DELL Technologies

Verbeter uw cyberbeveiliging en de Zero Trust volwassenheid.

Dicht de kloven in hulpmiddelen en kennis om uw verdediging te versterken tegen cyberaanvallen.

De snel veranderende bedreigingen van vandaag, met name met de opkomst van GenAI, leiden tot nieuwe en onverwachte uitdagingen voor zelfs de meest ervaren cybersecurityspecialisten. Ontdek hoe u door samen te werken met ervaren beveiligingsprofessionals cyberaanvallen kunt voorkomen en robuuste beveiligingspraktijken kunt handhaven.

Cyberbedreigingen zijn als mieren bij een picknick

U jaagt er een weg en de volgende komt er al weer aan.

In een wereld die steeds meer met elkaar verbonden raakt, waarin organisaties sterk afhankelijk zijn van digitale infrastructuren en data een verhandelbaar goed is geworden, kunt u er het beste van uitgaan dat een geavanceerde aanvaller uw IT-omgeving al is binnengedrongen.

Het goede nieuws is dat er ervaren partners zijn die gespecialiseerd zijn in technologie en cyberbeveiliging.

Dell Technologies biedt innovatieve oplossingen en waardevolle expertise die mogelijk niet onder eigen beheer beschikbaar zijn om u te helpen door de steeds veranderende bedreigingen te navigeren.

- Hard- en softwarebeveiliging
- Inzicht in opkomende risico's
- Inzicht in geavanceerde aanvalstechnieken
- AIOps om te voldoen aan snel veranderende bedreigingen
- Nieuwe beveiligingsstrategieën en best practices

Bouw verdedigingslagen die de beveiligingspraktijken voortdurend bevorderen en een Zero Trust-aanpak omarmen.

Dell Technologies is een partner voor cyberbeveiliging die uitgebreide professionele services, hardware- en softwareoplossingen en een robuust partnerecosysteem biedt die de kans op aanvallen beperkt, beveiligingslekken identificeert en minimaliseert en u helpt om bedrijfsactiviteiten snel te herstellen.

Beperk het aanvalsoppervlak →

Detecteer en reageer op cyberbedreigingen →

Herstel snel van een aanval →

Edge **Core** **Multicloud**

Professionele services

Ecosysteem voor bedrijven/technologiepartners **Beveiligde leveringsketen**

DELL Technologies

Beperk het aanvalsoppervlak

Versterk uw verdediging en maak uzelf een kleiner doel door de wegen te sluiten waar cybercriminelen graag misbruik van maken.

Om uw beveiligingsmentaliteit te versterken, moet u beveiligingslekken en toegangspunten identificeren en minimaliseren die applicaties, systemen of netwerken in verschillende domeinen in gevaar kunnen brengen, waaronder edge, core en cloud.

IDENTIFICEER kwetsbare punten

- Kwetsbaarheden in software
- Verkeerde configuraties
- Zwakke verificatiemechanismen
- Niet-gepatchte systemen
- Overmatige gebruikersbevoegdheden
- Open netwerkpoorten
- Slechte fysieke beveiliging

IMPLEMENTEER preventieve maatregelen

- Samenwerken met veilige leveranciers
- Uitgebreide netwerksegmentatie toepassen
- Isoleer kritieke gegevens
- Strikte toegangscontrole afdwingen
- Systemen en applicaties bijwerken en patchen
- Beveiligingslekken identificeren en aanpakken met behulp van AI, regelmatige evaluaties en testen

Omarm een Zero Trust-aanpak

Een Zero Trust-architectuur betekent dat uw organisatie niets binnen of buiten de perimeters automatisch vertrouwt. In plaats daarvan wordt alles dat probeert verbinding te maken met uw systemen geverifieerd voordat u toegang verleent. Het is een model dat is vastgesteld en voorgeschreven door het Amerikaanse Department of Defense dat **7 met elkaar verbonden pijlers** omvat die op een consequente wijze het ontwikkelingsniveau opbouwen.

1. Vertrouwen in de gebruiker
2. Vertrouwen in apparaten
3. Vertrouwen in data
4. Toepassing en workload
5. Netwerk en omgeving
6. Zichtbaarheid en analytics
7. Automatisering en integratie

DELL Technologies

Beperk het aanvalsoppervlak

Identificeer de zwakke punten die uw systemen onderuithalen voordat de problemen ontstaan.

