DELL Technologies

E-BOOK INTERACTIEVE SCENARIO'S VOOR CYBERBEVEILIGING

# Echte scenario's. Slimmere beslissingen. Sterkere verdediging.

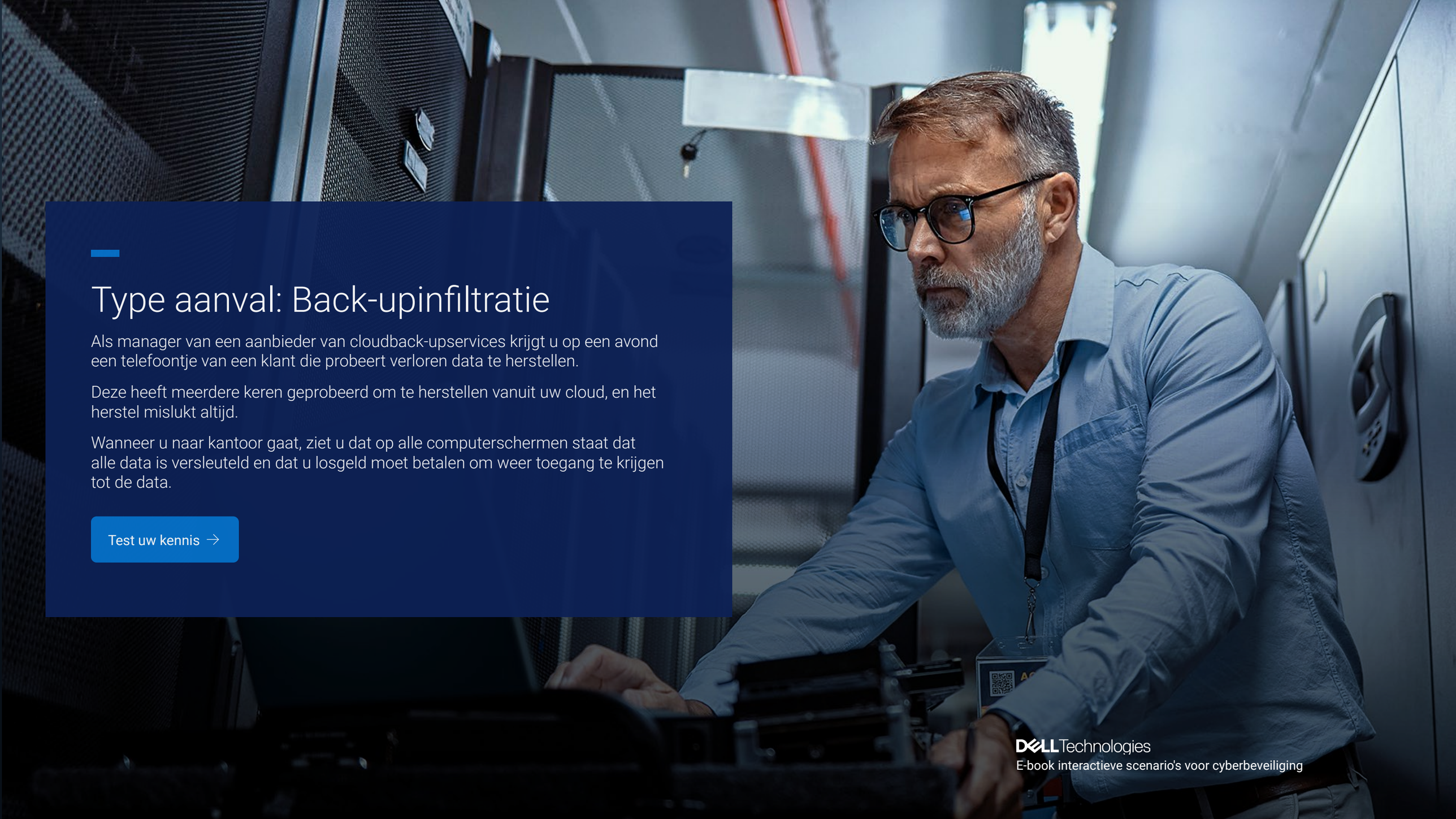
De inzet van Dell voor beveiliging vormt de kern van alles wat we doen. Door inzichten, best practices en innovatieve technologieën te delen, id het doel van dit e-book om u de tools en kennis te bieden die nodig zijn om opkomende cyberrisico's voor te blijven.

## Kies een aanvalsscenario

Cyberbeveiligingsdreigingen veranderen voortdurend en organisaties moeten effectief reageren om hun data te beschermen. Om uw organisatie zo goed mogelijk voor te bereiden, kunt u zich volledig onderdompelen in realistische simulatieoefeningen die u helpen bij het uitstippelen van uw cyberbeveiligingsstrategieën om cyberaanvallen te bestrijden.

Ontdek een breed scala aan aanvalstypen en branchespecifieke uitdagingen in sectoren zoals federale, staats- en lokale overheid, financiële dienstverlening en gezondheidszorg. Gaandeweg ontdekt u hoe de geïntegreerde beveiligingsoplossingen van Dell, van laptops en desktops tot bedrijfssystemen, zijn gebouwd om u te beschermen tegen deze bedreigingen.

- Infiltratie van back-ups →
- Ransomware →
- Distributed Denial of Service (DDoS) →
- Hardware van de leveringsketen →
- Bedreiging van binnenuit →
- Software van de leveringsketen →
- Man-in-the-Middle (MITM) →
- Zero-day →
- Prompt-/SQL-injectie →



# Type aanval: Back-upinfiltratie

Als manager van een aanbieder van cloudback-upservices krijgt u op een avond een telefoontje van een klant die probeert verloren data te herstellen.

Deze heeft meerdere keren geprobeerd om te herstellen vanuit uw cloud, en het herstel mislukt altijd.

Wanneer u naar kantoor gaat, ziet u dat op alle computerschermen staat dat alle data is versleuteld en dat u losgeld moet betalen om weer toegang te krijgen tot de data.

Test uw kennis →

# Type aanval: Back-upinfiltratie

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

U weet niet zeker welke back-upsystemen of klanten zijn getroffen. Wat is uw eerste stap?

- [ ] De autoriteiten op de hoogte stellen
- [ ] Alle systemen uitschakelen
- [ ] De bedreiging proberen te beperken en te isoleren
- [ ] Bepalen of u een schone back-up hebt om vanaf te herstellen

Bekijk het juiste antwoord →

DELL Technologies

E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Back-upinfiltratie

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

U weet niet zeker welke back-upsystemen of klanten zijn getroffen. Wat is uw eerste stap?

- ✗ De autoriteiten op de hoogte stellen
- ✗ Alle systemen uitschakelen
- ✓ De bedreiging proberen te beperken en te isoleren
- ✗ Bepalen of u een schone back-up hebt om vanaf te herstellen

Het onmiddellijk inperken en isoleren van een bedreiging voorkomt verdere verspreiding of schade en geeft tijd om de omvang van het incident te beoordelen, waardoor de impact op alle soorten cyberaanvallen, inclusief aanvallen met AI, mogelijk wordt geminimaliseerd.

Volgende vraag →

DELL Technologies
E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Back-upinfiltratie

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Uw prioriteit is om de data van uw klanten snel beschikbaar te maken. Hoe zou u dit bereiken?

- [ ] Het losgeld betalen
- [ ] De ransomwarevariant herkennen
- [ ] De autoriteiten op de hoogte stellen
- [ ] Identificeren welke data zijn gecompromitteerd

Bekijk het juiste antwoord →

DELL Technologies

E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Back-upinfiltratie

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Uw prioriteit is om de data van uw klanten snel beschikbaar te maken. Hoe zou u dit bereiken?

- ✗ Het losgeld betalen
- ✗ De ransomwarevariant herkennen
- ✗ De autoriteiten op de hoogte stellen
- ✓ Identificeren welke data zijn gecompromitteerd

Door gecompromitteerde data te herkennen, kunt u uw herstelinspanningen richten op het herstellen van de meest kritieke klantinformatie, waardoor data sneller beschikbaar is en onnodig werk aan niet-getroffen systemen wordt voorkomen.

Volgende vraag →

# Type aanval: Back-upinfiltratie

1 — 2 — 3: Herstellen na een cyberaanval — 4

U stelt vast dat u een back-up hebt om te herstellen. Wat is de eerste stap in uw proces zijn?

- [ ] Prioriteit geven aan het herstellen van kritieke systemen
- [ ] Forensische analyse gebruiken om te bevestigen dat de aanval volledig onder controle is
- [ ] Alle wachtwoorden wijzigen en gecompromitteerde inloggegevens intrekken
- [ ] Zero Trust-principes toepassen

Bekijk het juiste antwoord →

# Type aanval: Back-upinfiltratie

1 — 2 — 3: Herstellen na een cyberaanval — 4

U stelt vast dat u een back-up hebt om te herstellen. Wat is de eerste stap in uw proces zijn?

- ✗ Prioriteit geven aan het herstellen van kritieke systemen
- ✓ Forensische analyse gebruiken om te bevestigen dat de aanval volledig onder controle is
- ✗ Alle wachtwoorden wijzigen en gecompromitteerde inloggegevens intrekken
- ✗ Zero Trust-principes toepassen

Voordat u systemen herstelt, moet u ervoor zorgen dat de aanval volledig onder controle is om onbedoelde herinfectie en verdere schade te voorkomen, zodat bedreigingen in uw omgeving niet blijven voortduren of escaleren.

Volgende vraag →

DELL Technologies
E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Back-upinfiltratie

1 2 3 4: Algemene best practices

Wat zijn mogelijke manieren om het risico op dit probleem in de toekomst te beperken?

- [ ] Pas Zero Trust-principes toe
- [ ] Endpoint Detection and Response (EDR)-mogelijkheden inschakelen
- [ ] Onveranderlijke en air-gapped back-ups implementeren
- [ ] Alle bovenstaande opties

Bekijk het juiste antwoord →

# Type aanval: Back-upinfiltratie

1 2 3 4: Algemene best practices

## Wat zijn mogelijke manieren om het risico op dit probleem in de toekomst te beperken?

- [x] Pas Zero Trust-principes toe
- [x] Endpoint Detection and Response (EDR)-mogelijkheden inschakelen
- [x] Onveranderlijke en air-gapped back-ups implementeren
- [x] Alle bovenstaande opties

Het gebruik van een meerlaagse verdedigingsstrategie kan risico's verminderen, schade minimaliseren en de veerkracht van de organisatie verbeteren, omdat geen enkele maatregel op zichzelf voldoende is.

Bekijk oplossingen →

TYPE AANVAL: BACK-UPINFILTRATIE

# Samenvatting

Infiltratie van back-ups vindt plaats wanneer cybercriminelen beveiligingslekken in back-upsystemen misbruiken om kritieke hersteldata in gevaar te brengen, te vernietigen of te versleutelen. Deze geavanceerde aanvallen kunnen samenvallen met of volgen op andere incidenten, zoals ransomware- of malware-implementatie, waardoor de operationele en financiële gevolgen worden versterkt.

Bij Dell geloven we in het versterken van organisaties, zodat ze veerkrachtig blijven in het licht van steeds veranderende cyberdreigingen. Met onze geavanceerde oplossingen, deskundige services en vertrouwde partnerschappen helpen we u om te beschermen wat het belangrijkst is.

Meer informatie over onze oplossingen en hoe we de zwaarste cyberuitdagingen van vandaag aanpakken.

Bekijk het rapport over infiltratie van back-ups →

Terug naar scenario's

## PowerProtect portfolio›

Onze onveranderlijke, air-gapped en versleutelde back-upkluizen, aangedreven door AI-gestuurde CyberSense-analyses, zorgen voor snelle detectie en herstel, zodat u veerkrachtig kunt blijven.

## PowerEdge Servers ›

Met veilig opstarten, hardware root of trust en systeemvergrendeling biedt Dell de infrastructuur waarop u kunt vertrouwen om uw back-ups te beveiligen.

## Vertrouwde werkruimte ›

SafeBIOS- en SafeData-beveiligingen verminderen risico's en zorgen ervoor dat uw back-upsystemen ongeschonden blijven en klaar zijn voor gebruik wanneer u ze nodig hebt.

## Services voor beveiliging en veerkracht›

Van veilige implementatie tot proactieve incidentrespons, onze experts en partners helpen u veerkracht op te bouwen en sneller te herstellen.

## Netwerkoplossingen ›

Met netwerksegmentatie, meervoudige verificatie (MFA) en configuraties met minimale bevoegdheden, Dell helpt u de toegang te vergrendelen en uw kritieke data te beschermen.

