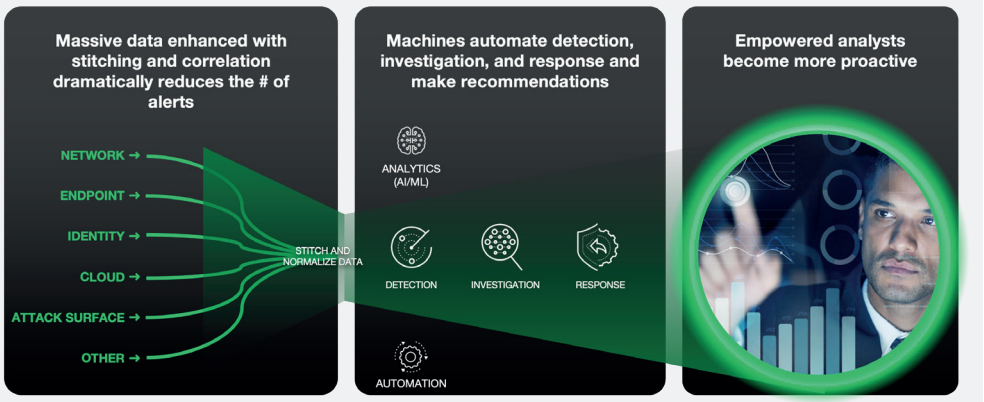
Umfassender Bedrohungsschutz mit blitzschneller Reaktion

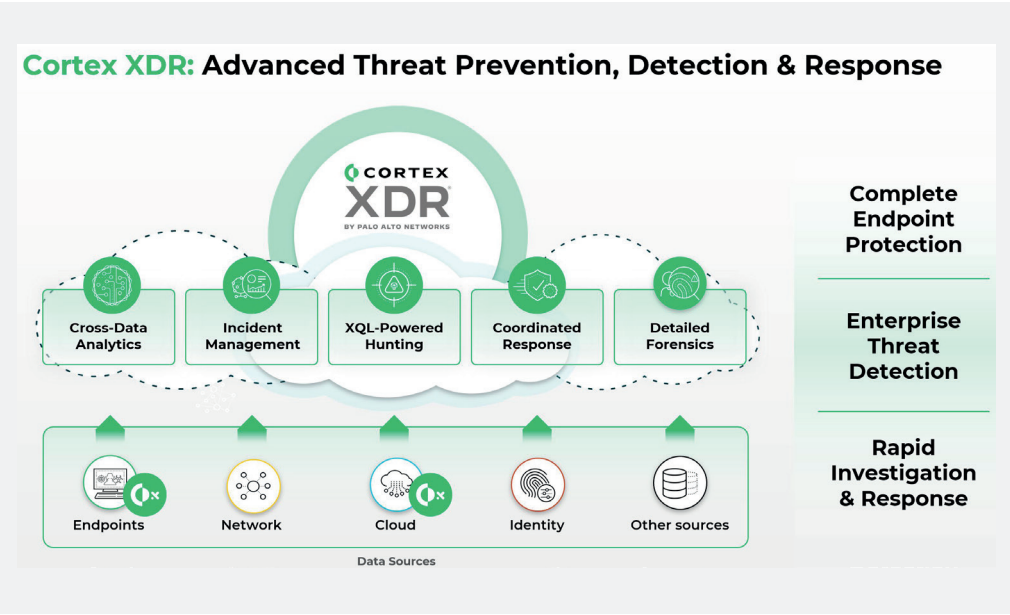
Die Cybersecurity-Lösung Cortex XDR von Palo Alto Networks bietet Endpunkt-, Netzwerk- und Cloud-Schutz in Form einer ganzheitlichen Plattform mit KI-Unterstützung und weitgehender Automatisierung der Erkennung von und Reaktion auf Sicherheitsvorfälle.

