Cisco Cybersecurity Overzicht 2018

Waarom beveiliging?

Cyberaanvallen zijn haast dagelijks in het nieuws. Effectieve beveiliging is dan ook een essentiële voorwaarde voor elke organisatie die in de economie van het digitale tijdperk succesvol wil zijn.

Bescherming tegen cyberdreigingen

Hoewel de toenemende connectiviteit en de opkomst van IoT-technologie nieuwe kansen biedt, brengt dit ook nieuwe risico's met zich mee. In het digitale tijdperk zijn cyberaanvallen aan de orde van de dag. Hackers zijn goed georganiseerd, beschikken over voldoende middelen en zijn financieel gemotiveerd. Geen bedrijf is te klein om een interessant doelwit voor een cybercrimineel te zijn.

Beperk de risico's, leef wet- en regelgeving na

Er is toenemende bezorgdheid onder leidinggevenden over cyberrisico's, informatiebeveiliging en wettelijke vereisten. Op grond van de toepasselijke wetgeving inzake gegevensbescherming zijn bedrijven over de hele wereld verplicht om adequate beveiligingsmaatregelen te implementeren. Op niet-naleving staan forse straffen.

Digitale transformatie mogelijk maken

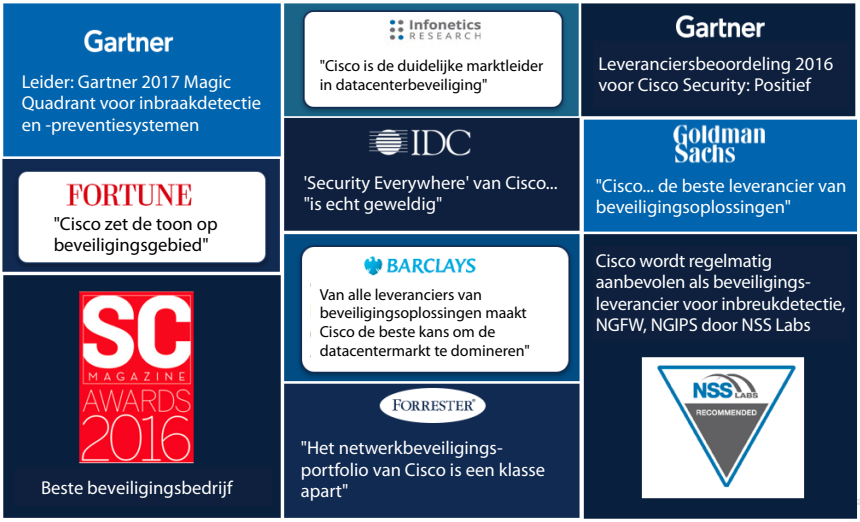
Zowel grote als kleine organisaties staan voor de taak om een digitaal bedrijfsmodel in te voeren. Doen ze dat niet, dan lopen ze het risico om structureel op achterstand gezet te worden door de concurrentie. Digitale transformatie vereist echter een solide fundament op het gebied van cyberbeveiliging. Bezorgdheid over de beveiliging kan ertoe leiden dat organisaties digitale initiatieven vertragen of stopzetten, met als gevolg dat hun innovatie- en groeipotentieel stokt.

Waarom Cisco?

Het meest effectieve, geïntegreerde beveiligingsportfolio

Cisco streeft ernaar om beveiliging minder complex te maken door een sterk geïntegreerde portfolio van oplossingen te leveren die op zichzelf al uitstekend zijn, maar nog veel krachtiger zijn wanneer ze in combinatie worden gebruikt. Wanneer de individuele onderdelen goed samenwerken, is effectieve beveiliging gegarandeerd. Probleemloos.