Cyberbeveiliging is geen eenmalige taak, maar een doorlopend proces. Regelmatige onderzoeken, penetratietests en evaluaties van kwetsbaarheden, met behulp van een ervaren beveiligingsservicepartner, kunnen helpen de kloven te identificeren en op te vullen om risico's te verminderen.

Veilige werkwijzen voor de leveringsketen	Beveiliging begint eerder dan u denkt. Creëer een betrouwbare basis met behulp van apparaten en infrastructuur die zijn ontworpen, vervaardigd en geleverd met behulp van een veilige leveringsketen, veilige ontwikkelingscyclus en rigoureuze bedreigingsmodellering.
Ingebouwde beveiliging	Werk met apparaten en infrastructuur met ingebouwde, hardwaregebaseerde beveiliging die is ontworpen om aanvallen te detecteren en af te dwingen voordat ze beschadigd raken.
Regelmatige patching en updates	Pak bekende beveiligingslekken aan en minimaliseer het risico op misbruik door applicaties, firmware en besturingssystemen up-to-date te houden met de nieuwste beveiligingspatches.
Minste privilege	Beperk gebruikers- en systeemaccounts tot de minimale toegangsrechten die nodig zijn om hun taken uit te voeren. Deze aanpak beperkt de potentiële gevolgen van het verkrijgen van onbevoegde toegang door een aanvaller.
Netwerksegmentatie	Isoleer kritieke assets om netwerktoegang te beperken door gebruik te maken van moderne netwerksegmentatie voor kritieke data en bedrijfsgroepen en applicaties. Dit bevat een aanval door laterale beweging te voorkomen.
Applicatie-beveiliging	Implementeer veilige coderingspraktijken, voer regelmatig beveiligingstests en code-evaluaties uit en gebruik van Web Application Firewalls (WAF's) om te helpen beschermen tegen veelvoorkomende aanvallen op applicatieniveau en vermindert het aanvalsoppervlak van webapplicaties.
Professionele services en partnerschappen	Werk samen met serviceproviders voor cyberbeveiliging en vorm samenwerkingen met zakelijke en technologische partners om expertise en oplossingen te bieden die mogelijk niet in eigen huis beschikbaar zijn.
Gebruikerstraining en bewustwording	Train werknemers en gebruikers om potentiële beveiligingsrisico's, phishing-pogingen en social-engineeringtactieken te herkennen en te rapporteren om de risico's die misbruik maken van menselijke kwetsbaarheden te minimaliseren.

DELL Technologies

Detecteer en reageer op cyberbedreigingen

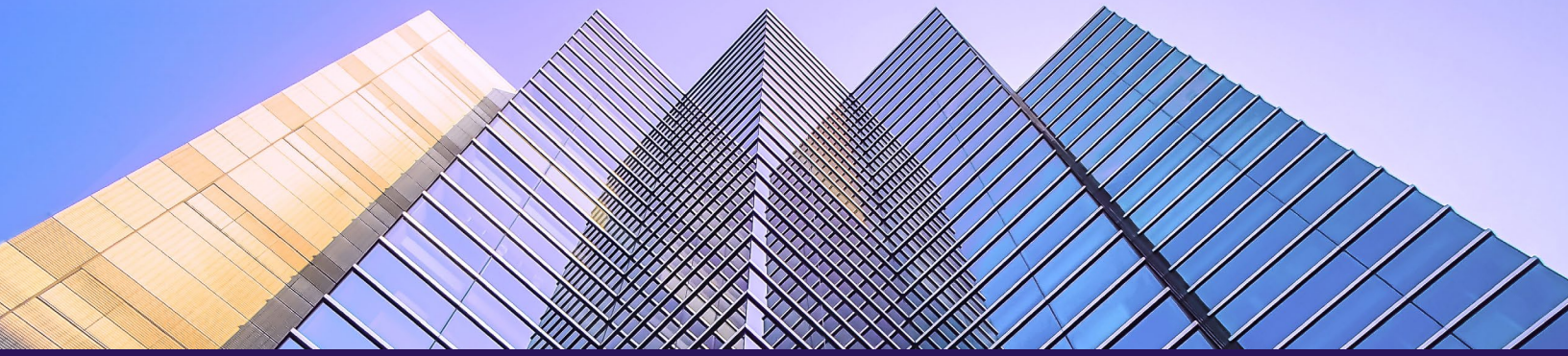
Ouderwetse beveiligingspraktijken zijn net als inbellen via internet; te traag en ineffectief in de huidige veeleisende omgeving.

