Cyber Security

Cyber Security

Expertise op het gebied van Cyber Security

Cyber security heeft staat bij menige directie hoog op de agenda. Oude beschermingstechnieken technieken zijn niet langer relevant in het uiterst geraffineerde bedreigingslandschap van vandaag. Een nieuwe benadering van cyberbeveiliging is vereist. Nuvias, in samenwerking met belangrijke innovatieve leveranciers die elk aspect van het cyber security spectrum bestrijken, kunnen u helpen de netwerken bij uw klanten te beveiligen.

Waarom samenwerken met Nuvias om uw Cyber Security business te laten groeien?

- Werk met een partner die vooruit blijft loopt als het om bedreigingen en de oplossingen die bescherming bieden.
- Complexe beveiligingsoplossingen worden vereenvoudigd door de expertise bij Nuvias.
- Alle expertise en assistentie die u nodig hebt om oplossingen te ontwikkelen en te leveren is aanwezig bij dezelfde vertrouwde distributeur.
- Wij zijn gericht op het leveren van technologische kwaliteit in alles wat we doen en zijn geaccrediteerd bij onze belangrijkste leveranciers.
- Wij hebben een omvangrijk technologieportfolio samengesteld van bestaande leveranciers en nieuwe marktpartijen.

Inhoudsopgave

Data Compliance & Incident Management

Het is tijd om de voortdurende informatie over bedreigingen om te zetten in bruikbare inzichten die de basis vormen voor de reactie op incidenten en de compliance ondersteunen.

Zelfs met de beste verdediging is het onvermijdelijk dat er zich beveiligingsincidenten voordoen. In dat geval moet de aandacht worden gericht op de reactie op incidenten en hoe een geplande, gecoördineerde en vooral snelle reactie kan worden opgezet om de gevolgen tot een minimum te beperken. Voor organisaties die in sterk gereguleerde markten opereren, is het voor het bereiken van compliance vaak van cruciaal belang om op dergelijke eventualiteiten voorbereid te zijn, net als het aantoonbare bewijs dat alle redelijke stappen zijn ondernomen om het risico te beperken.

Nuvias biedt een verscheidenheid aan oplossingen voor Compliance en Security Incident Response. Ze komen voort uit een gemeenschappelijke kern van Security Incident and Event Management (SIEM) en Unified Security Management (USM) tools, die de stroom van beveiligingswaarschuwingen van vaak ongelijksoortige beveiligingstools verwerken om de Indicators of Attack (IOA's) te correleren en te bepalen of er sprake is van een echt probleem dat moet worden aangepakt.

Ze bieden ook krachtige controletrajecten als bewijs voor de naleving van de regelgeving. Er zijn echter nog tal van andere beveiligingsmaatregelen die een belangrijke rol zullen spelen in de manier waarop uw klant ervoor kiest om Compliance en Incident Management aan te pakken:

- Data Archiving
- Compliance Management
- Policy Management
- Security Audit en Health-check
- Incident Reporting
- Threat Remediation

Best practice incident response

Naast de technologie kunnen we ook de beste practice Incident Response Plans definiëren en u helpen uw klant te begeleiden bij het implementeren van een gestructureerd proces voor het onderzoeken, escaleren en oplossen van cyberincidenten.

Samen reduceren deze oplossingen de tijd die nodig is om problemen op te lossen, verminderen ze de overheadkosten die nodig zijn voor triage, en zorgen ze voor een meer proactieve houding bij aanhoudende bedreigingsinformatie en stellen ze prioriteiten qua belangrijkheid.

Als uw klant bij u aanklopt omdat hij niet aan de compliancy-audit heeft voldaan, kunnen wij u ook advies geven over de beste beveiligingsoplossingen om deze kwetsbaarheden te verhelpen. Wij zijn goed thuis in veel van de gangbare normen waarmee uw klanten te maken kunnen krijgen, zoals de Payment Card Industry Data Security Standard (PCI DSS), ISO 27001, Cyber Essentials en het National Institute of Standards and Technology (NIST).