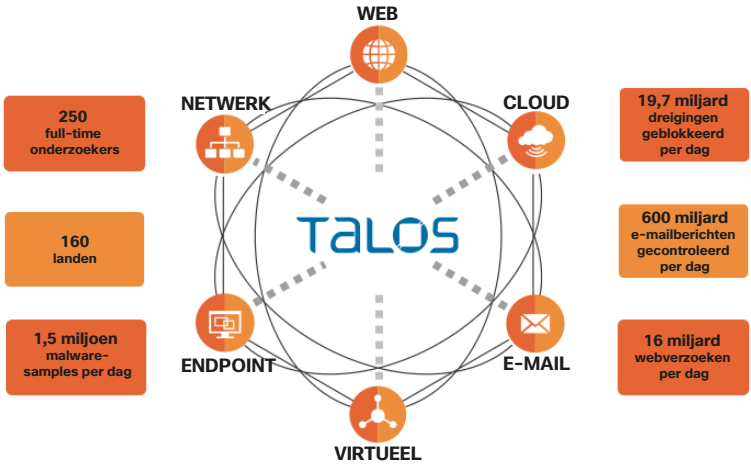
Cisco geniet binnen de industrie brede erkenning als leverancier van hoogwaardige oplossingen.



Onafhankelijke tests van de IT-beveiligingsoplossingen van Cisco bevestigen dat we effectieve en optimaal presterende oplossingen leveren. Niet voor niets komt Cisco elk jaar weer als beste naar voren in de tests.

Talos: Het toonaangevende beveiligingsinformatie- en onderzoeksteam van Cisco

De Talos Group is een eliteteam van beveiligingsexperts dat superieure informatie over cyberdreigingen verschaft. Klanten van Cisco profiteren ervan dat deze dreigingsinformatie is geïntegreerd in elke beveiligingsoplossing en -service die Cisco levert. Maar ook organisaties die geen klant zijn van Cisco kunnen profiteren van de onderzoeksinspanningen van Talos. Dankzij onze strenge toewijding aan het open-sourcemodel wordt de informatie voortdurend gedeeld met de totale gemeenschap, bijvoorbeeld via onderzoeksrapporten, blogs en de regelsets voor Snort, ClamAV, SenderBase en SpamCop.



In de afgelopen 10 jaar heeft Talos een van de meest uitgebreide platformen voor het verzamelen en analyseren van dreigingsinformatie opgebouwd. Talos detecteert dreigingen voor endpoints, netwerken, cloudomgevingen, internet en e-mail, biedt uitgebreid inzicht in cyberdreigingen en verschaft solide informatie waarop acties kunnen worden gebaseerd.

Website van Talos: http://www.talosintelligence.com
Blog van Talos: http://blog.talosintel.com
Talos op Twitter: twitter.com/talossecurity
YouTube-kanaal van Talos: http://cs.co/talostube
Beveiligingsrapporten van Cisco: http://www.cisco.com/go/securityreports

De beveiligingsstrategie van Cisco

Effectieve beveiliging centraal stellen

In een wereld waarin toenemende complexiteit de grootste belemmering voor effectieve veiligheid is, streeft Cisco naar vereenvoudiging. Cisco's geïntegreerde benadering van bescherming tegen dreigingen helpt organisaties de uitdagingen op het gebied van beveiliging in het digitale tijdperk aan te pakken.

Een combinatie van drie aspecten maakt het verdedigen van een netwerk moeilijker dan ooit:

Aangezien netwerken en nieuwe bedrijfsmodellen zich ontwikkelen en ook aanvallers steeds slimmer worden, moeten we onszelf bevrijden van complexiteit. IT-teams hebben steeds meer moeite om de toenemende aantallen IT-beveiligingsproducten goed te beheren. Het is voor hen dan ook steeds lastiger om goed inzicht te krijgen in de dreigingsactiviteit en de detectietijd (TTD) van zowel bekende als nieuwe dreigingen te verkorten. Uit onderzoek door de Talos Group van Cisco blijkt dat veel netwerkaanvallen vaak maandenlang onopgemerkt blijven en dat – wanneer ze eenmaal zijn ontdekt – het vaak nog weken duurt voordat ze volledig zijn geneutraliseerd en de aangerichte schade is hersteld.

