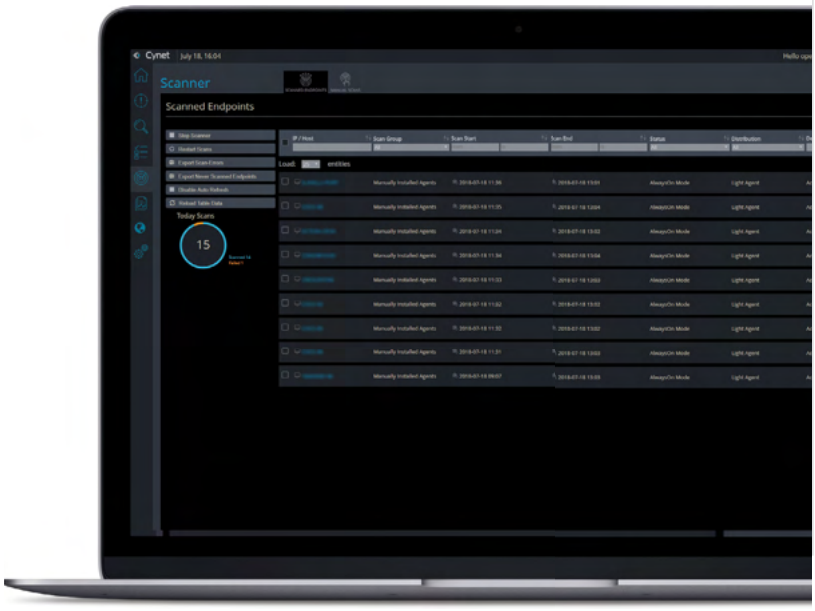
Cynet 360

Cynet ist auf Organisationen ausgelegt, die Sicherheit in Unternehmensqualität mit einem vollständigen Schutz innerhalb aller ihrer Bereiche wünschen – mit einer umfassenden Verteidigung der Endpunkte, des Netzwerks, der Dateien und der Benutzer – ohne die teure und arbeitsintensive Belastung, ein eingehendes Cyber-Fachwissen aufbauen zu müssen, und ohne Aufwand für die Integration und Verwaltung mehrerer Produkte.

Dadurch dass Cynet eine durchgängige cloud-basierende Architektur aufweist, eliminiert Cynet die Notwendigkeit, mehrere verschiedene Sicherheitslösungen und -services bereitzustellen und zu warten, und ist deshalb auch kompatibel mit jeder beliebigen Infrastruktur.

Cynet ermöglicht das Zusammenwachsen und schafft Synergien durch Technologie: Schutz der Endpunkte (Endpoint Protection – EDR), Schwachstellenmanagement, Täuschung, Informationen über Bedrohungen, Netzwerk- und Endbenutzer-Analytik sowie in der Praxis gewonnene Expertise: ein rund um die Uhr einsatzfähiges SWAT-Team, um auf Vorfälle zu reagieren, Malware zu analysieren, Bedrohungen zu jagen und Spuren zu sichern.

Cynet wird innerhalb von Stunden ohne Installation oder Einrichtung bereitgestellt und vereinfacht das Management mithilfe einer automatisierten Überwachung als sinnvolle Komplettierung für Expertenteams beliebiger Größe. Mit einer 360-Grad-Ansicht über die Benutzer, das Netzwerk, die Dateien und Endpunkte gewinnen Organisationen ein ungeahntes Maß an Transparenz für die Kontrolle und das Verständnis sowie die Eindämmung von Bedrohungen.



Nur mit der Cynet 360-Sicherheitsplattform genießen Organisationen:

360-Grad-Transparenz und -Schutz in umfassender Weise

- Schöpfen Sie mit einem vollständigen Verteidigungsportfolio aus dem Vollen, einschließlich der Abwehr von Malware, Insider-Bedrohungen, Ransomware und Vielem mehr für Organisationen beliebiger Größe.
- Restlose Transparenz bei Angriffen über Endpunkte, Benutzer, Dateien und das Netzwerk.
- Aggregierte Warnungen

Dramatisch vereinfachte Bereitstellung und Wartung.