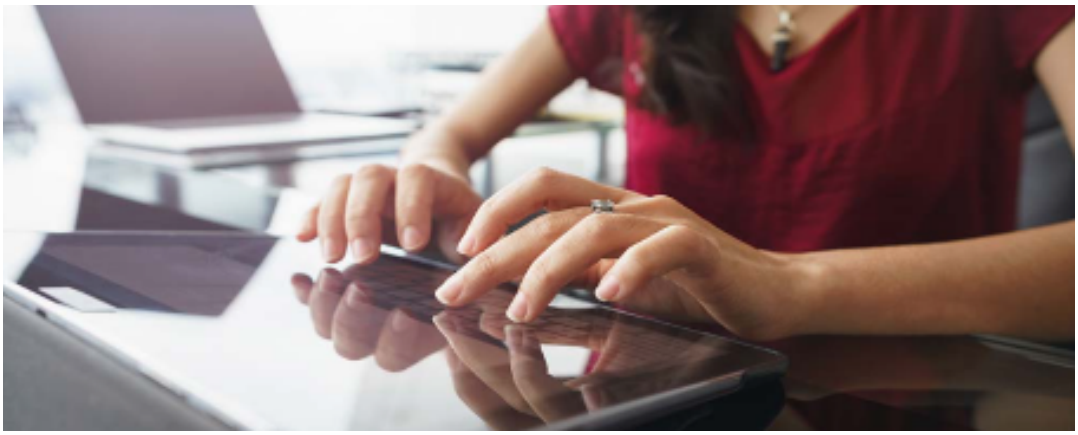
Waarom Nuvias betrekken bij Incident Management?

Wij zijn erkende professionals in beveiliging. In combinatie met ons omvangrijke portfolio van beveiligingsleveranciers, zijn wij goed in staat de technologie te bundelen en de best practices te delen die essentieel zijn voor succesvol Incident Management en Compliance.

Oplossingen moeten niet alleen in verhouding staan tot de risicobereidheid van uw klant, maar ook tot de kosten van het in stand houden van de capaciteit om dit risico te beperken. Onze kennis en ervaring zijn van vitaal belang om ervoor te zorgen dat de oplossingen die u voorstelt bij uw klanten in evenwicht zijn.

Data Security

De meeste organisaties beschouwen hun gegevens, of die nu betrekking hebben op klanten, intellectuele eigendom of gevoelige bedrijfsgegevens, als een belangrijk bezit wat koste wat kost beschermd dient te worden. Het volstaat niet langer om alleen maar te kijken naar oplossingen voor Data Loss Prevention (DLP) die alleen maar proberen gegevensverlies te beperken. Er is nu een nieuwe visie met betrekking tot gegevensbeveiliging. Het sleutelwoord is pro-activiteit, waarbij gegevens worden geïdentificeerd, geclassificeerd en beschermd op basis van hun waarde.



In een wereld die wordt gekenmerkt door compliance is een dergelijke aanpak absoluut noodzakelijk, met name wanneer het gaat om persoonlijk identificeerbare informatie (PII). Gegevensverwerkers moeten in staat zijn verzoeken om toegang tot gegevens (Data Subject Access Requests - DSAR) uit te voeren en in staat zijn te voldoen aan het recht om te worden vergeten.

Policy-driven data protection

De Nuvias Data Security-oplossingen volgen deze methode en zijn erop gericht om de gestructureerde en ongestructureerde gegevens van uw klanten te identificeren, deze te classificeren op basis van belangrijkheid om vervolgens passende beveiligingsmaatregelen te implementeren om deze zowel in ruste als bewegend te beschermen.

De beveiliging wordt georganiseerd aan de hand van gedetailleerd beschreven beleidslijnen en kan worden aangepast aan de toepassing of de gebruiker. Het beleid wordt toegepast op alle beveiligingsmaatregelen, inclusief gateways en endpoints, waarbij gebruik wordt gemaakt van een combinatie van gespecialiseerde technologieën en eventueel bestaande infrastructuur wordt hergebruikt.

Oplossingen zijn samengesteld uit een combinatie van:

- Data Backup
- Endpoint Encryption
- Email Encryption
- IPSec VPN
- SSL VPN
- Hardware Security Module (HSM)
- Password Management

Waarom Nuvias betrekken voor Data Security?