Echt effectieve beveiliging is eenvoudig, open en geautomatiseerd

- **Eenvoudig:** Cisco heeft manieren gevonden om de effectiviteit van de beveiliging te verhogen zonder deze nog complexer te maken. Om te zorgen dat beveiliging eenvoudig kan worden geïmplementeerd, geschaald en beheerd moeten we architecturen centraal stellen in plaats van individuele producten
- **Open:** Cisco bouwt producten met het oog op interoperabiliteit op elk niveau – niet alleen met andere producten uit het eigen portfolio, maar ook met producten van andere leveranciers
- **Geautomatiseerd:** De beveiligingsoplossingen van Cisco zijn geautomatiseerd voor fysieke, virtuele en cloudgebaseerde infrastructuur om de detectietijd (TTD) te verkorten en de schade veroorzaakt door aanvallen snel te herstellen

Ga voor meer informatie naar www.cisco.com/go/security

Belangrijkste beveiligingsproducten van Cisco

Next-Generation Firewall en Unified Threat Management

Houd dreigingen tegen en zorg dat aanvallen die toch door de verdediging heen breken weinig schade kunnen aanrichten dankzij de toonaangevende NGFW-oplossingen (Next-Generation Firewall) van Cisco. Beschikbaar op diverse appliancemodellen en in zowel fysieke als virtuele vormfactoren.

Cisco ASA met FirePOWER Services & Cisco Firepower NGFW

- Combineert de bewezen netwerkfirewall van Cisco met Cisco Next-Generation IPS (NGIPS) en Cisco Advanced Malware Protection (AMP)
- Breed aanbod van hardwaremodellen: appliances voor kleine en middelgrote bedrijven, middelgrote appliances voor de internetrand modulaire krachtige appliances voor datacenters, robuuste modellen voor industriële omgevingen

- Firewalldoorvoersnelheid van 256 Mbps tot 225 Gbps, Threat Inspection van 125 Mbps tot 90 Gbps, afhankelijk van het hardwaremodel

Cisco ASA Virtual Appliance (ASAv) NGFW

- Een gevirtualiseerde netwerkbeveiligingsoplossing gebaseerd op de ASA 5500-X firewalls, ontworpen voor hypervisoromgevingen
- Ondersteunt zowel traditionele als softwaregedefinieerde netwerken (SDN) en Cisco ACI-omgevingen (Application Centric Infrastructure).
- Geoptimaliseerd voor datacenterimplementaties met vSwitch-ondersteuning voor datacenters van Cisco en andere leveranciers

Cisco Meraki MX Unified Threat Management (UTM)

- Een complete netwerkoplossing die beveiligingsbeheer aanzienlijk vereenvoudigt voor organisaties met gedistribueerde locaties
- Geïntegreerde firewall, IPS, switching, draadloos LAN, VPN en apparaatbeheer op afstand via één 100% cloudbeheerde appliance
- Stateful Next-Generation Firewall, op SNORT® gebaseerde Intrusion Prevention (IPS), Advanced Malware Protection, URL-filtering, zelfherstellende Auto VPN

Cisco Meraki: meraki.cisco.com/products/appliances
Cisco Next-Generation Firewalls: www.cisco.com/go/firewalls

Next-Generation Intrusion Prevention System (NGIPS)

Inspecteer het netwerkverkeer om het gedrag van gebruikers op het netwerk beter te begrijpen, abnormaal verkeer op te sporen en inbreuken op te sporen en te blokkeren.

Cisco Firepower Next-Generation IPS

- Verschillende hardwaremodellen om aan verschillende doorvoerbehoeften te voldoen: van campus- en bedrijfsimplementaties tot serviceproviders en datacenters
- Threat Inspection-doorvoersnelheid van 10 Gbps tot 90 Gbps, afhankelijk van het hardwaremodel

Cisco Virtual Next-Generation IPS for VMware

- Biedt een gevirtualiseerde Cisco Firepower NGIPS-oplossing met volledige functionaliteit, inclusief opties voor geavanceerde malware-bescherming, inzicht in en beheer van applicaties, URL-filtering
- Herstelt de inzichtelijkheid die u kwijtraakt door virtualisatie en breidt naleving van de PCI-normen (Payment Card Industry) uit naar virtuele omgevingen
- Threat Inspection-doorvoersnelheid tot 800 Mbps

Beveiligingsbeheer

Netwerkbeveiligingsoplossingen beheren in complexe omgevingen is een uitdaging. Cisco biedt operationele tools om beveiligingsbeheer te vereenvoudigen en te stroomlijnen.

