Ist Cyber Crucible ein EDR, XDR, MDR? Oder etwas anderes wie Agentic AI?

Kurze Antwort: Es weist Elemente sowohl von EDR als auch von XDR auf, aber die Frage nach der Kategorie ist die falsche. Entscheidend ist, *wo die Entscheidung getroffen wird*. Die Reaktionslogik von Cyber Crucible läuft vollständig auf dem Endpunkt und nutzt ausschließlich die dort im Moment des Angriffs verfügbaren Informationen — denn entfernte Analyseserver bringen zwei fatale Schwächen mit sich: Latenz und Anfälligkeit.

Die ehrliche Antwort auf die Frage nach der Bezeichnung

- **Als EDR:** Wenn ein EDR Endpunkt-Telemetrie nutzt, um Entscheidungen zu treffen, dann ist die automatisierte Reaktion von Cyber Crucible ein EDR. Es unterbindet Erpressungsverhalten in Millisekunden, allein anhand lokaler Informationen.
- **Als XDR:** Telemetriedaten werden auch an eine Datenbank (Kunden-Appliance oder zentral) gesendet, für Korrelation, Threat Hunting, Insider-Threat-Arbeit und IT-Audits. Nach der Marketingdefinition von XDR erfüllt dies die Kriterien.

Das Team ist mit der Bezeichnung „EDR zur Erpressungsabwehr" einverstanden, auch wenn Edge Computing in manchen Kreisen als Technologie der vorletzten Generation angesehen wird. Die folgende Argumentation zeigt, warum diese Sichtweise rückständig ist.

Warum entfernte Analytik zu einem Risiko wurde — Latenz

Das „X" in XDR steht dafür, Analyserechenleistung auf entfernte Server zu verlagern. Das bringt Rechenleistung, kostet aber Zeit — und Angreifer haben ihr Vorgehen genau auf diese Lücke ausgerichtet:

- **Geschwindigkeit:** Angriffe wurden beschleunigt, sodass irreversible Aktionen abgeschlossen sind, bevor ein Analyseserver reagieren kann. Dies zeigt sich besonders deutlich bei kleinen, hochwertigen Objekten wie Passwörtern.

- **Parallelität:** Viele Endpunkt-Tools prüfen ein Programm, warten, und gehen dann zum nächsten über. Angreifer führen mehrere Erpressungsprogramme gleichzeitig aus — 5.000 Dateien werden parallel statt 500 nacheinander angegriffen.
- **Verteilung:** Erpressungsangriffe laufen gleichzeitig auf vielen Maschinen ab. Cyber Crucible hat bereits rund 75 Maschinen gleichzeitig beobachtet. Ein Tool steht dann vor 50 Programmen auf 75 Maschinen — 3.750 zu prüfenden Programmen.
- **Steuerungsprozesse:** Manche Angreifer betreiben einen lokalen Controller, der jedes beendete Erpressungstool sofort neu startet.

Detection-and-Response-Strategien warten naturgemäß, bis der Angriff bereits im Gange ist. Der treffendere Vergleich ist, Bankräuber an der Tür zu stoppen, statt erst zu reagieren, wenn bereits eine bestimmte Menge Bargeld aus dem Tresor verschwunden ist.

Warum entfernte Analytik zu einem Risiko wurde — Anfälligkeit

Rund 80 % der EDR- und XDR-Lösungen benötigen Zugriff auf entfernte Analyseserver, um optimal zu funktionieren, und sind ohne dieses Cloud-„Gehirn" kaum funktionsfähig.

Angreifer nutzen dies gezielt aus: Verschaffen sie sich ausreichend Zugriff, um Firewall-Regeln zu ändern und das Endpunkt-Tool daran zu hindern, seine Analyseserver zu erreichen, verliert das Tool seine Fähigkeit zur Analyse und Reaktion. Es bleibt unangetastet, installiert, aktiv — und nahezu vollständig wirkungslos.

Was Cyber Crucible stattdessen tut

Da Latenz und Anfälligkeit eine Cloud-Abhängigkeit für die Erpressungsabwehr untragbar machen, hat Cyber Crucible eine Erkennungs- und Reaktionsfunktion entwickelt, deren Verhaltensanalytik **ausschließlich Informationen nutzt, die zum Zeitpunkt des Angriffs auf dem Endpunkt verfügbar sind**. Die Unterbindung erfolgt lokal, typischerweise in unter 200 Millisekunden, ohne Cloud-Kommunikation im kritischen Ablaufpfad.

Die Telemetriedaten, die dennoch an die Datenbank übermittelt werden, dienen der Untersuchung und nicht dem Schutz — Threat Hunting, Insider-Threat-Erkennung, IT-Audits — und eine offene API ermöglicht die Einspeisung in offene XDR-Plattformen, SOAR- oder RPA-Tools. Diese Arbeit ist wertvoll, steht aber niemals zwischen Ihnen und einem laufenden Angriff.

Revision #1
Created 2026-07-24 04:30:41 UTC by Dennis Underwood
Updated 2026-07-24 04:30:41 UTC by Dennis Underwood