Hoher automatischer Schutz für meine Computer landschaft

Cynet und die Endpoint- Security steht auf Auto-Pilot!

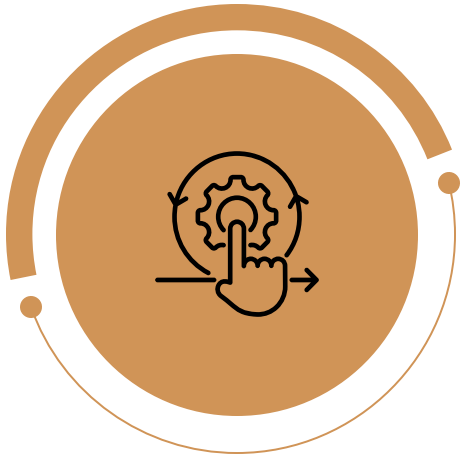
Philipp Schwarz
Head of Sales - Cybersecurity

PS@WeDoIT-Group.de / PS@cynet.de

+49 176 74583169

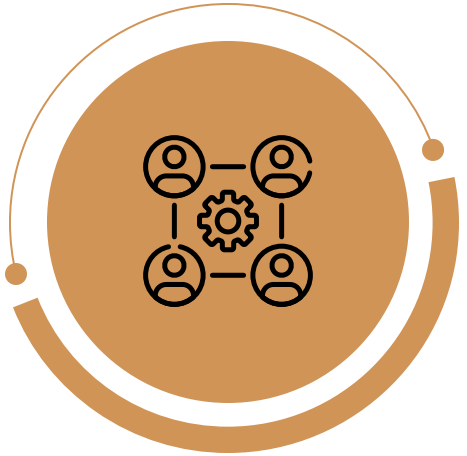
Cynet 360 Aut0XDR™

Comprehensive cybersecurity has never been easier



Radically Simple

Super Efficient



Zero Resource-drain

Agenda

- Exkurs: Anti-Virus und die offenen Scheunentore
- XDR: Nur eine weitere Abkürzung, oder wirklich sinnvoll?
- Cynet 360 AutoXDR -> AutoPilot für die Endpoint- Security
- 24/7, aber nicht nur Support!

Exkurs: Antivirus

Schutz

- Scanner (Echtzeit, manuell, online)
- Reaktiv / Proaktiv
- Signaturbasiert, verhaltensbasiert, maschinelles learning
- Virendefinitionen online

Aber

- Teils hohe Systemauslastung durch scan(s)
- Virendefinitionen aktuell?
- Anwendungen und Seiten werden pauschal geblockt
- Hoher manueller Aufwand
- Reaktiver Schutz durch scan (Zeitfenster / Systemressourcen)

Was ist mit dem Schutz im Netzwerk, dem user, in der cloud und weiteren Anwendungen?

Vom Antivirus über den EDR zum XDR

XDR = X-tended Detection & Response (Erweitert? Aber was denn genau?)