Cisco Firepower Management Center

- Voorziet in geïntegreerd beheer voor Cisco firewalls (NGFW), applicatiebeheer, inbraakpreventie (NGIPS), URL-filtering en geavanceerde malwarebescherming (AMP)
- Maakt het beheer van de firewall en applicaties eenvoudig, evenals het onderzoeken en herstellen van malware-uitbraken

Cisco Defense Orchestrator

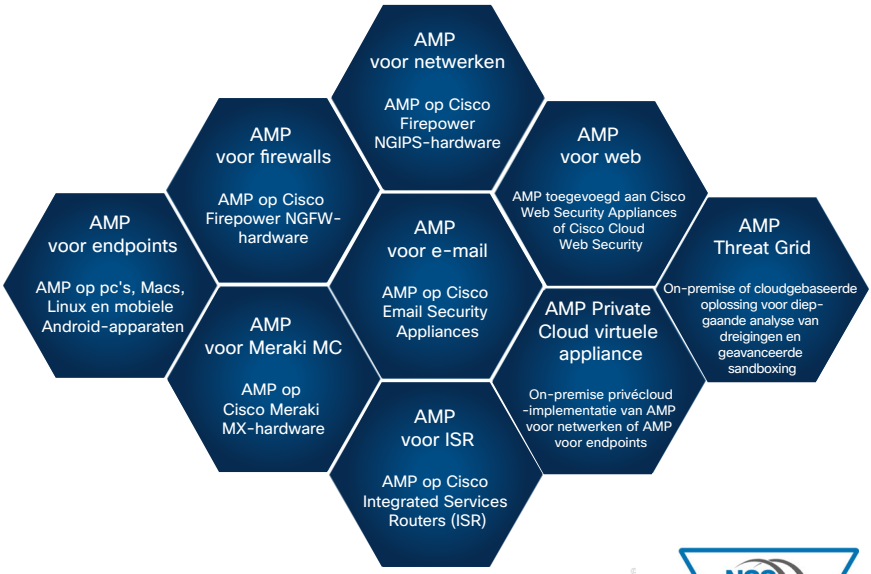
- Cloudgebaseerde beleidsbeheeroplossing voor Cisco Next-Generation Firewalls en NGIPS, inclusief Advanced Malware Protection en Cisco Umbrella
- Zorgt voor consequente handhaving van regels tussen geografisch verspreide locaties, ontdekt en herstelt problemen zoals onjuiste configuraties en dubbele beleidsregels en maakt snelle on-boarding van nieuwe apparaten mogelijk

Cisco Next-Generation IPS: www.cisco.com/go/ips
Cisco Security Management: www.cisco.com/go/securitymanagement

Advanced Malware Protection

Cisco Advanced Malware Protection (AMP) gaat verder dan Point-in-Time-bescherming en pakt de gehele levenscyclus van het malwareprobleem aan. AMP blokkeert malware in real-time om inbreuken te voorkomen (Point-in-Time). Omdat u echter niet alleen op preventie mag vertrouwen, analyseert AMP ook voortdurend het netwerk om geavanceerde malware die de eerste verdedigingslinie heeft weten te omzeilen en toch het netwerk is binnengedrongen snel te herkennen en te verwijderen (retrospectieve beveiliging).

Cisco AMP werkt op abonnementsbasis, wordt beheerd via een webgebaseerde beheer-console en kan op verschillende platforms worden ingezet:



Cisco werd in 2016 voor het derde jaar op rij uitgeroepen als winnaar van de inbreukdetectietest van NSS Lab, waarbij 100% van de malware, exploits en omzeilingen werden gedecteerd – met de kortste detectietijd.

Overzicht van de AMP-serie: www.cisco.com/go/amp
AMP Threat Grid: www.cisco.com/go/amptg

Netwerkinzicht en analyse

Verkrijg diepgaand inzicht in alles wat zich op het netwerk afspeelt. Zo krijgt u onder andere in real-time een overzicht van waar gebruikers, apparaten en het verkeer zich bevinden binnen het netwerk, in het datacenter en in de cloud.

