij rekening met de actuele versie van OWASP Top 10 versie 2021, het meest recente database van kwetsbaarheden (CVE) en CVSS 3.1 scores.

Hoe werkt een Vulnerability Scan?

Als u externe IP-adressen wilt testen, dan kan dit remote worden uitgevoerd. Bij een scan voor interne IP-adressen hebben wij toegang nodig tot uw netwerk middels een VPN verbinding. De uitgebreide automatische scan is toepasbaar voor bijvoorbeeld webservers, mailservers, file servers enz. Alle (open) poorten worden hiermee gecontroleerd op kwetsbaarheden. Na afloop krijgt u de resultaten van de scan gedeeld in de vorm van een automatische rapportage. Dit rapport wordt in het Engels verstrekt. De resultaten kunt u gebruiken om gerichte stappen te ondernemen naar een betere beveiliging van uw netwerk.

Het doel van de Nessus Vulnerability Scan:

- Netwerk scannen op kwetsbaarheden
- Geautomatiseerd proces inclusief rapportage
- OWASP Top 10 versie 2021
- Recente database van kwetsbaarheden (CVE) en CVSS 3.1 scores

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Acunetix Web Application Scan

Scan uw(web)applicatie op kwetsbaarheden.

Techniek | Vulnerability Scan & Management | Identify

Wat is een Acunetix Web Application Scan?

De Web Application Scan is een uitgebreide scan die scant op kwetsbaarheden via een volledig geautomatiseerd proces op basis van bekende beveiligingsfouten. U kunt hiermee uw (web)applicatie laten scannen. De scan houdt daarbij rekening met de actuele versie van OWASP Top 10 versie 2021, het meest recente database van kwetsbaarheden (CVE) en CVSS 3.1 scores.

Hoe werkt een Web Application Scan?

De uitgebreide automatische scan is toepasbaar voor alle applicaties. Deze worden hiermee gecontroleerd op kwetsbaarheden. Na afloop krijgt u de resultaten van de scan gedeeld in de vorm van een automatische rapportage. Dit rapport wordt in het Engels verstrekt. De resultaten kunt u gebruiken om gerichte stappen te ondernemen naar een betere beveiliging van uw applicaties.

Het doel van de Acunetix Web Application Scan:

- (Web)applicaties scannen op kwetsbaarheden
- Gecombineerde DAST + IAST scanresultaten
- Detecteer meer dan 7.000 kwetsbaarheden, waaronder SQL-injecties, XSS, verkeerde configuraties, zwakke wachtwoorden, blootgestelde databases en andere kwetsbaarheden.
- Met de geavanceerde macro-opname technologie kunt u complexe formulieren met meerdere niveaus en zelfs met een wachtwoord beveiligde delen van uw site scannen.

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

WithSecure Exposure Management

Scan en beheer kwetsbaarheden in uw Netwerk.

Techniek | Vulnerability Scan & Management | Identify

Wat is Exposure Management?

WithSecure Elements Exposure Management (XM) is een continue en proactieve oplossing die inbreuken op de bedrijfsmiddelen en bedrijfsvoering van uw bedrijf voorspelt en voorkomt. Elements XM biedt inzicht in uw aanvalsoppervlak en de (AI) aanbevelingen zorgen voor een efficiënte aanpak van uw grootste risico's vanuit één overzicht. Één oplossing voor 360° beheer van digitale blootstelling en overzicht over uw externe aanvalsoppervlak en interne beveiligingshouding, om cyberaanvallen proactief te voorkomen.

Hoe werkt Exposure Management?

1. Elements Exposure Management integreert gegevens uit uw interne en externe omgevingen tot een holistisch overzicht van uw aanvalsoppervlak
2. Elements XM gebruikt kwetsbaarheden, misconfiguraties en andere blootstellingen in uw omgeving om potentiële aanvalspaden te identificeren.
3. Het overzicht dat het Exposure Dashboard biedt, helpt bij het prioriteren van herstelacties en geeft je een risicogebaseerd overzicht van de geïdentificeerde zwakke plekken in je aanvalsoppervlak.

Het doel van de WithSecure Exposure Management:

- Ontdekken

Ontdek uw digitale perimeter en identificeer de meest kritieke bedrijfsmiddelen en identiteiten.

- Prioriteiten stellen

Onze bevindingen over welke blootstelling prioriteit moet krijgen bij herstel zijn gebaseerd op simulatie van aanvalspaden waarbij gegevens van bedreigingsinformatie van WithSecure en uw bedrijfscontext worden geïntegreerd.

- Handelen

Voer geprioriteerde herstelacties uit om uw aanvalsoppervlak te verkleinen en het risiconiveau van uw bedrijf te verlagen, met behulp van bruikbare richtlijnen en AI aanbevelingen.

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Qualys VMDR 2.0

Eén oplossing voor cyberbeveiligingsrisico's, ontdekking, beoordeling, detectie en reactie.

Techniek | Vulnerability Scan & Management | Identify | Detect | Respond

Wat is VMDR 2.0?

