Cynet
Advanced Threat Detection & Response

CYNET 360

SECURITY MADE SIMPLE

In het snel ontwikkelende bedreigingslandschap van vandaag is het uitoefenen van beveiligingsmaatregelen door een organisatie net zo belangrijk als hun product of dienst. Bij de inspanningen om hun bezittingen te beschermen gebruiken organisaties meerdere beveiligingsoplossingen, daarmee op potentiële bedreigingen proberen te anticiperen en kwetsbaarheden tegen te gaan voordat ze zich voordoen.

Tegelijkertijd wordt het succes en de efficiëntie van organisatorische cybersecurity beïnvloed door factoren zoals budget en prioritering van noodzakelijkheden. Organisaties bevinden zich vaak in een moeizame rol om hun belangen veilig te houden zodra er nieuwe bedreigingen ontstaan. Zij moeten vechten om hun beveiligingsnoodzakelijkheden in te vullen, terwijl prioriteiten op financieringsvlak veranderen. Ongeacht de reden eindigen oplossingsaankopen, mankracht en andere middelen vaak op de bezuinigingstafel.

Onder deze omstandigheden, als organisaties een veilige cyberomgeving nastreven, zien IT- beveiligingsteams zichzelf vaak gebruikmakend van een verscheidenheid aan beveiligingsoplossingen om hun detectie-, bescherming- en responsbehoeften te realiseren. Beveiligingsanalisten besteden uren aan de massale informatie die op hun afkomt vanaf een veelvoud aan beveiligingsoplossingen die niet 'dezelfde taal spreken'. Het is eenvoudig te zien hoe de zichtbaarheid verloren gaat aangezien de echte bedreigingen uiteindelijk verborgen zijn in een berg van schijnbare bevindingen.

BELANGRIJKSTE VOORDELEN

SNOEIT IN DE KOSTEN
Biedt velerlei mogelijkheden en inzicht in systemen voor meer effectieve bescherming, detectie en respons met minder uitgaven.

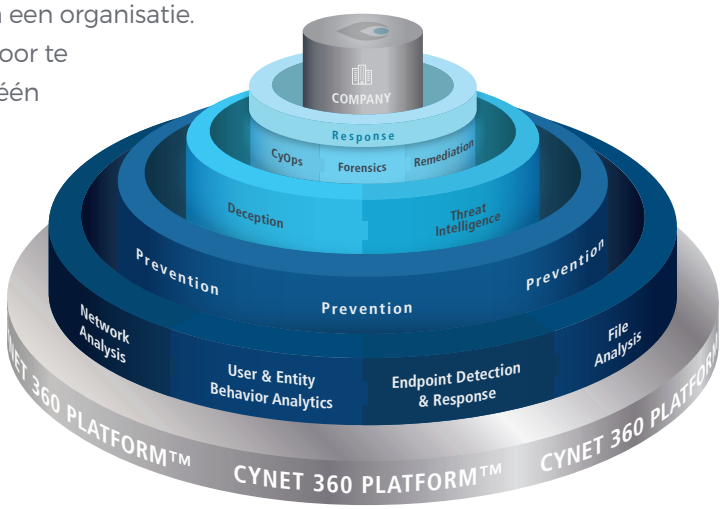
VERLAAGT HET RISICO
Geeft een complete inkijk op de beveiligingskaart van de organisatie met daarbij een snelle en zeer nauwkeurig respons.

VERHOOGT DE EFFICIENCY
Zorgt ervoor dat IT-beveiligingsteams een compleet pakket aan gereedschappen en mogelijkheden hebben, waarmee ze snel bedreigingen kunnen opsporen en nauwkeurig verminderen.

BESCHERMD IN MINUTEN
Installeert, detecteert en analyseert tienduizenden eindpunten in minder dan 2 uur, zonder IT-downtime.

