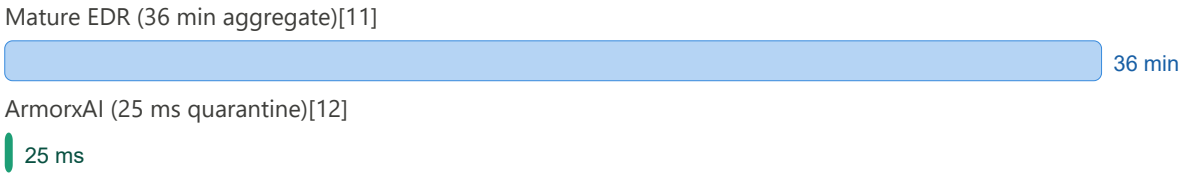
Kill Chain Coverage Map

Where mature EDR operates — and where ArmorxAI adds value

Attack Stage	Mature EDR Coverage	ArmorxAI Adds Value
1. Initial Access Phishing, stolen creds, VPN	Network + Identity layer (outside EDR scope)	MFA gap detection via IOA credential harvesting score begins
2. Execution Process spawn, scripts, LOLBAS	IOA behavioral detection cloud-correlated, 4 min MTTD[11]	eBPF at sched_process_exec 1–4 sec local detection[12]
3. Defense Evasion BYOVD, driver kill-list, EDR disablement	⚠ Structural Gap Single sensor architecture: kill agent = blind endpoint	Decentralized mesh[10] Patent 63/250,409: neighbor watchdog survives kill-list[10]
4. Privilege Escalation sudo, token theft, LSA dump	IOA detection cloud alert, SOC triage required	eBPF at LSM commit_creds NSA IOA score increments[13]
5. Lateral Movement SMB, RDP, service creation	Network + behavioral IOA strong detection coverage	IOA sequence scoring continues score accumulates toward 10.0[12]
6. Collection / Staging Bulk file access, archiving, pre-exfil staging	⚠ Dwell Time Gap Alerts fire; triage queue delays. Medibank: 6 wks[7]	eBPF at vfs_write/file_open bulk-access pattern triggers IOA threshold score[12]
7. Encryption / Impact Ransomware execution, file encryption	Behavioral detection fires 36-min response aggregate[11] analyst action required	25 ms in-process quarantine no cloud, no analyst required IOA threshold: 10.0 trigger[12]

Response Speed Comparison



Mature EDR — strong coverag Architectural gap in EDR model ArmorxAI advantage zone