Cisco StealthWatch

- Continue analyse van real-time NetFlow-gegevens om abnormaal gedrag binnen het netwerk op te sporen. Zo wordt de dreigingsdetectie en de reactie op incidenten drastisch verbeterd
- Naadloze integratie met Identity Services Engine (ISE), Cisco TrustSec en de netwerkportfolio van Cisco. Hierdoor kan het netwerk als beveiligingssensor fungeren en de naleving van beleidsregels afdwingen

- Identificeer en segmenteer kritieke netwerkonderdelen en monitor het gebruiksbeleid om de toegangscontrole en de naleving van de regelgeving te verbeteren

Cloudbeveiliging

Beveiliging tot voorbij de firewall van de netwerkperimeter, vanuit en voor de cloud: Bescherm gebruikers, data, applicaties en apparaten, ongeacht waar ze zich bevinden. Snelle implementatie, geen hardware om te installeren, geen software om te onderhouden.

Cisco Umbrella

- Vanuit de cloud geleverde netwerkbeveiligingsservice die gebruikers binnen en buiten het netwerk beschermt, waar ze ook naartoe gaan, zelfs wanneer ze geen VPN gebruiken
- Biedt handhaving op zowel DNS- als IP-laagniveau om malware, phishing en 'command & control'-callbacks via willekeurige poorten of protocollen te blokkeren

Cisco Cloudlock

- Vanuit de cloud geleverde CASB-oplossing (Cloud Access Security Broker) die organisaties helpt om sneller tot een veilige cloudimplementatie te komen
- Beschermt gebruikers, data en apps in cloudcomputingarchitecturen, zoals SaaS (Software-as-a-Service), IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) en IDaaS (Identity-as-a-Service)

Cisco Stealthwatch: www.cisco.com/go/stealthwatch
Cisco Umbrella: umbrella.cisco.com
Cisco CloudLock: www.cloudlock.com

Web- en e-mailbeveiliging

E-mail en internet zijn de twee belangrijkste aanvalsvectoren voor malware. Cisco biedt krachtige oplossingen om organisaties te beschermen tegen schadelijk e-mail- en internetverkeer.

Cisco Email Security Appliance

- Wordt gebruiksklaar op locatie geleverd, met diverse appliance-opties, waaronder virtuele appliances
- Biedt anti-spam, anti-virus en bescherming tegen phishing, uitbraakfilters, voorkoming van dataverlies (DLP) en encryptie

Cisco Cloud Email Security

- Een kosteneffectief, betrouwbaar SaaS-product dat geen appliance op locatie – en dus ook geen onderhoud of upgrades – vereist
- Bij een hybride implementatie worden een (fysieke of virtuele) appliance op locatie gecombineerd met de cloudservice; ideaal voor organisaties die hun vertrouwelijke data op locatie willen bewaren

Cisco Web Security Appliance

- Een lokale webbeveiligingsoplossing die verschillende appliance-opties biedt, waaronder virtuele appliances
- Biedt websitereputatieanalyse, fijnmazige beleidsregels voor internetgebruik, geavanceerde opties voor inzicht in en beheer van applicaties, met inbegrip van social media, en voorkoming van dataverlies (DLP)

Cisco Cloud Web Security

- Een vanuit de cloud geleverd, kostenefficiënt SaaS-product dat geen on-premise appliance – en dus ook geen hardware- en software-onderhoud – vereist
- Aanpasbare rapporten en een verscheidenheid aan rapportage- en analysetools geven inzicht in webgebruiksgegevens

Cisco Cognitive Threat Analytics

- Een cloudgebaseerde oplossing voor het opsporen van inbreuken die alle vormen van webverkeer analyseert, of dat nu via HTTP, HTTPS of zelfs via anonieme protocollen zoals Tor plaatsvindt
- Ontdekt schadelijke activiteiten die de eerste verdedigingslinie hebben weten te omzeilen of via ongecontroleerde kanalen (zoals verwisselbare media) zijn binnengekomen en die nu binnen het netwerk van de organisatie plaatsvinden

E-mailbeveiliging van Cisco: www.cisco.com/go/emailsecurity
Webbeveiliging van Cisco: www.cisco.com/go/websecurity
Cisco Cognitive Threat Analytics: www.cisco.com/go/cognitive

Beleid en toegang

Verbeter het inzicht in en de controle over het netwerk met identiteitsbewuste oplossingen voor beveiligde toegang beleidsbeheer.