Der cloud-basierende Ansatz erlaubt eine Bereitstellung innerhalb von wenigen Stunden ohne die Kosten für langfristige Wartung und ohne Aufwände für die Installation oder Einrichtung.

Komplettieren Sie Ihre interne Sicherheitsexpertise durch externe Spezialisten – vor allem, wenn Sie noch keine aufgebaut haben.

Nur Cynet gewährleistet eine kontinuierliche Überwachung mithilfe eines erfahrenen Zentrums für den Sicherheitsbetrieb – ungeachtet der heute vorliegenden Erfahrung.

Technologie zum Schutz Ihrer Assets

Plattform zum Schutz von Endpunkten (Endpoint Protection Platform – EPP)

Deckt Bedrohungen über Tausende von Endpunkte rasch auf. Im Gegensatz zu anderen Endpunkt-Technologien sorgt Cynet für ein Whitelisting kritischer Komponenten, einen Schutz des Speichers sowie die Sicherung von Berechtigungsnachweisen. Zu den anderen Fähigkeiten zählen:

- Anti-Malware
- Anti-Ransomware
- Anti-Exploit
- Schutz vor dateilosen Angriffen
- Antivirus der nächsten Generation
- Sandboxing

Aufdeckung und Reaktion am Endpunkt (Endpoint detection and response – EDR)

Cynets EDR bietet einen detailliert nachspielbaren Verlauf dessen, was an einem Endpunkt während und nach einem Angriff stattfand, um in allen Einzelheiten nachzuvollziehen, wie ein Hacker einen Angriff lancierte und sich dann zur Seite zu bewegen versuchte. Mit Cynets EDR können Organisationen potenziell infizierte Maschinen vom Netzwerk abtrennen, um weitere Schädigungen zu vermeiden. Die EDR-Fähigkeiten von Cynet zeichnen sich aus durch:

- Umfassende und automatisierte Reaktion und Behebung
- Jagd auf Bedrohungen
- Verfolgen der Konfiguration von Endpunkten

Analytik des Verhaltens von Benutzern und anderen Objekten (User and entity Behavior Analytics – UBA)

Im Gegensatz zu anderen UBA-Tools vermag Cynet die Mitarbeiter zu bitten, ihr Verhalten selbst zu verifizieren. Weitere Funktionalitäten betreffen analytische Verfahren zum Aufdecken von:

- Anomalien im Benutzerverhalten
- Insider-Bedrohungen
- Seitwärtsbewegungen
- Eskalierende Privilegien

Zusammenlaufende Netzwerk-Analytik

Im Unterschied zu anderen Netzwerk-Analytiktools sammelt und korreliert Cynet die breiteste Palette an verfügbaren Eingangsinformationen, einschließlich TAP-/Port-Mirroring/Syslog integriert mit Informationen über bekannte Bedrohungsmuster, Endpunkte und Firewalls zur Schaffung einer vollständigen Transparenz und Analyse des Netzwerkverkehrs, um folgende Bedrohungsszenarien aufzuspüren:

- Vermeidung der Datenexfiltration
- Feststellung von Netzwerk-Angriffen, einschließlich
  - Scannen von Ports, SMBs und IPs
  - ARP- und DNS-Cache-Vergiftung
  - ICMP-, HTTP-, C&C- und DNS-Tunnelung
  - Seitwärtsbewegungen Umgehung des Hashs und Umgehung von Tokens.