# Type aanval: Distributed Denial of Service (DDoS)

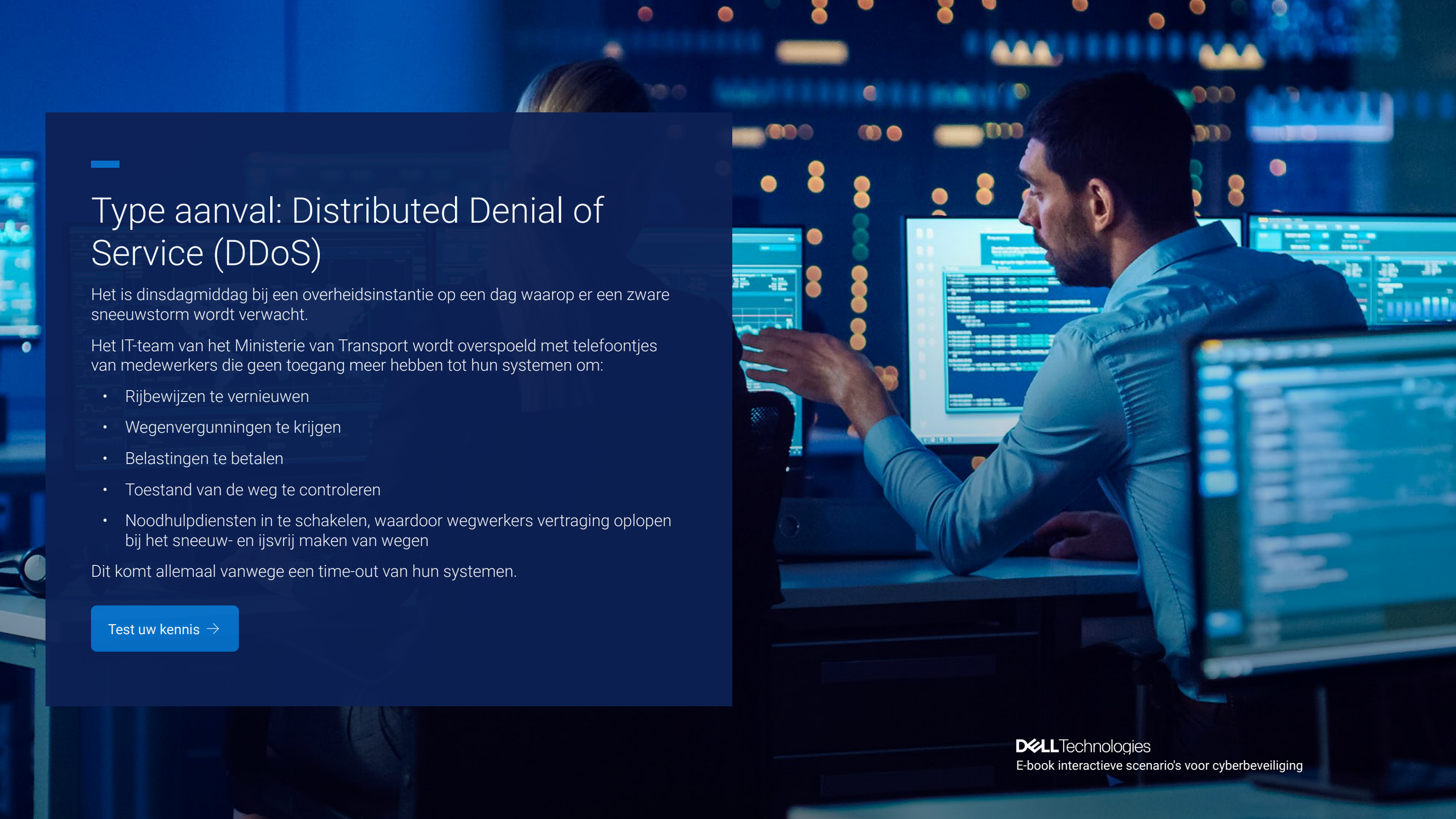
Het is dinsdagmiddag bij een overheidsinstantie op een dag waarop er een zware sneeuwstorm wordt verwacht.

Het IT-team van het Ministerie van Transport wordt overspoeld met telefoontjes van medewerkers die geen toegang meer hebben tot hun systemen om:

- Rijbewijzen te vernieuwen
- Wegenvergunningen te krijgen
- Belastingen te betalen
- Toestand van de weg te controleren
- Noodhulpdiensten in te schakelen, waardoor wegwerkers vertraging oplopen bij het sneeuw- en ijsvrij maken van wegen

Dit komt allemaal vanwege een time-out van hun systemen.

Test uw kennis →



# Type aanval: Distributed Denial of Service (DDoS)

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Waar moet u als eerste kijken om te zien wat er mogelijk aan de hand is?

- [ ] Netwerkapparaten controleren op plotselinge, onverklaarbare pieken in inkomend verkeer
- [ ] Netwerkapparaten controleren op ongebruikelijk verkeer van één of beperkt aantal IP-adressen
- [ ] De logboeken van firewall- of netwerkzichtbaarheidstools controleren op overmatige mislukte verbindingen of verkeersblokkeringsgebeurtenissen
- [ ] Alle bovenstaande opties

Bekijk het juiste antwoord →

# Type aanval: Distributed Denial of Service (DDoS)

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

## Waar moet u als eerste kijken om te zien wat er mogelijk aan de hand is?

- [x] Netwerkapparaten controleren op plotselinge, onverklaarbare pieken in inkomend verkeer
- [x] Netwerkapparaten controleren op ongebruikelijk verkeer van één of beperkt aantal IP-adressen
- [x] De logboeken van firewall- of netwerkzichtbaarheidstools controleren op overmatige mislukte verbindingen of verkeersblokkeringsgebeurtenissen
- [x] Alle bovenstaande opties

Om wijdverbreide systeemstoringen correct te diagnosticeren, moet u tegelijkertijd de activiteit van netwerkapparaten en de logboeken van firewall- of zichtbaarheidstools controleren om snel ongebruikelijke patronen of blokkeringsgebeurtenissen te detecteren. Dit maakt snellere, nauwkeurigere incidentrespons mogelijk omdat u onderscheid kunt maken tussen cyberincidenten en infrastructuurproblemen.

Volgende vraag →

DELL Technologies
E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Distributed Denial of Service (DDoS)

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

U vermoedt dat dit een DDoS-aanval is. Wat is uw eerste stap?

- [ ] Alle netwerkverkeer omleiden via een DDoS-beveiligingsdienst
- [ ] WAF-regels (Web Application Firewall) activeren om schadelijke patronen uit te filteren
- [ ] Controleren of de piek in het verkeer te wijten is aan legitieme bronnen
- [ ] Intern en extern communiceren wat er aan de hand is

Bekijk het juiste antwoord →

# Type aanval: Distributed Denial of Service (DDoS)

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

U vermoedt dat dit een DDoS-aanval is. Wat is uw eerste stap?

- ✗ Alle netwerkverkeer omleiden via een DDoS-beveiligingsdienst
- ✗ WAF-regels (Web Application Firewall) activeren om schadelijke patronen uit te filteren
- ✓ Controleren of de piek in het verkeer te wijten is aan legitieme bronnen
- ✗ Intern en extern communiceren wat er aan de hand is

Voordat u DDoS-tegenmaatregelen activeert, is het essentieel om de legitimiteit van een piek in het dataverkeer te verifiëren. Zo voorkomt u dat legitieme gebruikers per ongeluk worden geblokkeerd, voorkomt u onderbrekingen voor kritieke belanghebbenden en zorgt u dat eventuele verdere beschermende acties correct en nauwkeurig zijn gericht, waardoor de negatieve impact op openbare activiteiten en de algehele bedrijfscontinuïteit wordt geminimaliseerd.

Volgende vraag →

# Type aanval: Distributed Denial of Service (DDoS)

1 — 2 — 3: Herstellen na een cyberaanval — 4

Wat zijn enkele stappen die u kunt nemen om een DDoS-aanval in de toekomst te voorkomen?

- [ ] De IP-adressen blokkeren die het probleem veroorzaken
- [ ] Regelmatig penetratietests uitvoeren met DDoS-simulaties
- [ ] Alle applicaties naar de cloud verplaatsen omdat cloudproviders meestal geen DDoS-aanvallen krijgen
- [ ] Zero Trust-principes toepassen

Bekijk het juiste antwoord →

# Type aanval: Distributed Denial of Service (DDoS)

1 — 2 — 3: Herstellen na een cyberaanval — 4

## Wat zijn enkele stappen die u kunt nemen om een DDoS-aanval in de toekomst te voorkomen?

- ✗ De IP-adressen blokkeren die het probleem veroorzaken
- ✓ Regelmatig penetratietests uitvoeren met DDoS-simulaties
- ✗ Alle applicaties naar de cloud verplaatsen omdat cloudproviders meestal geen DDoS-aanvallen krijgen
- ✓ Zero Trust-principes toepassen

Proactieve penetratietests met DDoS-simulaties identificeren en versterken hiaten in uw verdediging, terwijl Zero Trust-principes gericht zijn op het minimaliseren van risico's door toegang met minimale bevoegdheden te allen tijde af te dwingen. Dit helpt het risico te verminderen dat essentiële systemen, zoals de coördinatie van noodhulp of realtime verkeerslichtbesturing, die zelfs tijdens een aanval operationeel moeten blijven, worden verstoord.

Volgende vraag →

# Type aanval: Distributed Denial of Service (DDoS)

1 2 3 4: Algemene best practices

Wie moet u als onderdeel van uw algehele incidentrespons- en herstelplan (IRR) op de hoogte stellen?

- [ ] Uw juridische team
- [ ] Uw leverancier van cyberverzekeringen
- [ ] CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [ ] Alle bovenstaande opties

Bekijk het juiste antwoord →

# Type aanval: Distributed Denial of Service (DDoS)

1 2 3 4: Algemene best practices

Wie moet u als onderdeel van uw algehele incidentrespons- en herstelplan (IRR) op de hoogte stellen?

- [x] Uw juridische team
- [x] Uw leverancier van cyberverzekeringen
- [x] CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [x] Alle bovenstaande opties

Overweeg tijdens een groot cyberincident om te coördineren met juridische, verzekerings- en overheidsinstanties met betrekking tot naleving, claims en wetshandhaving. Nadat u ervoor hebt gezorgd dat aan alle wettelijke vereisten is voldaan, kan uw organisatie het incident effectief beheersen, oplossen en herstellen.

Bekijk oplossingen →

TYPE AANVAL: DISTRIBUTED DENIAL OF SERVICE (DDOS)

# Samenvatting

Bij een DDoS-aanval wordt geprobeerd de normale werking van een netwerk, service of server te verstoren door deze te overweldigen met een enorme vloedgolf aan verkeer vanuit meerdere bronnen. Deze aanvallen worden uitgevoerd door botnets. Dit zijn netwerken met geïnfecteerde apparaten die op afstand door aanvallers worden beheerd.

Bij Dell helpen we organisaties om weerbaar te blijven tegen DDoS-aanvallen door geavanceerde detectie- en mitigatietechnologieën te combineren met deskundige diensten en een Zero-Trust-aanpak, waardoor een snelle reactie, minimale verstoringen en versterkte verdedigingsmechanismen worden gegarandeerd.

Meer informatie over geavanceerde strategieën voor cybertolerantie en hoe Dell u kan helpen uw organisatie te beschermen tegen DDoS.

Bekijk het rapport over DDoS →

Terug naar scenario's

## Netwerkoplossingen ›

Schakel netwerksegmentatie, microsegmentatie en handhaving van minimale bevoegdheden in om kritieke assets te isoleren, de verspreiding van aanvallen te beperken en snelle DDoS-beheersing te garanderen.

## PowerEdge Servers ›

Met hardware root of trust, secure boot, systeemvergrendeling en realtime sabotagebewijs biedt Dell veerkrachtige, krachtige DDoS-bescherming en versneld herstel.

## Vertrouwde apparaten ›

Geïntegreerde SafeBIOS, SecureData en geautomatiseerde detectie en respons verminderen het aanvalsoppervlak van eindpunten met wel 70%, waardoor DDoS-gedreven afleidingen geen inbreukvectoren kunnen worden.

## PowerProtect portfolio›

Versleutelde, onveranderlijke en air-gapped back-upomgevingen, aangestuurd door AI-gedreven dreigingsanalyses, zorgen voor een snelle, gevalideerde herstelprocedure en behouden de bedrijfscontinuïteit tijdens DDoS-storingen.

## Services voor beveiliging en veerkracht›

Managed Detection and Response (MDR), incidentrespons en herstel (IRR), dreigingsdetectie en richtlijnen voor veerkrachtige architectuur verbeteren de paraatheid voor DDoS-aanvallen en versterken de verdedigingsmogelijkheden.

# Type aanval: Bedreiging van binnenuit

Het is 08:00 uur op een dinsdag. De werkdag is nog maar net begonnen voor werknemers bij een Amerikaans gezondheidszorgbedrijf.

Een ervaren medewerker die werkt met zeer gevoelige patiëntgegevens meldt zich aan na een late avond op kantoor.

Ze merkt wijzigingen in een map waar ze de avond ervoor aan werkte. Nadat ze het met haar team heeft besproken, dient ze een vraag in bij IT.

Na onderzoek ontdekken ze dat een beginnend IT-medewerker met contacten bij een misdaadorganisatie een senior medewerker heeft overgehaald om een USB Rubber Ducky in zijn apparaat te steken, waardoor het Basic Input/Output System (BIOS) wordt gedowngraded naar een kwetsbare versie en het systeem in gevaar komt.

Test uw kennis →

# Type aanval: Bedreiging van binnenuit

1: Het aanvalsoppervlak beperken — 2 — 3 — 4 — 5

De kwaadwillende insider heeft deze aanval uitgevoerd met behulp van twee methoden die worden gevolgd door het MITRE Adversarial Tactics, Techniques, and Common Knowledge-framework, ook wel MITRE ATT&CK genoemd. Wat zijn dit?

- [ ] Vertrouwde relatie + replicatie via verwisselbare media
- [ ] Social-engineering + replicatie via verwisselbare media
- [ ] Social-engineering + externe services
- [ ] Vertrouwde relatie + hardware-toevoegingen

Bekijk het juiste antwoord →

# Type aanval: Bedreiging van binnenuit

1: Het aanvalsoppervlak beperken — 2 — 3 — 4 — 5

De kwaadwillende insider heeft deze aanval uitgevoerd met behulp van twee methoden die worden gevolgd door het MITRE Adversarial Tactics, Techniques, and Common Knowledge-framework, ook wel MITRE ATT&CK genoemd. Wat zijn dit?