Onze Cyber Security afdeling is gespecialiseerd in de opkomende technologieën die de gegevensbeveiliging bevorderen en de steeds vaker voorkomende druk van de regelgeving waarop moet worden gereageerd. Onze beveiligingsspecialisten zijn vooraanstaande deskundigen op dit gebied, die hun kennis en expertise met ondersteunende diensten aanbieden.

Bovendien kunnen wij via door de leverancier geaccrediteerde cursussen en opleidingsprogramma's voor u of uw klanten verzorgen. Budgetten voor oplossingen zijn realistisch en zijn afgestemd op het risicoprofiel van de te beschermen gegevens.

Cloud Security

Hoewel de cloud nu echt mainstream is geworden, blijven er veel zorgen over de veiligheidsrisico's bestaan. Voor elk risico is er echter een antwoord.

De cloud is een aantrekkelijk alternatief voor het traditionele computergebruik. Het garandeert bijna onbeperkte toegang, flexibiliteit, schaalbaarheid en reactiesnelheid. Maar net als bij traditioneel computergebruik brengt de cloud een aantal veiligheidsproblemen met zich mee.

Het is zelfs zo aantrekkelijk geworden dat individuele gebruikers de voordelen van de cloud buiten het zicht van IT-teams benutten en zo een min of meer alternatief netwerk opzetten. Van gegevensopslag tot berichtentoepassingen, de cloud zorgt voor een fundamentele verschuiving in de beveiliging, waardoor gegevens en diensten aan nieuwe bedreigingen worden blootgesteld. Er zijn intelligente nieuwe beveiligingsmaatregelen ontwikkeld om de risico's het hoofd te bieden.

Secure cloud apps, data en access

Voor organisaties die gebruik maken of overwegen gebruik te maken van de cloud, zijn er belangrijke vragen die moeten worden beantwoord. Welke digitale activa bevinden zich in de cloud? Hoe worden deze beschermd? Wie heeft er toegang toe en hoe kunnen we die mensen persoonlijk identificeren? Welke interfaces gebruiken we om gebruikers en diensten met elkaar te verbinden? Voor we het weten, escaleren de beveiligingsproblemen met betrekking tot vertrouwelijkheid, integriteit, beschikbaarheid en verantwoordingsplicht.

Nuvias helpt u om samen met uw klant tot de kern van deze vragen te gaan en de beste oplossing te bieden voor het gebruik van de cloud. Wij voeren kritische conversaties met uw klanten over het gebruik van de cloud en zorgen er zo voor dat hun beveiligingsbeleid correct is. Met de juiste maatregelen kunnen we de beveiliging aanzienlijk verbeteren zonder de voordelen uit te hollen die de cloud in de eerste plaats zo veelbelovend maakten.

Wij hebben alle know-how, leveranciers en diensten verzameld zodat u oplossingen kunt realiseren voor cloud-omgevingen.

- Firewall (Virtual – Next-Generation)
- Cloud Services
- Container Security
- Security for Virtualisation

Deze oplossingen zorgen niet alleen voor een robuust beveiligingsplatform, maar kunnen u ook helpen het vertrouwen van uw klanten te vergroten en hun gebruik van de cloud uit te breiden door een eventuele angst met betrekking tot beveiliging weg te nemen.

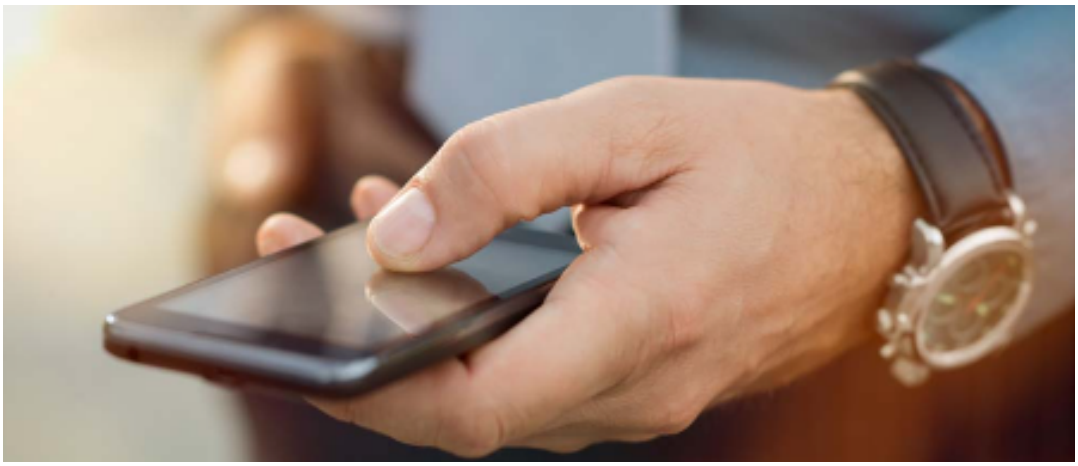
Waarom Nuvias betrekken bij cloud beveiliging?

