Verbesserte Reaktionsfähigkeit durch Endpoint Detection and Response (EDR).

Was ist Endpoint Detection and Response?

In der Regel sind Endgeräte die Einfallstore für gezielte Attacken (Advanced Persistent Threats/APTs) sowie für Angriffskampagnen, wie z. B. Ransomware. Diese Attacken sind darauf ausgerichtet, traditionelle signaturbasierte Antivirus Lösungen zu umgehen. Es bedarf innovativer Sicherheitstechnologie, und Experten, die diese Technologie beherrschen, um gezielte Attacken zu erkennen und abzuwehren.

Endpoint Detection and Response Lösungen sind eine sinnvolle Ergänzung zu APT Sensorlösungen, um Indikatoren auf Endpunkten im Unternehmen automatisch zu verifizieren.

Der kontinuierliche Incident-Response-Fall ist heute leider „Daily-Business“ und keine seltene Ausnahme!

Für wen ist eine Endpoint Detection and Response Lösung sinnvoll?

Für Unternehmen,

- die IOCs (Indicators of Compromise) auf ihren Endpoints verifizieren und Gegenmaßnahmen auf den Endpoints zentral steuern möchten.
- die bereits Sensorsysteme im Einsatz haben oder IOCs anderweitig beziehen.
- mit eigenem CSIRT (Computer Security Incident Response Team) sowie als effektive Ergänzung zum TÜV Rheinland CSIRT: Die Reaktionsfähigkeit von Security Teams lässt sich mit Endpoint Detection and Response wesentlich stärken und verbessern.

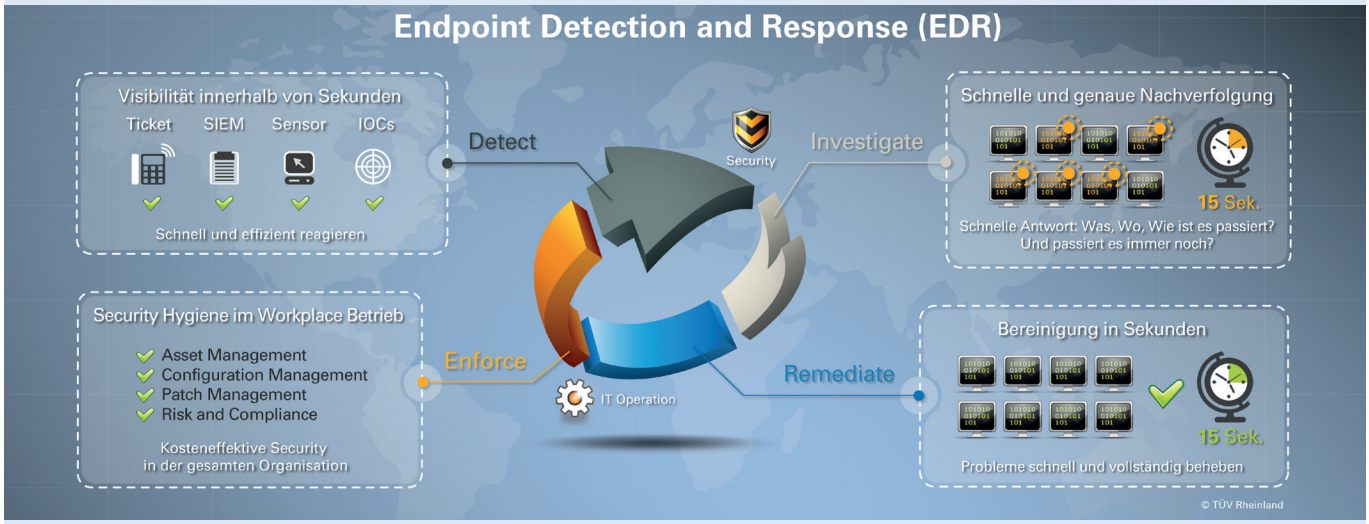
www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

So funktioniert Endpoint Detection and Response:

Die Lösung ist spezialisiert auf die Erkennung, Untersuchung und Reaktion auf verdächtige und schadhafte Aktivitäten auf Endpoints. Typische Funktionalitäten sind:

- Indikatoren (durch Sandbox Analysen ermittelte oder von externen Quellen bezogene) lassen sich in kürzester Zeit auf allen Endpunkten innerhalb der Organisation verifizieren.
- Bedrohungen werden eingedämmt – möglichst automatisiert, z. B. durch selbst definierbare Aktionen wie Ausführung von Scripten, Abziehen von Daten für forensische Analysen, Beenden von Prozessen etc.
- Automatisierung und Integration in bestehende IT-Sicherheitslösungen, um schneller auf verdächtigen Datenverkehr, Prozesse oder Malware reagieren zu können.
- Verarbeitung und Korrelation aktueller und gesammelter Daten mithilfe von Threat Intelligence.
- Endpoints werden von unbekannten und nicht berechtigten Objekten bereinigt, um wieder zu einer sicheren Konfiguration sowie in einen sicheren Betrieb zu gelangen.



Unsere Leistungen und Services

- Umfassende Beratung über die Möglichkeiten von Endpoint Detection and Response (EDR). Gemeinsam mit Ihnen definieren wir Ihren individuellen Schutzbedarf.
- Unsere IT-Sicherheitsexperten konfigurieren die Lösung speziell für Ihre Anforderungen.
- Integration der EDR-Lösung in bestehende Incident Response Prozesse.
- Neben klassischem Produktsupport für EDR bieten wir Ihnen Incident Response Services im Rahmen unseres CSIRT (Computer Security Incident Response Team) an. In Kombination mit einer EDR-Lösung ist das CSIRT deutlich schneller und effizienter in der Lage, Indikatoren eines Angriffs zu verifizieren, forensische Untersuchungen durchzuführen und entsprechende Response Aktivitäten auszurollen.

Gerne unterstützen wie Sie in allen Fragen rund um Endpoint Detection and Response. Fragen Sie uns!

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
service@i-sec.tuv.com