Qualys VMDR 2.0 biedt een all-inclusive risk-based vulnerability management oplossing om kwetsbaarheden en assets te prioriteren op basis van risico en bedrijfskritiek. Met VMDR 2.0 krijgen ondernemingen zichtbaarheid en inzicht in cyberrisico's, waardoor kwetsbaarheden, bedrijfsmiddelen of groepen bedrijfsmiddelen eenvoudig op basis van bedrijfsrisico's kunnen worden geprioriteerd. Beveiligingsteams kunnen actie ondernemen om de risico's te beperken, zodat de onderneming het werkelijke risico kan meten en de risicovermindering in de loop van de tijd kan volgen. Ontdek, beoordeel, prioriteer en patch kritieke kwetsbaarheden en verminder cybersecurity risico's in realtime IT-, OT- en IoT-landschap. Detecteer en inventariseer alle bekende en onbekende assets die verbinding maken met uw wereldwijde hybride-IT omgeving - inclusief, on-premises apparaten en applicaties, mobiel, OT en IoT. Inclusief Qualys Passive Scanning Sensors. Correleer automatisch kwetsbaarheden en patches voor specifieke hosts, waardoor uw reactietijd voor herstel wordt verkort. Zoek naar CVE's en identificeer de nieuwste vervangende patches.Verwijder of update kwetsbare apps, waarschuw gebruikers, reset of vergrendel apparaten, wijzig wachtwoorden en meer.

Het doel van de Qualys VMDR 2.0:

- Begrijp en beheer cybersecurity risico's
- Identificeer alle bedrijfsmiddelen in uw omgeving
- Herstel bedreigingen snel op schaal
- Automatiseer herstel
- Analyseer kwetsbaarheden en misconfiguraties

Meer informatie nodig? Lees verder op onze website

Mobile Device Management

Beheren en beveiligen van data op endpoints is belangrijker dan ooit.

Techniek | Informatie Beveiliging | Security Awareness | Identify | ISO27001 | Respond | NIS2

Wat is Mobile Device Management?

Mobiele apparaten worden steeds vaker gebruikt om toegang te krijgen tot bedrijfsinformatie en om productief te werken, zowel binnen als buiten het kantoor. Zonder een goede security oplossing kunnen bedrijven echter te maken krijgen met beveiligingsrisico's, datalekken en verlies van controle over gevoelige informatie. Mobile Device Management ook wel MDM of UEM (Unified Endpoint Management) genoemd, draagt bij aan het mitigeren van de risico's. Voor bedrijven is Mobile Threat Defense (MTD) essentieel om mobiele apparaten te beschermen tegen cyberbedreigingen, zoals phishing-aanvallen, man-in-the-middle-aanvallen of geïnfecteerde apps, die kunnen leiden tot datalekken.MTD biedt real-time detectie en bescherming, zodat gevoelige bedrijfsdata veilig blijft, zelfs buiten het kantoor.

Waarom Mobile Device Management?

Bedrijfsdata te beschermen door security af te dwingen, zoals het verplicht stellen van wachtwoorden, encryptie en het beheren van applicaties. Bedrijven te helpen voldoen aan regelgeving, zoals GDPR of andere industrie-specifieke eisen,
door de juiste beveiligingsprotocollen toe te passen.Bij verlies of diefstal kunnen apparaten op afstand worden gewist of geblokkeerd, waardoor gevoelige bedrijfsdata veilig blijft.

De MDM-oplossingen waar wij mee werken zijn:

- Ivanti Neurons for MDM (voorheen MobileIron)
- BlackBerry UEM
- Omnissa Workspace One (voorheen VMware Workspace One)
- Microsoft Intune
- Jamf
- Samsung Knox Manage

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

BlackBerry Cylance Endpoint

Bescherm uw endpoints met een oplossing in de cloud.

Techniek | Endpoint Beveiliging | Protect

Wat is BlackBerry Cylance Endpoint?

BlackBerry Cylance Endpoint Protection is een geavanceerde endpoint beveiligingsoplossing die gebruikmaakt van kunstmatige intelligentie (AI) en machine learning om endpoints te beschermen tegen malware, ransomware, en andere bedreigingen.

Wat Cylance Endpoint bijzonder maakt, is zijn vermogen om bedreigingen te detecteren en te voorkomen door AI-gestuurde analyse van bestandskenmerken en gedrag. In plaats van te vertrouwen op handtekeningen van bekende bedreigingen, maakt het gebruik van algoritmen die verdachte patronen en gedragingen identificeren, zelfs bij nog niet eerder geziene bedreigingen.

Hierdoor kan Cylance Endpoint sneller reageren op nieuwe bedreigingen en biedt het een proactieve beveiligingsaanpak voor endpoints, wat essentieel is in de moderne cybersecurity-landschap.

Het doel van BlackBerry Cylance Endpoint:

Snelle, eenvoudige cloud beheerde bescherming tegen bedreigingen voor al uw Windows®-, Mac®-, Linux®-, Android™- en iOS®-apparaten.