Cloud beveiliging is een opkomende markt die we tijdig als zodanig hebben ingeschat. Dat geldt zowel voor het portfolio van leveranciers die we hebben gekozen om mee samen te werken als voor de expertise die we in ons team hebben verzameld. Het is ook een snel evoluerende markt, clouddiensten kunnen eenvoudig worden getest en vervolgens in productie worden genomen.

Onze partners kunnen zich tot ons wenden met het vertrouwen dat wij snel en professioneel kunnen acteren om te helpen bij het kwalificeren, ontwerpen en leveren van relevante oplossingen op basis van de behoeften van uw klanten.

Endpoint en Mobile Security

Het aantal apparaten en 'dingen' dat verbinding maakt met het netwerk groeit met de dag. Endpoint en Mobile Security is erop gericht om ervoor te zorgen dat de bescherming hierdoor niet wordt verzwakt.



Endpoint protection bestaat uit vele onderdelen, zoals Endpoint Defend and Respond (EDR), User Behaviour Analysis (UBA), Mobile Device Management (MDM), encryptie, poortcontrole, Strong Identification, Security Awareness Training, Network Access Control (NAC), Whitelisting en Privilege Management, om maar een paar belangrijke zaken te noemen.

Het is een complex labyrint van mogelijke oplossingen die elkaar aanvullen en elkaar in de weg kunnen zitten. Tenzij u een door de wol geverfde beveiligingsfreak bent, is het een bijna onmogelijk om voor de juiste oplossing te kiezen. Gelukkig heeft Nuvias een team van endpoint-specialisten samengesteld om u te helpen bij het inzichtelijk maken van de huidige situatie en welke stappen uw klant moet zetten om te komen waar hij moet zijn.

Wij helpen u het juiste evenwicht te vinden tussen de mate van beveiliging en de gebruikerservaring. Het spreekt voor zich dat naarmate er meer bescherming wordt toegevoegd, de apparaten die worden beschermd langzamer werken. Het zijn de gebruikerservaring en innovatieve benaderingen van dit dilemma wat onze keuze voor leveranciers heeft bepaald.

Naast traditionele oplossingen werken we nu ook aan geavanceerde oplossingen die gebruikmaken van geavanceerde anti-exploit-tools en gebruikmaken van Indicators of Compromise (IOC's) en Indicators of Attack (IOA's) om apparaten te beschermen vóór en na de lancering van de code. Bovendien voeden we gebruikers bij uw klanten op door trainingen op het beveiligingsbewustzijn waardoor risico's bij klanten kunnen worden beperkt en zij bovendien kunnen aantonen dat zij geavanceerde maatregelen hebben genomen om zichzelf te beschermen.

Onze oplossingen zijn zeer uitgebreid:

- Anti-Ransomware
- Anti-Exploit
- Anti-Malware
- Anti-Virus
- Application Privilege Control
- Endpoint Data Recovery
- Endpoint Security
- Endpoint Firewall
- Multi-Factor Authentication
- Mobile en Smartphone Security
- Mobile Device Management (MDM)

Waarom Nuvias betrekken bij Endpoint en Mobiliteitsbeveiliging?

Nuvias heeft de middelen, vaardigheden en ervaring om u te helpen om elke Endpoint Security uitdaging aan te gaan. Met een schat aan ervaring op dit gebied onderkennen wij de enorme veranderingen die plaatsvinden op het endpoint en de diverse mix van apparaten die nu verbinding maken met het netwerk - die allemaal het potentieel hebben om te worden besmet.