Cisco Identity Services Engine (ISE)

- Hiermee kunnen organisaties alle gebruikers en apparaten die verbinding maken met het bedrijfsnetwerk zien en beheren, inclusief BYOD en gasttoegang. Beschikbaar als fysieke of virtuele appliance
- Maakt gebruik van Cisco TrustSec softwaregedefinieerde netwerksegmentatie om beleidsregels in de routerings- en switching-laag af te dwingen
- Integreert nauw met een breed scala aan oplossingen van technologiepartners. Daarbij worden gebruikers- en apparaatgegevens gedeeld voor snellere identificatie en herstel van dreigingen

Cisco TrustSec

- Netwerksegmentatie is essentieel om kritieke bedrijfsmiddelen te beschermen. De traditionele IP-gebaseerde segmentatiebenaderingen (VLAN) zijn echter complex om te beheren
- De softwaregedefinieerde netwerksegmentatie van TrustSec categoriseert endpoints in beveiligingsgroepen op basis van bedrijfsrollen in plaats van IP-adressen. Dit maakt beleidsbeheer een stuk eenvoudiger
- Nauw geïntegreerd met Cisco Identity Services Engine (ISE) en geïntegreerd in meer dan 40 Cisco productfamilies en een groot aantal producten van technologiepartners

Cisco AnyConnect Secure Mobility

- Geavanceerde VPN-oplossing die gebruikers op afstand zeer veilige toegang tot het bedrijfsnetwerk biedt – vanaf elk apparaat en elke locatie
- Werkt samen met andere beveiligingsoplossingen van Cisco, zoals Cisco Identity Services Engine, AMP voor endpoints, Cisco Cloud Web Security en Cisco Firepower Firewalls voor ondernemingsbrede bescherming tegen dreigingen
- De geïntegreerde Cisco Umbrella-functionaliteit zorgt voor permanente beveiliging en beschermt gebruikers die niet verbonden zijn met de VPN

Cisco ISE: www.cisco.com/go/ise
Cisco TrustSec: www.cisco.com/go/trustsec
Cisco AnyConnect: www.cisco.com/go/anyconnect

Security Channel Partner-programma

Beveiliging is een van de snelst groeiende segmenten in de IT-sector en is de meest winstgevende Cisco architectuur voor partners. Op de volgende twee pagina's vindt u de informatie die u nodig hebt om uw activiteiten op het gebied van beveiliging op te starten en uit te bouwen.

Cisco specialisaties

Cisco specialisaties zijn een belangrijk onderdeel van het Cisco Channel Partner -programma. Beveiligingsspecialisaties bereiden u voor op het verkopen, ontwerpen, installeren en ondersteunen van effectieve oplossingen.
www.cisco.com/go/specializations

Security Ignite

Via het Security Ignite-programma ontvangen partners met een beveiligingsspecialisatie automatisch extra kortingen vooraf op nieuwe beveiligingsproducten.
www.cisco.com/go/securityignite

Opportunity Incentive Program (OIP)

Een dealregistratieprogramma dat ontworpen is om het zelf aanboren van nieuwe zakelijke kansen door partners te stimuleren en te belonen (nieuwe omzet binnenhalen)
http://www.cisco.com/go/hunting

Teaming Incentive Program (TIP)

Een dealregistratieprogramma dat ontworpen is om partners te belonen voor activiteiten met toegevoegde waarde als vervolg op door Cisco geïnitieerde zakelijke kansen (samenwerken met Cisco)
http://www.cisco.com/go/teaming

Security Promotions

Verhoog uw inkomstenpotentieel met programma's voor korting vooraf en uitbetaling achteraf, alsook speciale promoties die zijn ontworpen om u beveiligingsproducten en -oplossingen van Cisco te helpen te verkopen.
www.cisco.com/go/promotions -> Filtercategorie ‘Security’