- ✗ Vertrouwde relatie + replicatie via verwisselbare media
- ✓ Social-engineering + replicatie via verwisselbare media
- ✗ Social-engineering + externe services
- ✗ Vertrouwde relatie + hardware-toevoegingen

Door zich te richten op MITRE ATT&CK-technieken voor zowel menselijke manipulatie als replicatie via draagbare opslagmedia, maakte de aanvaller gebruik van social-engineering om een senior medewerker te misleiden en een USB Rubber Ducky aan te sluiten, waardoor gecompromitteerde data via verwisselbare media werden geleverd.

Volgende vraag →

# Type aanval: Bedreiging van binnenuit

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4 — 5

## Waarom moest de aanvaller beide methoden gebruiken?

- [ ] Het netwerk binnengaan als algemene beheerder om het Basic Input/Output System (BIOS) te downgraden
- [ ] De beheerder phishen om het BIOS te kunnen downgraden
- [ ] De DNS-provider (Domain name System) van het apparaat wijzigen om referenties te verkrijgen die nodig zijn voor eenmalige netwerktoegang
- [ ] Malware op een apparaat installeren om referenties te verkrijgen die nodig zijn voor continue netwerktoegang

Bekijk het juiste antwoord →

# Type aanval: Bedreiging van binnenuit

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4 — 5

## Waarom moest de aanvaller beide methoden gebruiken?

- ✗ Het netwerk binnengaan als algemene beheerder om het Basic Input/Output System (BIOS) te downgraden
- ✗ De beheerder phishen om het BIOS te kunnen downgraden
- ✗ De DNS-provider (Domain name System) van het apparaat wijzigen om referenties te verkrijgen die nodig zijn voor eenmalige netwerktoegang
- ✓ Malware op een apparaat installeren om referenties te verkrijgen die nodig zijn voor continue netwerktoegang

De aanvaller moest beide methoden gebruiken (de installatie van malware via de USB Rubber Ducky om het apparaat te compromitteren en de inloggegevens om voortdurende toegang tot het netwerk mogelijk te maken) om blijvende, ongeautoriseerde controle over de doelomgeving te verkrijgen.

Volgende vraag →

# Type aanval: Bedreiging van binnenuit

1 2 3: Cyberbedreigingen detecteren en hierop reageren 4 5

Wat is een manier om onregelmatige netwerkactiviteit te detecteren?

- [ ] Applicatiebeheer
- [ ] Extended Detection and Response (XDR)
- [ ] Next-gen antivirus (NGAV)
- [ ] Geofencing van eindpunten

Bekijk het juiste antwoord →

# Type aanval: Bedreiging van binnenuit

1 — 2 — 3: Cyberbedreigingen detecteren en hierop reageren — 4 — 5

## Wat is een manier om onregelmatige netwerkactiviteit te detecteren?

- ✗ Applicatiebeheer
- ✓ Extended Detection and Response (XDR)
- ✗ Next-gen antivirus (NGAV)
- ✗ Geofencing van eindpunten

Als het gaat om het bieden van brede, gecorreleerde zichtbaarheid voor snelle detectie van bedreigingen, is XDR het beste voor het detecteren van verdachte netwerkactiviteiten, omdat het voortdurend de activiteit in eindpunten, netwerken en cloudomgevingen bewaakt en analyseert.

Volgende vraag →

# Type aanval: Bedreiging van binnenuit

1 2 3 4: Herstellen na een cyberaanval 5

Welke geïntegreerde pc-beveiliging kan verdachte activiteiten vroeg in de aanvalsketen detecteren?

- [ ] SIEM (Security Information and Event Management)
- [ ] Extended Detection and Response (XDR)
- [ ] Indicators of Attack (IOA)
- [ ] Op rollen gebaseerde toegangscontrole (RBAC)

Bekijk het juiste antwoord →

# Type aanval: Bedreiging van binnenuit

1 2 3 4: Herstellen na een cyberaanval 5

Welke geïntegreerde pc-beveiliging kan verdachte activiteiten vroeg in de aanvalsketen detecteren?

- ✗ SIEM (Security Information and Event Management)
- ✗ Extended Detection and Response (XDR)
- ✓ Indicators of Attack (IOA)
- ✗ Op rollen gebaseerde toegangscontrole (RBAC)

IOA richt zich op het detecteren van gedrag van aanvallers en verdachte activiteitspatronen wanneer deze zich voordoen, zodat beveiligingsteams bedreigingen eerder kunnen identificeren dan methoden op basis van handtekeningen en kunnen ingrijpen voordat er aanzienlijke schade optreedt.

Volgende vraag →

# Type aanval: Bedreiging van binnenuit

1 2 3 4 5: Algemene best practices

Welke maatregel kunt u nemen om te herstellen van soortgelijke toekomstige inbreuken en deze te voorkomen nadat u de initiële toegangsmethode hebt vastgesteld?

- [ ] BIOS bijwerken naar de nieuwste versie
- [ ] De optie voor BIOS-downgrade uitschakelen
- [ ] USB-poorten uitschakelen
- [ ] Granulaire controle implementeren om veilig gebruik van USB-apparaten mogelijk te maken en de verspreiding van malware te voorkomen
- [ ] Alle bovenstaande opties

Bekijk het juiste antwoord →

# Type aanval: Bedreiging van binnenuit

1 2 3 4 5: Algemene best practices

Welke maatregel kunt u nemen om te herstellen van soortgelijke toekomstige inbreuken en deze te voorkomen nadat u de initiële toegangsmethode hebt vastgesteld?

- [x] BIOS bijwerken naar de nieuwste versie
- [x] De optie voor BIOS-downgrade uitschakelen
- [x] USB-poorten uitschakelen
- [x] Granulaire controle implementeren om veilig gebruik van USB-apparaten mogelijk te maken en de verspreiding van malware te voorkomen
- [x] Alle bovenstaande opties

Door verschillende aanvalsvectoren aan te pakken om ervoor te zorgen dat hardware veilig is en downgrades worden geblokkeerd, kunnen USB-bedreigingen worden beheerst en wordt de verspreiding van malware op meerdere punten tegengehouden. Zo ontstaat een uitgebreide, gelaagde verdediging die getroffen systemen herstelt en beschermt tegen toekomstige inbreuken.

Bekijk oplossingen →

DELL Technologies

E-book interactieve scenario's voor cyberbeveiliging

TYPE AANVAL: BEDREIGING VAN BINNENUIT

# Samenvatting

Een aanval door een bedreiging van binnenuit vindt plaats wanneer iemand binnen een organisatie zijn toegang misbruikt om gegevens te compromitteren, activiteiten te verstoren of gevoelige informatie te stelen voor persoonlijke, financiële of concurrentiedoeleinden. Deze persoon kan een werknemer, aannemer, partner of iemand met legitieme toegang tot de systemen en netwerken van het bedrijf zijn.

Dell verdedigt tegen kwaadaardige cyberaanvallen van binnenuit door middel van een combinatie van geavanceerde technologieën en strikte beveiligingsprotocollen.

Kom meer te weten over geavanceerde strategieën voor cybertolerantie en hoe Dell u kan helpen uw organisatie te beschermen tegen schadelijke aanvallen van binnenuit.

Bekijk het rapport over bedreiging van binnenuit →

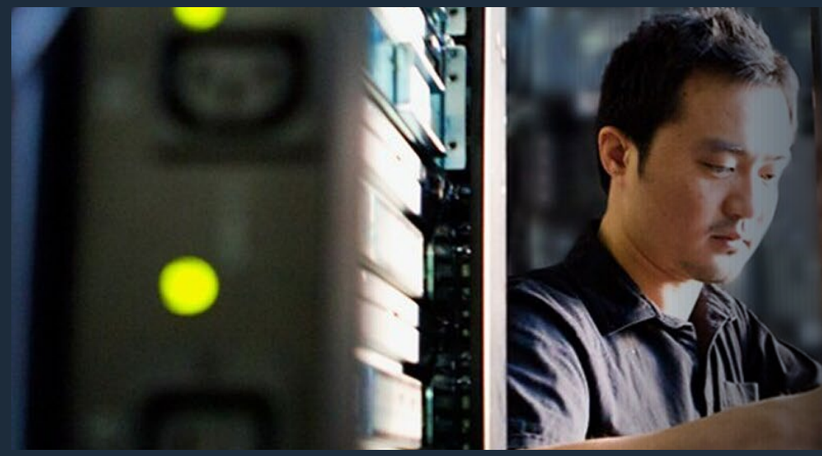
Terug naar scenario's

## Vertrouwde apparaten en infrastructuur ›

Geïntegreerde 'least privilege', meervoudige verificatie (MFA), op rollen gebaseerde toegangscontrole (RBAC), dubbele authenticatie en Zero Trust-beveiliging beschermen eindpunten en infrastructuur, waardoor de risico's op bedreigingen van binnenuit worden verminderd.

## PowerEdge Servers ›

Hardware root of trust, veilig opstarten, dynamisch USB-poortbeheer en systeemvergrendeling beschermen tegen manipulatie en stoppen fysieke of op firmware gebaseerde aanvallen van binnenuit.



## PowerProtect portfolio›

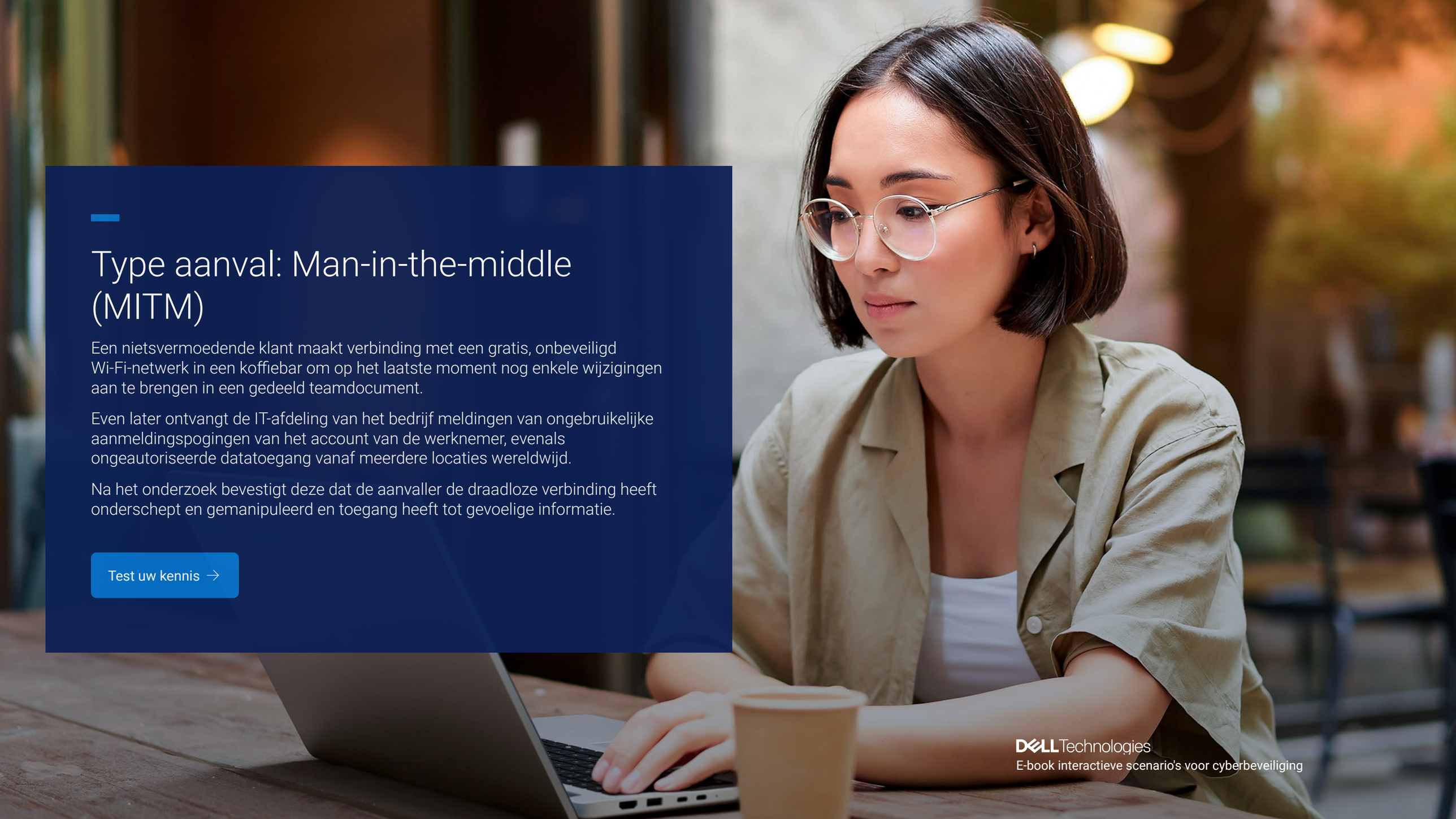
Onveranderlijke, geïsoleerde back-ups zorgen voor data-integriteit, snel herstel en vroege detectie van pogingen tot datamanipulatie, waardoor herstel na incidenten door insiders mogelijk wordt.

## Services voor beveiliging en veerkracht›

Deskundige training, penetratietests, het opsporen van bedreigingen, incidentrespons en herstelservices na inbreuken versterken de paraatheid en veerkracht tegen door insiders aangestuurde gebeurtenissen.

## Beveiligingspartners ›

Geïntegreerde endpointdetectie en -respons (EDR), uitgebreide detectie en respons (XDR) en geautomatiseerde Threat Intelligence identificeren, beperken en verminderen complexe interne dreigingen in realtime.



# Type aanval: Man-in-the-middle (MITM)

Een nietsvermoedende klant maakt verbinding met een gratis, onbeveiligd Wi-Fi-netwerk in een koffiebar om op het laatste moment nog enkele wijzigingen aan te brengen in een gedeeld teamdocument.

