Axera

DATASHEET

Axera NDR

Network Detection & Response for Kubernetes: process-attributed incidents, MITRE ATT&CK kill-chain fusion, and active containment with closed-loop verification.

Red Hat certified operator | CNI-agnostic | On-prem & air-gapped | eBPF-based

Detection and response, built for the cluster

Segmentation stops most lateral movement. Axera NDR catches what gets through — and contains it before it spreads.

Detect

- Process-attributed incidents — who, from which binary, to what
- MITRE ATT&CK kill-chain fusion across signals
- Real DNS telemetry detection
- Mesh & identity threat detection
- Denied-connection spray and scanning
- Runtime exec / privilege-escalation detection
- Threat-intel expansion and adaptive thresholds
- Crown-jewel asset registry to prioritize what matters

Respond

- Contain a workload with NetworkPolicy / AdminNetworkPolicy
- Closed-loop verification — confirm containment, auto-reopen if not
- Learn the observed egress baseline into a NetworkPolicy
- Response playbooks with an opt-in auto-response master switch
- Context-rich AI triage to explain and prioritize

> Auto-response ships opt-in behind a master switch. You decide how much Axera does on its own — every action is verified and auditable.