Cisco Rewards

Een loyaliteitsprogramma voor geregistreerde Cisco partners. Ze worden beloond voor het verkopen van in aanmerking komende Cisco producten en services en het deelnemen aan bepaalde activiteiten.
www.cisco.com/go/ciscorewards

Marketing en vraagstimulering

De kosteloze, gebruiksklare marketingcampagnes zijn ontworpen om u te helpen de beveiligingsproducten en -oplossingen van Cisco effectief te verkopen aan klanten.
www.ciscopartnermarketing.com

Beveiligingsoplossingen van Cisco demonstreren

Cisco dCloud, de Cisco Demo Cloud, biedt gescripte, aanpasbare demo-omgevingen met complete beheertoegang.
dcloud.cisco.com

Interactieve webinars voor partners

Eén uur durende trainingswebinars voor partners over verkoop of technische aspecten, verzorgd door Cisco beveiligingsexperts. Als u maandelijks een uitnodiging wilt ontvangen voor deze webinars, kunt u zich aanmelden door een mailtje te sturen naar piw_enquiry@cisco.com.
http://cs.co/SecurityPIW

Nieuwsbrief voor Cisco Security Connections-partners

In deze maandelijkse publicatie leest u alles met betrekking tot Cisco Security. Abonneer u op de nieuwsbrief voor informatie over de laatste productupdates, verkooptools, trainingen en promotieacties.
https://info.sourcefire.com/SCNL_Partner-Subscription-Opt-In

SalesConnect

Cisco SalesConnect is hét kanaal voor snelle toegang tot productmaterialen, verkoopkits, verkoopvaardigheidstraining, interactieve demo's en meer. Voor toegang vanaf mobiele apparaten kunt u de SalesConnect-app downloaden via iTunes of Google Play.
salesconnect.cisco.com

Security PitchZone

De Security PitchZone is een gratis opleidingsprogramma voor verkoop- en technische functies. Leer hoe Cisco zich onderscheidt, hoe u de beveiligingsoplossingen van Cisco positioneert, kansen herkent en deals binnenhaalt.
https://communities.cisco.com/docs/DOC-57626

Continuum

Blijf op de hoogte van het nieuws uit de beveiligingsbranche. Hier leest u alles wat er momenteel speelt en relevant is voor de toekomst van de branche.
continuum.cisco.com

Meer informatie

Security Partner Community
https://communities.cisco.com/community/partner/security/emear

Blog van Cisco over beveiliging
blogs.cisco.com/security

Ondersteuning voor partners
www.cisco.com/web/partners/support

Training en certificering
www.cisco.com/web/learning

Trackingsysteem voor certificeringen
cisco.pearsoncred.com

Concurrentie-informatie
www.cisco.com/web/partners/sell/competitive

Cisco Security Intelligence Operations
tools.cisco.com/security/center/home.x

Cisco Umbrella verkopen (voorheen OpenDNS Partner Portal)
https://communities.cisco.com/docs/DOC-64565

Woordenlijst

Point-in-Time-beveiliging

Basisbeveiligingsmethoden die door fundamentele beveiligingstechnologieën (firewall, inbraakpreventiesoftware, anti-virus) worden gebruikt om bestanden of verbindingen te scannen om te bepalen of ze schadelijk zijn of kunnen worden toegestaan. Point-in-Time-beveiliging is een essentieel onderdeel van een beveiligingsoplossing, maar deze moet dan wel worden aangevuld door continue analyse. Malware kan zich immers aan Point-in-Time-scans onttrekken en wanneer dergelijke schadelijke software eenmaal het netwerk is binnengedrongen, is deze lastig op te sporen en vaak nog lastiger te elimineren.

Continue analyse

Aggregatie van gegevens uit het hele netwerk en gebruik van 'big data'-analyses voor continue, algemeen toegepaste bestandstracking en -analyse. Dit komt neer op een 'continue' analyse van bestanden, zelfs nadat deze naar een andere plek binnen het netwerk of tussen endpoints zijn verplaatst. Als toch een bestand is binnengedrongen – bijvoorbeeld omdat het aanvankelijk als onschadelijk werd beoordeeld, maar later toch als schadelijk wordt geïdentificeerd – dan kan het achteraf alsnog als schadelijk worden aangemerkt. Hierdoor kan ook de omvang van de inbreuk worden vastgesteld, de uitbraak worden ingedamd en de malware worden geëlimineerd.