HET CYNET 360 PLATFORM

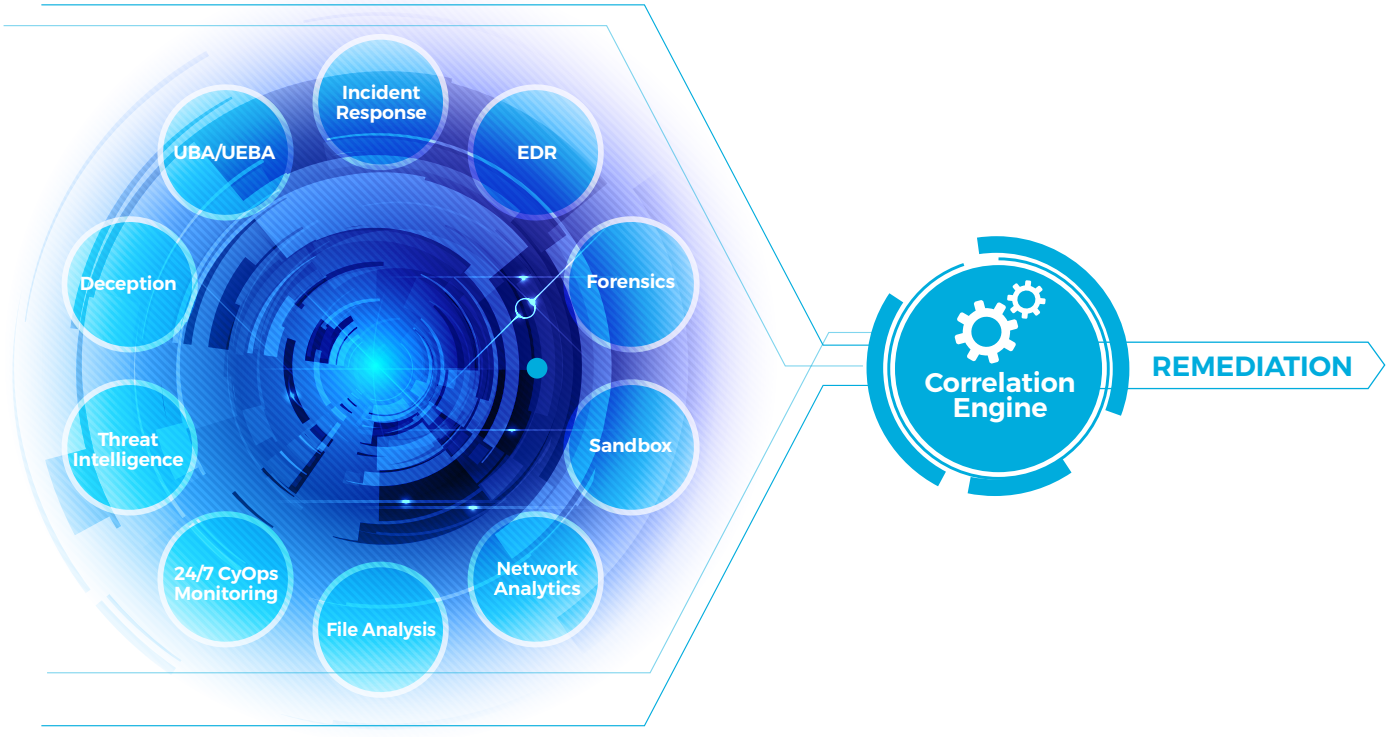
Het Cynet 360 geavanceerde bedreigingsdetectie en response platform vereenvoudigt bedrijfsbeveiliging door een holistisch antwoord te bieden op alle bescherming en preventie behoeften van een organisatie. Cynet 360 vermindert de beveiligingsuitgaven door te voorzien in een veelvoud van mogelijkheden in één enkele oplossing, met minder organisatorische middelen, mankracht en budget. Bovendien biedt het 360-platform het hoogste niveau van bedrijfsbeveiliging door het correleren van indicatoren dwars over systemen, dus toenemend inzicht en nauwkeurigheid van detectie in de hele organisatie zonder de noodzaak van meerdere cyber beveiligingsoplossingen.



Het Cynet 360 Platform

HOE DOEN WE HET

Zonder dat installatie nodig is lanceert het Cynet 360-platform zich binnen zo'n 2 uur over tienduizenden endpoints. Eenmaal uitgerold begint het platform met analyseren en correleren van indicatoren over het netwerk, bestanden, gebruikers en endpoints, het geven van risicoklasseringen voor mogelijk afwijkend gedrag, het waarborgen van het laagste aantal schijnbare resultaten en het verkrijgen van een duidelijk beeld van de aanvallen in de tijd. Cynet 360's machineleer- en geautomatiseerde remediëringsmogelijkheden betekenen dat processen gestroomlijnd zijn, waardoor minder inspanning gelegd wordt bij de IT-beveiligingsmedewerkers.



HET CYNET 360 PLATFORM – GEBRUIKSMOGELIJKHEDEN

Het Cynet 360 detectie- en responsplatform voor geavanceerde bedreigingen biedt een uitgebreide set van bedrijfsmatige beveiligingsmogelijkheden voor organisaties die het hoogste niveau van bescherming en preventie vereisen in duizenden endpoints.