Technologie zum Schutz Ihrer Assets

Schwachstellenmanagement

Zu den Möglichkeiten zählen:

- Patch-Management von Anwendungen
- Management der Patches für das
- Betriebssystem
- Verifizierung von Agenten
- Risikoreiche Anwendungen ausfindig machen

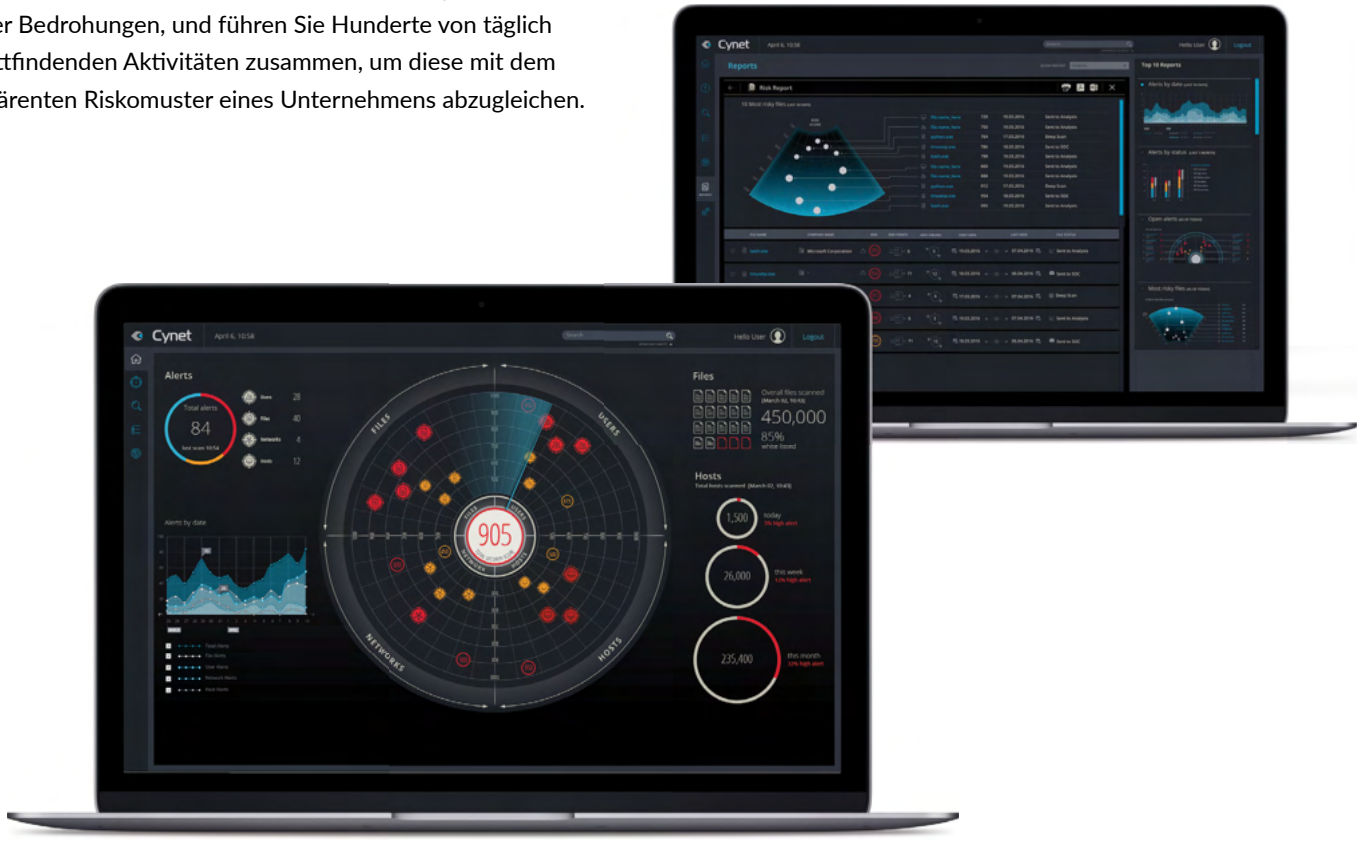
Korrelierte Informationsbasis über bekannte Bedrohungen

Nutzen Sie mehr als 20 externe Informationsquellen über Bedrohungen, und führen Sie Hunderte von täglich stattfindenden Aktivitäten zusammen, um diese mit dem inhärenten Riskomuster eines Unternehmens abzugleichen.