Die Bedrohungen durch Cyberkriminelle, denen sich Unternehmen entgegenstellen müssen, werden immer zahlreicher und ausgeklügelter – zumal sich Angreifer zunehmend künstlicher Intelligenz bedienen, um ihre Attacken noch breitflächiger und effektiver zu gestalten. Angriffe zielen dabei meist auf die Endpunkte ab, die damit das wichtigste Einfallstor darstellen. Ein umfassender, strikter Endpunktschutz ist deshalb für jedes Unternehmen ein absolutes Muss.

Extended Detection and Response

Moderne Endpunktschutzlösungen gehen weit über die Möglichkeiten konventioneller Antivirus-Software hinaus. Sie arbeiten verhaltensbasiert (User and Entity Behavior Analytics, UEBA), erkennen und analysieren Anomalien auf den Endpunkten und identifizieren so auch bisher unbekannte Bedrohungen, vieles davon mit Unterstützung durch KI und Machine Learning. Zusätzlich bieten sie Unterstützung zur Behebung von Problemen (Alerts/Incidents) wie etwa Isolation der Endpunkte, Zugriff auf die Endpunkte via Terminal und Skript, Löschen von schädlichen Dateien und forensische Analysen – und all dies möglichst weitgehend automatisiert, damit die Security-Spezialisten entlastet werden und sich um die «Knacknüsse» kümmern können, die doch menschliches Eingreifen erfordern. Bei solchen Lösungen spricht man von Endpoint Detection and Response (EDR). Deckt die Lösung weitere Bereiche wie Netzwerk und Cloud ab, handelt es sich um Extended Detection and Response (XDR).





Führende XDR-Plattform der ersten Stunde

Der Security-Spezialist Palo Alto Networks (PAN) hat 2019 mit Cortex XDR als erster Hersteller eine vollständige XDR-Plattform lanciert, die nach wie vor als führend gilt. So listet Forrester PAN 2024 als Leader bei XDR-Plattformen, ebenso Gartner im Magic Quadrant 2023 für Endpunktschutz, und bei den MITRE ATT@CK Evaluations führt PAN bei praktisch allen Parametern die Rangliste deutlich an. Im Durchschnitt dauert es lediglich 10 Sekunden, bis Cortex XDR einen Angriff erkennt. Von 133 erkannten Problemen werden deren 125 vollautomatisch gelöst, nur 8 Alerts müssen von Security-Analysten weiterbearbeitet werden – dies eine Erkenntnis aus dem Security Operations Center von PAN selbst. Das zeigt, dass das Security-Team durch die Intelligenz und die weitgehende Automatisierung der Lösung massgeblich entlastet wird und effizienter arbeiten kann.

Cortex XDR ist modular aufgebaut und fasst Funktionen für Endpunktschutz (EPP), EDR, Network Detection and Response, Cloud Detection and Response sowie User Behavior Analytics in einer ganzheitlichen Plattform mit einheitlicher Bedienung und kompletter Visibilität über alle Bereiche und Datenquellen hinweg – Endpunkte, Netzwerk, Identitäten, Cloud-Daten, vom Cortex-XDR-Agenten gesammelte Bedrohungsdaten des Unternehmens und anderer PAN-Kunden sowie Bedrohungsinformationen aus weiteren Quellen. Für die Erkennung und Bearbeitung der Bedrohungen werden all diese Daten kombiniert, mithilfe von Machine Learning und Analyse des Verhaltens von Endpunkten und weiteren Systemen und Prozessen analysiert und die Bedrohungen gemeldet oder die Probleme automatisch abgewehrt und behoben.

Die Grundlage für eine automatische, rasche Erkennung und Problemlösung und damit letztlich für das Training der KI-Modelle sind qualitativ hochwertige und umfassende Daten. Auch hier liegt PAN auf einer Spitzenposition. Dies dank der Möglichkeit, Daten aus verschiedensten Quellen zu integrieren. Im Cortex-Produktportfolio existieren seit Jahren etablierte Prozesse, wie diese Daten integriert und die KI-Modelle getestet und implementiert werden – eine solide Basis für die Zuverlässigkeit und Vertrauenswürdigkeit von Cortex XDR.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60
info@boll.ch
www.boll.ch