Om geavanceerde cyberbedreigingen tegen te gaan, hebt u betere beveiligingsmaatregelen nodig, zoals AI en ML die zijn ingebouwd in applicaties en methodieken die bekend en onbekend identificeren en reageren op wat er bekend en onbekend is.

Krachtige systemen voor intrusiedetectie en -preventie implementeren

Maak gebruik van AI en ML voor anomaliedetectie

Real-time bewaking van netwerkverkeer en gebruikersgedrag instellen



Verhoog de tolerantie door samen te werken met ervaren professionele services om specialistische expertise op te verkrijgen.

Als ervaren technologiepartner kan Dell Technologies u helpen bij het opstellen van een proactieve incidentrespons- en herstelprotocollen die een overzicht geven van rollen en verantwoordelijkheden en naadloze communicatie en coördinatie tussen betrokkenen waarborgen.

Verbeter uw vermogen om proactief cyberbedreigingen te detecteren en te reageren met behulp van geavanceerde:

- Threat intelligence
- Incidentrespons
- Beveiligingsinformatie en gebeurtenisbeheer
- Bescherming van eindpunten
- Gedragsanalyse

Faciliteer een efficiënt, snel herstel en minimaliseer dataverlies met:

- Een duidelijk gedefinieerd incidentresponsplan en samenwerking
- Regelmatige back-ups van kritieke data en systemen
- Veilige off-site storageoplossingen en dataversleuteling

DELL Technologies

Cyberbedreigingen detecteren en hierop reageren

Blijf alert en onderneem snel actie.

Het detecteren van en reageren op cyberdreigingen betekent alert blijven en plannen voor het slechtst mogelijke scenario. Stel een respons- en herstelplan op dat voortdurend wordt bijgewerkt en routinematig wordt uitgevoerd, zodat uw hele organisatie weet hoe u de gevolgen van een aanval kunt verminderen. Het is een doorlopend en iteratief proces dat een combinatie van technologie, deskundig personeel, duidelijk gedefinieerde processen en teamsamenwerking vereist.

Continu toezicht	Beveiligingstools zoals Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), logboekanalyse en bedreigingsinformatie helpen bij het identificeren van tekenen van ongeautoriseerde toegang, intrusie, malware-infecties en datalekken.
Bedreigings-detectie	Maak gebruik van AI en ML om data te analyseren om patronen, afwijkingen en indicatoren van compromissen (IoC's) te identificeren die kunnen wijzen op een bedreiging. Dit omvat het herkennen van bekende aanvalssignalen en het identificeren van afwijkend gedrag.
Waarschuwingen en meldingen	Vroegtijdige waarschuwingen geven om onderzoek te vragen en te reageren. Breng waarschuwingen en meldingen naar het oppervlak voor snelle actie met geïntegreerde beveiliging. Voer telemetrie op apparaatniveau boven het besturingssysteem in om de detectie van bedreigingen te versnellen en beveiligingspersoneel of een Security Operations Center (SOC) te ontketenen wanneer potentiële bedreigingen of incidenten worden gedetecteerd.
Incident respons	Start een responsplan om bevestigde beveiligingsincidenten te onderzoeken en te beperken. Hierbij moet de impact worden beschreven, de hoofdoorzaak worden vastgesteld en de noodzakelijke acties worden ondernomen om systemen te herstellen en verdere schade te voorkomen.
Forensische Analyse	Gedetailleerde analyse van incidenten uitvoeren om inzicht te krijgen in de aanvalsmethodiek, de omvang van de inbreuk te bepalen, getroffen systemen of data te identificeren en bewijs te verzamelen om zwakke plekken in de beveiliging te vinden en aan te pakken.
Oplossing en herstel	Neem stappen om beveiligingslekken te verhelpen, systemen te herstellen, malware te verwijderen en verbeterde beveiligingsmaatregelen te implementeren om soortgelijke incidenten te voorkomen. Herstel de getroffen systemen en data naar hun normale staat om het herstelproces te voltooien.

DELL Technologies

Herstellen van cyberaanvallen

Geef wat gas bij en krijg uw bedrijf weer in de volgende versnelling.