Tarnen und Täuschen

Im Gegensatz zu anderen Werkzeugen zur Vortäuschung fügt Cynet anpassbare Leuchtfeuer in die Dokumente ein. Da Cynets Endpunkt-Technologie bereits an den Endpunkten aktiv ist, besteht kein Bedarf für das sukzessive weitere Aufstellen von Honigtöpfen. Zu den anderen Fähigkeiten zählen:

- Platzierung von Ködern in Dateien, Berechtigungsnachweisen, Konfigurationen und im Netzwerkverhalten, um einen Angreifer in vorab bereitgestellte Fallen zu locken.
- Mechanismen verfolgen und dann überwachen und ein klares Bild der Aktivitäten der Angreifer zeichnen.



Expertise

Ohne zusätzliche Kosten umfasst Cynet ein rund um die Uhr verfügbares SWAT-Team, um praktische Erfahrungen vorzuhalten, die sicherstellen, dass Organisationen auch bei sich schnell wandelnden und verschiedenartig ausprägenden Bedrohungsszenarien auf der sicheren Seite zu bleiben. Im Gegensatz zu anderen verwalteten Services, die sich nur auf Endpunkte fokussieren, sorgt Cynets Telemetrie mit äußerster Zuverlässigkeit für umfassende Transparenz bei Angriffen über Endpunkte, Benutzer, Dateien und das Netzwerk. Noch bedeutsamer ist, dass Organisationen sich mithilfe der Cynet-Plattform des Kopfzerbrechens bezüglich der Verwaltung der Infrastruktur entledigen können.

Rundum die Uhr umfasst das Cyber-SWAT-Team:

Wesentliche personelle Ressourcen

- → **Stufe 1** Sicherheitsanalysten
- → **Stufe 2** Sicherheitsrechercheure
- → **Stufe 3** Malware-Rechercheure

Wesentliche Dienstleistungen

Reaktion auf Vorfälle (Incident response – IR): Geleitet durch ein Team von erfahrenen Sicherheitsexperten bietet Cynet angegriffenen Organisationen IR jeden Tag über 24 Stunden hinweg, wenn das erforderlich ist.

Forensik: Tiefgehende forensische Untersuchungen ermöglichen ihnen die rasche Identifizierung und Untersuchung verdächtiger Vorfälle.

Jagd auf Bedrohungen: Kombiniert über das Netzwerk, die Endpunkte, die Dateien und die Benutzerdaten, um hochentwickelte Bedrohungen aufzudecken.

Malware-Analyse: Identifizierung von Fähigkeiten, Ursprung und potenziellen Auswirkungen von Malware, die in Ihrer Organisation entdeckt wurde.

Vorteile

Geringeres Risiko mit vollständigem Schutz vor Cyber-Angriffen hinter einer einzigen Glasscheibe mit einem Dashboard und einem Agenten für eine einfach zu verwaltende und konsolidierte Transparenz der Risiken.

Optimierung der Ausgaben für Sicherheit: Verbesserung von Effizienz und Effektivität Ihres Sicherheitsteams und aktuelle technische Investitionen zu einem bezahlbaren Preis.

Totaler Schutz in Stunden: Installation und Bereitstellung innerhalb von nur wenigen Stunden. Einfache Einhaltung der Vorschriften bei Audits.

Strafferer Sicherheitsbetrieb mit vollständig automatisierten Sicherheitsreaktionen Zu den Fähigkeiten zählen:

- → Automatisierung der Behebung und
- → Reagieren auf Vorfälle
- → Gefährliche Prozesse löschen oder unter Quarantäne stellen
- → Bösartige Dateien
- → Deaktivierung der Benutzer und der Ausführung von Befehlen
- → Abschaltung und Neustart von Hosts
- → Schädigenden Datenverkehr isolieren oder blockieren

Sicherheitsereignisse präzise eingrenzen und gründlich untersuchen, um falsch-positive (Fehlalarme) und falsch-negative Alarme zu verringern: Identifizierung von mehr Angriffen sowie Verbesserung der Genauigkeit von Blockaden und der Untersuchung

Vollständige Transparenz über das Netzwerk hinweg. Kreuzkorrelation über Netzwerke, Benutzer, Dateien und Endpunkte.