EDR= Endpoint Detection & Response
Daten beim Endpoint

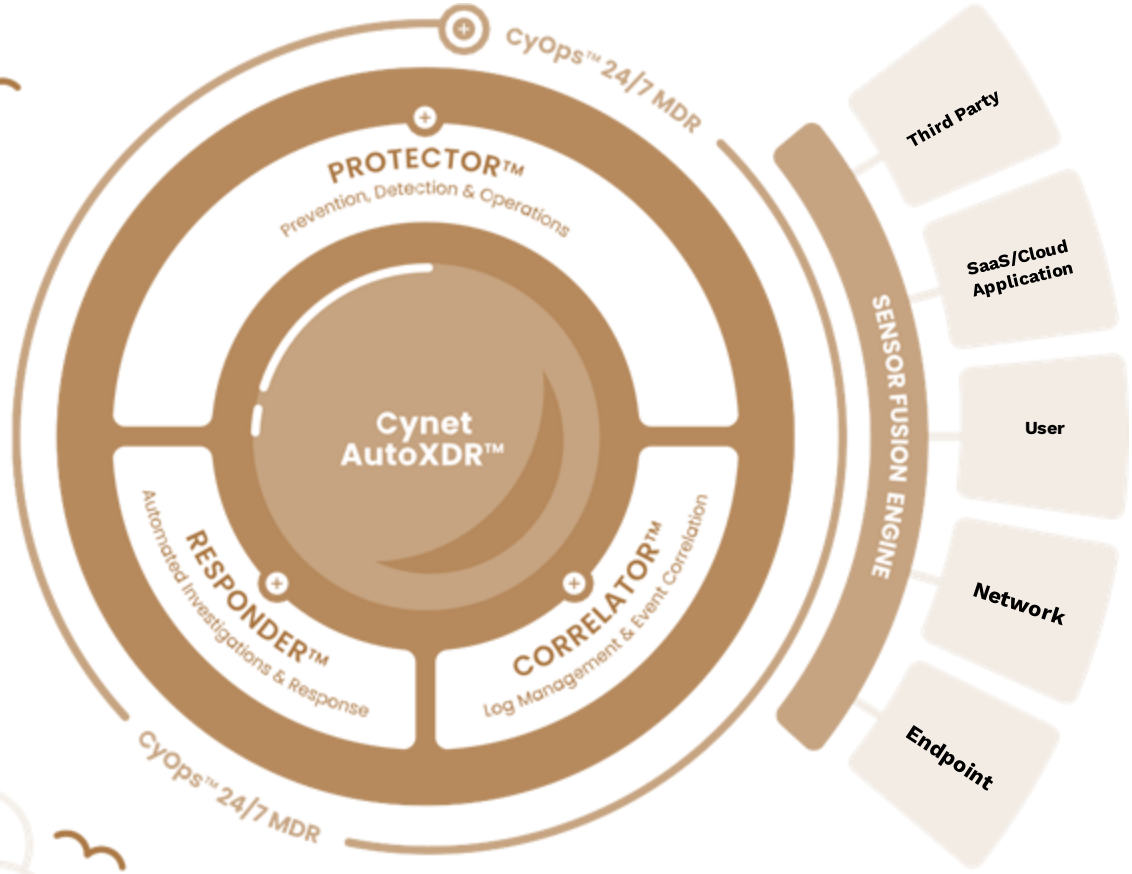
XDR erfasst und korreliert Daten automatisch auf mehreren Ebenen:

- Endpoint
- Server
- Cloud
- Netzwerk
- User

Cynet 360 Aut0XDR™

Purpose-built for lean IT Security teams

Voll ausgestattete, automatisierte, einfach zu bedienende Plattform.