Twee type licenties:

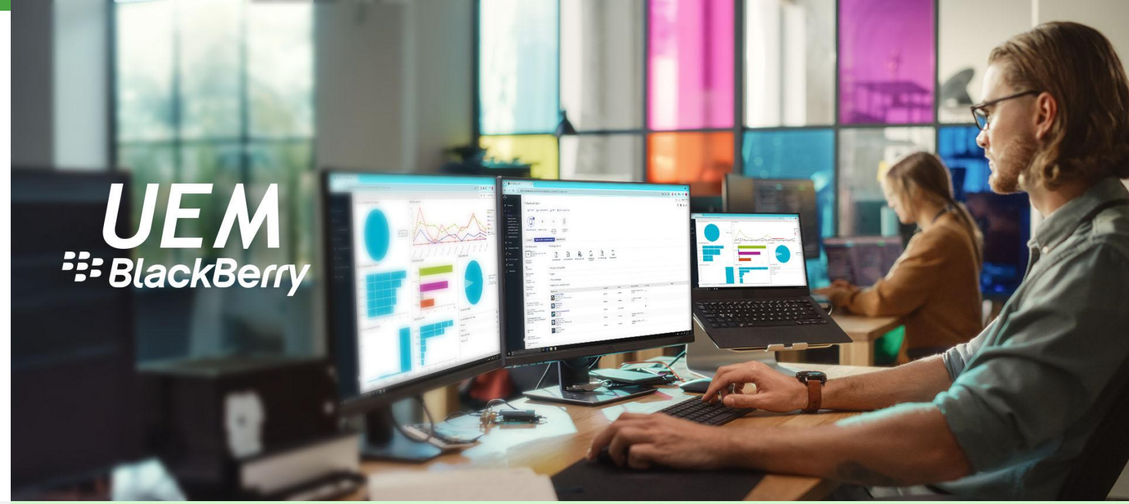
- Standard: EPP
- Advanced: EPP + EDR

Meer informatie nodig? Lees verder op onze website

BlackBerry Unified Endpoint Management

Bescherm uw endpoints met een oplossing in de cloud.

Techniek | Endpoint Beveiliging | Protect



Wat is BlackBerry Unified Endpoint Management?

BlackBerry Unified Endpoint Management (UEM) is een oplossing die organisaties helpt bij het beheren en beveiligen van alle endpoints binnen hun netwerk vanuit één centraal platform. Dit omvat verschillende apparaten zoals smartphones, tablets, laptops, en desktops, ongeacht het besturingssysteem (iOS, Android, Windows, macOS, etc.).

Beveilig alle endpoints

- Implementeer bedrijfsapps veilig op BYO-apparaten
- Productiviteit beveiligen
- Onderteken documenten veilig op mobiele apparaten
- Veilige communicatie tussen apparaten
- Momenteel de enige UEM-oplossing die is opgenomen in de NATO Information Assurance Product Catalogue (NIAPC)

Het doel van BlackBerry UEM:

Centralisatie: Beheer en configureer alle eindpunten vanuit één dashboard, wat de administratieve last vermindert en de efficiëntie verhoogt.

Beveiliging: Biedt uitgebreide beveiligingsmaatregelen zoals gegevens -versleuteling, applicatiebeheer, en beleids configuratie om gevoelige informatie te beschermen.

Toegang en Identiteit: Beheer gebruikers identiteiten en toegangsniveaus, en pas beveiligingsmaatregelen toe op basis van gebruikersrollen en apparaat specificaties.

Compliance: Ondersteunt naleving van regelgeving en beleidsnormen door gedetailleerde rapportage en monitoring van apparaten en gegevens.

Flexibiliteit: Ondersteunt verschillende besturingssystemen en apparaten, wat zorgt voor een consistente ervaring over diverse platformen heen.

Meer informatie nodig? Lees verder op onze website

WithSecure Endpoint Protection

Bescherm uw endpoints met een oplossing in de cloud.

Techniek | Endpoint Beveiliging | Protect

Wat is Endpoint Protection?

De Endpoint Protection oplossing identificeert en blokkeert bekende bedreigingen. Het biedt een centrale locatie voor het installeren, beheren en bewaken van de beveiliging van alle endpoints. De oplossing beschermt computers (Mac / Windows), mobiele apparaten (iOS / Android) en diverse server platforms. WithSecure Elements Security Center beheert alle beveiliging via één console in de cloud. Met threat intelligence en machine learning biedt het proactieve bescherming tegen de bedreigingen van vandaag, waaronder ransomware en zero-day-aanvallen. Servers zijn missiekritisch voor uw communicatie, samenwerking en gegevensopslag.

WithSecure Elements Endpoint Protection voor Servers biedt beveiliging voor uw servers.
WithSecure Elements Mobile Protection is een proactieve oplossing met volledige dekking voor de bescherming van uw mobiele apparaten. Bestrijd phishing-pogingen via verschillende sociale apps, bescherm uw medewerkers tegen toegang tot schadelijke websites, blokkeer malware en houd uw bedrijfskritische gegevens veilig, zelfs wanneer u gebruikmaakt van onveilige netwerkverbindingen.