Cyberweerbaarheid is nodig in de huidige datagestuurde wereld en wordt door zowel klanten als partners verwacht. Om succesvol te zijn, zijn meerdere beschermingslagen vereist om ervoor te zorgen dat kritieke data worden beschermd en geïsoleerd, zodat deze snel met vertrouwen kunnen worden hersteld na een aanval. Beoordeel uw cyberweerbaarheid ›

Onderneem actie om de schade te beperken die wordt veroorzaakt door een cyberaanval

Bouw gecompromitteerde of verstoorde services en apparaten opnieuw op

Analyseer het incident om toekomstige aanvallen te voorkomen

Voldoe aan zakelijke SLA's en zorg ervoor dat alles weer normaal werkt

Creëer een uitgebreide strategie voor cyberbeveiliging, zodat uw organisatie effectief en efficiënt kan herstellen.

Herstellen na een cyberaanval vereist een gecoördineerde inspanning van IT-teams, cybersecurityprofessionals, management en soms externe experts. De sleutel tot herstel is om systemen en bewerkingen snel weer normaal te maken, terwijl u leert van het incident om onderbrekingen en downtime te verminderen, services en data-integriteit te herstellen, de impact op financiën en reputatie te minimaliseren en cyberbeveiliging te versterken om soortgelijke aanvallen in de toekomst te voorkomen.

- Beoordeel de impact van een aanval op bedrijfsactiviteiten
- Geef prioriteit aan kritieke services
- Implementeer databeschermingssystemen
- Communiceer over eventuele incident- en herstelvoortgang
- Ontwikkel een plan en oefen voortdurend om de continuïteit te waarborgen

DELL Technologies

Herstel van cyberaanvallen

Kom terug in actie door systemen, netwerken en data na een incident opnieuw leven in te blazen.

Door een strategie voor cyberweerbaarheid te bereiken, worden mensen, processen en technologie opgenomen in een holistisch framework dat een hele organisatie of entiteit beschermt.

Incident-insluiting

De eerste stap is het isoleren en insluiten van de impact van de cyberaanval. Hierbij moet u de betreffende systemen loskoppelen van het netwerk, gecompromitteerde accounts uitschakelen en maatregelen implementeren om verdere verspreiding of schade te voorkomen.

Systeem- of apparaatherstel

Zodra een incident is ingesloten, worden getroffen systemen en netwerken hersteld naar een schone en veilige staat. Dit kan het opnieuw opbouwen van gecompromitteerde systemen, het opnieuw installeren van software en het toepassen van beveiligingspatches en updates inhouden. Automatisering en zelfherstel kunnen een belangrijke rol spelen bij het weer operationeel worden.

Data herstel

Data die tijdens de aanval zijn gecompromitteerd, versleuteld of verwijderd, moeten worden hersteld. Dit kan het herstellen van data uit back-ups of het gebruik van gespecialiseerde datahersteltechnieken omvatten om verloren of versleutelde bestanden terug te krijgen.

Forensische Analyse

Na een aanval is het cruciaal om te begrijpen hoe de inbreuk heeft plaatsgevonden, welke beveiligingslekken werden misbruikt en de stappen om soortgelijke aanvallen te voorkomen. Systemen zoals Security Information and Event Management (SIEM) en mogelijkheden zoals BIOS-vergelijkingen buiten de host bieden nuttige inzichten.

Beoordeling van incidentrespons

Na herstel is het essentieel om het incidentresponsproces te evalueren en verbeteringspunten te identificeren. Lessen uit de aanval kunnen worden gebruikt om de beveiligingspraktijken te verbeteren, plannen voor incidentrespons bij te werken en betere bescherming te bieden tegen toekomstige incidenten.

Professionele services en partnerschappen

Serviceproviders en technologiepartners voor cyberbeveiliging bieden waardevolle expertise en bronnen om uw organisatie te helpen herstellen. Ze kunnen helpen met taken zoals forensische analyse, het identificeren van het optreden van de inbreuk en het aanbevelen van maatregelen om toekomstige incidenten te voorkomen.

DELL Technologies

Breid cyberbeveiliging uit naar edge en cloudomgevingen

Naarmate netwerken van de core naar de edge naar de cloud worden verspreid, zijn omgevingen een cruciale kwetsbaarheid geworden.

Als u uw cyberbeveiligingsstrategie een voorsprong geeft, moet uw organisatie de Zero Trust-principes uitbreiden naar de edge en de cloud om strikte toegangscontrole, continue verificatie en uitgebreide zichtbaarheid en controle over netwerkverkeer te garanderen. Naarmate het bedreigingslandschap verandert, is het verstandig om AI-mogelijkheden te implementeren als een eerste verdedigingslinie. Bovendien is een strategie alleen voltooid als uw kernnetwerk- en cloudomgevingen beveiligingsmaatregelen hebben, zoals netwerksegmentatie, versleuteling en continue bewaking.

Professionele cyberbeveiligingsservices kunnen u helpen een holistische aanpak te hanteren.

Het verbinden van verschillende beveiligingsoplossingen kan een uitdaging zijn. Samenwerken met professionele services die gespecialiseerd zijn in edge, core- en cloudbeveiliging biedt u de expertise om effectieve maatregelen te nemen die uw organisatie vanuit alle hoeken beschermen.

Edge

Stel meerdere beveiligingslagen in aan de rand, in het netwerk en binnen de hardware en software.

Core

Stem uw infrastructuur af op een Zero Trust-aanpak met behulp van AI, ML en automatisering.

Multicloud

Bescherm elke workload in elke omgeving, inclusief public cloud, containers en native workloads in de cloud.

DELL Technologies

GenAI: Een paradox voor cyberbeveiliging

De volgende generatie AI brengt snel nieuwe risico's met zich mee, maar verbetert ook de beveiliging.

Als de volgende fase in AI omvat GenAI systemen die kennis kunnen begrijpen, leren, aanpassen en implementeren in een reeks taken.

Aan de ene kant belooft het verbeterde dreigingsdetectie en -respons, voorspellende mogelijkheden en operationele efficiëntie. Aan de andere kant brengt het nieuwe uitdagingen met zich mee die veranderende strategieën voor cyberbeveiliging vereisen die risico's aanpakken door middel van robuuste beveiligingsmaatregelen, continue bewaking, regelmatige updates en patches en een steeds veranderende benadering van dataprivacy en -ethiek.

Beveiligen van organisaties met GenAI

GenAI is een cruciale bondgenoot geworden in cyberbeveiliging en biedt nieuwe manieren om organisaties te beschermen.

- Verbeter de effectiviteit van bedreigingsdetectie en -respons.
- Voorspel toekomstige bedreigingen of identificeer mogelijke kwetsbaarheden.
- Automatiseer de detectie van bedreigingen en bied efficiëntie.
- Forensische analyse om snel patronen, afwijkingen en indicatoren van compromissen te identificeren.
- Gepersonaliseerde trainingen in bewustwording van veiligheid
- Schaal beveiligingsactiviteiten met snellere toegang tot rijkere inzichten.

Beveiligen van GenAI-systemen

Hoewel GenAI aanzienlijke beveiligingsvoordelen biedt, kan de functionaliteit ervan kwaadwillig worden gebruikt als dit niet op de juiste manier wordt beveiligd.

- Zorg voor dataprivacy en -integriteit.
- Verminder tegenslagen die zijn ontworpen om AI-systemen te beschadigen die storingen veroorzaken.
- Detecteer en reageer op misbruik van het systeem door schadelijke AI.
- Controleer en verzacht ethische problemen en vooroordelen.
- Implementeer sterke toegangscontroles voor AI-systemen.
- Bescherm en herstel grote taal modellen (LLM) op een veilige manier.

DELL Technologies

Moderne cyberbeveiliging moet intelligent, schaalbaar en geautomatiseerd zijn

Dell Technologies kan u helpen bij het opzetten van uitgebreide beveiliging die bescherming biedt tegen ontwikkelende cyberbedreigingen. Naarmate de technologie toeneemt, blijft onze aanpak van cyberbeveiliging een stap voor. Hierbij gebruiken we de kracht van AI en ML om uw digitale infrastructuren te beschermen en het vertrouwen in de digitale wereld te behouden. Waar u ook bent op het gebied van cyberbeveiliging, wij werken met u samen om verder te gaan dan alleen het beschermen van uw organisatie met stappen die u flexibel en veerkrachtig houden.

DELL Technologies

Dell.com/SecuritySolutions

Laat u terugbellen

Chatten met een beveiligingsadviseur

Bel 1-800-433-2393