Even later ontvangt de IT-afdeling van het bedrijf meldingen van ongebruikelijke aanmeldingspogingen van het account van de werknemer, evenals ongeautoriseerde datatoegang vanaf meerdere locaties wereldwijd.

Na het onderzoek bevestigt deze dat de aanvaller de draadloze verbinding heeft onderschept en gemanipuleerd en toegang heeft tot gevoelige informatie.

Test uw kennis →

# Type aanval: Man-in-the-middle (MITM)

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

\Wat is de eerste plaats die het IT-team moet onderzoeken nadat het ongebruikelijke inlogpogingen heeft gedetecteerd?

- [ ] Firewall, inbraakdetectiesysteem (IDS), logboeken van inbraakpreventiesysteem (IPS) en uitgebreide detectierespons (XDR)
- [ ] De laptop van de betreffende werknemer
- [ ] Netwerkverkeer op de onbeveiligde Wi-Fi van de koffiebar
- [ ] Verificatielogboeken van de systemen van het bedrijf

Bekijk het juiste antwoord →

# Type aanval: Man-in-the-middle (MITM)

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

\Wat is de eerste plaats die het IT-team moet onderzoeken nadat het ongebruikelijke inlogpogingen heeft gedetecteerd?

- ✓ Firewall, inbraakdetectiesysteem (IDS), logboeken van inbraakpreventiesysteem (IPS) en uitgebreide detectierespons (XDR)
- ✗ De laptop van de betreffende werknemer
- ✗ Netwerkverkeer op de onbeveiligde Wi-Fi van de koffiebar
- ✓ Verificatielogboeken van de systemen van het bedrijf

Door deze firewall- en IDS/IPS- en authenticatielogboeken te analyseren, kunnen IT-teams ongeautoriseerde toegangspogingen traceren, gecompromitteerde accounts beoordelen en een beter inzicht krijgen in de omvang van het incident.

Volgende vraag →

# Type aanval: Man-in-the-middle (MITM)

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Welke onmiddellijke actie moet het IT-team ondernemen na bevestiging van de MITM-aanval?

- [ ] Het apparaat van de gecompromitteerde werknemer onmiddellijk loskoppelen van het netwerk en isoleren voor analyse
- [ ] Firewallregels en netwerkconfiguraties bijwerken om verdere onbevoegde toegang te stoppen
- [ ] Wachtwoorden opnieuw instellen voor alle werknemersaccounts
- [ ] Getroffen systemen uitschakelen om data-exfiltratie te voorkomen

Bekijk het juiste antwoord →

# Type aanval: Man-in-the-middle (MITM)

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

## Welke onmiddellijke actie moet het IT-team ondernemen na bevestiging van de MITM-aanval?

- ✓ Het apparaat van de gecompromitteerde werknemer onmiddellijk loskoppelen van het netwerk en isoleren voor analyse
- ✓ Firewallregels en netwerkconfiguraties bijwerken om verdere onbevoegde toegang te stoppen
- ✗ Wachtwoorden opnieuw instellen voor alle werknemersaccounts
- ✗ Getroffen systemen uitschakelen om data-exfiltratie te voorkomen

Het onmiddellijk loskoppelen en isoleren van het gecompromitteerde apparaat stopt de toegang van de aanvaller en behoudt forensisch bewijs, terwijl het bijwerken van firewall- en netwerkregels verdere schadelijke verbindingen blokkeert en het bredere netwerk beschermt tegen voortdurende inbreuken.

Volgende vraag →

# Type aanval: Man-in-the-middle (MITM)

1 — 2 — 3: Herstellen na een cyberaanval — 4

Welke preventieve maatregelen hadden de kwetsbaarheid voor de MITM-aanval kunnen verminderen?

- [ ] Get gebruik van Virtual Private Network (VPN) afdwingen voor alle werknemers
- [ ] Zero Trust-beveiligingsprincipes implementeren zoals meervoudige verificatie (MFA)
- [ ] Openbare Wi-Fi vermijden
- [ ] Gevoelige bestanden versleutelen die via e-mail worden gedeeld

Bekijk het juiste antwoord →

# Type aanval: Man-in-the-middle (MITM)

1 — 2 — 3: Herstellen na een cyberaanval — 4

## Welke preventieve maatregelen hadden de kwetsbaarheid voor de MITM-aanval kunnen verminderen?

- [x] Get gebruik van Virtual Private Network (VPN) afdwingen voor alle werknemers
- [x] Zero Trust-beveiligingsprincipes implementeren zoals meervoudige verificatie (MFA)
- [ ] Openbare Wi-Fi vermijden
- [ ] Gevoelige bestanden versleutelen die via e-mail worden gedeeld

Door VPN-gebruik op onbeveiligde netwerken af te dwingen, wordt het internetverkeer van werknemers versleuteld om onderschepping te voorkomen, terwijl Zero-Trust-beveiliging en MFA ervoor zorgen dat elk toegangsverzoek continu wordt geverifieerd.

Volgende vraag →

# Type aanval: Man-in-the-middle (MITM)

1 — 2 — 3 — 4: Algemene best practices

Welke langetermijnstrategieën moet uw organisatie implementeren na het aanpakken van de inbreuk?

- [ ] Systemen regelmatig controleren en patchen
- [ ] De netwerksegmentatie verhogen om gevoelige data en systemen te isoleren
- [ ] Endpoint Detection and Response- (EDR) en Managed Detection and Response (MDR)-oplossingen implementeren
- [ ] Robuuste en regelmatige training voor werknemers implementeren
- [ ] Alle bovenstaande opties

Bekijk het juiste antwoord →

# Type aanval: Man-in-the-middle (MITM)

1 — 2 — 3 — 4: Algemene best practices

## Welke langetermijnstrategieën moet uw organisatie implementeren na het aanpakken van de inbreuk?

- [x] Systemen regelmatig controleren en patchen
- [x] De netwerksegmentatie verhogen om gevoelige data en systemen te isoleren
- [x] Endpoint Detection and Response- (EDR) en Managed Detection and Response (MDR)-oplossingen implementeren
- [x] Robuuste en regelmatige training voor werknemers implementeren
- [x] Alle bovenstaande opties

Om bescherming te bieden tegen verschillende bedreigingen, vormen deze langetermijnstrategieën samen een uitgebreide, veerkrachtige beveiligingsmentaliteit die aanvallers verhindert om misbruik te maken van zwakke plekken en zorgt voor een snelle, effectieve reactie op inbreuken.

Bekijk oplossingen →

TYPE AANVAL: MAN-IN-THE-MIDDLE (MITM)

# Samenvatting

Een Man-in-the-Middle-aanval (MITM) vindt plaats wanneer een cybercrimineel in het geheim communicatie tussen twee partijen onderschept, zoals tussen een werknemer en een bedrijfsserver of een klant en een bedrijfswebsite. Het doel van de aanvaller kan variëren, maar het resultaat is hetzelfde: een inbreuk op vertrouwen en beveiliging.

Bij Dell leveren we innovatieve, schaalbare beveiligingsoplossingen, waarmee organisaties MITM-bedreigingen kunnen neutraliseren, assets kunnen beschermen en de bedrijfsintegriteit kunnen behouden met de tools en expertise die nodig zijn om vol vertrouwen te detecteren, erop te reageren en te herstellen.

Lees meer over geavanceerde strategieën voor cybertolerantie en ontdek hoe Dell u kan helpen uw organisatie te beschermen tegen MITM-aanvallen.

Lees het rapport over MITM-aanvallen →

Terug naar scenario's

## Vertrouwde apparaten ›

Met hardwareverificatie, firmwarebeveiliging zoals SafeBIOS en SafeID, robuuste versleuteling en Zero Trust-frameworks beveiligt Dell eindpunten en data in transit.

## PowerEdge Servers ›

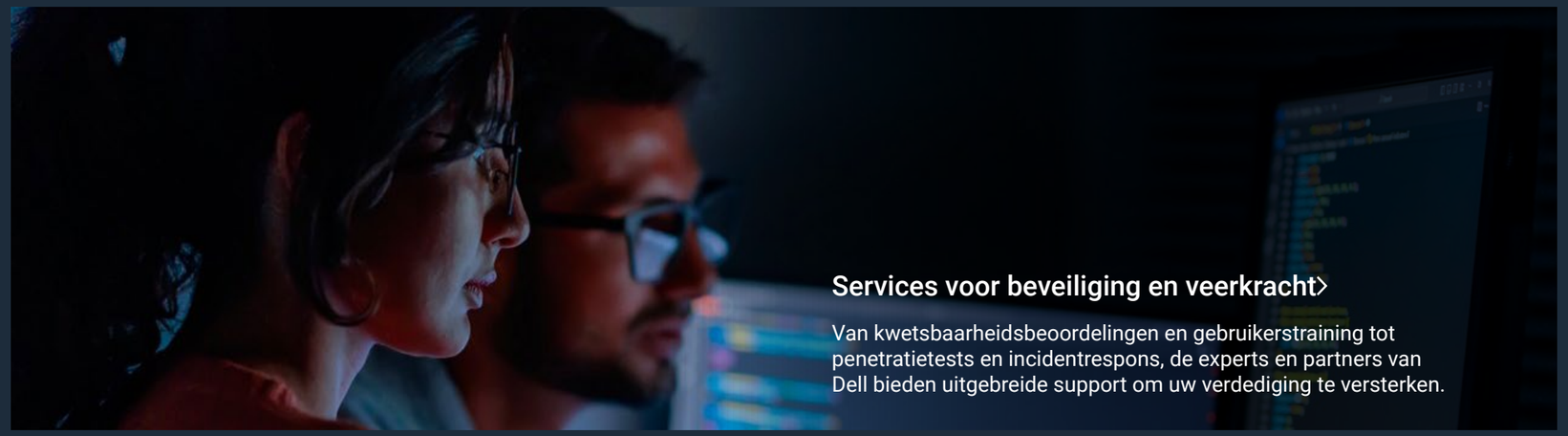
Veilig opstarten, Silicon root of trust, dynamisch USB-poortbeheer en systeemvergrendeling zorgen voor hardware-integriteit en beschermen kritieke workloads tegen netwerkbedreigingen.

## Storageoplossingen ›

Versleutelde inactieve data en data tijdens verzending, in combinatie met geïsoleerde snapshots en snelle herstelfuncties, zorgen ervoor dat bestanden veilig blijven en snel kunnen worden hersteld na een MITM-aanval.

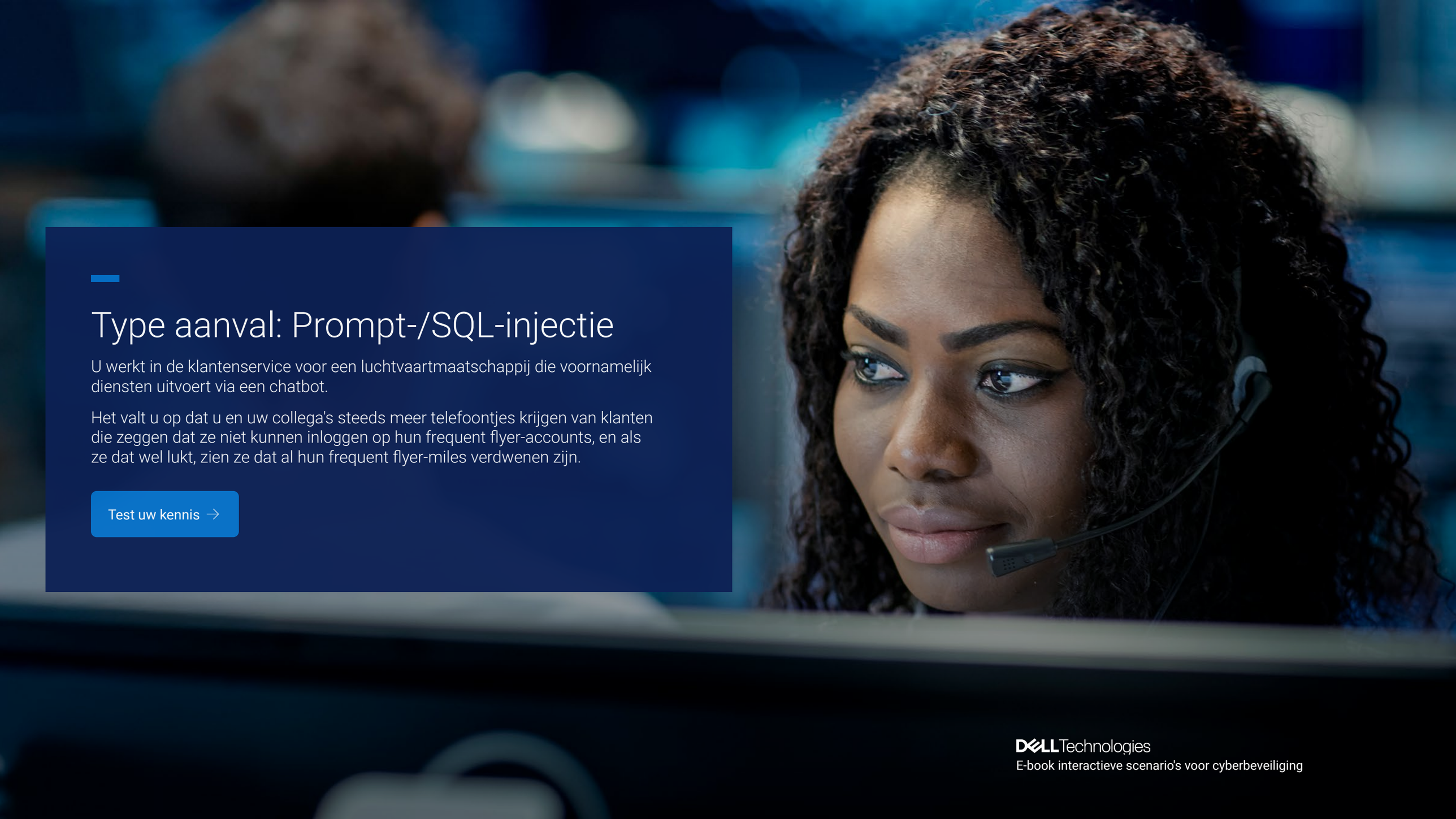
## PowerProtect portfolio›

Onveranderlijke, geïsoleerde back-ups en AI-gestuurde CyberSense analytics maken snel herstel en betrouwbaar dataherstel mogelijk in het geval van een MITM-aanval.