Het doel van de WithSecure Endpoint Protection:

- Computer Protection
- Server Security
- Mobile Protection
- Software Updater
- Centraal beheer via WithSecure Elements Security Center

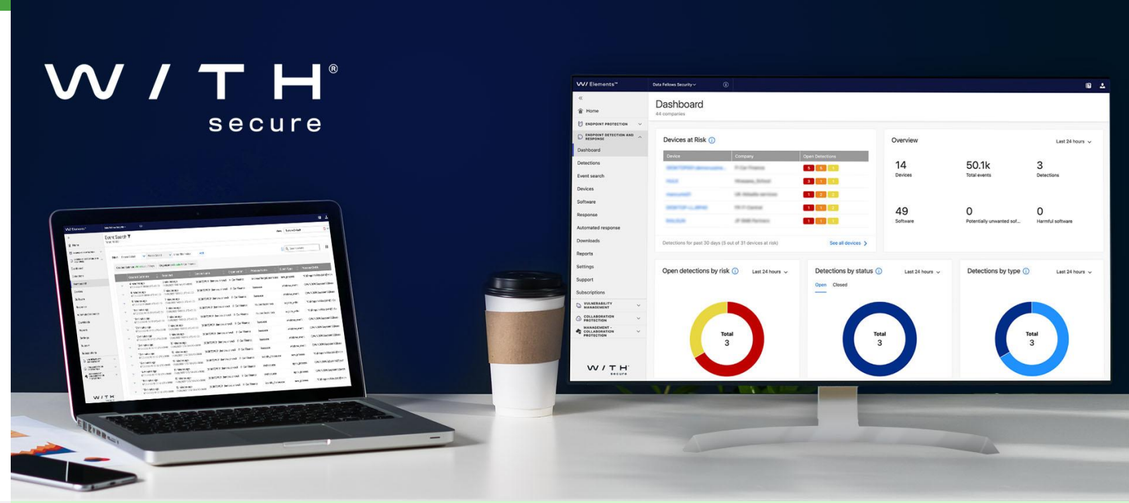
Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

WithSecure Endpoint Detection and Response

Bescherm uw organisatie tegen gerichte cyberaanvallen.

Techniek | Endpoint Beveiliging | Protect | Detect | Respond



Wat is Endpoint Detection & Response?

WithSecure Elements Endpoint Detection and Response biedt bescherming tegen geavanceerde gerichte cyberaanvallen. WithSecure Elements Endpoint Detection and Response geeft u direct inzicht in uw IT-omgeving en beveiligingsstatus vanuit één enkel security overzicht. Het houdt uw bedrijf en gegevens veilig door aanvallen snel te detecteren en te reageren met deskundige begeleiding. Dankzij een uitgebreid overzicht van uw IT-omgeving en cloud-diensten kunt u de blootstelling aan bedreigingen en kans op datalekken terugdringen.

De oplossing biedt in een oogwenk een overzicht van alle actieve processen op endpoints binnen uw netwerk om ongewenste, onbekende en schadelijke applicaties uit te lichten. U kunt potentieel schadelijke applicaties en cloud-diensten eenvoudig blokkeren om te voorkomen dat er datalekken optreden. De niet-belastende sensoren voor alle computers binnen uw organisatie verzamelen op de achtergrond gedragsinformatie op basis van gedocumenteerde mechanismen.

Het doel van de WithSecure Endpoint Detection and Respons:

- Snelle detectie van beveiligingsincidenten
- Direct inzicht in de status van uw IT-omgeving en beveiliging
- Detecteert abnormale activiteiten op uw eindpunten
- Geautomatiseerde incident response.
- De EDR-oplossing maakt gebruik van real-time gedrags-, reputatie-big data-analyse en machine learning

Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Keeper Password Manager

Een digitale kluis voor al uw wachtwoorden.

Techniek | Endpoint Beveiliging | Protect

Wat is Keeper Password Manager?

Keeper is een zakelijke oplossing voor centraal gecoördineerd en volledig versleuteld wachtwoordbeheer. Gebruikers krijgen een eigen versleutelde kluis om wachtwoorden, aanmeldingsgegevens, bestanden en vertrouwelijke klantgegevens in op te slaan. Keeper ondersteunt op rollen gebaseerde toegang, 2FA, controles en incidentrapportage. Hiernaast hanteert Keeper een zero-knowledge policy.

Waarom Keeper Password Manager?

Keeper maakt willekeurige, sterke wachtwoorden voor al uw websites en toepassingen, en bewaart ze vervolgens in een veilige kluis op al uw apparaten. Bespaart medewerkers tijd en frustratie, en elimineert de noodzaak om wachtwoorden te herstellen, hergebruiken en onthouden. Keeper password manager slaat je wachtwoorden veilig op en vult automatisch de inloggegevens in wanneer je een website of app bezoekt. Dit bespaart tijd en moeite bij het onthouden en invoeren van wachtwoorden. Wachtwoorden worden opgeslagen in een versleutelde kluis. Medewerkers kunnen tevens veilig onderling data uitwisselen.

