T Security

Managed Cyber Defense

Effektiver Schutz durch umfassenden SOC-Service in Kombination mit Endpoint Security

Warum traditionelle Security nicht mehr ausreicht

Nicht nur die Zahl der Cyberangriffe nimmt stetig zu, sondern zugleich steigt auch ihre Komplexität, wodurch es immer schwieriger wird, Angriffe eindeutig zu identifizieren.

Die Folgen der Angriffe reichen von Datendiebstahl und Betriebsausfällen bis hin zu Spionage und finanziellem Schaden. Auch die Reputation des Unternehmens steht auf dem Spiel. Jede Art von Imageschaden wirkt sich langfristig auf die Einnahmen aus.

Eins steht fest: Die Kosten im Falle eines Angriffs sind gravierend. Klassische Firewalls und Antiviren-Lösungen reichen aus, um Unternehmensressourcen angemessen zu schützen. Sie schützen zwar effizient vor bekannten Bedrohungen, doch unbekannte Bedrohungen, die von außerhalb des Perimeters kommen, könnten unentdeckt bleiben. Gleichzeitig mangelt es oft an Zeit und Geld, um ganzheitliche Sicherheitsprojekte umzusetzen.

Lösung: Endpoint Detection and Response

Eine EDR-Lösung (Endpoint Detection and Response) ist raffinierter als eine Antiviren-Software. Sie umfasst Antivirenfunktionen sowie die Erkennung fortgeschrittener anhaltender Bedrohungen (APT), erweiterte Analysen, Reaktionsmechanismen, Geräteverwaltung und mehr. Wenn beispielsweise ein Endpunkt infiziert ist, löst eine EDR-Lösung einen Alarm aus, isoliert den Endpunkt und stellt dem Security Team forensische Informationen für die Analyse zur Verfügung.

Ohne den kontinuierlichen Einsatz erfahrener Expertenteams bleibt die Wirksamkeit von EDR jedoch begrenzt, da sie auf manuelle Eingriffe angewiesen ist. Deshalb ist Managed Cyber Defense notwendig, um eine ganzheitliche und wirksame Abwehr sicherzustellen.

Wie Managed Cyber Defense den richtigen Schutz für Ihr Unternehmen ermöglicht:

1. Full-scale SOC mit kontinuierlicher Analyse
2. Einleitung und Durchführung von Maßnahmen
3. Regelmäßige Überprüfung und Erkennung von komplexen Angriffen
4. Wöchentliche Abstimmung mit unseren Sicherheitsexpert:innen und laufende Optimierung Ihres Sicherheitsniveaus
5. Mehr als 20 Jahre Erfahrung mit Sicherheitsprojekten

Managed Cyber Defense: Die optimal integrierten Komponenten für Ihre Cybersicherheit.

The Security Operations Center

Kontinuierliche Analyse verdächtiger Aktivitäten

1. Zugang zu den Erkenntnissen aus dem SOC.
2. Echtzeitdaten und –berichte über den aktuellen Sicherheitsstatus.
3. Wöchentliche Beratungstermine zum aktuellen Status und zu Verbesserungsmaßnahmen.
4. Echtzeit-Support bei Sicherheitsvorfällen.

Protection: Endpoint Protection

Blockiert die Ausführung von verdächtigen Prozessen und Dateien

1. Sicherung aller Endpunkte wie Clients und Server.
2. Modernste Sicherheitslösungen gewährleisten mehrstufige Schutzmechanismen.
3. Machine Learning Algorithmen verhindern die Ausführung schädlicher Aktionen und Bedrohungen können frühzeitig erkannt und abgewehrt werden.
4. Zentrale Managementplattform ermöglicht eine umfassende Sicherheitsanalyse und ersetzt die vorhandene Antivirenlösung.

Detection: EDR und SOC

Prozessdatensammlung zur Analyse durch SOC-Expert:innen

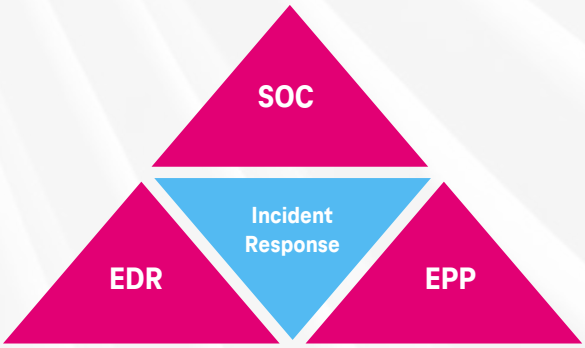
1. Prüfung und Einstufung von Warnmeldungen zur Bestimmung des Schweregrads und der Handlungsempfehlungen.
2. Kontinuierliches Finetuning zur Reduzierung von Fehlalarmen.
3. Eingehende Analyse von Prozessen, die verdächtiges Verhalten verursachen.
4. Remote-Sitzungen auf Endpoints zur erweiterten Analyse und Suche über EDR.
5. Regelmäßige Suche nach Bedrohungen, um potenzielle Gefährdungen zu prüfen und raffinierte, unauffällige Angreifer zu finden, die keine Warnungen auslösen.

Unsere Expert:innen beraten Sie gerne
cyber.security@t-systems.com

Response: EDR und Incident Response

Einleiten von Abwehrmaßnahmen im Falle eines Angriffs

1. SOC löst auf der Grundlage von Analyseergebnissen Reaktionsmaßnahmen aus der Ferne aus, z.B. die Isolierung von Hosts, das Anhalten von Prozessen und das Blockieren von ausführbaren Dateien.
2. Ein Incident Response Team reagiert auf groß angelegte Angriffsversuche.



EDR: Endpoint Detection & Response
EPP: Endpoint Protection
SOC: Security Operations Center

Wann Sie Managed Cyber Defense in Betracht ziehen sollten:

- Sie verfügen intern nur über **begrenzte Ressourcen.**
- Das **Security Know-how** in Ihrem Unternehmen ist eingeschränkt.
- Ihre aktuellen EDR-Lösungen können **fortgeschrittene Bedrohungen** nicht erkennen.
- Ihre bestehenden **Sicherheitsstufen** müssen sich noch **weiterentwickeln.**
- Sie möchten sich vor allem auf Ihr **Kerngeschäft** und Ihre strategischen Initiativen konzentrieren.

Herausgeber

Deutsche Telekom AG
Friedrich-Ebert-Allee 140 , 53113 Bonn, Germany
security.telekom.de
t-systems.com