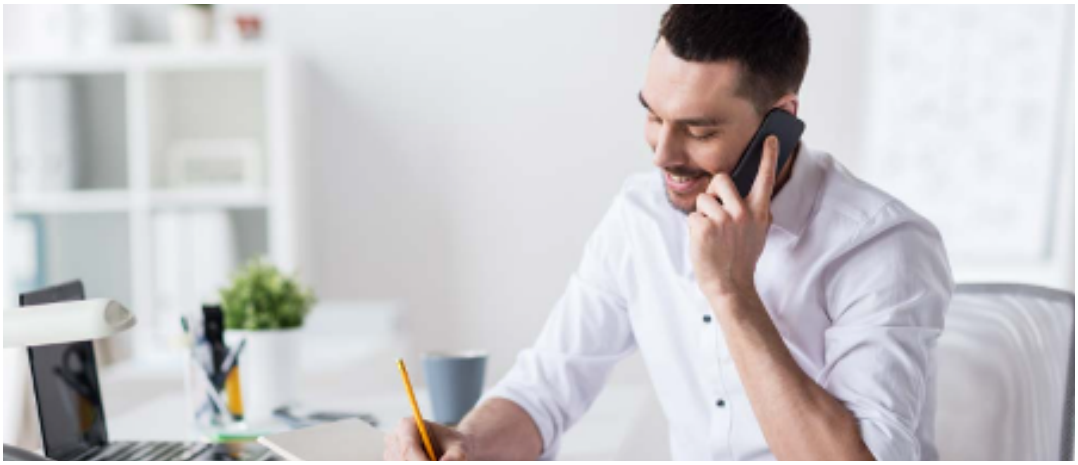
De leverancierskeuzes die wij hebben gemaakt en de oplossingen die wij bieden, zorgen ervoor dat u op de hoogte bent van wat er in de markt gebeurt en van de soorten aanvallen die uw klant nu kan duchten.

Endpoint Security is meer dan ooit een adviserende verkoop geworden, die veel ruimte biedt voor u om u te onderscheiden met diensten en praktijkvoorbeelden die verder gaan dan de technologie. Gebruik onze kennis en expertise binnen uw propositie met als gevolg dat de kansen om de opdracht binnen te halen toenemen.

Interne Beveiliging

Het inzichtelijk maken van mogelijke kwetsbaarheden binnen het netwerk is een vereiste als het gaat om de interne beveiliging en het beheer.

De meeste malware maakt tegenwoordig gebruik van een kwetsbaarheid in een applicatie of -apparaat. Inzicht in waar deze kwetsbaarheden zich bevinden is dan ook van cruciaal belang voor het in stand houden van een gezond netwerk. Alleen met inzicht kunnen risico's effectief worden beheerd en netwerken worden beveiligd.



Nuvias werkt samen met u en uw klanten om ervoor te zorgen dat netwerken veilig blijven. Wij denken Out of the Box en proberen altijd slimme, nieuwe ideeën aan te dragen die uw klant zullen helpen hun systemen op orde te houden. Immers, de bedreigingen stoppen nooit en veranderen voortdurend, evenals de beveiligingsmaatregelen.

Gelukkig beschikken we over geweldige technologieën.

Door middel van een proces waarbij netwerkverkeer in kaart wordt gebracht, risico's worden vastgesteld en vervolgens wordt bepaald wat de beste verdediging tegen die risico's is, helpen wij u om tot de juiste oplossing te komen. Het is een combinatie van ervaring en het benutten van het beste van bestaande- en opkomende technologieën die betrekking hebben op:

- Enterprise Single Sign-On
- Identity en Access Management (IAM)
- Network Monitoring
- Patch Management
- Vulnerability Management
- WAN en Application Optimisation
- Wireless Security
- Security Awareness Training
- VOIP Security
- Technische Training

Zo helpen wij u met veel zaken, variërend van inzicht in hoe het netwerkverkeer verloopt tot het signaleren van afwijkend gedrag en het isoleren, in quarantaine plaatsen en elimineren van risico's. Om dit te bereiken, maken we samen gebruik van een groot aantal tools, waaronder scannen naar kwetsbaarheden, diepgaand netwerkonderzoek en Network Access Control (NAC).

Van eenvoudige antivirus tot complexe zero-tolerant netwerken, onze experts beschikken over de benodigde kennis en expertise om gevoelige beveiligingskwesties aan te pakken.

Waarom Nuvias betrekken voor interne veiligheid?

Wij begrijpen netwerkbeveiliging. Via ons brede ecosysteem van leveranciers hebben we zwaar geïnvesteerd in de vaardigheden en middelen die u nodig heeft om oplossingen op dit gebied te begrijpen en te implementeren. Onze experts staan klaar om uw team uit te breiden of om u te helpen uw eigen capaciteiten te ontwikkelen op het gebied van marketing, verkoop en implementatie van onze oplossingen.

Beveiliging van de grenzen van het Netwerk

De grenzen van het netwerk vervagen, maar het belang van de juiste beveiligingsmaatregelen is nog nooit zo duidelijk geweest.

Ondanks de steeds geraffineerdere bedreigingen blijft de meest waarschijnlijke plaats voor een inbraak in de beveiliging de buitengrens van het netwerk en de gateway naar het internet. Bij enkele van de meest beruchte aanvallen van de laatste tijd is dit zelfs de beste aanvalsmethode gebleken.

De grenzen van het netwerk zijn veel ruimer geworden dan de traditionele LAN's dankzij nieuwe trends in mobiliteit, thuiswerken, Bring Your Own Device (BYOD) en zelfs Internet of Things (IoT). Beveiligingsmaatregelen aan de grenzen van het netwerk zijn daarom een cruciaal onderdeel van de beveiliging van elke infrastructuur.

Nuvias heeft ervaringen kent vele oplossingen

De Nuvias Cyber Security afdeling heeft veel expertise op het gebied van beveiliging van de buitengrenzen van het netwerk. Ons succes is gebaseerd op de basis van het echt oplossen van het probleem met de juiste oplossing in plaats van het simpelweg verkopen van de gevraagde oplossing.

Wij helpen u en uw klant te ontdekken waar verbindingen met het internet bestaan, wie ze heeft en voor welke doeleinden, en vervolgens de beste manier te bepalen om ze te beveiligen zonder het bedrijf of de gebruikers in de weg te zitten.

Gewapend met deze kennis kunnen wij vervolgens specifieke aanbevelingen doen over wat de beste bescherming zal bieden. In sommige gevallen kan dit een alles-in-één oplossing zijn uit het groeiende aanbod van Unified Threat Management en Next-Generation Firewalls, in andere gevallen een gespecialiseerde oplossing voor specifieke bedreigingen, of wanneer een zeer fijnmazig beleid en controle over het beleid vereist zijn.

Afstemmen op wat belangrijk is

Hoe dan ook, wij zorgen ervoor dat het gewenste beveiligingsbeleid, de technologie en het budget op elkaar worden afgestemd om een passende oplossing te leveren.

- Next-Generation Firewall
- Web Application Firewall
- Unified Threat Management (UTM)
- Intrusion Prevention
- Advanced Persistent Threat (APT)
- Advanced Sandboxing en Threat Emulation
- Application Delivery Control
- Load Balancing
- Application Inspection
- Bandwidth en Traffic Management
- Content Security
- Anti-Spam / Email Security
- Anti-Phishing
- Anti-Malware
- Anti-Virus
- Distributed Denial of Service (DDoS)
- Data Loss Prevention (DLP)
- Application Control
- HTTPS and SSL Inspection
- Web en URL Filtering
- User en Entity Behaviour Analytics (UEBA)