Het doel van de Keeper Password Manager:

- Beveiliging
- Unieke wachtwoorden
- Veilig delen
- Gemak
- Synchronisatie
- Veilige opslag
- Wachtwoordgenerator
- Herinneringen

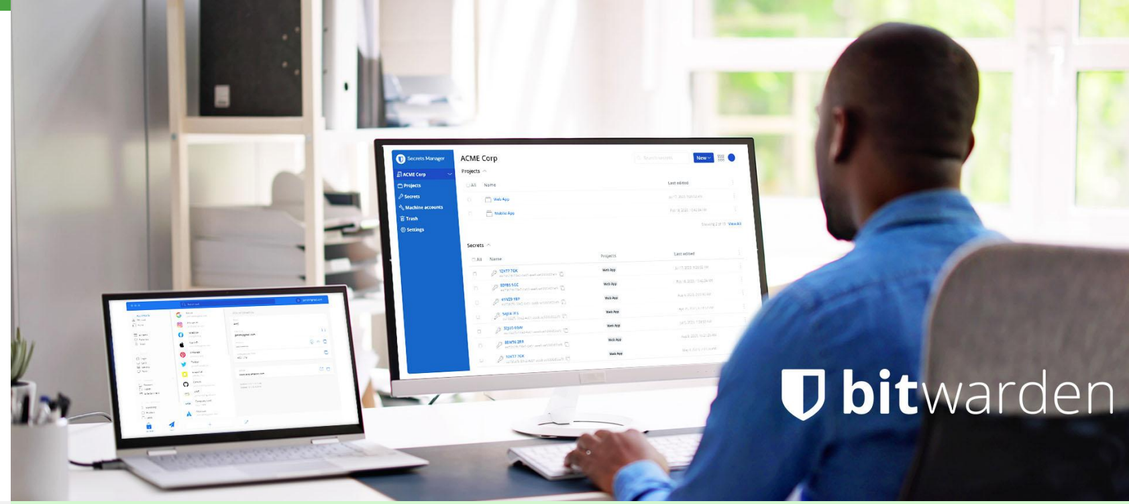
Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

Bitwarden Password Manager

Bewezen veiligheid en transparantie in wachtwoordbeheer.

Techniek | Endpoint Beveiliging | Protect



Wat is Bitwarden Password Manager?

Bitwarden is een populaire applicatie voor wachtwoordbeheer, ontworpen om gebruikers te helpen hun wachtwoorden en andere gevoelige informatie veilig op te slaan en te beheren. Het biedt functies zoals het genereren van wachtwoorden, veilige opslag van wachtwoorden, versleuteling en platformonafhankelijke compatibiliteit, waardoor gebruikers toegang hebben tot hun wachtwoorden vanaf verschillende apparaten en web browsers.

Waarom Bitwarden Password Manager?

Bijna 81% van de inbraken door hackers is te wijten aan gestolen of zwakke wachtwoorden Wachtwoordmanagers stellen werknemers in staat om sterke, unieke wachtwoorden te genereren en deze veilig te delen. Wachtwoordbeheerders stellen bedrijven in staat om een sterke cybersecurity cultuur op te bouwen door middel van algemene beleidsregels.
Bedrijven die een sterke cybersecurity cultuur creëren, verlagen hun risico op cyberdreigingen aanzienlijk. Bewaar alle zakelijke wachtwoorden en andere gevoelige informatie in een end-to-end versleutelde kluis. Beheerders kunnen de toegang en het verificatieproces beheren met protocollen zoals Single Sign-On en tools zoals organisatiebrede Enterprise Policies.

Het doel van Bitwarden Password Manager:

- Veilig samenwerken en wachtwoorden delen
- Snel en eenvoudig implementeren en beheren
- Overal toegang op elk apparaat
- Eenvoudige, flexibele SSO en SCIM integraties
- Gratis familieplan voor gebruikers
- Snelle import- en migratie tools
- Eenvoudige, gestroomlijnde gebruikerservaring
- Prioriteit ondersteuning en trainers

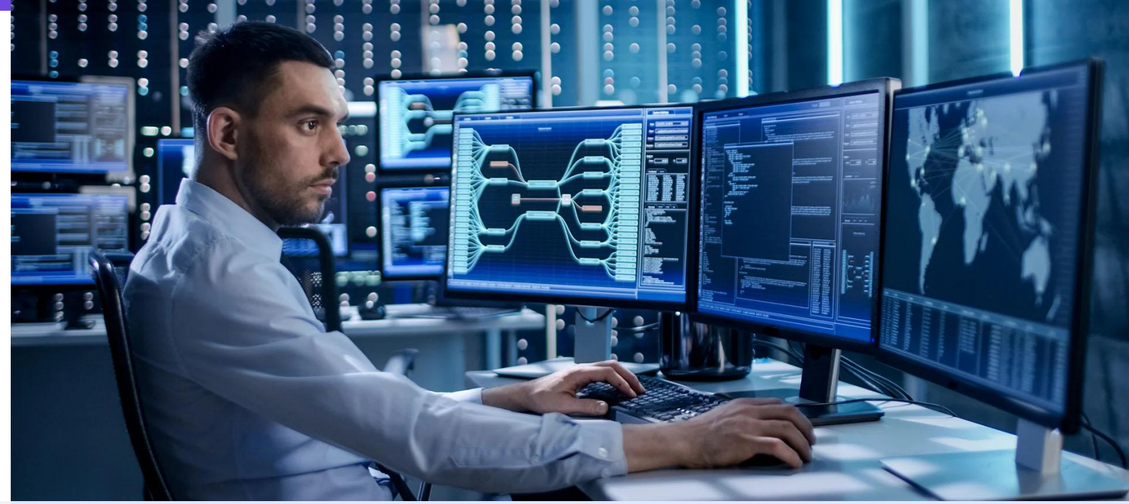
Meer informatie nodig? Lees verder op onze website