## Services voor beveiliging en veerkracht›

Van kwetsbaarheidsbeoordelingen en gebruikerstraining tot penetratietests en incidentrespons, de experts en partners van Dell bieden uitgebreide support om uw verdediging te versterken.



# Type aanval: Prompt-/SQL-injectie

U werkt in de klantenservice voor een luchtvaartmaatschappij die voornamelijk diensten uitvoert via een chatbot.

Het valt u op dat u en uw collega's steeds meer telefoontjes krijgen van klanten die zeggen dat ze niet kunnen inloggen op hun frequent flyer-accounts, en als ze dat wel lukt, zien ze dat al hun frequent flyer-miles verdwenen zijn.

Test uw kennis →

# Type aanval: Prompt-/SQL-injectie

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Na onderzoek ziet u enkele fouten in de logboeken: *Syntaxisfout in de SQL-instructie (Structured Query Language) of Ongeldige kolomnaam 'admin'*. Welk type cyberincident is dit?

- [ ] Gestolen inloggegevens
- [ ] Prompt- of SQL-injectie
- [ ] Man-in-the-Middle-aanval (MITM)
- [ ] Phishing

Bekijk het juiste antwoord →

DELL Technologies
E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Prompt-/SQL-injectie

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Na onderzoek ziet u enkele fouten in de logboeken: *Syntaxisfout in de SQL-instructie (Structured Query Language)* of *Ongeldige kolomnaam 'admin'*. Welk type cyberincident is dit?

- ✗ Gestolen inloggegevens
- ✓ Prompt- of SQL-injectie
- ✗ Man-in-the-Middle-aanval (MITM)
- ✗ Phishing

'Prompt- of SQL-injectie' is correct omdat logfouten zoals "Syntaxisfout in SQL-instructie" of "Ongeldige kolomnaam 'admin'" aantonen dat aanvallers de invoervelden van de chatbot hebben misbruikt met kwaadaardige SQL-code om toegang te krijgen tot klantaccountgegevens of deze te wijzigen. Dit zijn duidelijke technische indicatoren van een SQL-injectieaanval die overeenkomt met de beschreven verdachte activiteit.

Volgende vraag →

# Type aanval: Prompt-/SQL-injectie

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

U realiseert zich dat u bent getroffen door een prompt/SQL-injectie via uw klantenservicechatbot. Wat moet u doen?

- [ ] De bot offline halen
- [ ] Database-logboeken onderzoeken op ongeautoriseerde toegang en gestolen, gewijzigde of verwijderde data
- [ ] Voldoen aan alle wetten voor openbaarmaking van datalekken
- [ ] Alle bovenstaande opties

Bekijk het juiste antwoord →

# Type aanval: Prompt-/SQL-injectie

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

U realiseert zich dat u bent getroffen door een prompt/SQL-injectie via uw klantenservicechatbot. Wat moet u doen?

- [x] De bot offline halen
- [x] Database-logboeken onderzoeken op ongeautoriseerde toegang en gestolen, gewijzigde of verwijderde data
- [x] Voldoen aan alle wetten voor openbaarmaking van datalekken
- [x] Alle bovenstaande opties

Om te reageren op een prompt-/SQL-injectieaanval moet de chatbot offline worden gehaald, moeten de databaselogboeken worden onderzocht op ongeautoriseerde toegang en moet worden gezorgd voor naleving van de wetgeving inzake openbaarmaking. Deze stappen zijn essentieel om misbruik te stoppen, schade te beoordelen en te voldoen aan wettelijke en ethische verplichtingen.

Volgende vraag →

# Type aanval: Prompt-/SQL-injectie

1 2 3: Herstellen na een cyberaanval 4

## Welke maatregelen moet u nemen om Prompt-/SQL-injecties te voorkomen?

- [ ] De ontwikkelingsteams instrueren om voorbereide uitspraken en geparametriseerde query's als coderingspraktijk te gebruiken
- [ ] Managed Detection and Response (MDR)-tools
- [ ] Toegang implementeren met minimale bevoegdheden, zoals meervoudige verificatie (MFA), op rollen gebaseerde toegangscontrole (RBAC), firewall voor webapplicaties (WAF), enz.
- [ ] Back-enddatabases/knowledge bases segmenteren

Bekijk het juiste antwoord →

# Type aanval: Prompt-/SQL-injectie

1 — 2 — 3: Herstellen na een cyberaanval — 4

## Welke maatregelen moet u nemen om Prompt-/SQL-injecties te voorkomen?

- ✓ De ontwikkelingsteams instrueren om voorbereide uitspraken en geparametriseerde query's als coderingspraktijk te gebruiken
- ✗ Managed Detection and Response (MDR)-tools
- ✓ Toegang implementeren met minimale bevoegdheden, zoals meervoudige verificatie (MFA), op rollen gebaseerde toegangscontrole (RBAC), firewall voor webapplicaties (WAF), enz.
- ✗ Back-enddatabases/knowledge bases segmenteren

Door ontwikkelingsteams te trainen in het gebruik van voorbereide instructies en geparametriseerde query's worden SQL-injectieaanvallen bij de bron geblokkeerd, terwijl het afdwingen van toegangsbeperkingen met minimale rechten, zoals MFA, RBAC en WAF, de impact van pogingen tot injectie beperkt door te voorkomen dat aanvallers hun rechten kunnen uitbreiden of zich lateraal kunnen verplaatsen.

Volgende vraag →

# Type aanval: Prompt-/SQL-injectie

1 2 3 4: Algemene best practices

Welke stappen zou u nemen om de klantdata van de luchtvaartmaatschappij terug te krijgen?

- [ ] De gestolen data opsporen
- [ ] Klanten hun profielen opnieuw laten opbouwen
- [ ] De data terugkopen van de cyberaanvallers
- [ ] Herstellen vanaf de meest recente onbeschadigde back-up om frequent flyer-miles te herstellen en klanten te informeren dat ze hun wachtwoorden moeten wijzigen en hun creditcards moeten controleren

Bekijk het juiste antwoord →

# Type aanval: Prompt-/SQL-injectie

1 — 2 — 3 — 4: Algemene best practices

Welke stappen zou u nemen om de klantdata van de luchtvaartmaatschappij terug te krijgen?

- ✗ De gestolen data opsporen
- ✗ Klanten hun profielen opnieuw laten opbouwen
- ✗ De data terugkopen van de cyberaanvallers
- ✓ Herstellen vanaf de meest recente onbeschadigde back-up om frequent flyer-miles te herstellen en klanten te informeren dat ze hun wachtwoorden moeten wijzigen en hun creditcards moeten controleren

Het herstellen van verloren accountdata uit de nieuwste compromisloze back-up helpt de data-integriteit te behouden en downtime te verminderen. Door klanten onmiddellijk te verzoeken hun wachtwoorden te resetten en hun creditcardactiviteiten in de gaten te houden, wordt de naleving van de regelgeving na een destructieve injectieaanval verder ondersteund.

Bekijk oplossingen →

TYPE AANVAL: PROMPT-/SQL-INJECTIE

# Samenvatting

Prompt- en SQL-injectieaanvallen hebben herhaaldelijk bewezen tot de schadelijkste en meest wijdverbreide methoden van cyberaanvallen te behoren die door cybercriminelen worden gebruikt. Deze aanvallen maken misbruik van beveiligingslekken in gebruikersquery- of databasesystemen, waardoor kwaadwillenden servers kunnen manipuleren, data kunnen stelen en workflows kunnen verstoren.

Het beschermen van uw organisatie tegen steeds veranderende Prompt-/SQL-injectiedreigingen en -aanvallen maakt deel uit van het voortdurende streven van Dell naar cyberbeveiliging. Wij bieden de tools en expertise die nodig zijn voor detectie, respons en herstel.

Ontdek geavanceerde strategieën voor cybertolerantie en ontdek hoe Dell uw organisatie in staat kan stellen zich te verdedigen tegen prompt- en SQL-injectieaanvallen.

Bekijk het rapport over prompt/SQL-injectie →

Terug naar scenario's

## Vertrouwde werkruimte en vertrouwde infrastructuur ›

Beveiligt eindpunten en vermindert het risico dat gecompromitteerde inloggegevens worden misbruikt bij injectieaanvallen.

## PowerEdge Servers ›

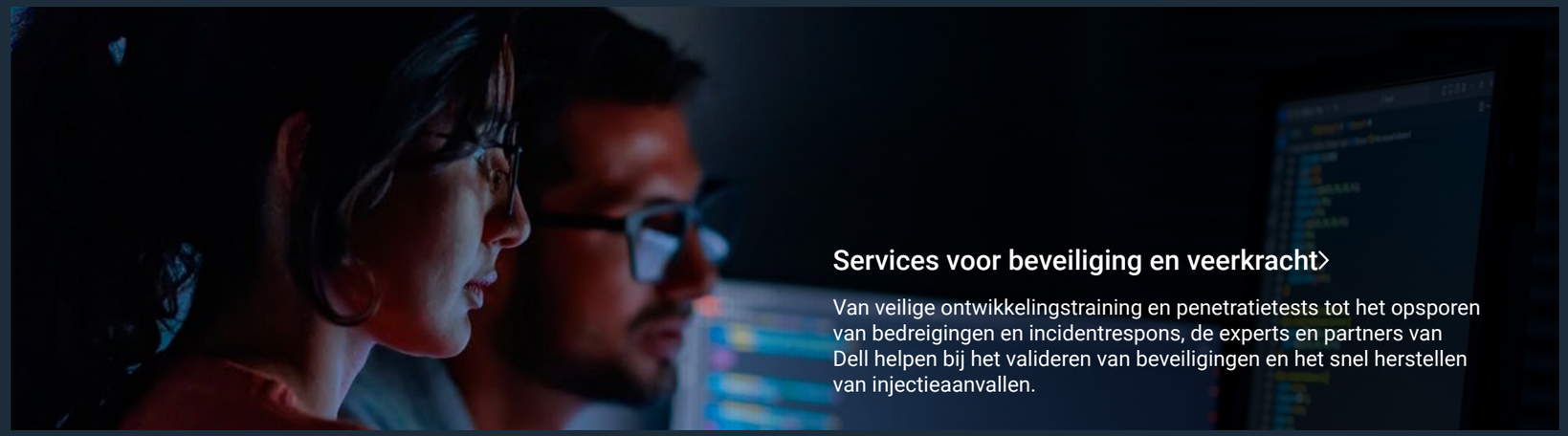
Met hardware root of trust, secure boot, silicon-based beveiliging en realtime configuratievalidatie zorgen Dell PowerEdge servers voor een fraudebestendige infrastructuur waarop alleen vertrouwde code wordt uitgevoerd.

## Beveiligingspartners ›

Met fijnmazige toegangscontrole, geavanceerde Threat Intelligence en externe detectie en respons helpen Dell Security Partners bij het identificeren en beperken van SQL- en prompt-injectiepogingen.

## PowerProtect portfolio›

De onveranderlijke, air-gapped back-ups en geavanceerde Cyber Recovery-analyses van Dell bieden vertrouwde herstelpunten, waardoor snel herstel na databeschadiging of -exfiltratie mogelijk is.



## Services voor beveiliging en veerkracht›

Van veilige ontwikkelingstraining en penetratietests tot het opsporen van bedreigingen en incidentrespons, de experts en partners van Dell helpen bij het valideren van beveiligingen en het snel herstellen van injectieaanvallen.

# Type aanval: Ransomware

U bent IT-professional in een regionaal ziekenhuis dat bekend staat om zijn gekoppelde medische systemen, waaronder elektronische patiëntendossiers (EPD's), slimme infuuspompen en radiologiebeelden die allemaal zijn aangesloten op een gecentraliseerd netwerk.

Gisteravond begonnen verschillende systemen tegelijk te crashen. 's Ochtends melden klinische medewerkers dat ze geen toegang meer hebben tot patiëntendossiers.

De volgende losgeldeis verschijnt op verschillende terminals:

"Uw bestanden zijn versleuteld. Betaal 20 Bitcoin binnen 72 uur of patiëntgegevens worden vrijgegeven."

Test uw kennis →

# Type aanval: Ransomware

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

De helpdesk ontvangt meer dan 100 rapporten over bestandsversleuteling en applicatiefouten. Beveiligingslogboeken tonen ongebruikelijke bestandshernoemingsactiviteit van een intern domeinaccount. Wat is uw eerste stap?

- [ ] Onmiddellijk het losgeld betalen om kritieke services te herstellen
- [ ] De politie en de juridische adviseur informeren
- [ ] Alle getroffen eindpunten opnieuw imagen
- [ ] Geïnfecteerde systemen loskoppelen van het netwerk

Bekijk het juiste antwoord →

# Type aanval: Ransomware

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

De helpdesk ontvangt meer dan 100 rapporten over bestandsversleuteling en applicatiefouten. Beveiligingslogboeken tonen ongebruikelijke bestandshernoemingsactiviteit van een intern domeinaccount. Wat is uw eerste stap?