Endpoint Detectie & Respons – Het Cynet 360 platform rolt snel uit en detecteert bedreigingen over duizenden endpoints binnen 2 uur. Als onderdeel van een uitgebreide oplossing correleert Cynet 360 indicatoren en biedt volledig inzicht over het gehele bedrijf.

Gebruiker en Entiteit Gedragsanalyse – De UEBA (User & Entity Behavior Analytics) mogelijkheden van het Cynet 360-platform helpen IT-beveiligingsteams malafide insiders, gecompromitteerde accounts en gerichte aanvallen te identificeren voordat er schade wordt aangericht.

Netwerk Analyse – Het Cynet 360-platform biedt volledig zicht in en analyse van netwerkverkeer en -activiteiten in de organisatie..

UBA Verificatie – Gebaseerd op de Cynet 360 Gebruiker en Entiteit Gedragsanalyse mogelijkheid, biedt de UBA-verificatie aan bedrijfsbeveiligingsteams de mogelijkheid om gebruikersactiviteiten te analyseren en ervoor te zorgen dat degenen die toegang hebben tot bedrijfsmiddelen zijn wie ze zeggen dat ze zijn.

Incident Respons – Het Cynet 360-platform biedt organisaties die onder aanval liggen een 24/7 wereldwijd Incident Respons service, geleid door een team van hooggekwalificeerde beveiligingsdeskundigen.

24/7 CyOps Monitoring – Cynet's volledig functionerende CyOps Monitoring team hanteert een meekijk benadering op gebeurtenissen in real-time, signaleert verdachte activiteiten en het beveiligen van de perimeter van de organisatie.

Threat Intelligence – Het Cynet 360 platform maakt gebruik van 20 interne en externe databases die de laatste informatie in Threat Intelligence bevatten, maar ook input van IOCs integreert. Dit biedt organisaties een extra beschermingslaag tegen verdachte en kwaadaardige activiteiten.

Forensisch onderzoek – Cynet 360 zorgt voor het gemakkelijk volgen van waarschuwingen, bedreigingen en bijbehorende processen binnen de vriendelijke Cynet gebruikersinterface. IT-Beveiligingsteams beheren eenvoudig diepgaande forensische onderzoeken, waardoor ze snel verdachte incidenten kunnen identificeren en onderzoeken.

Misleiding – Het Cynet 360-platform plaatst strategisch lok-bestanden, -mappen, -servers en -shares, die een aanvaller lokken naar vooraf ingestelde vallen. Traceermechanismen monitoren dat en geven een heldere beeld van de activiteit van de aanvaller.

Sandbox – Het Cynet 360 platform biedt een sandbox voor zowel statische analyse van bestanden en dynamische analyse van processen voor veilig onderzoek naar verdachte items.

SECTOREN DIE PROFITEREN VAN CYNET 360

Grote bedrijven over de hele wereld, waaronder wereldwijde marktleiders, rekenen op het Cynet 360 geavanceerde bedreigingsdetectie en respons platform om hun meest waardevolle bedrijfsmiddelen te beschermen. Sectoren omvatten:

- Banken / Financiële instellingen
- Verzekeraars
- Gezondheidszorg
- Detailhandel
- Industrie
- Kritische infrastructuur
- Overheid
- Onderwijs

SIMPLIFY YOUR SECURITY

OVER CYNET

Cynet is een pionier en leider in detectie en respons van geavanceerde bedreigingen. Cynet vergemakkelijkt de beveiliging door het bieden van een schaalbaar, gemakkelijk inzetbaar beveiligingsplatform dat preventie levert, precieze bevindingen en geautomatiseerde respons op geavanceerde bedreigingen met vrijwel nihil aantal valse resultaten, verkorting van de tijd van detectie tot resolutie en beperking van schade aan een organisatie.
Om meer te weten te komen bezoek: www.cynet.com

CYNET'S UNIEKE EIGENSCHAPPEN

- Omvat tienduizenden endpoints in minder dan 2-uur
- Heuristische analyse engine identificeert afwijkend gedrag en beschermt tegen bedreigingen van binnenuit
- Kruiscorrelatie over netwerken, gebruikers, bestanden en endpoints betekent volledig zicht over het netwerk
- Stelt in staat om regels te creëren voor automatische Remediatie en automatische Incident Respons
- Voorziet in een complete oplossing voor organisatorische cybersecurity inclusief anti-malware, anti- ransomware, anti-APT en anti-exploit mogelijkheden
- Meekijkend Incident Response team iedere dag , 24/7

Cynet
Advanced Threat Detection & Response

www.cynet.com.