NETWORKING4ALL

24/7 Managed Security Monitoring SOC SIEM

Monitoren, alarmeren, adviseren & Incident Response

Techniek | Monitoring | Identify | Protect | Detect | Respond | Recover



Wat is Managed Security Monitoring?

De oplossing biedt een volledig beheerde dienst met uitgebreide detectie en respons mogelijkheden, inclusief integratie met bestaande tools zoals firewalls en SIEM-oplossingen. Dit pakket biedt 24/7 dreigingsmonitoring, incident response en direct contact met een team van cybersecurity-specialisten. Ondersteund door een $1M* garantie!.

- 24/7 Monitoring & Incident Response
- Direct contact met een team van cybersecurity specialisten
- Ondersteund door een $1 miljoen garantie! (*voorwaarden van toepassing)
- Integratie met uw bestaande tools (EPP, EDR, Firewalls, SIEM oplossing etc.)

Om een beveiligingsincident te voorkomen of te onderdrukken, is het van belang dat meldingen worden gemonitord en geanalyseerd. Het is van groot belang dat er zo snel mogelijk wordt gereageerd om schade zoveel mogelijk te beperken. Wij als uw Managed Security Monitoring Provider verzorgen en ontzorgen u op het gebied van implementatie, monitoring, analyse, incident response en rapportage/advies.
(*voorwaarden van toepassing)

Het doel van 24/7 Managed Security Monitoring:

- 24/7 Monitoring & Detectie
- 24/7 Incident Response (Minimaal 20 uur consultancy)
- 24/7 Threat Hunting & Threat Detection
- 24/7 Triage & Response
- 24/7 Support via telefoon
- Dedicated Blue team
- Forensisch onderzoek (Minimaal 20 uur consultancy)
- Ondersteunt 300+ integraties (Endpoint - Netwerk - Cloud - Email - SaaS - Identity)
- Geavanceerde AI Algoritmen Technologie
- Uitgebreide onboarding en implementatie ondersteuning
- Interactieve rapportage inclusief deskundig advies
- Security information and event management (SIEM)
- GDPR Compliant
- Garantie tot $1 miljoen*
- Additionele Incident response en forensisch onderzoek diensten

Meer informatie nodig? Lees verder op onze website ➟

Incident Response

Monitoren, alarmeren, adviseren & Incident Response

Techniek | Monitoring | Identify | Protect | Detect | Respond | Recover

Wat is Incident Response?

Incident response is de manier waarop een organisatie omgaat met cyberaanvallen en cyberbeveiligingsincidenten. Het doel van Incident Response is het beperken en minimaliseren van de schade die wordt veroorzaakt door een inbreuk en het verminderen van de hersteltijd en -kosten.

Wij kunnen helpen - of je nu wordt aangevallen, een inbreuk moet indammen of een incident response plan wilt ontwikkelen. Middels een samenwerking met BlackBerry Cybersecurity hebben wij 24/7 een internationaal incident response team voor u klaar staan. Omdat wij verschillende landen in de EU bedienen is de voertaal Engels.

24/7 Internationaal Incident Reponse Team
Bel direct op +31(0) 20 788 1036 of meld een incident, waarna wij contact met u opnemen.

Het doel van Incident Response:

Wij kunnen u helpen de gevolgen van een inbreuk te beperken, ervoor te zorgen dat uw herstel volgens best practices verloopt en uw IT-omgeving te beveiligen voor de toekomst. Onze cyberbeveiligingsdeskundigen geven antwoord op uw vragen;

- Hoe is de aanvaller in mijn omgeving gekomen?
- Hoe hebben ze zich binnen de omgeving verplaatst?
- In welk tijdsbestek vond de aanval plaats?
- Tot welke netwerken, systemen en gegevens hadden ze toegang?
- Wat waren de acties en doelen van de aanvaller?
- Heeft de aanvaller gegevens gestolen?
- Hoe kan ik het risico op een toekomstige aanval minimaliseren?

Meer informatie nodig? Lees verder op onze website

Digitaal Forensisch Onderzoek

Monitoren, alarmeren, adviseren & Incident Response

Techniek | Monitoring | Identify | Protect | Detect | Respond | Recover

Wat is Digitaal Forensisch Onderzoek?

Wanneer gevoelige gegevens worden gecompromitteerd of gestolen, loopt een organisatie risico. Digitaal forensisch onderzoek is gerelateerd aan de reactie op cyberbeveiligings incidenten en omvat onderzoek naar datalekken, bedreigingen van binnenuit en andere soorten cybercriminaliteit, insluiting van incidenten, chain of custody,
forensisch computeronderzoek, forensisch cloudonderzoek en forensisch netwerkonderzoek. Digitaal Forensische onderzoek kan ook een onderdeel zijn van onze Incident Response dienst.

Wij kunnen helpen - of het nu gaat om een onderzoek naar een inbreuk op de cyberbeveiliging, een bedreiging van binnenuit of een ander type forensisch computeronderzoek en/of digitaal onderzoek.

Het doel van Digitaal Forensisch Onderzoek:

Elk digitaal forensisch onderzoek bestaat uit vier hoofdonderdelen:

- Scope bepalen
- Plan maken
- Forensische verwerving van elektronische gegevens
- Analyse van de verworven gegevens

Ook kunnen getuigenverklaringen van deskundigen worden geleverd voor het geval het geproduceerde en geanalyseerde bewijs in een rechtbank moet worden besproken. De minimale afname is 20 uur.

Meer informatie nodig? Lees verder op onze website

SSL CERTIFICATEN

SSL/TLS Certificaten

Networking4all biedt een uitgebreid SSL (TLS) portfolio met diverse grote merken zoals Digicert en oplossingen, vanuit één uitgebreide portal. Daarbij hebben wij dedicated account managers en security specialisten voor u klaar staan voor een helder en duidelijk advies tijdens, voor en na SSL aanvragen. Met ons zelf ontwikkelde en tevens award-winning portal kunt u tijd besparen, risico's beperken en direct reageren op eventuele kwetsbaarheden. Hiernaast bieden we tevens een aantrekkelijke eigen (whitelabel) SSL lijn.

Onze SSL-certificaten zijn beschikbaar op drie verschillende validatieniveaus:

Domein validatie | DV

Domein validatie (DV) is geschikt voor niet-publieke websites. Er wordt gecontroleerd of de aanvrager beschikt over het beheer van het domein waarvoor het certificaat wordt aangevraagd. DV certificaten worden veel gebruikt voor persoonlijke, niet-commerciële websites, of privé domeinen die gebruikt worden voor testdoeleinden.

Organisatie validatie | OV

Voor een publieke website zonder commerciële doelstelling of overheidsfunctie biedt een Organisatie validatie (OV) certificaat vaak uitkomst. Naast de controle over het beheer van het domein worden de bedrijfsgegevens van de aanvrager gecontroleerd. De bedrijfsgegevens worden in het certificaat opgenomen en zijn in de meeste browsers gemakkelijk te controleren door de details van het certificaat op te vragen.

Uitgebreide validatie | EV

Een certificaat met een Uitgebreide validatie (Extended Validation, of EV) is geschikt voor commerciële websites zoals bijvoorbeeld webshops en banken, maar ook voor overheidsinstanties. Voor dit type validatie worden de bedrijfsgegevens uitgebreid gecontroleerd met behulp van een openbaar register, zoals het handelsregister van de Kamer van Koophandel. Als resultaat worden de bedrijfsgegevens weergegeven in de certificaat details in de browser.

Naast SSL Certificaten bieden we ook oplossen voor:

- Code signing | Onderteken software
- Email & ID signing | Onderteken emails en inzetbaar als client authenticatie
- Document signing | Onderteken PDF documenten
- Verified Mark Certificaten | Logo naast uw mail in de inbox van uw klanten.

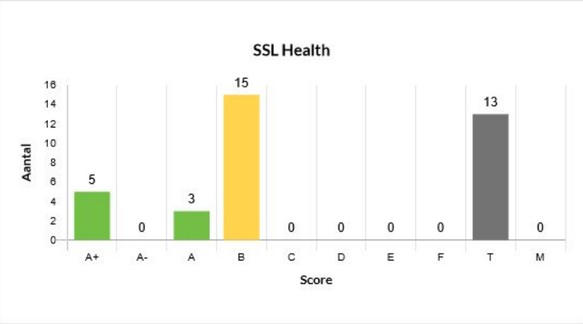
SSL Beheer

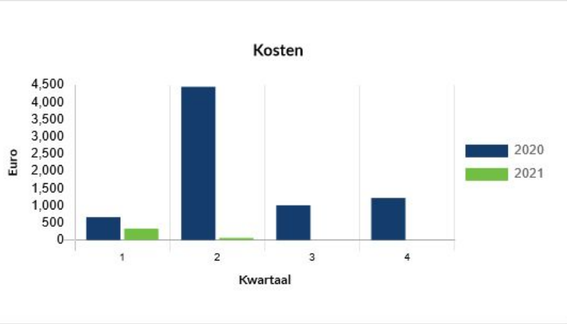
U kunt SSL certificaten aanvragen, heruitgeven, domeinnamen toevoegen en zelfs monitoren op installatie en configuratie. Daarnaast kunt u reminders configureren en standaarden instellen zodat uw SSL aanvraag nog sneller verloopt.