- ✗ Onmiddellijk het losgeld betalen om kritieke services te herstellen
- ✗ De politie en de juridische adviseur informeren
- ✗ Alle getroffen eindpunten opnieuw imagen
- ✓ Geïnfecteerde systemen loskoppelen van het netwerk

Door geïnfecteerde ziekenhuissystemen onmiddellijk los te koppelen en te isoleren, wordt verspreiding van ransomware tegengegaan, worden kritieke medische apparatuur en gevoelige patiëntgegevens beschermd, blijft bewijsmateriaal voor onderzoek bewaard en wordt kostbare tijd gewonnen voor een gecoördineerde reactie en herstel.

Volgende vraag →

# Type aanval: Ransomware

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Het incident Response-team ontdekt dat de aanval waarschijnlijk begon vanaf een gecompromitteerd account dat werd gebruikt om toegang te krijgen tot een server zonder meervoudige authenticatie (MFA). Welke van de volgende factoren heeft het meest direct bijgedragen aan de aanval?

- [ ] Verouderde antivirusdefinities
- [ ] Een blootgestelde database voor elektronische medische dossiers (EHR)
- [ ] Gebrek aan MFA bij externe toegang
- [ ] Zwak e-mailfilter

Bekijk het juiste antwoord →

# Type aanval: Ransomware

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Het incident Response-team ontdekt dat de aanval waarschijnlijk begon vanaf een gecompromitteerd account dat werd gebruikt om toegang te krijgen tot een server zonder meervoudige authenticatie (MFA). Welke van de volgende factoren heeft het meest direct bijgedragen aan de aanval?

- ✗ Verouderde antivirusdefinities
- ✗ Een blootgestelde database voor elektronische medische dossiers (EHR)
- ✓ Gebrek aan MFA bij externe toegang
- ✗ Zwak e-mailfilter

Het ontbreken van MFA bij externe toegang maakte de serverinbraak mogelijk doordat aanvallers konden inloggen met gestolen of geraden inloggegevens zonder een extra verificatiestap. Met MFA is zelfs voor gehackte accounts een tweede factor vereist, waardoor het risico op ongeautoriseerde toegang drastisch wordt verminderd.

Volgende vraag →

# Type aanval: Ransomware

1 — 2 — 3: Herstellen na een cyberaanval — 4

Medisch personeel vertrouwt nu op papieren workflows. Patiënten die vandaag voor een operatie zijn ingepland, kunnen niet in het systeem worden geverifieerd. Wat is de beste kortetermijnactie ter ondersteuning van ziekenhuisactiviteiten?

- [ ] De basisdatabaseserver opnieuw opstarten om opnieuw te initialiseren
- [ ] Alle oude back-ups inschakelen, zelfs als ze zes maanden oud zijn
- [ ] De handmatige downtime-procedures van het ziekenhuis activeren en escaleren naar het noodhulpteam
- [ ] Het personeel per geval laten beslissen hoe het verder gaat

Bekijk het juiste antwoord →

# Type aanval: Ransomware

1 — 2 — 3: Herstellen na een cyberaanval — 4

Medisch personeel vertrouwt nu op papieren workflows. Patiënten die vandaag voor een operatie zijn ingepland, kunnen niet in het systeem worden geverifieerd. Wat is de beste kortetermijnactie ter ondersteuning van ziekenhuisactiviteiten?

- ✗ De basisdatabaseserver opnieuw opstarten om opnieuw te initialiseren
- ✗ Alle oude back-ups inschakelen, zelfs als ze zes maanden oud zijn
- ✓ De handmatige downtime-procedures van het ziekenhuis activeren en escaleren naar het noodhulpteam
- ✗ Het personeel per geval laten beslissen hoe het verder gaat

Door handmatige downtime-procedures te activeren en het noodhulpteam in te schakelen, wordt de onmiddellijke continuïteit van kritieke klinische workflows gewaarborgd, wordt de veiligheid van patiënten gewaarborgd en wordt een gestandaardiseerd proces voor het verifiëren en documenteren van zorg ingesteld. Deze aanpak minimaliseert fouten, beheert risico's en resources efficiënt en ondersteunt specialisten bij het veilig herstellen van digitale systemen.

Volgende vraag →

# Type aanval: Ransomware

1 2 3 4: Algemene best practices

De lokale media hebben het verhaal opgepikt. Het management wil weten of ze een openbare verklaring moeten afgeven, en de juridische afdeling vraagt naar de verplichtingen op grond van de Health Insurance Portability and Accountability Act (HIPAA). Wat is de meest geschikte volgende stap?

- [ ] Het incident openbaar ontkennen totdat er meer informatie beschikbaar is
- [ ] Een persbericht publiceren waarin de externe IT-leverancier wordt beschuldigd
- [ ] Regelgevers op de hoogte stellen en interne meldingsprocedures voor inbreuken starten
- [ ] Onmiddellijk het losgeld betalen en publieke aandacht vermijden

Bekijk het juiste antwoord →

# Type aanval: Ransomware

1 2 3 4: Algemene best practices

De lokale media hebben het verhaal opgepikt. Het management wil weten of ze een openbare verklaring moeten afgeven, en de juridische afdeling vraagt naar de verplichtingen op grond van de Health Insurance Portability and Accountability Act (HIPAA). Wat is de meest geschikte volgende stap?

- ✗ Het incident openbaar ontkennen totdat er meer informatie beschikbaar is
- ✗ Een persbericht publiceren waarin de externe IT-leverancier wordt beschuldigd
- ✓ Regelgevers op de hoogte stellen en interne meldingsprocedures voor inbreuken starten
- ✗ Onmiddellijk het losgeld betalen en publieke aandacht vermijden

Het onmiddellijk melden van inbreuken op beschermde gezondheidsinformatie aan autoriteiten en betrokken personen, zoals vereist door HIPAA en staatswetten, zorgt voor naleving van de regelgeving, juridische bescherming en transparantie volgens de beste praktijken om juridische schade en reputatieschade te voorkomen, verplichte openbaarmakingsverplichtingen na te komen en goede communicatie met patiënten, personeel en belanghebbenden tot stand te brengen.

Bekijk oplossingen →

TYPE AANVAL: RANSOMWARE

# Samenvatting

Ransomware is een type schadelijke software (malware) die de toegang tot een computersysteem of data blokkeert totdat er losgeld wordt betaald. Het is een van de meest verstorende soorten cyberaanvallen. Vijftig procent van de organisaties wereldwijd is in het afgelopen jaar ten minste één keer getroffen door ransomware en de gemiddelde downtime na een ransomware-aanval is drie weken, wat leidt tot aanzienlijke operationele onderbrekingen.

Bij Dell geven we prioriteit aan het beschermen van uw organisatie met Zero Trust-frameworks, eindpuntbescherming en netwerksegmentatie om de toegang tot ransomware te blokkeren en de verspreiding ervan te beperken. Met deskundige incidentresplanning helpen we u veerkrachtig te blijven en snel te herstellen van aanvallen.

Kom meer te weten over geavanceerde strategieën voor cybertolerantie en hoe Dell u kan helpen uw organisatie te beschermen tegen ransomware-aanvallen.

Bekijk het rapport over ransomware-aanvallen →

Terug naar scenario's

## Vertrouwde infrastructuur ›

Blokkeer ransomware op infrastructuurniveau met hardwareverificatie, meervoudige verificatie (MFA), op rollen gebaseerde toegangscontrole (RBAC) en Zero Trust-frameworks.

## Netwerken en PowerEdge servers ›

Beperk de verspreiding van ransomware. Met netwerksegmentatie, veilig opstarten, Silicon root of trust, dynamisch USB-poortbeheer en systeemvergrendeling.

## Vertrouwde werkruimte ›

Integreer tools voor SafeBIOS, SafeID, SafeData en Endpoint Detection and Response (EDR) om proactieve dreigingsinformatie, realtime detectie en geautomatiseerde malwarebeheersing op apparaatniveau te leveren.

## PowerProtect portfolio›

Bescherm kritieke data met onwijzigbare, air-gapped back-ups, intelligente Cyber Recovery-analyses en snelle herstelmogelijkheden om afpersing te voorkomen en veerkracht mogelijk te maken.

## Services voor beveiliging en veerkracht›

Werk samen met experts zoals CrowdStrike om te helpen bij beoordelingen, kwetsbaarheidsbeheer, training in beveiligingsbewustzijn, penetratietests en incidentrespons.

# Type aanval: Hardware voor de leveringsketen

Uw bedrijf implementeert 500 nieuwe laptops in haar wereldwijde kantoren. Om het proces te versnellen, hebt u de imaging en hardwarevoorbereiding uitbesteed aan een externe IT-logistieke leverancier. Deze verzendt vooraf geconfigureerde machines rechtstreeks naar werknemers.

Binnen een paar dagen ontvangt u verschillende oproepen vanuit het veld met de vermelding:

- Verzoeken om meervoudige authenticatie (MFA) worden omzeild en werken niet goed.
- Het beveiligingsteam ziet een aantal ongeautoriseerde beheerdersaanmeldingen op ongebruikelijke tijdstippen.
- Ze zien ook VPN-verkeer (Virtual Private Network) van gebruikers die zogenaamd offline zijn.

Test uw kennis →

# Type aanval: Hardware voor de leveringsketen

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Een werknemer meldt dat push-meldingen voor meervoudige authenticatie (MFA) worden ontvangen terwijl deze niet hebben geprobeerd zich aan te melden. Het beveiligingsdashboard van uw organisatie toont dat de aanmelding afkomstig is van een apparaat met een door het bedrijf uitgegeven asset-tag. Wat is de meest logische eerste stap voor het SOC-team (Security Operations Center)?

- [ ] Het account van de gebruiker uitschakelen en de laptop op afstand wissen
- [ ] De aanmeldings-IP en vingerafdruk van het apparaat vergelijken met andere bekende gecompromitteerde gebruikers
- [ ] Escaleren naar HR, ervan uitgaande dat de gebruiker in gebreke is gebleven
- [ ] Een bedrijfsbrede waarschuwing uitgeven om wachtwoorden onmiddellijk te wijzigen

Bekijk het juiste antwoord →

# Type aanval: Hardware voor de leveringsketen

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Een werknemer meldt dat push-meldingen voor meervoudige authenticatie (MFA) worden ontvangen terwijl deze niet hebben geprobeerd zich aan te melden. Het beveiligingsdashboard van uw organisatie toont dat de aanmelding afkomstig is van een apparaat met een door het bedrijf uitgegeven asset-tag. Wat is de meest logische eerste stap voor het SOC-team (Security Operations Center)?

- ✗ Het account van de gebruiker uitschakelen en de laptop op afstand wissen
- ✓ De aanmeldings-IP en vingerafdruk van het apparaat vergelijken met andere bekende gecompromitteerde gebruikers
- ✗ Escaleren naar HR, ervan uitgaande dat de gebruiker in gebreke is gebleven
- ✗ Een bedrijfsbrede waarschuwing uitgeven om wachtwoorden onmiddellijk te wijzigen

Wanneer uw SOC-team vaststelt of verdachte activiteiten deel uitmaken van een bredere aanval of een op zichzelf staande aanval, is gerichte incidentrespons en het beperken van verdere risico's de logische eerste stap bij het identificeren van een aanval op de hardware van de toeleveringsketen, zodat snel patronen kunnen worden herkend.

Volgende vraag →

# Type aanval: Hardware voor de leveringsketen

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Uw incidentresponsteam constateert dat meerdere getroffen laptops SSD-firmwareversies hebben die niet overeenkomen met de officiële releaseopmerkingen van de leverancier. Endpoint Detection Response (EDR) toont geen schadelijke processen. Wat geeft dit waarschijnlijk aan?

- [ ] Een configuratiefout van de IT-leverancier
- [ ] Een nieuw type ransomware dat zichzelf verwijdert
- [ ] Een inbreuk op de leveringsketen op firmwareniveau
- [ ] Normaal gedrag tijdens imaging

Bekijk het juiste antwoord →

# Type aanval: Hardware voor de leveringsketen

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Uw incidentresponsteam constateert dat meerdere getroffen laptops SSD-firmwareversies hebben die niet overeenkomen met de officiële releaseopmerkingen van de leverancier. Endpoint Detection Response (EDR) toont geen schadelijke processen. Wat geeft dit waarschijnlijk aan?

- ✗ Een configuratiefout van de IT-leverancier
- ✗ Een nieuw type ransomware dat zichzelf verwijdert
- ✓ Een inbreuk op de leveringsketen op firmwareniveau
- ✗ Normaal gedrag tijdens imaging

Ongeautoriseerde SSD-firmware op meerdere laptops, die niet door EDR wordt gedetecteerd en niet overeenkomt met officiële releases, duidt op opzettelijke manipulatie van hardware of firmware: een kenmerk van een inbreuk op de toeleveringsketen op firmwareniveau.

Volgende vraag →

# Type aanval: Hardware voor de leveringsketen

1 — 2 — 3: Herstellen na een cyberaanval — 4

U hebt 100 verdachte apparaten geïsoleerd met kwaadaardige SSD-firmware. U moet beslissen hoe u verder wilt gaan zonder de aanvaller, die mogelijk op externe toegang heeft, te alarmeren. Wat is de beste volgende stap?

- [ ] Alle apparaten uitschakelen en naar forensisch onderzoek sturen
- [ ] Live geheugendumps uitvoeren en onderzoeken terwijl systemen actief zijn
- [ ] De externe leverancier op de hoogte stellen dat er een inbreuk heeft plaatsgevonden
- [ ] Alle apparaten wissen en nieuwe laptops uitgeven aan alle gebruikers wereldwijd

Bekijk het juiste antwoord →

# Type aanval: Hardware voor de leveringsketen

1 — 2 — 3: Herstellen na een cyberaanval — 4

U hebt 100 verdachte apparaten geïsoleerd met kwaadaardige SSD-firmware. U moet beslissen hoe u verder wilt gaan zonder de aanvaller, die mogelijk op externe toegang heeft, te alarmeren. Wat is de beste volgende stap?

