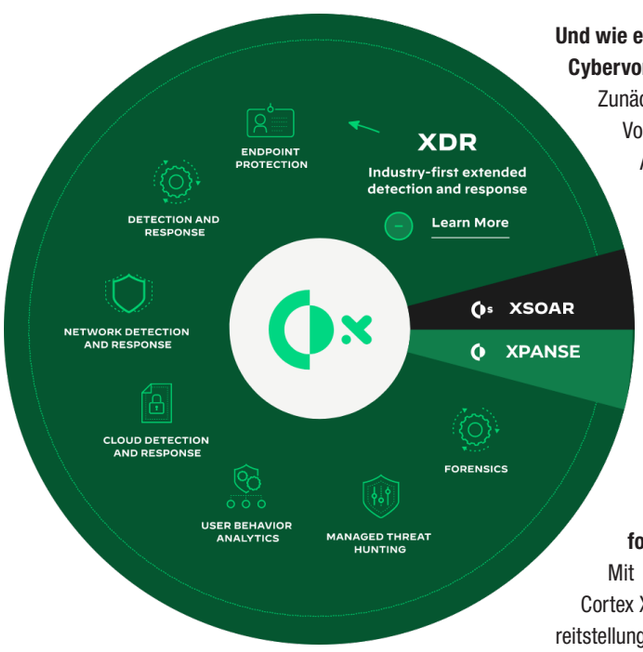
Endpoint Protection der Sonderklasse

Klassischer Endpunktschutz hat ausgedient. Heute ist XDR das Gebot der Stunde, wenn es um die Erkennung und Abwehr von Cyberangriffen geht. Rolf Bamert, Sales Engineer beim IT-Security-Distributor BOLL, erklärt am Beispiel der XDR-Lösung von Palo Alto Networks, worum es geht.

Was bedeutet XDR?
Rolf Bamert: XDR steht für Extended Detection and Response – für umfassende Schutzlösungen, die Sicherheitsinformationen auf dem Endpunkt, im Netzwerk sowie in der Cloud sammeln und verarbeiten, um komplexe Angriffe zu stoppen. XDR kombiniert Prävention, Erkennung, Analyse und Reaktion auf Cyberangriffe auf einer einzigen Plattform – dies gewährleistet höchste Sicherheit und kommt der betrieblichen Effizienz entgegen.

Wie sieht der Markt für XDR-Lösungen aus?
Es gibt eine ganze Reihe von Cybersecurity-Anbietern, die Produkte unter dem Label XDR offerieren. Doch nicht alle Lösungen bieten den gleichen Schutz, wie etwa der Vergleichstest MITRE ATT&CK Round 3 Evaluation von 2021 zeigt. Den höchsten kombinierten Erkennungs- und Schutzwert erzielte dabei Cortex XDR von Palo Alto Networks.

Wie funktioniert Cortex XDR?
Mit einem schlanken Agenten, der Endgeräte durch verhaltensbasierten Schutz und KI-gesteuerte lokale Analyse zuverlässig vor Ransomware, Malware, Exploits und dateilosen Angriffen schützt. Der Agent greift dabei auf einen umfangreichen Präventionsstack mit innovativen Schutzmechanismen zurück, um Malware-Infektionen zu verhindern.



In welcher Weise kommt dabei künstliche Intelligenz ins Spiel?
Ein Beispiel: Dateien werden von einer selbstlernenden, lokalen Analyse-Engine untersucht und bewertet, um auch unbekannte, neue Angriffstechniken abzuwehren. Mithilfe maschinellen Lernens erstellt Cortex XDR zudem kontinuierlich Profile des Benutzer- und Endpunktverhaltens, um ungewöhnliche Aktivitäten aufzudecken und Angriffe frühzeitig zu erkennen.

Ein wichtiger Aspekt der Cybersecurity ist die umfassende Visibilität aller Risiken. Wie löst Cortex diese Herausforderung?
Cortex XDR sammelt und verarbeitet Daten aus beliebigen Quellen. Endpunkt-, Netzwerk-, Cloud- und Identitätsdaten werden automatisch kombiniert, um Angriffe präzise zu erkennen und Untersuchungen zu vereinfachen. Da die gesamte Umgebung eingebunden ist, entstehen auch keine «blinden Flecken». Warnmeldungen von Drittanbietern lassen sich dynamisch integrieren, um das Lagebild zu vervollständigen.

Und wie erleichtert die Lösung die Reaktion auf Cybervorfälle?
Zunächst durch eine Reduktion der zu prüfenden Vorfälle: Cortex XDR verknüpft die einzelnen Alarme durch intelligente Zusammenfassung zu Ereignissen. So kann sich das Security-Personal trotz der meist knappen personellen Ressourcen auf die wirklich wichtigen Vorkommnisse konzentrieren. Dabei wird jeder Vorfall mit wichtigen Artefakten und integrierten Bedrohungsdaten angereichert. So entsteht ein komplettes Bild bezüglich der Abfolge von Ereignissen und deren Ursache.

Cortex XDR ist eine cloudbasierte Plattform. Was bedeutet dies für die Anwender?
Mit einer Cloud-Plattform als Basis ermöglicht Cortex XDR die zentrale Verwaltung und einfache Bereitstellung des Endpunktschutzes, und zwar ganz ohne Installation von Servern, einer Managementsoftware oder von Netzwerksensoren vor Ort. Die Daten werden dabei im Cortex Data Lake gesammelt, einem skalierbaren und effizienten Cloud-Datenspeicher.

Rolf Bamert, Sales Engineer beim IT-Security-Distributor BOLL

Palo Alto Networks hat Cortex XDR kürzlich in der Version 3.0 freigegeben. Was sind die wichtigsten Neuerungen?
Der Major Release 3.0 steht unter dem Motto «Deeper Detection, Broader Investigation, Faster Response». So bietet die neue Version Integration mit Daten von HR-Systemen und ermöglicht eine Risikoeinschätzung für die einzelnen Nutzer. Der Agent wurde durch ein integriertes Forensikmodul ergänzt und sammelt Daten zusätzlicher Drittherstellerlösungen. Und das Incident Management glänzt mit einer neuen Oberfläche, präsentiert ein MITRE-ATT&CK-Mapping von Bedrohungsnachweisen und Artefakten und enthält ein SOC-Manager-Dashboard.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch