Managed Detection & Response

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

Unternehmen brauchen mehr als traditionelle Security

Nicht nur die Zahl der Cyberangriffe nimmt ständig zu, sondern auch die Komplexität der Angriffe steigt immer mehr und macht es schwieriger, diese zu erkennen.

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 nicht aus, um Unternehmensressourcen angemessen zu schützen. Warum? Sie schützen zwar effizient vor bekannten Bedrohungen, aber es besteht die Gefahr, dass unbekannte Bedrohungen, die von außerhalb des Perimeters kommen, unentdeckt bleiben. Gleichzeitig mangelt es aber 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 den Security Teams forensische Informationen für die Analyse zur Verfügung.

EDR erfordert jedoch manuelle Eingriffe und ist nur halb so effektiv, wenn keine Expertenteams eingreifen können. **Daher wird Managed Detection & Response (MDR) benötigt.**

Wie MDR Ihnen helfen kann, die passende Verteidigung aufzubauen:

1. Full-scale SOC mit kontinuierlicher Analyse
2. Maßnahmen können ausgelöst und durchgeführt werden
3. Regelmäßiges Überprüfen und Erkennen von komplexen Angriffen
4. Wöchentliche Abstimmung mit unseren Sicherheitsexperten und laufende Optimierung Ihres Sicherheitsniveaus
5. Mehr als 20 Jahre Erfahrung mit Sicherheitsprojekten

T Systems

Let's power higher performance

MDR: Die besten Komponenten für Sie zusammengestellt.

T-Systems Security Operations Center

Kontinuierliche Analyse verdächtiger Aktivitäten

1. Zugang zu den Erkenntnissen aus dem SOC-Center.
2. Echtzeitdaten und -berichte über den aktuellen Sicherheitsstatus.
3. Wöchentliche Sprechstunden zum aktuellen Stand der Sicherheit und mögliche Verbesserungen.
4. Echtzeit-Support bei Sicherheitsvorfällen.

Response: EDR und Incident Response

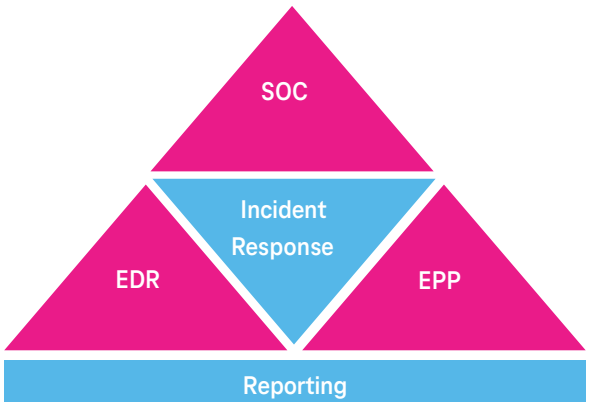
Einleiten von Abwehrmaßnahmen im Falle eines Angriffs

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.

Protection: Endpoint Protection

Blockiert 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.



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

Detection: EDR und SOC

Prozessdatensammlung zur Analyse durch SOC-Experten

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 potenziell Gefährdungen zu prüfen und raffinierte, unauffällige Angreifer zu finden, die keine Warnungen auslösen.

Wann Sie MDR in Betracht ziehen sollten:

- Sie haben intern nur begrenzte Ressourcen.
- Ihr Fachwissen über Sicherheit im Unternehmen ist begrenzt.
- Ihre aktuellen EDR-Lösungen können fortgeschrittene Bedrohungen nicht erkennen.
- Ihre bestehenden Sicherheitsstufen müssen sich noch entwickeln und reifen.
- Sie wollen sich vor allem auf Ihr Kerngeschäft und Ihre strategischen Initiativen konzentrieren.

Unsere Kunden vertrauen auf einen der besten MDR-Dienstleister der Branche.

Expertenkontakt

Andreas Pecka
Head of International Expert Sales & Presales Cyber Security
a.pecka@t-systems.com

Veröffentlicht von

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
E-Mail: cyber.security@t-systems. com
Internet: www.t-systems.com

Last update: 04/2023

T Systems

Let's power higher performance