- ✗ Alle apparaten uitschakelen en naar forensisch onderzoek sturen
- ✓ Live geheugendumps uitvoeren en onderzoeken terwijl systemen actief zijn
- ✗ De externe leverancier op de hoogte stellen dat er een inbreuk heeft plaatsgevonden
- ✗ Alle apparaten wissen en nieuwe laptops uitgeven aan alle gebruikers wereldwijd

Live geheugendumps zijn cruciaal voor het bewaren van vluchtig bewijsmateriaal, zoals actieve malware en rootkits. Ze maken een gerichte reactie op incidenten mogelijk door verborgen bedreigingen en access points bloot te leggen voordat ze verloren gaan of aanvallers worden gewaarschuwd.

Volgende vraag →

# Type aanval: Hardware voor de leveringsketen

1 2 3 4: Algemene best practices

Uw Chief Information Security Officer vraagt om een samenvatting van hoe deze aanval uw omgeving is binnengedrongen. U moet een beknopte uitleg geven aan het directieteam. Hoe moet u de aanval uitleggen?

- [ ] Er is per ongeluk een virus gedownload via een phishing-koppeling
- [ ] Er is een verkeerde netwerkconfiguratie geweest die externe toegang mogelijk maakte
- [ ] Kwaadaardige firmware werd geïntroduceerd via een gecompromitteerde hardwareleverancier tijdens de levering van laptops
- [ ] Een van onze ontwikkelaars heeft onveilige code naar productie gepusht

Bekijk het juiste antwoord →

# Type aanval: Hardware voor de leveringsketen

1 — 2 — 3 — 4: Algemene best practices

Uw Chief Information Security Officer vraagt om een samenvatting van hoe deze aanval uw omgeving is binnengedrongen. U moet een beknopte uitleg geven aan het directieteam. Hoe moet u de aanval uitleggen?

- ✗ Er is per ongeluk een virus gedownload via een phishing-koppeling
- ✗ Er is een verkeerde netwerkconfiguratie geweest die externe toegang mogelijk maakte
- ✓ Kwaadaardige firmware werd geïntroduceerd via een gecompromitteerde hardwareleverancier tijdens de levering van laptops
- ✗ Een van onze ontwikkelaars heeft onveilige code naar productie gepusht

De niet-overeenkomende firmwareversies en de afwezigheid van actieve malware bevestigen dat dit een aanval op firmwareniveau was die afkomstig was van de leverancier, niet een gebruikersfout of verkeerde configuratie.

Bekijk oplossingen →

TYPE AANVAL: HARDWARE VOOR DE LEVERINGSKETEN

# Samenvatting

Aanvallen op de leveringsketen zijn de afgelopen jaren aanzienlijk toegenomen. Door fysieke apparaten te manipuleren tijdens productie, verzending of implementatie of door zwakke plekken in softwareleveranciers te vinden, krijgen aanvallers de middelen om kwaadaardige componenten of code in te voegen, systemen te corrumperen of gevoelige data te exfiltreren. Slachtoffers kunnen variëren van kleine bedrijven tot wereldwijde ondernemingen, met gevolgen zoals ernstige financiële verliezen, verminderd vertrouwen van klanten en juridische gevolgen.

Dell beperkt aanvallen op hardware in de leveringsketen door rigoureuze risicobeoordelingen van leveranciers te integreren en Zero Trust-principes in te bouwen naast continue apparaatvalidatie en onafhankelijke integriteitscontroles. We versterken de integriteit van hardware gedurende de gehele levenscyclus.

Kom meer te weten over geavanceerde strategieën voor cybertolerantie en hoe Dell u kan helpen uw organisatie te beschermen tegen aanvallen op de hardware in de toeleveringsketen.

Bekijk het rapport over hardware-aanvallen in de leveringsketen →

Terug naar scenario's

## Leveringsketengarantie ›

Met geavanceerde herkomstgegevens, fraudebestendige logistiek en transparante inkoop zorgt de toeleveringsketen van Dell ervoor dat hardware, firmware en leveranciers grondig worden gecontroleerd voordat ze uw organisatie bereiken.

## Secure Component Verification (SCV) ›

Cryptografische verificatie van pc-componenten in de fabriek en tijdens de installatie zorgt voor authenticiteit, detecteert verborgen wijzigingen en beperkt risico's op sabotage in de leveringsketen.

## Vertrouwde werkruimte en vertrouwde infrastructuur ›

Op hardware gebaseerde authenticatie en continue integriteitscontroles van firmware beschermen eindpunten en waarschuwen u voor ongeautoriseerde wijzigingen of schadelijke implantaten voordat ze bedreigingen worden.

## Asset Tracking en ProSupport Suite met SupportAssist ›

Uitgebreide asset tracking, realtime monitoring van de herkomst van apparaten en proactieve integriteitscontrole zorgen voor snelle detectie van afwijkingen en beveiliging van alle apparaten.

## Beveiligingspartners: AI-gestuurde detectie en respons ›

AI-gestuurde beveiligingstools maken continue bewaking, forensisch onderzoek en geautomatiseerde beheersing van sabotage of afwijkend apparaatgedrag mogelijk, waardoor snelle actie tegen bedreigingen van de leveringsketen wordt gegarandeerd.

# Type aanval: Software voor de leveringsketen

Uw bedrijf biedt cloudgebaseerde analysesoftware die wordt gebruikt door ziekenhuizen. Uw back-endservices zijn afhankelijk van een veelgebruikte open-source logboekbibliotheek die wordt onderhouden door een vertrouwde externe ontwikkelaar op GitHub.

Zonder de hulp van uw ontwikkelingsteam hebben aanvallers het GitHub-account gecompromitteerd en een schadelijke update ingevoegd die verborgen code bevat die is ontworpen om:

- Omgevingsvariabelen te exfiltreren, waaronder API-sleutels (Application Programing Interface) en JWT-geheimen (JavaScript Object Notation Web Tokens)
- Een omgekeerde shell te maken wanneer specifieke IP's verzoeken indienen
- Inactief te blijven tenzij op afstand geactiveerd

Test uw kennis →

# Type aanval: Software voor de leveringsketen

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Uw API begint plotseling 500-fouten te retourneren aan belangrijke klanten. Cloudmonitoring signaleert uitgaande verbindingen van uw gecontaineriseerde services naar een domein dat nog niet eerder is gezien. Wat is uw eerste reactie?

- [ ] Al het uitgaande netwerkverkeer van containers uitschakelen
- [ ] De getroffen services opnieuw starten om eventuele geheugenproblemen te wissen
- [ ] Controleren op recente code-commits in uw GitHub-repository
- [ ] Contact opnemen met de hostingprovider van het domein

Bekijk het juiste antwoord →

# Type aanval: Software voor de leveringsketen

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Uw API begint plotseling 500-fouten te retourneren aan belangrijke klanten. Cloudmonitoring signaleert uitgaande verbindingen van uw gecontaineriseerde services naar een domein dat nog niet eerder is gezien. Wat is uw eerste reactie?

- ✓ Al het uitgaande netwerkverkeer van containers uitschakelen
- ✗ De getroffen services opnieuw starten om eventuele geheugenproblemen te wissen
- ✗ Controleren op recente code-commits in uw GitHub-repository
- ✗ Contact opnemen met de hostingprovider van het domein

Door al het uitgaande netwerkverkeer vanuit containers uit te schakelen, wordt onmiddellijk voorkomen dat aanvallers gevoelige data kunnen stelen of extern toegang kunnen krijgen via de gecompromitteerde logboekbibliotheek. Zo wordt uw omgeving in realtime geïsoleerd en wint u kostbare tijd om onderzoek te doen, API-sleutels en geheimen te beveiligen en te voorkomen dat slapende aanvalsmechanismen worden geactiveerd.

Volgende vraag →

# Type aanval: Software voor de leveringsketen

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Uw engineering lead bevestigt de automatisch uit GitHub gehaalde code van de applicatie drie dagen voordat de problemen begonnen. Die versie is nog niet als schadelijk gemarkeerd in openbare databases. Wat is de meest verantwoordelijke onmiddellijke actie?

- [ ] Rechtstreeks contact opnemen met de bibliotheekonderhouder via GitHub
- [ ] Alle lokale projectafhankelijkheden verwijderen en opnieuw opbouwen
- [ ] Wachten op veelvoorkomende kwetsbaarheden en blootstellingen (CVE) voordat u verdere actie onderneemt
- [ ] Terugkeren naar de laatst bekende veilige versie van de code

Bekijk het juiste antwoord →

# Type aanval: Software voor de leveringsketen

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Uw engineering lead bevestigt de automatisch uit GitHub gehaalde code van de applicatie drie dagen voordat de problemen begonnen. Die versie is nog niet als schadelijk gemarkeerd in openbare databases. Wat is de meest verantwoordelijke onmiddellijke actie?

- ✗ Rechtstreeks contact opnemen met de bibliotheekonderhouder via GitHub
- ✗ Alle lokale projectafhankelijkheden verwijderen en opnieuw opbouwen
- ✗ Wachten op veelvoorkomende kwetsbaarheden en blootstellingen (CVE) voordat u verdere actie onderneemt
- ✓ Terugkeren naar de laatst bekende veilige versie van de code

Door terug te keren naar de laatst bekende veilige codeversie wordt de gecompromitteerde update onmiddellijk verwijderd, wordt de voet aan de grond van de aanvaller weggenomen en wordt de operationele integriteit hersteld om risico's proactief te beperken en gevoelige data te beschermen.

Volgende vraag →

# Type aanval: Software voor de leveringsketen

1 — 2 — 3: Herstellen na een cyberaanval — 4

Analyse bevestigt dat de bibliotheek API-sleutels en cloudinloggegevens exfiltreerde. U hebt meerdere containers geïdentificeerd die zijn gebouwd met de gecompromitteerde versie. Welke stap is het belangrijkst in uw inperkingsstrategie?

- [ ] Alle inloggegevens in de getroffen omgevingen intrekken en wijzigen
- [ ] Een nieuwe image van de containers maken met behulp van een bijgewerkte image van het besturingssysteem (OS)
- [ ] De laptops van het ontwikkelingsteam wissen
- [ ] Een verwijderingsverzoek indienen voor de GitHub-repository

Bekijk het juiste antwoord →

# Type aanval: Software voor de leveringsketen

1 — 2 — 3: Herstellen na een cyberaanval — 4

Analyse bevestigt dat de bibliotheek API-sleutels en cloudinloggegevens exfiltreerde. U hebt meerdere containers geïdentificeerd die zijn gebouwd met de gecompromitteerde versie. Welke stap is het belangrijkst in uw inperkingsstrategie?

- ✓ Alle inloggegevens in de getroffen omgevingen intrekken en wijzigen
- ✗ Een nieuwe image van de containers maken met behulp van een bijgewerkte image van het besturingssysteem (OS)
- ✗ De laptops van het ontwikkelingsteam wissen
- ✗ Een verwijderingsverzoek indienen voor de GitHub-repository

Het intrekken en roteren van inloggegevens is de eerste cruciale stap na een cloudinbreuk. Hiermee wordt voorkomen dat aanvallers toegang krijgen tot diensten, wordt datadiefstal tegengegaan en worden systemen beveiligd, ongeacht de omvang van de inbreuk.

Volgende vraag →

# Type aanval: Software voor de leveringsketen

1 2 3 4: Algemene best practices

U wordt gevraagd om uit te leggen wat er is gebeurd aan uw Chief Technology Officer en juridische/compliance-teams. Wat is de meest nauwkeurige en duidelijke uitleg? Hoe vat u het incident samen?

- [ ] Onze interne tooling voor continue integratie en continue implementatie/levering (CI/CD) heeft gefaald, waardoor slechte code kon worden geïmplementeerd
- [ ] Een afhankelijkheid van software van een derde partij werd gecompromitteerd en onze automatisering heeft deze in productie genomen
- [ ] Een ontwikkelaar heeft niet-geteste code opgenomen in een versnelde release
- [ ] Een aanvaller heeft onze GitHub-repository met brute aanvallen gehackt

Bekijk het juiste antwoord →

# Type aanval: Software voor de leveringsketen

1 2 3 4: Algemene best practices

U wordt gevraagd om uit te leggen wat er is gebeurd aan uw Chief Technology Officer en juridische/compliance-teams. Wat is de meest nauwkeurige en duidelijke uitleg? Hoe vat u het incident samen?

- ✗ Onze interne tooling voor continue integratie en continue implementatie/levering (CI/CD) heeft gefaald, waardoor slechte code kon worden geïmplementeerd
- ✓ Een afhankelijkheid van software van een derde partij werd gecompromitteerd en onze automatisering heeft deze in productie genomen
- ✗ Een ontwikkelaar heeft niet-geteste code opgenomen in een versnelde release
- ✗ Een aanvaller heeft onze GitHub-repository met brute aanvallen gehackt

De hoofdoorzaak was een aanval op de toeleveringsketen: aanvallers braken in op een externe softwareafhankelijkheid en het geautomatiseerde bouwproces haalde de kwaadaardige update rechtstreeks naar de productie, waardoor de integriteit van applicaties en gevoelige omgevingen werden beïnvloed en het risico op schadelijke updates in vertrouwde externe afhankelijkheden werd benadrukt.