Cynet 360 Aut0XDR™

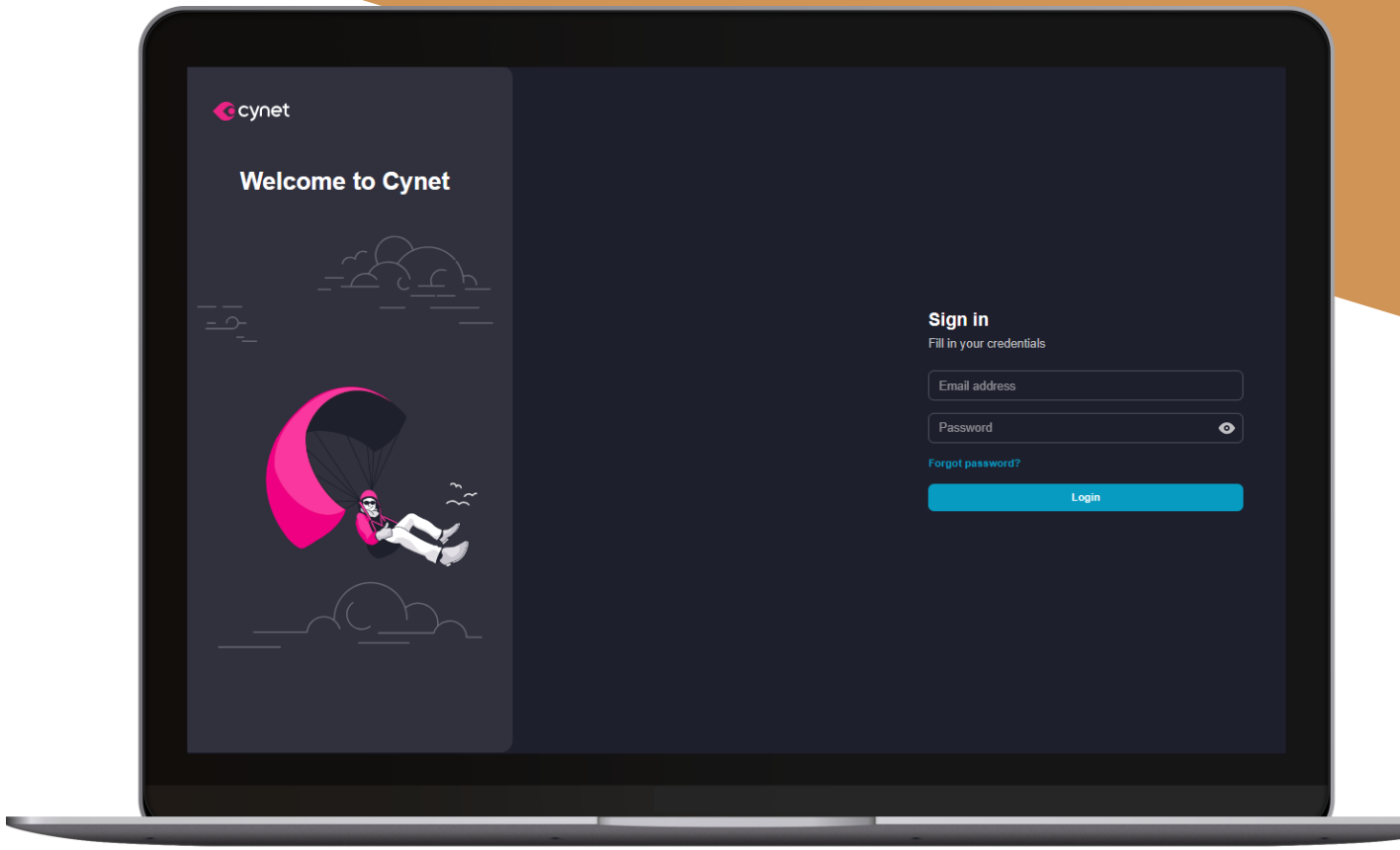
Purpose-built for lean IT Security teams

Cynet Vorteile / Kundenanforderungen

- End-to-end
- Nativ, automatisiert
- Höchste Genauigkeit
- Unmittelbar zu installieren / kein reboot!
- Benutzerfreundlich
- Sehr guter TCO TransparenteLizenzkosten
- 24/7 MDR- Service inkl.
- Minimale Voraussetzungen

Für weitere Informationen

und eine kurze Demonstration der Plattform schreiben Sie uns:
www.cynet.de




Responder™
Automated Investigation & Response
Automated Investigation
Automated Remediation
Custom Playbooks
Protector™
Prevention, Detection, IT & Security Operations
Threat Detection
Endpoint Protection
SaaS & Cloud Security
Security & IT Operations
Endpoint Detection & Response (EDR)
Network Detection & Response (NDR)
User Behaviour Analytics (UBA)
Deception
Sandbox
Threat Intelligence
Next Gen Antivirus
Device Control
Critical Resource Protection
CSPM
SSPM
IT Hygiene
Asset Inventory
Vulnerability Management
Correlator™
Log Management & Event Correlation
Centralized Log Management
Event Correlation
Forensics
Sensor Fusion Engine™
Endpoints
Servers
VDI
Cloud/SaaS Apps
Firewalls
Active Directory
XDR Integrations
CyOps™ 24/7 MDR Services
Incident Response
Continuous Monitoring
Attack Reports
Threat Hunting
CyOps™ 24/7 MDR Services
Supported OS:
Windows
Mac OS
Linux
Deployment Options:
Cloud First
Hybrid
On-Prem

24/7, aber nicht nur Support!

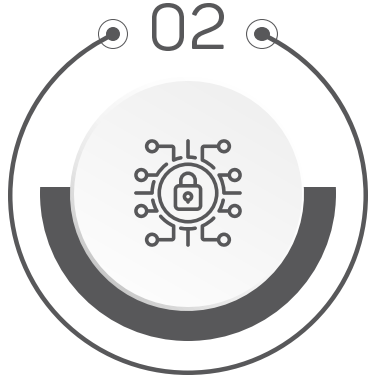
24x7 MDR

CyOps - 24x7 Managed Detection & Response Team

01

Erweitern Sie ihr Security Team

02



Zugewinn von erstklassigem Know-How in der Cybersecurity

03

Nutzen der Erkenntnisse von den anderen Endkunden weltweit

04

Bereits inklusive, ohne Mehrkosten

24/7, aber nicht nur Support!