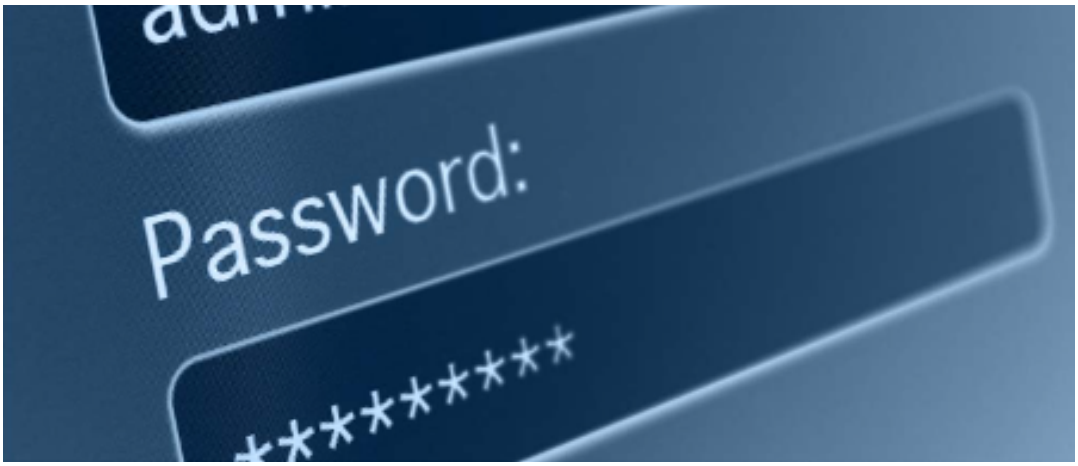
Waarom Nuvias inschakelen?

Wij bieden onze partners alle ondersteuning die zij nodig hebben om succesvol te zijn in de beveiliging van de grenzen van het netwerk. Van kwalificatie en scoping assistentie, proof-of-concepts, tot installatie, training en after-sales ondersteuning. Wij kunnen u zelfs helpen nieuwe manieren te ontdekken om de oplossingen te vercommercialiseren als onderdeel van cloud- of doorlopende beheerde diensten die u mogelijk wilt creëren.

Specialist Security

Voor organisaties die voor hun activiteiten afhankelijk zijn van de bescherming van hun kritieke infrastructuur, is een nieuwe dimensie van beveiliging in aantocht.

Naarmate meer machines, industriële besturingssystemen zoals SCADA (Supervisory Control and Data Acquisition), HMI (human-machine interface) en Internet of Things (IoT)-apparaten verbinding maken met netwerken, worden ze blootgesteld aan digitale bedreigingen. Het uitvallen van deze systemen kan catastrofaal zijn voor de bedrijfsvoering. Daarom zijn de hoogste beveiligingsniveaus vereist om deze organisaties te helpen productief te blijven en in extreme gevallen zelfs mensenlevens te beschermen.



Beveiliging van kritieke infrastructuur

Nuvias heeft een reeks gespecialiseerde beveiligingsoplossingen samengesteld die verder gaan dan de raditionele beveiliging van gegevens, toepassingen en identiteit van personen, en ook de bescherming van kritieke infrastructuur omvatten. Het is een zeer gespecialiseerd gebied, maar wij zijn volledig op de hoogte van de systemen, machines en apparaten die bescherming nodig hebben, waaronder vaak verouderde technologieën die hun eigen unieke kwetsbaarheden bevatten. Wij begrijpen ook de belangrijke uitdagingen die uw klant zal tegenkomen en de risico's die hij tot een minimum wil beperken.

Met technieken die vergelijkbaar zijn met de manier waarop wij netwerken beschermen, waaronder firewalling, authenticatie van gebruikers en toepassingen en toleranties voor wat normale IP-commando's aan het apparaat zijn, werken wij policy-driven oplossingen uit ter bescherming van deze kritieke infrastructuur.

- SCADA Security
- Internet of Things (IoT) Security
- Critical Infrastructure Security

Gespecialiseerde Cyber Security leveranciers

Naast ons eigen team van professionals hebben wij via ons netwerk van Cyber Security leveranciers ook toegang tot enkele van de beste experts in de branche. Dit betekent dat wij ervoor kunnen zorgen dat u de kansen op het gebied van Specialist Security op deskundige wijze inschat, met slimme oplossingen die voldoen aan de unieke vereisten van uw klanten. We kunnen u ook helpen uw vaardigheden te ontwikkelen door middel van geaccrediteerde opleidingsprogramma's en labervaring in voor ons speciaal gebouwde faciliteiten.

Wilt u meer weten?

Scan de QR code en neem direct contact op met ons team.
Wij gaan graag direct met u aan de slag om onze technologieën zo optimaal mogelijk in te zetten binnen uw business model