Bekijk oplossingen →

TYPE AANVAL: SOFTWARE VOOR DE LEVERINGSKETEN

# Samenvatting

Cyberaanvallen op software in de toeleveringsketen maken gebruik van beveiligingslekken in software-updates, integraties van derden en ontwikkelomgevingen om schadelijke code in te sluiten die zich verspreidt over netwerken. Deze aanvallen kunnen leiden tot wijdverbreide datalekken, operationele onderbrekingen en volledige ecosystemen in gevaar brengen, wat gevolgen heeft voor bedrijven van elke omvang.

Dell zet zich in voor cybertolerantie door de nadruk te leggen op transparantie, veilige ontwikkeling en continue bewaking, terwijl een robuust incidentresponsplan wordt gehandhaafd om snel herstel en communicatie met belanghebbenden te garanderen.

Lees meer over geavanceerde strategieën voor cybertolerantie en ontdek hoe Dell u kan helpen uw organisatie te beschermen tegen aanvallen op Supply Chain Software.

Bekijk het rapport over aanvallen op software voor de leveringsketen →

Terug naar scenario's

## Leveringsketengarantie ›

Met geavanceerde herkomstgegevens, fraudebestendige logistiek en transparante inkoop zorgt de toeleveringsketen van Dell ervoor dat hardware, firmware en leveranciers grondig worden gecontroleerd voordat ze uw organisatie bereiken.

## Secure Development Lifecycle (SDL) ›

Implementeert toonaangevende veilige ontwikkelingspraktijken om risico's van externe afhankelijkheden te verminderen en softwareaanvallen te voorkomen in geleverde oplossingen.

## Vertrouwde werkruimte en vertrouwde infrastructuur ›

SafeBIOS, SafeID en SafeDataDelivers hardware-verificatie helpen ervoor te zorgen dat eindpunten alleen vertrouwde code uitvoeren en zorgen voor een snelle detectie van ongeautoriseerde of kwaadaardige softwarewijzigingen.

## Asset Tracking en ProSupport Suite met SupportAssist ›

Realtime bewaking van apparaten en software maakt snelle detectie en respons mogelijk op afwijkingen die door de leveringsketen worden geïntroduceerd.

## Beveiligingspartners: AI-gestuurde detectie en inperking ›

Detecteer, blokkeer en verhelp snel aanvallen op de toeleveringsketen van software, inclusief aanvallen die worden geïntroduceerd via open-source- of externe code.

# Type aanval: Zero-Day

U bent een beveiligingsanalist die de authenticatielogboeken van een bedrijf controleert. Onlangs hebben gebruikers onbevoegde toegang tot hun accounts gemeld, ook al hebben ze hun inloggegevens niet gedeeld.

Bij het onderzoeken van de logboeken vindt u de volgende activiteit:

```
[INFO] 2025-04-02 14:05:12 - Gebruikerslogin - Gebruikers-ID: 1023 - IP: 192.168.1.15 - JWT-token uitgegeven
[INFO] 2025-04-02 14:07:35 - Gebruikerslogin - Gebruikers-ID: 1023 - IP: 5.62.60.12 - JWT-token hergebruikt
[INFO] 2025-04-02 14:08:00 - Gebruikerslogin - Gebruikers-ID: 1023 - IP: 203.0.113.45 - JWT-token hergebruikt
```

Tegelijkertijd identificeert een beveiligingsonderzoeker een beveiligingslek in de API (Application Programming Interface):

- JavaScript Object Notation Web Tokens (JWT) verlopen nooit.
- Tokens worden opgeslagen in lokale storage in plaats van HTTP-only cookies.
- Er wordt geen meervoudige verificatie (MFA) afgedwongen.

Test uw kennis →

# Type aanval: Zero-Day

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Als beveiligingsteam vermoedt u, aangezien er geen alarmbellen zijn afgegaan, dat dit een Zero-Day-aanval is. Hoe zou u dit bevestigen?

- [ ] Alle gebruikers afmelden van hun systemen
- [ ] Belangrijk afwijkend authenticatiegedrag in logboeken vaststellen
- [ ] Vrienden van andere bedrijven bellen om te zien of ze hetzelfde probleem hebben
- [ ] Verbanden proberen te leggen met andere abnormale beveiligingsactiviteiten

Bekijk het juiste antwoord →

DELL Technologies

E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Zero-Day

1: Het aanvalsoppervlak beperken — 2 — 3 — 4

Als beveiligingsteam vermoedt u, aangezien er geen alarmbellen zijn afgegaan, dat dit een Zero-Day-aanval is. Hoe zou u dit bevestigen?

- ✗ Alle gebruikers afmelden van hun systemen
- ✓ Belangrijk afwijkend authenticatiegedrag in logboeken vaststellen
- ✗ Vrienden van andere bedrijven bellen om te zien of ze hetzelfde probleem hebben
- ✓ Verbanden proberen te leggen met andere abnormale beveiligingsactiviteiten

Het opsporen van afwijkend authenticatiegedrag, zoals ongebruikelijke inlogtijden, hergebruik van inloggegevens of toegang vanaf atypische apparaten, en het verband leggen met andere abnormale beveiligingsactiviteiten, zoals afwijkingen in datatoegang of escalatie van privileges, bevestigt een gecoördineerde Zero-Day-aanval.

Volgende vraag →

# Type aanval: Zero-Day

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Aangezien het beveiligingslek onbekend is, moeten beveiligingsteams de schade tijdens het onderzoek beperken. Hoe zou u dit doen?

- [ ] Alle verificatiesessies systeembreed ongeldig maken
- [ ] Alle resources op het beginpunt van de aanval richten
- [ ] Alleen aanmeldingen met meervoudige authenticatie (MFA) toestaan
- [ ] Vertrouwen op de huidige statische firewalls of WAF-regels (Web Application Firewall)

Bekijk het juiste antwoord →

DELL Technologies

E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Zero-Day

1 — 2: Cyberbedreigingen detecteren en hierop reageren — 3 — 4

Aangezien het beveiligingslek onbekend is, moeten beveiligingsteams de schade tijdens het onderzoek beperken. Hoe zou u dit doen?

- ✓ Alle verificatiesessies systeembreed ongeldig maken
- ✗ Alle resources op het beginpunt van de aanval richten
- ✓ Alleen aanmeldingen met meervoudige authenticatie (MFA) toestaan
- ✗ Vertrouwen op de huidige statische firewalls of WAF-regels (Web Application Firewall)

Samen versterken deze acties de beveiliging en minimaliseren ze risico's terwijl ze de toegang van de aanvaller blokkeren, zodat beveiligingsteams het onderliggende beveiligingslek kunnen onderzoeken en oplossen.

Volgende vraag →

# Type aanval: Zero-Day

1 — 2 — 3: Herstellen na een cyberaanval — 4

Dell pc's hebben technologieën zoals Secure Boot, Trusted Platform Modules (TPM), Basic Input/Output System (BIOS) Password Protection en SafeBIOS. Hoe kunnen deze helpen bij een Zero-Day-aanval?

- [ ] Beschermt tegen credential dumping-aanvallen waarbij API-tokens (Application Programming Interface) worden gestolen
- [ ] Voorkomt dat een aanvaller met fysieke toegang de beveiliging van het besturingssysteem omzeilt om malware te installeren die verificatietokens steelt
- [ ] Zorgt ervoor dat aanvallers de BIOS-instellingen niet kunnen manipuleren om de beveiliging van het besturingssysteem te verzwakken, wat kan leiden tot API-sessiekaping
- [ ] Alle bovenstaande opties

Bekijk het juiste antwoord →

DELL Technologies

E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Zero-Day

1 2 3: Herstellen na een cyberaanval 4

Dell pc's hebben technologieën zoals Secure Boot, Trusted Platform Modules (TPM), Basic Input/Output System (BIOS) Password Protection en SafeBIOS. Hoe kunnen deze helpen bij een Zero-Day-aanval?

- [x] Beschermt tegen credential dumping-aanvallen waarbij API-tokens (Application Programming Interface) worden gestolen
- [x] Voorkomt dat een aanvaller met fysieke toegang de beveiliging van het besturingssysteem omzeilt om malware te installeren die verificatietokens steelt
- [x] Zorgt ervoor dat aanvallers de BIOS-instellingen niet kunnen manipuleren om de beveiliging van het besturingssysteem te verzwakken, wat kan leiden tot API-sessiekaping
- [x] Alle bovenstaande opties

Deze gelaagde aanpak biedt uitgebreide bescherming tegen Zero-Day-aanvallen die gericht zijn op BIOS, firmware, inloggegevens en systeemconfiguraties. Door manipulatie, onbevoegde toegang en diefstal van referenties te voorkomen, blijven deze technologieën effectief, zelfs wanneer nieuwe kwetsbaarheden worden ontdekt door aanvallers.

Volgende vraag →

DELL Technologies
E-book interactieve scenario's voor cyberbeveiliging

# Type aanval: Zero-Day

1 2 3 4: Algemene best practices

Wat is de beste manier om Zero-Day-aanvallen te voorkomen?

- [ ] Geen open source-software gebruiken
- [ ] Zero trust-beveiligingsprincipes toepassen
- [ ] Alles gepatcht houden, waaronder besturingssystemen (OS), firmware, API's (Application Programming interfaces), bibliotheken en containers
- [ ] Een hek onder stroom zetten rondom het bedrijf om de bedreigers buiten te houden

Bekijk het juiste antwoord →

# Type aanval: Zero-Day

1 2 3 4: Algemene best practices

## Wat is de beste manier om Zero-Day-aanvallen te voorkomen?

- ✗ Geen open source-software gebruiken
- ✓ Zero trust-beveiligingsprincipes toepassen
- ✗ Alles gepatcht houden, waaronder besturingssystemen (OS), firmware, API's (Application Programming interfaces), bibliotheken en containers
- ✗ Een hek onder stroom zetten rondom het bedrijf om de bedreigers buiten te houden

Als er onbekende kwetsbaarheden of niet-gepatchte systemen bestaan, voorkomen Zero Trust-principes Zero-Day-aanvallen door impliciet vertrouwen van gebruikers en apparaten te verwijderen, continue authenticatie af te dwingen, toegang te beperken tot alleen noodzakelijke informatie en bewegingen van tegenstanders in te perken om het organisatorische risico van onontdekte bedreigingen aanzienlijk te verminderen.

Bekijk oplossingen →

TYPE AANVAL: ZERO-DAY

# Samenvatting

Een Zero-Day-aanval houdt in dat misbruik wordt gemaakt van een niet bekendgemaakte beveiligingslek in software of hardware voordat er een patch of oplossing beschikbaar is. Aanvallers profiteren van de kans die zich voordoet en veroorzaken vaak grootschalige verstoringen voordat de kwetsbaarheid wordt ontdekt en verholpen.

Dell pakt Zero-Day-aanvallen aan met Zero-Trust-controles, netwerksegmentatie, snelle insluiting en gebruikersvoorlichting, waardoor de verdediging tegen opkomende bedreigingen verder wordt versterkt.

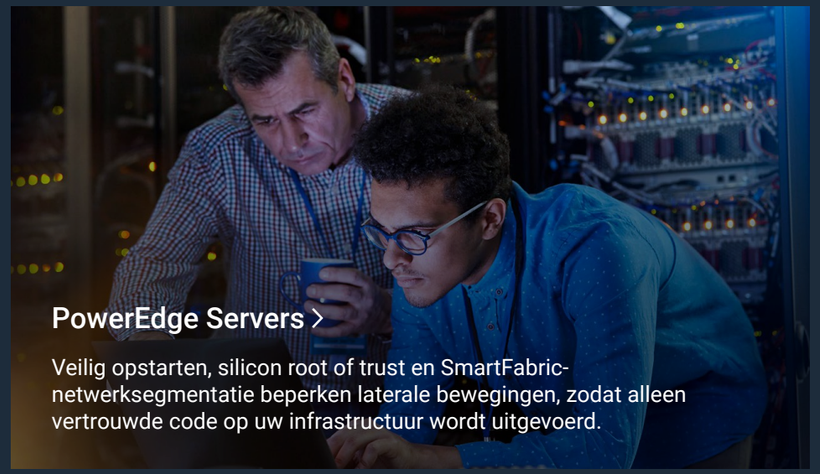
Kom meer te weten over geavanceerde strategieën voor cybertolerantie en hoe Dell u kan helpen uw organisatie te beschermen tegen Zero-Day-aanvallen.

Bekijk het rapport over Zero-Day-aanvallen →

Terug naar scenario's

## Vertrouwde werkruimte en vertrouwde infrastructuur >

Verdedig eindpunten en infrastructuur. Met SafeBIOS, SafeID, SafeData-beveiligingen en Zero-Trust-frameworks zoals meervoudige authenticatie (MFA) en op rollen gebaseerde toegangscontrole (RBAC) biedt Dell gelaagde beveiliging om exploitatiepaden te beperken en hardware-authenticatie te garanderen.



## PowerEdge Servers >

Veilig opstarten, silicon root of trust en SmartFabric-netwerksegmentatie beperken laterale bewegingen, zodat alleen vertrouwde code op uw infrastructuur wordt uitgevoerd.

## Beveiligingspartners >

Geavanceerde Threat Intelligence, Managed Detection and Response (MDR), Extended Detection and Response (XDR) en gedetailleerde toegangscontroles helpen bij het detecteren, opsporen en beperken van Zero-Day-aanvallen voordat deze zich verspreiden.

## PowerProtect portfolio>

Onveranderlijke back-ups, geïsoleerde Cyber Recovery-kluizen en AI-gestuurde CyberSense analytics zorgen voor snel herstel en veerkracht na Zero-Day-inbreuken.

## Services voor beveiliging en veerkracht>

Van patchbeheer tot incidentrespons: de experts van Dell zorgen voor snelle beheersing, forensisch onderzoek en veerkrachtplanning om Zero-Day-bedreigingen tegen te gaan.


DELL Technologies