24x7 MDR

CyOps - 24x7 Managed Detection & Response Team

Detection

- Kontinuierliches alert monitoring zur Validierung und Optimierung von Präzision und Handlungsfähigkeit
- Proaktives threat hunting um verborgene Bedrohungen zu finden
- Lateral Movement Erkennung

Investigation

- Deep-dive in den Angriff zur vollständigen Aufdeckung von Ursache, Umfang, Verweildauer und dessen Auswirkungen
- Den client mit aktuellen IOCs versorgen
- Expert Advice, Playbooks, White/Black-Listing, Ausschlüsse ... per E-Mail, Telefon oder direkt aus der GUI

Response

- Unterstützung bei Remote Incident Response mit Untersuchung, umfassenden Abhilfeplänen und Anleitung
- Bewertung der Sicherheitslage über die gesamte Organisation
- Threat Detection detailierte attack reports

Cynet AutoXDR -

Der umfassendste autonome Schutz vor Sicherheitsverletzungen

- Schnelle Wertschöpfung
- Ein einziger Blickwinkel für Endpunkte, SaaS und Drittanbieter
- Vereinfachung von SecOps für kleine Sicherheitsteams
- Bestes Preis-Leistungs-Verhältnis

Eine Plattform

- ✓ SaaS-first
- ✓ MSSP Partner
- ✓ Einfache UX
- ✓ CyOps MDR
- ✓ Geringer TCO
- ✓ Plattform- agn.

Autonomes IR

- ✓ Incident Workflows
- ✓ Anpassbare Remediations
- ✓ Out-of-the-box Playbooks
- ✓ Anpassbare Alerts

Umfassender Schutz

- ✓ SaaS Security Posture
- ✓ URL Filtering & Phishing
- ✓ SIEM + Data Lake
- ✓ Win, Linux & Mac
- ✓ Über alle Angriffsvektoren
- ✓ MITRE ATT&CK

SOAR Integration

- ✓ Anpassb. Playbooks
- ✓ Identity: AD, Azure AD, OKTA
- ✓ Netzwerk: Proxy, RMM, TCP->HTTP
- ✓ Security: FW, SWG
- ✓ Ops: Ticketing

CyOps 24/7 MDR Team

- ✓ Neue Erkennungsmethoden
- ✓ On Demand Analyse
- ✓ Remediation Anleitungen
- ✓ Proaktives Monitoring
- ✓ Keine Bots, aber Experten

CYNET MITRE ATT&CK Evaluations

Cynet has achieved outstanding results in the 2023 MITRE Enginuity ATT&CK Evaluations

100%

Detection 19 of 19 Attack Steps with
NO CONFIGURATION CHANGES

100%

Visibility 143 of 143 Attack Sub-Steps with
NO CONFIGURATION CHANGES

100%

Analytic Coverage 143 of 143 Detections with
NO CONFIGURATION CHANGES

100%

Real-Time Detection
0 Delays

CYNET MITRE ATT&CK Evaluations

Cynet has achieved outstanding results in the 2023 MITRE Enginuity ATT&CK Evaluations

Highlights:

- Cynet erreichte 100% Detection* in jedem der 19 evaluierten MITRE ATT&CK Schritte!
- Cynet erreichte 100% Sichtbarkeit* in jedem der 143 evaluierten Teilschritte!
- Cynet erreichte eine 100%ige analytische Abdeckung* in jedem der 143 evaluierten Teilschritte!
- Cynet ist der erste Hersteller überhaupt, der 100% Visibility und Analytic Coverage in der gleichen Evaluierung* erreicht hat!
- Cynet erreichte 100% Echtzeit-Erkennung über alle 143 bewerteten Teilschritte, keine verzögerten Erkennungen!

***ohne Konfigurationsanpassungen!**

VIELEN DANK

Für Ihre Aufmerksamkeit!

Philipp Schwarz

+49 176 74583169

PS@WeDoIT-Group.de / PS@Cynet.de

www.WeDoIT-Group.de / www.Cynet.de