# EDR

## Inhaltsverzeichnis



EDR (Endpoint Detection and Response) überwacht Endgeräte kontinuierlich auf verdächtiges Verhalten und ermöglicht Untersuchung sowie Reaktion auf Incidents – über klassische Antiviren-Signaturen hinaus.

## 1 Funktionsweise

Agenten auf Clients und Servern erfassen Telemetrie (Prozesse, Dateien, Netzverbindungen). Analysen erkennen Auffälligkeiten; Security-Teams können isolieren, forensisch nachvollziehen und gegensteuern.

- **Telemetry:** kontinuierliche Endpoint-Signale
- **Detection:** Verhalten und IOCs
- **Response:** z. B. Isolation, Kill Process, Collect

## 2 Typische Einsatzbereiche

- Schutz von Workstations und Servern
- Ransomware- und Lateral-Movement-Erkennung
- Incident Response mit Endpoint-Kontext

## 3 Wichtige Hinweise

- Ohne Response-Prozesse bleibt EDR reine Datenflut.
- Agenten-Coverage und Ausnahmen pflegen.
- Datenschutz und Admin-Rechte klar regeln.

## 4 Fazit

EDR macht Endpunkte sichtbar und handlungsfähig – zentraler Baustein moderner Abwehr jenseits reiner Malware-Scanner.