Retrospectieve beveiliging

Het gebruik van continue analyse voor het waarschuwen voor en herstellen van bestanden die in eerste instantie veilig werden geacht, maar later toch schadelijk werden bevonden. Retrospectieve beveiliging stelt de omvang van uitbraken vast, damt ze in en zet als het ware de klok terug om malware automatisch te herstellen. Cisco Advanced Malware Protection (AMP) biedt zowel Point-in-Time-beveiliging als retrospectieve beveiliging.

Netwerkinzicht

In real-time een duidelijk beeld verkrijgen van apparaten, gebruikers, applicaties, data en hun onderlinge relaties. Combineert verzamelde gegevens met analyses om context te verschaffen en de ruwe gegevens te interpreteren en zo gegevens om te zetten in bruikbare informatie waarop acties kunnen worden gebaseerd.

Naleving en regelgeving

Regelgevende instanties vereisen strenger beveiligings- en privacybeheer dan ooit tevoren, wat gevolgen heeft een groeiend aantal branches. Als een organisatie niet in staat is om effectief en efficiënt aan deze eisen te voldoen, worden haar kansen om mee te doen in de digitale economie drastisch verkleind.

Mix van individuele producten – geïntegreerde beveiligingsarchitectuur

Organisaties moeten ervoor waken om een ad-hoc architectuur te implementeren, dat wil zeggen niet lukraak oplossingen (zelfs als deze de beste producten omvatten) gaan kopen wanneer zich een probleem voordoet. Denk holistisch en bedenk hoe de bestaande producten en nieuwe technologieën kunnen worden gecombineerd tot een geïntegreerd systeem (bewust samengestelde architectuur). Silo's die door puntoplossingen ontstaan, leiden tot onnodige operationele kosten en het risico van zichtbaarheidshiaten.

Internet of Things (IoT)

Het Internet of Things (IoT) is een alsmaar groeiend netwerk van fysieke objecten die met elkaar communiceren via internet. Verbonden via bekabelde en draadloze netwerken maken ze processen en bedrijfsmodellen mogelijk die nooit eerder beschikbaar waren. Volgens studies uitgevoerd door de Cisco Internet Business Solutions Group (IBSG), ontstond IoT tussen 2008 en 2009: op het moment dat meer objecten met internet verbonden waren dan mensen.

Digitale transformatie

Het gebruik van digitale technologie om nieuwe bedrijfsmodellen, diensten, software en systemen op te bouwen die resulteren in meer inkomsten, een groter concurrentievoordeel en een hogere efficiëntie. Bedrijven realiseren dit door hun traditionele bedrijfsmodellen te transformeren.

Digitaal zakendoen

" Digitaal zakendoen is het creëren van nieuwe bedrijfsconcepten die niet alleen mensen en bedrijven met elkaar verbinden, maar ook mensen en bedrijven met zaken verbinden om inkomsten en efficiëntie te verhogen. Digitaal zakendoen elimineert belemmeringen die nu bestaan binnen industriesegmenten en creëert waardeketens en mogelijkheden die traditionele bedrijven kunnen niet bieden."
- Gartner, 2015

Internet of Things (IoT) is een concept dat digitaal zakendoen mogelijk maakt. IoT verwijst naar objecten die kunnen communiceren en interageren met de externe omgeving.

Digitale transformatie is het proces waarbij traditionele bedrijfsmodellen worden omgezet in digitale bedrijfsmodellen

Digitaal zakendoen combineert en maakt optimaal gebruik van ontwikkelingen op het gebied van bedrijfsnetwerken, beveiliging, datacenter, cloud, samenwerking, IoT en analyse

Cyberbeveiligingsmodellen moeten radicaal veranderen om het juiste beschermingsniveau te bieden voor deze met elkaar verbonden wereld. Regelgevende instanties vereisen strenger beveiligings- en privacybeheer dan ooit tevoren. Als een organisatie niet in staat is om effectief en efficiënt aan deze eisen te voldoen, worden haar kansen om mee te doen in de digitale economie drastisch verkleind.


CISCO