XDR

Inhaltsverzeichnis

XDR (Extended Detection and Response) korreliert Sicherheitsignale über Endpunkte, Netz, Cloud und Identität hinweg. Ziel ist eine zusammenhängende Erkennung statt isolierter Toolsilos.

1 Funktionsweise

Daten aus mehreren Domänen fließen in eine Analyseebene. Korrelation verknüpft z. B. verdächtigen Login, Endpoint-Verhalten und Netztraffic zu einem Fall.

- **Multi-Domain Telemetry:** Endpoint, Mail, IdP, Cloud, Netz
- **Correlation:** Angriffsketten statt Einzelalarme
- **Unified Response:** Maßnahmen über mehrere Kontrollen

2 Typische Einsatzbereiche

- Organisationen mit heterogenem Security-Stack
- Schnellere Investigation verteilter Angriffe
- Entlastung von SIEM-/SOC-Prozessen

3 Wichtige Hinweise

- XDR ist kein Ersatz für saubere Basis-Hygiene.
- Vendor-Lock und Datenqualität beachten.
- Use Cases und Zuständigkeiten definieren.

4 Fazit

XDR erweitert Detection über Toolgrenzen hinweg – wertvoll, wenn Telemetrie wirklich integriert und betreibbar ausgewertet wird.