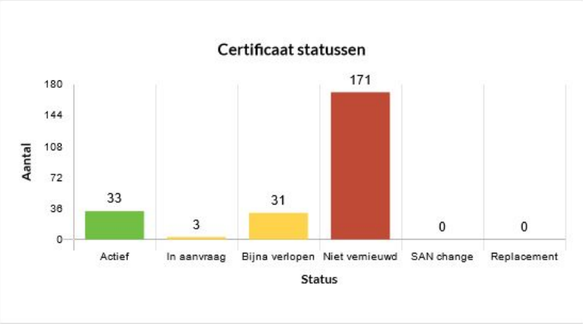
Ook kunt u bestaande (niet bij ons afgenomen) certificaten toevoegen en hiervoor reminders instellen voor tijdige verlengingen zodat u uit één portal kunt werken en anticiperen.

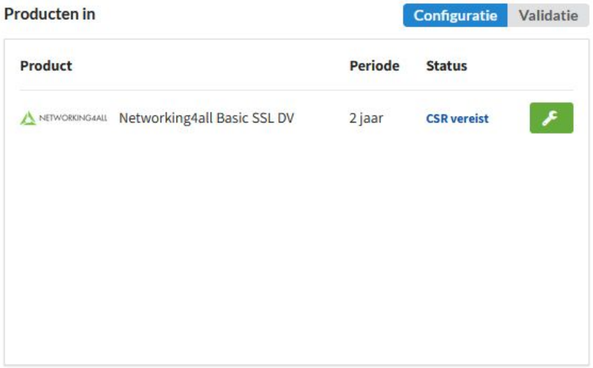
Tevens monitoren wij uw SSL Certificaten en achterliggende servers op configuratie, kwetsbaarheden en scores. Uw SSL portfolio wordt wekelijks of maandelijks gecontroleerd. Inzichtelijk in uw dashboard en tevens als rapportage te downloaden.

Middels ons visueel sterk validatieproces weet u precies bij welke stap het proces zich bevindt. Beheer uw contactpersonen, eindklanten en locaties. U heeft tevens een duidelijk overzicht van uw certificaten, bestellingen, prijslijsten, facturen en kunt veilig met 2FA inloggen.









SSL Automatiseren

In de moderne IT-omgevingen, waarin schaalbaarheid en snelheid van groot belang zijn, is de automatisering van SSL-certificaten een cruciaal aspect geworden voor zowel veiligheid als efficiëntie. Traditionele handmatige processen voor het aanvragen, valideren en vernieuwen van SSL-certificaten kunnen foutgevoelig zijn en vereisen veel tijd. Gelukkig bieden Rest-API's en het ACME-protocol (Automated Certificate Management Environment) een oplossing

Waarom SSL Automatiseren?

Tijd besparen: Handmatig certificaten beheren kost veel tijd. Door automatisering kun je certificaten binnen seconden aanvragen en vernieuwen.

Verlopen certificaten voorkomen: Door certificaten automatisch te vernieuwen, voorkom je onverwachte downtime en beveiligingsproblemen door verlopen certificaten.

Schaalbaarheid: Voor grote organisaties of cloud-native omgevingen met honderden of duizenden certificaten is handmatige beheer niet praktisch. Automatisering zorgt voor consistentie en minder fouten.

Rest-API

Onze Rest-API stelt je in staat om de hele levenscyclus van een certificaat te beheren via programmatische methoden. Van aanvraag tot (her) uitgifte.
Lees meer in onze API documentatie

ACME

ACME is een protocol waarmee je SSL-certificaten automatisch kunt aanvragen en beheren zonder menselijke tussenkomst. Het protocol vereenvoudigt het proces van aanvragen, valideren, installeren en vernieuwen van certificaten door interactie tussen een ACME-client (op jouw server) en een certificaatautoriteit (CA).
Lees meer in onze ACME Documentatie

Certificate as a Service | CaaS

Networking4all draagt zorg voor uw volledige SSL Portfolio beheer. Op basis van een gestructureerd proces ontzorgen we u van het gehele proces van aanvraag tot uitgifte. U hoeft enkel nog het certificaat te installeren. Hiernaast adviseren we aan de hand van onze SSL Best Practices. Onderlinge afspraken en processen worden in een contract vastgelegd.

Problematieken welke we vaak tegenkomen:

- Men weet niet precies welke SSL certificaten men heeft
- Geen overzicht/inzicht wie/welke SSL besteld (verschillende afdelingen)
- Geen certificaat bestel policy
- Er worden geen best-practices gehanteerd, waardoor kwetsbaarder
- Een slechte/incomplete configuratie van het certificaat / achterliggende server

Middels Certificate as a Service bieden we ontzorging, één centraal punt voor uw SSL beheer.

De Meern, Utrecht | Hoofdkantoor

Wilt u een vrijblijvend en oriënterend gesprek met ons om te bekijken wat we voor u of eventueel voor elkaar, kunnen betekenen? Dit onder het genot van een heerlijk bakje koffie of thee? Neem dan contact op voor een afspraak op locatie.

"Veilig internet voor iedereen"